UPTEC STS07 024
Examensarbete 20 p
Maj 2007

Common cause failure analysis

Methodology evaluation using Nordic experience data

Sandra Lindberg

UPPSALA
UNIVERSITET

Teknisk- naturvetenskaplig fakultet
UTH-enheten

Besöksadress:
Ångströmlaboratoriet
Lägerhyddsvägen 1
Hus 4, Plan 0

Postadress:
Box 536
751 21 Uppsala

Telefon:
018 – 471 30 03

Telefax:
018 – 471 30 00

Hemsida:
http://www.teknat.uu.se/student

Abstract

Common cause failure analysis - Methodology evaluation using Nordic experience data

Sandra Lindberg

Within the nuclear industry there is an extensive need for evaluation of the safety of the plant. In such evaluations there is one phenomenon requiring some particular treatment, namely common cause failure (CCF). This involves the occurrences of components failing dependently, meaning failures that can overcome the applied redundancy or diversity. The impact of CCF is relatively large, but unfortunately the process of CCF analysis is complicated by the complex nature of CCF events and a very sparse availability of CCF data.

Today, there are a number of methods for CCF analysis available with different characteristics, especially concerning their qualitative and quantitative features. The most common working procedure for CCF treatment is to divide the analysis in a qualitative and a quantitative part, but unfortunately the development of tools for the qualitative part has to a certain extent got behindhand. This subject is further explored in a comparative study focused on two totally different approaches for CCF analysis, the impact vector method and the unified partial method. Based on insights from this study an integrated impact vector and 'Relations of Defences, Root causes and Coupling factors' (RDRC) methodology is suggested to be further explored for progress towards a methodology incorporating both qualitative and quantitative aspects.

Handledare: Gunnar Johanson
Ämnesgranskare: Bengt Carlsson
Examinator: Elisabet Andrésdóttir
ISSN: 1650-8319, UPTEC STS07 024

Populärvetenskaplig sammanfattning

Inom kärnkraftsindustrin är säkerhet det högst prioriterade området. Man använder sig i regel av en djupförsvarsprincip där redundans och diversifiering ingår som multipla lager av skydd. Ändå förekommer det händelser som inte hindras av dessa lager av försvar. När ett fel inträffar där två eller fler komponenter slås ut samtidigt av en gemensam orsak kan händelsen vara av typen ”common cause failure” (CCF). Detta är ett fenomen som har stor påverkan och ofta betydande effekt på resultaten vid probabilistiska analyser av anläggningars säkerhet, vilket innebär att analys och modellering av CCF är av stor betydelse.

Det finns idag ett flertal metoder för CCF-analys, med varierade egenskaper. Det vanligaste tillvägagångssättet innebär en uppdelning i dels en kvalitativ och dels en kvantitativ analys. När det gäller metodikutveckling har mestadels kvantifieringsmetoder varit i fokus till nackdel för kvalitativa metoder, och faktum är att det inte finns någon etablerad metod för kvalitativ analys som fått större genomslag. I Storbritannien har dock ett helt annat angreppssätt etablerats, där förhållandet är det omvända; kvalitativa egenskaper finns inbygga i metodiken, medan dess kvantifieringsförmåga kan anses vara bristfällig.

Syftet med detta examensarbete är att undersöka möjligheten att hitta ett förfarande för CCF-analys som tillgodoser både kvalitativa och kvantitativa aspekter. I rapporten presenteras en komparativ utredning av en del befintliga metoder, för att identifiera önskvärda egenskaper. Med utnyttjande av den brittiska metodikens grundfilosofi har ett förfarande utvecklats för kvalitativ utvärdering, en ”Relations of Defences, Root causes and Coupling factors” (RDRC)-approach. Metoden kan förväntas ge en bra grund för att bättre kunna beakta både kvalitativa och kvantitativa aspekter.

Acknowledgements

Since this work started, just over six months ago, I have experienced an incredible journey. I have been introduced into a world incorporating advanced technological solutions interweaved into complex system structures. In this world I have met so many people with so much experience and I am truly thankful to everyone's willingness to share their experience. This has of course been very useful in my work on this Thesis, although the greatest profit has been its influence on my personal development and experience.

I wish to express my sincere gratitude to my mentor Gunnar Johanson at ES Konsult for his devoted help and for being the greatest source of inspiration. All the co-workers at ES Konsult deserve a special appreciation for being so very supportive. I am also very grateful to all the participating organisations within the EWG project for giving me this opportunity. For providing input to the report, I would like to thank prof. Bengt Carlsson. Finally, to my always supportive friends and family – thank you.

Solna, May 2007

Sandra Lindberg

List of Content

List of figures

List of tables

1 Introduction

In many sectors the need of evaluation of the safety in processes, support of system design has for a long time been an obvious issue. The most widely adopted approach toward this is currently the use of probabilistic safety analysis (PSA), also referred to as probabilistic risk analysis (PRA) or quantitative risk analysis (QRA). One sector where PSA, in many countries, has become not only an exceptionally useful tool for assessment and control of the risk related to the operation, but also a regulatory framework by authorities is within the nuclear industry. (OECD/NEA, 2002)

Nuclear power plants are very complex systems where safe design is crucial. A widespread model for this purpose is the use of a defence in depth philosophy where redundant and diverse components serve as multiple layers defence. If assuming that components always fail independently this concept would provide a high level of protection, but unfortunately this is not always the case. In reality components may also fail dependently and thereby overcome the applied redundancy or diversity. In fact, the experience is that dependent component failures are a significant contributor to system unavailability. (Parry, 1991) The sources of dependencies are numerous and often result in special treatment in the different analyses being performed. One category of dependent failure is referred to as common cause failure (CCF). This group of dependent failures possesses the special characteristic that they can not be explicit modelled in PSA, but constitute the residual part of the wider class of dependent failures. The treatment of CCF is instead handled by implicit quantification through parameters that does not distinguish between particular causes or dependencies. The relatively large impact of CCFs has directed a lot of attention to the field of CCF modelling.

For the purpose of modelling CCF two separate paths are to be found; one that focuses on the quantitative aspects of the problems involved and one that instead engages the qualitative points of view. The most common way of performing CCF assessments are by the use of an impact vector approach (Mosleh et.al, 1998). This is an approach devoted to quantitative assessment that, as will be shown, unfortunately lacks incorporation of qualitative aspects. In the UK though, another approach is adopted, namely the Unified Partial Method (UPM) (Brand, 1996). This is a methodology that covers many of the deficiencies of the impact vector approach, but on the other hand it can not provide high-quality quantitative results to the same extent as the impact vector approach. The situation of different models positioning in qualitative and quantitative aspects is illustrated in Figure 1.

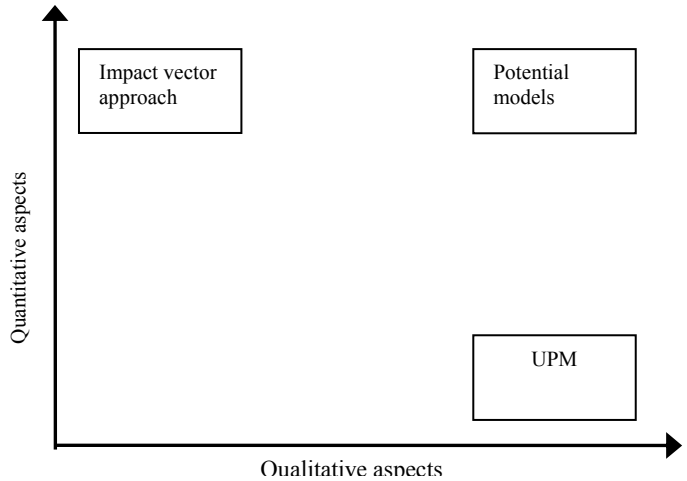

Figure 1. Positioning of CCF models.

In Figure 1 the idea of potential models is also indicated. This concerns models that are able to integrate both qualitative and quantitative aspects and thereby constitute a class of models that are complete. A development of CCF methodologies in a direction towards such a potential model is main subject of this thesis.

1.1 Objectives of the research

The present most widely adopted tactic towards CCF modelling is to perform quantitative and qualitative assessments separately, where the main focus is quantification of CCF impact. When it comes to the subject of qualitative CCF models there is unfortunately a lack of literature devoted. In particular, this concerns the specific issue of defences against dependent failures, although one example of research progress within the area is found in Bourne et. al. (1981). This shortage of literature was also expressed in Hellström et. al. (2004). Therefore, the comprehensive objective and the main theme of this thesis is to shed some light on the need of redirecting the method development into a course focusing on finding a working process that considers both quantitative and qualitative aspects.

The intention is to *examine the possibilities of finding a working procedure for CCF modelling that incorporate both qualitative and quantitative aspects*. An obvious alternative then, that also is adopted, is to assess the potential of development of the 'currently adopted' approach, i.e. the impact vector method. For this purpose UPM becomes of particular interest and the ambition is to identify qualities of interest in UPM and examine how such qualities can contribute to other methods. This will be performed by accomplishing two tasks; first (1) by studying the characteristics of the method, and then (2) to examine the applicability of UPM on generic data. In this way an attempt to join established methodologies can hopefully be completed.

Currently an important work is being performed in a European working group (EWG)[1], where methods applied in Sweden, Finland and Germany are to be studied and compared by application on generic CCF data. This thesis will partially be in process in parallel to the work of the EWG-project so an additional intention is that some of the results could hopefully also be found as useful for the work by the EWG.

[1] A co-operation between VGB and NPSAG, both to be further presented in Chapter 3.

1.2 Undertaken procedures

The assigned task for this thesis concerns CCF method development. Since the starting point was the existing methods a comparative survey of these was necessary. To manage this, a study of articles and reports devoted to CCF methodology, and UPM in particular, was performed. The literature study aims at providing insights about the main philosophies as well as characteristics of the different methods needed for the comparative survey.

Another extensive study that is needed for two purposes involves CCF data. Firstly, knowledge about the characteristics of CCF data in general is needed to enable any deeper understanding for how the methods under consideration are applied and what might be required from these methods. Secondly, to be able to perform a trial application of any method a study of the data is of course necessary but it is also likely to be more successful with more profound insights about the data under consideration.

The performed assessment of CCF methods was then used as basis for discussion and proposal of possible development of CCF methodology. This also included a harmonization of proposed interpretations and methodologies by Zitrou (2003), Paula and Parry (1990) and Marshall et. al. (1998).

To cope with this task some delimitations have been necessary. The primary one concerns the methods to be examined. It can be expected that numerous CCF methods exists and are used in various extent worldwide, although this thesis is concentrated on the impact vector approach and UPM. Other methods will be disregarded, not because they are not likely to have potential but due to the need of limiting the scope of this work. When it comes to the area of application of CCF methods it needs to be emphasised that the area of attention within this thesis is the nuclear industry. The concept of dependencies is of course relevant in many sectors, but other areas will not be considered. A final delimitation that has been made is the set of data included in the assessment. This data set has been limited to only include Nordic CCF data for emergency diesel generators (EDGs). This choice is based on the fact that this is a data set that has already been included in previous thorough assessments, for example in Johanson et. al. (2003), which renders the possibility for comparative evaluations.

1.3 Report outline

To profit from this report it is necessary to comprehend certain concepts. Therefore a review of the CCF phenomena, treatment of it and related terminology are provided in Chapter 2. Extended descriptions of certain terms, essential for this work, are provided in Appendix C.

In Chapter 4, a comparative survey of CCF methods, in terms of the impact vector approach and UPM, is presented. This is then used as a foundation for development of a new approach, which is described in Chapter 5. This chapter also includes a trial application of the suggested procedure together with a brief presentation of employed data and is concluded with an assessment of the performed application exercise.

In the final chapters, 6 and 7, the performed work is summarized and conclusions are presented. Here is also a discussion conducted concentrated on examination of the possibilities and difficulties of finding a working procedure for CCF modelling that incorporate both qualitative and quantitative aspects.

For readers with no previous experience of CCF methods Appendix A is suggested. The main objectives, reasoning and conclusions of the main report can still be followed even if this appendix is neglected. To achieve a more profound understanding though, it is recommended since it provides more comprehensive descriptions of parametric methods and UPM. Appendix B is an extension of section 5.2.2 intended for the interested. For readers who are already very familiar with the area of CCF analysis, including modelling techniques, application and associated terminology, the more interesting part of this report begin in section 4.4, and the previous can therefore be disregarded.

2 Dependency and other useful concepts

The core subject of this research area concerns the concept of dependency, which is a matter that needs to further explained before any further theories can be reviewed. This chapter is devoted to description of the concept of dependency, the special characteristics and associated terminology.

2.1 Different kinds of dependency

An independent failure is an occurrence in which the probability of failure of one component is not related to the failure of another component, i.e. $P_{System} = P(AB) = P(A) \cdot P(B)$, where P(A) and P(B) are the independent probabilities of failure of components A and B respectively. On the contrary a dependent failure is an occurrence of failure of two or more components where the failure is probabilistically not independent. This is given by $P_{System} = P(AB) \neq P(A) \cdot P(B)$. Consideration of this is of course of particular importance in cases where $P(AB) > P(A) \cdot P(B)$, i.e. where the multiple failure probability increases due to dependency.

There are a number of different definitions in the terminology flourishing in the literature. A discussion of what terms to be used, and their meanings, is therefore required. Not surprisingly distinct dependencies are of different nature and character. In Johanson et al. (2003a) a distinction is made between functional dependencies and physical dependencies. In this distinction functional dependencies include interaction between systems, components and structures such as shared components, auxiliary systems, automatic control and manual control while physical dependencies include interactions where the location of systems, components and structures is important (shared location). In quantitative analysis known dependencies, both functional and physical, can be explicit modelled. This can not be made for dependencies where the shared cause is unknown, which constitute a residual part of the wider class of dependencies. These residual dependencies are modelled as common cause failures (CCF).

Different kinds of dependencies and their consideration in safety analysis are given in Table 1 (Johanson et. al., 2003a).

Dependency		Known	Unknown
Functional (direct or indirect)	Failure cause makes two or more components unavailable.	Connected systems, structures and components: Cooling, ventilation, signals, common parts, procedures, tools, operators etc.	Common cause failures. Causes and failure coupling mechanisms are explicitly 'unknown'.
Physical (direct on indirect)	A common environmental condition makes two or more components unavailable.	Area events (fire, flood), external events (air plane crash, earthquake), dynamic effects after LOCA[2], environment impact.	

Table 1. Dependencies and their consideration in safety analysis.

Further, the definition of CCF is here as within the International Common Cause Failure Data Exchange (ICDE) project (OECD/NEA, 2004):

> 'Common cause failure is a dependent failure in which two or more component fault states exist simultaneously, or within a short time interval, and are a direct result of a shared cause.'

The ICDE project is a very important arrangement for research on CCF and will be further presented in Chapter 3.

Another frequently used term in the literature is common mode failure (CMF). CMF and CCF are terms not to be considered as interchangeable, since CMF concerns failure of the same mode, i.e. failures with identical appearance or effect, and is not necessarily a CCF. Since the difference might in practise be insignificant and is unlikely to affect the data, and thereby the modelling of the data, the terms to be used throughout this thesis is CCF, to provide the discussion with. This is also supported by the fact that the centre of attention in this work is defences against the causes of failures, not their effect.

2.2 Treatment of common cause failure

A procedural guide has been developed to be used as a structural framework for understanding and assessment of the impact of CCF on the performance of a system. The guide is divided into four steps, as shown in Figure 2. In the first stage of the procedure the analyst is to become familiar with the system to be assessed and the problems to be solved. The basic component level logic model is to be developed in this phase, just as if an analysis of independent events without consideration of common cause failures is to be performed. Stage two focuses on the screening process. This includes definition concerning the scope of the modelling and the detailed quantitative analysis. In stage three the modelling is performed and information, both qualitative and quantitative, is extracted from the data. In the fourth, and final, stage a system level quantification, as well as interpretation and assessment of the modelling results is made. (Fleming et. al., 1987) (IAEA, 1992)

[2] LOCA is the notation for a Loss Of Coolant Accident.

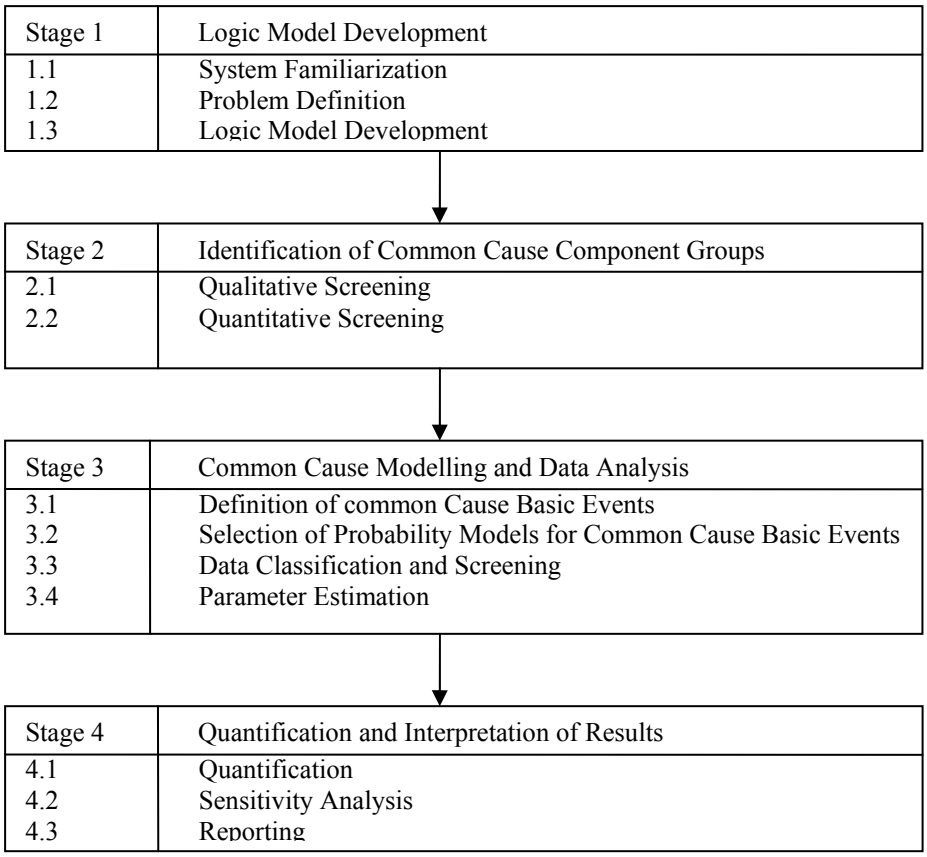

Figure 2. Procedural framework for CCF analysis.

Today CCF events are often major contributors to the overall results of PSAs. This does not only indicate the great importance of the occurrence but also the need of adequate methods for CCF modelling to secure the results of the analyses. This is unfortunately where some main difficulties appear. The most common way of modelling CCF, i.e. the use of parametric probability models, requires a statistical estimation of model parameters. The suggested estimation techniques demands system-specific data that describes failures of all possible multiplicities to be available, i.e. for a system of m components, the data necessary for parameter estimation is of the form $n = (n_1, ..., n_m)$ where n_k is the number of CCF events that involve k components, $k = 1, ..., m$, observed out of N system demands or during T observation time. Reality though, does seldom meet these expectations when it comes to the availability of CCF data. The fact that CCF events are relatively sparse, and that they are of a complex nature, causes different sources of uncertainty in the quantification of the CCF parameters (Mosleh, Siu, 1987). This has also made expert judgment to become an essential part of the process.

The sparse availability of CCF events makes the number of observations that is relevant to a specific system, or plant, limited. This means that in most cases there is not enough data for adequate parameter estimation, and the need of generic CCF data is obvious. The use of a generic database is made by customization of the database into a record that is relevant for the target system. This process renders the possibility to access a much larger amount of data, but will also bring a considerable amount of uncertainty related to the applicability of the generic events to the target system. The complex nature of CCF events often causes the event reports to be vague or incomplete. This, in turn, complicates the understanding of failure mechanisms, identification of potential root causes and coupling factors. Since CCF data analysis is often a rather subjective process lack of sufficient information will lead to further

incorporation of uncertainties in the analysis. (Mosleh et. al., 1994) A provided approach to incorporate expert judgment is the impact vector method, which will be given in more detail in Chapter 4.

The aspect of expert judgments incorporated in the methodologies have for a long time been a subject of discussion. A lot of work is being made for improvement of the probability methods and also the tools for treating uncertainties. Examples of this are found in Vaurio (2002) and Apostolakis (1986).

2.3 Terminology

The area of CCF analysis is thrived with different terms and expressions, so before entering the subject more deeply a short introduction of useful notions will be given. When studying CCF events several aspects that are of great importance for the occurrence of CCF are considered and for each event some main characteristics are determined. Some of these aspects will be more significant than others in the continuation of this report and is therefore being stated in the following.

Quantitative modelling is done within the area of *Probabilistic Safety Analysis* (PSA). To be able to include the influence of CCF in PSA factors representing the impact of CCF need to be quantified. This is done by the use of different CCF methods, which is a subject to be further reviewed in Chapter 4. When working with any kind of CCF analysis a basic step to be completed is the identification of the components to be included in the assessment. This is done by determination of the *Common Cause Component Group* (CCCG) that is a set of components that are considered to have a high potential for failure due to a common cause. In most cases the components of CCCGs are redundant, identical components of a system, all performing the same function. With the use of CCF methods the impact of CCF on a defined CCCG is estimated and can then be used in PSA. When considering EDGs the CCCG size vary from two to five, where plants with four or five EDGs share some or all EDGs with a second unit at the same site (OECD/NEA, 2004).

A *failure event* is an event in which a specific set of components becomes unavailable to perform its function. The function that the components fail to perform is described by the *failure mode*. For EDGs the functional fault modes are failure to start, failure to run and failure to stop (OECD/NEA, 2004).

A *root cause* is the most basic reason for the component's failure, representing the common cause. A categorisation of different kinds of root causes is made within ICDE (OECD/NEA, 2004), which will also be applied within this work. These categories are:

- State of other component(s)
- Design, manufacture or construction inadequacy
- Abnormal environmental stress
- Human actions
- Maintenance
- Internal to component, piece part
- Procedure inadequacy
- Other
- Unknown

A *coupling factor* describes the mechanism that ties multiple impairments together and identifies the influences that created the conditions for multiple components to be affected. This means that a coupling factor is a property of a group of components or piece parts that identifies them as being susceptible to the same mechanisms of failure. A categorisation of different kinds of coupling factors is made within ICDE (OECD/NEA, 2004), which will also be applied within this work. The categories are:

- Hardware (component, system configuration, manufacturing quality, installation configuration quality)
- Hardware design
- System design
- Hardware quality deficiency
- Operational (maintenance/test (M/T) schedule, M/T procedures, M/T staff, operation procedure, operation staff)
- Maintenance/test (M/T) schedule
- M/T procedure
- M/T staff
- Operation procedure
- Operation staff
- Environmental (internal, external)
- Environmental internal
- Environmental external
- Unknown

Further descriptions of this categorisation of root causes and coupling factors are provided in Appendix C.

A *defensive tactic*, or a *defence*, is a measure (operational testing, maintenance, design etc.) that can be taken to diminish the frequency or impact of failure. There are several suggestions on how categorisation of different types of defences can be structured. Examples are found in Paula and Parry (1990) and Marshall et. al. (1998), but the one adopted within this work is the one provided within UPM (Brand, 1996). Those categories are:

- Redundancy / Diversity
- Separation
- Understanding
- Analysis
- Operator interaction (or MMI)
- Safety culture
- Environmental control
- Environmental testing

Further descriptions of this categorisation of defences are provided in Appendix A.

3 ICDE and the CCF database

The International Common-Cause Failure Data Exchange (ICDE) project was established by several member countries of the Nuclear Energy Agency of the Organisation for Economic Cooperation and Development (OECD/NEA) to encourage multilateral cooperation in the collection and analysis of data relating to CCF events. (OECD/NEA, 2004) The resulted record of CCF data will further on be referred to as ICDE data and the ICDE database.

When using a generic database heterogeneity becomes an issue to handle. Event reports, especially when they come from different countries, often lack homogeneity causing a lot of work for harmonization. Because there are usually national guidelines for CCF event recording and data interpretations, and the fact that event reports are usually written in the native language where the event was observed, the issue of heterogeneity need some special consideration. In the working progress of dealing with this a general coding guideline was developed by ICDE (OECD/NEA, 2004). To each event in the database a number of features are assigned, according this coding structure. These feature include for example root cause, coupling factor, degradation status for each component, time factor indicating time difference between the component failures, shared cause factor indicating the uncertainty that the component failed indeed due to a shared cause, failure mode, detection mode, component group size. The coding makes use of the information in statistical analysis possible which bring about an important advantage towards the availability of CCF data.

One research group that has carried out important research partially based on the ICDE database is 'Nordiska arbetsgruppen för CCF-studier' (NAFCS), which is a part of the activities of the Nordic PSA Group (NPSAG)[3]. The comprehensive goal with the working group is to support safety by studying potential and real CCF events with the use of ICDE data, process statistical data and report conclusions and recommendations that can improve the understanding of these events eventually resulting in increased safety. The project has also surveyed and assessed strategies of defence against different kind of dependencies as well as methods for identification and analysis of these. (Johanson et. al., 2003a) A continuation of this work is now performed by in the EWG-project[4] where different approaches for CCF modelling are being mapped out and compared. The intention with this project is to proceed towards harmonization concerning issues such as view on CCF and CCF methodology. (VGB/NPSAG, 2006)

In Johanson et. al. (2003a) the following figure is given to illustrate the NAFCS project idea for how 'to improve the understanding of CCF events eventually resulting in increased safety', see Figure 3.

[3] NPSAG was formed in December 2000 by all Nordic nuclear companies. The group constitutes a forum for consultations concerning PSA of national and international plants and also coordination of some research efforts.
[4] The NPSAG is represented by Kalle Jänkälä (Fortum), Gunnar Johanson (ES Konsult) and Michael Knochenhauer (Relcon). VGB is represented by Bernd Schubert (Vattenfall Europe), Ralf Wohlstein (E.ON Kernkraft) and Günter Becker (RiSA).

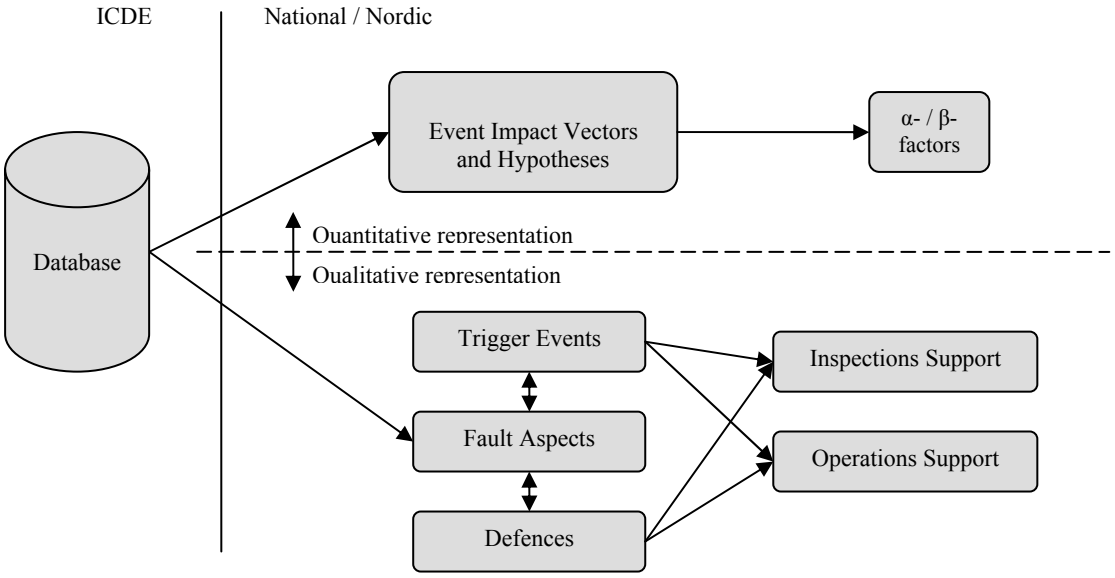

Figure 3. NAFCS project idea.

An interesting notice to be made is that there is a complete separation of the quantitative and the qualitative representation and also how these two different areas are being analysed (quantitatively and qualitatively respectively). When it comes to analysis tools there are several procedure guides and methods developed for the quantitative element, but this is not the case for the qualitative part of the analysis. These matters will be further discussed later on in this report.

4 Comparative survey and assessment of CCF methods

In this chapter very brief introductions to the impact vector approach and UPM are given. For readers not very familiar with these methodologies more detailed surveys are provided in Appendix A. This survey is performed in a comparative and evaluating purpose so the chapter is completed with an explicit comparison of the methods in section 4.3, and a trial application of UPM in section 4.4.

4.1 Impact vector approach

The most common technique for treating CCF quantification is the use of impact vectors. Detailed method description as well as descriptive application is found in Johanson et. al. (2003b). This methodology addresses issues such as intermediate component statuses, dispersal of component failures in time and uncertainty regarding the existence of a shared cause. With the impact vector method the estimated probability that different number of components would fail if an actual demand should occur during the presence of CCF impact is expressed, given an observed CCF. The impact vector contains, for a group of 'n' components, 'n+1' elements, one for each order of failure including the case of no failure:

$v = [v_0, v_1, v_2, \ldots, v_n]$.

Hence, a single failure event, for a component group of size three, is presented by:

$v_{single} = [0, 1, 0, 0]$.

To meet the need of treatment of situations where the outcome is not perfectly known to be a certain failure state the impact vector approach provides a possibility to express a spectrum of chances. The primary tool for this purpose is the use of alternative scenarios, or hypotheses,

about the CCF impact, where probabilities related to each scenarios, based on judgments, constitute the basis for design of the impact vector.[5] In this way the elements of the impact vector describe the probability distribution for the outcome states of an assumed demand. (Mosleh et. al., 1998)

For use of impact vectors there are several parametric methods available for expressing the impact of CCFs on a system as parameters, so called CCF parameters, quantified through statistical analysis. Since impact vectors is the general way for presentation of failure statistics compatible results are obtained irrespective of which parametric methods is applied. Even if they all aim to present the dependence in multiple failure probabilities the do have different benefits in some respects and in some special application due to their different features. The most common of these parametric methods is the Alpha Factor (AF) method, which is applicable for up to six redundant components. Two other methods that are rather similar to the AF method are the Direct Estimation, or Basic Parameter, (BP) method and the Multiple Greek Letter (MGL) method. The BP method differs from the AF method in the sense of how the parameters are determined and is not as commonly used. The MGL method used to be commonly applied in PSA but has some deficiencies when it comes to uncertainty analysis. For applications on very large groups of components the Common Load method (CLM) is recommended. For treatment of component groups of size two the Beta Factor (BF) method can be applied. The BF method can also be applied on higher multiplicities, but it is then recommended only to be used as a crude cut-off. (Johanson et. al., 2006) An important feature is the group-invariance property[6], which only holds for the BP method while the other mentioned methods lack this property. Further descriptions of these parametric methods are provided in Appendix A.

These methods, as well as other ones, have different properties that in some cases make them more useful that others but the different approaches are also used together to complete each other. Nonetheless it needs to be emphasized that irrespective of which method is used approximately the same results is obtained when the data are consistently applied. This uncovers the great importance of data classification and screening, indicated as step 3.3 in Figure 2 (Rasmuson, 1991). In general parametric models are good, useful quantification tools, but on the down-side they can be considered as black-box approaches providing limited diagnostic value.

This type of modelling technique, as presented in this section, will further on be referred to as the impact vector approach or parametric methods.

4.2 Unified partial method

In this section a very brief introduction to the unified partial method (UPM) will be provided. A more detailed survey is given in Appendix A.

UPM is a predictive reliability analysis tool for obtaining an estimation of a factor, for the vulnerability of the system to dependent failures, which is to be used as a complement to the

[5] Assume for example that for a CCF event two possible scenarios concerning the number of failed components is found. If one scenario is that two components failed the related vector is $I_1 = [0, 0, 1, 0]$ and if the other scenario is that three components failed the corresponding vector is $I_2 = [0, 0, 0, 1]$. The analyst is then to assign weights to the different scenarios. So, if it is judged that there is a 90 % chance that scenario I_1 is true and 10 % chance that scenarios I_2 is true the impact vector will be $I = 0.9I_1 + 0.I_2 = [0, 0, 0.9, 0.1]$.

[6] The expressed probability is then not dependent of the specific combination of components, only the multiplicity affects.

independent failure analysis result obtained via PSA. The foundation of the method is defences against dependent failure and this is also what forms the structure of the method. Another important gist of the method is judgement. The estimation of the dependent failure factor is made essentially based on the analyst's judgement of the involved defences against dependent failure. These judgements are made transparent by being recorded throughout the analysis. Two common techniques applied for dependent failure assessment are the Reliability Cut-Off method and the Partial Beta Factor (PBF) method. The PBF method is based on the BF method, which was also referred to in section 4.1. The Reliability Cut-Off method is usually applied in system level assessment, while the PBF method usually is applied to component level assessments. The difference is that while the cut-off method is a holistic approach the PBF method is component oriented, and subsequently the definitions of the factors are different and they need to be calibrated differently. The work procedures for system and component level assessment are identical though. (Brand, 1996)

In Brand (1996) a step by step user guide for application of UPM is provided, which is illustrated in Figure 4.

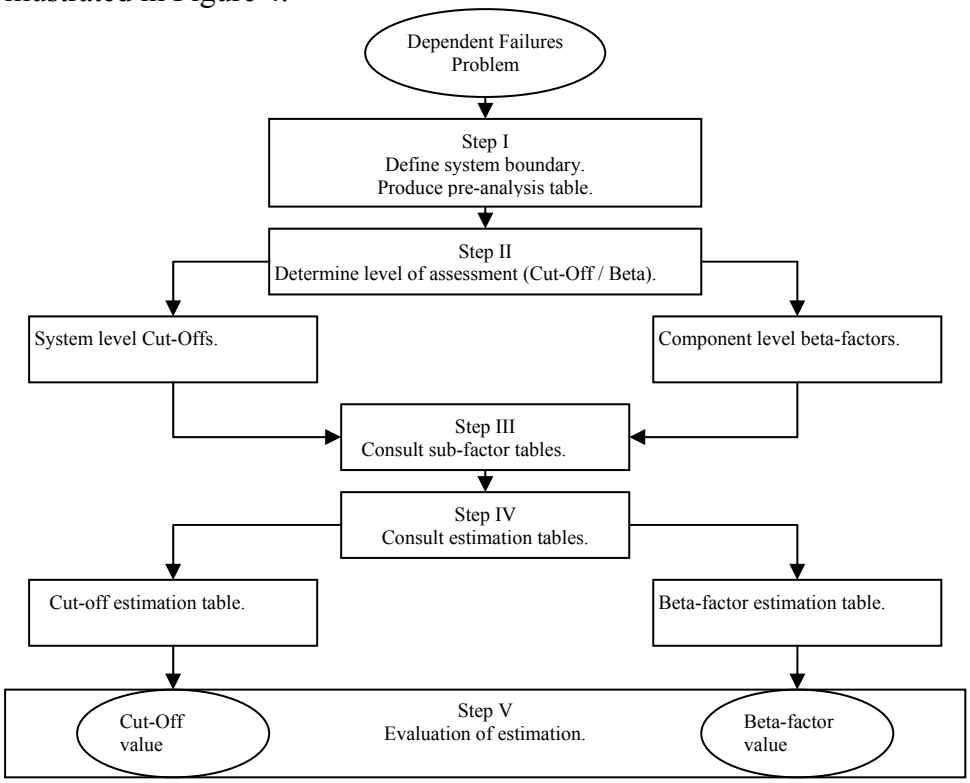

Figure 4. Illustration of UPM application guide.

In the first step the analyst is to define the physical boundary of the system in interest. In this first stage a pre-analysis table is to be produced. The pre-analysis table is to be used for assessing the work that is to be done but also to provide a quality rating on the assessment. Step two covers a choice between Cut-Off and PBF method, i.e. assessment on system or component level.

In the third step different defences' effectiveness in defending against dependent failures are assessed. Different defence strategies are categorized into eight different groups; Redundancy (and Diversity), Separation, Understanding, Analysis, MMI (Man Machine Interface), Safety Culture, Environmental Control and Environmental Testing. Sub-Factor tables, one for each category of defence against CCF, are provided and a review of these Sub-Factor tables is to

be done. In the Sub-Factor tables five criteria are given, where each criterion correspond to a defined level of quality of the defence. The analyst is to complete the Sub-Factor tables, by evaluating the system in terms of the given criteria. Depending on the judged level of effectiveness in defending against dependent failures, different scores are obtained for each Sub-Factor via Cut-Off and β-factor estimation tables. Thus, the distribution of these score will depend on the judged quality of each category of defence, but in addition to this the different categories of defence are also assigned different weighting based on established expert conclusions. In this procedure a judgement table is also to be created, where the judgment made for each Sub-Factor is recorded.

In the final steps the overall estimation of the system Cut-Off-factor ($\hat{Q}$) or Beta factor ($\hat{\beta}$) is obtained by calculation of the made judgements, i.e. the scores provide via the Sub-Factor tables.

4.3 Comparison between UPM and the impact vector approach

The impact vector approach and UPM are two different models for CCF quantification, but with substantially different features. In this section some of the quantitative and qualitative properties of these models will be considered.

A basic difference of these models is their respective origin. UPM was developed on expert judgement basis. This applies also for further developments, or extensions, of the method. An example of this, and perhaps the only one in its kind, is found in Zitrou (2006). The development of the impact vector approach though was based on experience data. This is an essential contrast between these models, since this to a large extend has formed their respective characteristics.

The idea of the impact vector approach is to provide quantification of the impact of CCFs by estimation of the probability that certain components fail under impact of CCF. This is basically done by calculation of the probability of occurrence of a number of hypotheses concerning the CCF impact. UPM though, provides a totally different approach where, instead of trying to quantify impact of CCFs, the quality of the defence against CCFs is assessed and from that assessment an estimation of a probability that the defence against dependencies is not enough is provided, i.e. a probability that a component in the system, or the system, fails dependently, given that it fails. While the impact vector approach could be described as a tool for data analysis to statistically find the week points of the system (i.e. to find out what needs to be improved) UPM can be said to go the other way by analysing the quality of the systems defence against dependencies to find out what defences needs to be improved. Although both types of approaches suffer loss from the benefit of the other there seems to be no obvious way of integrating these different methods. The current situation for analysis requires a choice between a model suitable for assessment of multiple failure analysis or a qualitative analysis approach. In Zitrou (2006) a very revealing figure is given, illustrating the general situation of CCF methods. This is provided here in Figure 5.

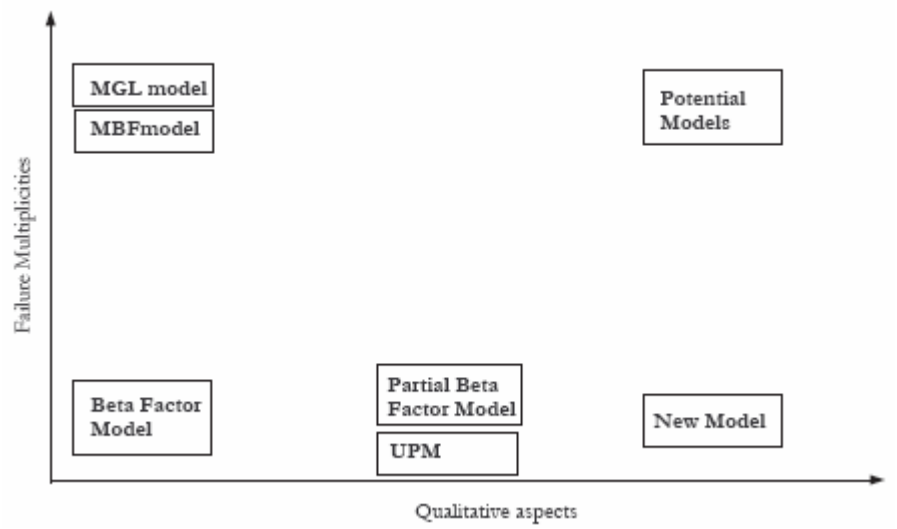

Figure 5. CCF methods positioning.

In her thesis she proposes a 'New Model' as indicated in Figure 5 above, but she also argues for further research for 'Potential Models'. It is just these 'potential' models that would be needed for fully integrating the benefits from parametric models and UPM and escape from the choice between qualitative and quantitative analysis.

Unlike the impact vector approach UPM provides a way to revert to the origin of the CCF contribution to the PSA results. This is a benefit worth considering for finding ways of movement, for the impact vector approach, towards what's pointed out as 'potential models' in Figure 5.

Within the 'parametric area' there are great developments that have been and are being made regarding quantification methods, but when it comes to the qualitative analysis there is actually no established working process. This was earlier indicated, when presenting the work within NAFCS, and is indirect the main subject of this thesis.

If the intention is to achieve a method with reliable quantitative properties and useful diagnostic characteristic it can be concluded that in fact both UPM and the impact vector approach should be disqualified; UPM due to its deficient quantitative properties and the impact vector approach due to lack of qualitative aspects.

4.4 The meeting between UPM and ICDE data

In the following sections UPM will be further explored with the intention to find out how the method can be applied on generic experience data. First though, it needs to be pointed out that when doing these analysis the question of interpretation is often raised. How, exactly, is for example the different categories of defence within UPM to be interpreted? Concerning one of these categories, MMI, a different concept will be used from now on. The made interpretation defence related to this category represents is considered to be better described by a category of 'Operator interaction'. Such a notion is also in better consistency with other current research in the area and therefore the UPM defence category of MMI will be replaced by an Operator interaction-category. The intention is of course to as clear as possible state what interpretations are made, but the very presence of this issue need to be bared in mind.

The initial consideration for this thesis was to study UPM as a method and to directly apply this method on ICDE data. During the study of the method features of the method gradually appeared indicating that a direct application of the method on real experience data, in terms of a generic database, might be more complicated than expected. Besides from that a direct application of the method also demands a specific format of the data to be used, i.e. the data need to include information needed for application of the method. As of today the information in the ICDE database does not contain information about contributing defences, which is the central aspect in UPM. Another aspect to be considered is the difficulties of making judgement about different defence's significance for a particular event based on the information given in the ICDE database. For application of UPM a rather good understanding or at least adequate amount of information, of the specific system, is necessary for being able to make the judgement needed for the assessment. This makes UPM not suited for application on a generic database of CCF events, but rather to assessment of a specific system or plant. This difficulty of application of the method, as well as modified versions of it, was also stated by Zitrou (2006). Although, because of some great advantages of the method it seems simply unwise to completely let go of the idea of exploring the field of interaction between actual experience data and UPM.

In a categorical comparison between UPM and parametric models some major differences soon becomes obvious, which was also stated in the previous chapter. The advantages of UPM are not concerning the quantification of a probability, beta or cut-off, factor but rather the qualitative results that can be recognized from the assessment. Here the designated qualitative results are the great potential of locating the weaker points of the system and also the defences to be reinforced for protection against CCF. When considering the parametric models the situation is the opposite. The great advantage of parametric models is their ability to provide quantification of a probability factor, but can only provide deficient qualitative results concerning ways of protecting against CCF. Although this is a very categorical and rough comparison it provides insights on how these different approaches possibly could balance each other.

On the issue of assessment of ICDE data much work has been done within the NAFCS project. Surveys have been done for different component groups, and for each component group each event has been examined and assessed resulting in net impact vectors for each separate event. Although (as previous pointed out) the qualitative and the quantitative analysis are done completely separated. This is something that with the use of UPM could be changed, by adding a UPM influenced analysis beside the impact vector construction. The question is though; if UPM can not directly be applied to ICDE data then how can this be done? With the ICDE database in one hand and UPM in the other a way of connecting them needs to be found, with the intention to find a way to apply the favourable features of UPM on available information. This could perhaps be done by studying ICDE events and with the assistance of UPM find those defences that would have prevented the failure(s). When trying to define which defence(s) could have prevented a particular event the question of interest is of course the underlying cause of the event. CCF events can be defined as the consequence of two separate elements: root cause and coupling factor. When identifying the root cause(s) of an event, the basic reason(s) why the component(s) fail is found. The coupling factor describes the mechanism that ties multiple impairments together and identifies the influences that created the conditions for multiple components to be affected. Therefore, identification of root cause(s) and coupling factor(s) can be seen to be tied to the identification of the significant defences for a specific event.

One methodology in this area has been developed by Paula and Parry (1990) when they presented a methodology referred to as a Cause-Defence Approach to the understanding and analysis of CCF. Their work was developed from insight about the, until then, existing methods' inability to explicit and systematically account for the impact of plant-specific defences (Parry, 1991). Their approach has no explicit connection with UPM, but is rather an attempt of turning some light on the parametric model's shortcomings in the qualitative analysis. Although, with UPM as a starting point a work in a corresponding direction have also been done by Zitrou for development of an extension of UPM, or more precise 'to explore the application of advanced mathematical techniques in order to further extend the Unified Partial Method (UPM) for CCF modelling' (Zitrou, 2006, p.7). What Zitrou has done is to suggest a modification of UPM to improve its deficient quantification ability. These two different research areas can be seen as examples of attempts to deal with their respective deficiencies. An analogue feature of these works (M. Paula and W. Parry, 1990, and Zitrou, 2006) is the use of connections between root causes, coupling factors and defined defences as a foundation for the analysis of CCF. In the ICDE database information is provided regarding root cause and coupling factor for each event. This if of course of great interest and the possibilities of how this can be used needs to be explored.

In Zitrou's work (Zitrou, 2006) a methodology based on Influence Diagram (ID) formalism is developed. This means it is a method that 'include decision and value nodes, and allow the representation and comparison of alternative actions and the determination of strategies regarding the decisions involved' (Zitrou, 2006, p. 90). For the development of this model the relationships between root causes, defences and coupling factors are explored and the resulting interpretation of these relationships is based on judgement by an expert panel. (Zitrou 2006) An interpretation of the relationships between root causes, defences and coupling factors is also made in (Paula, Parry, 1990). Further, in (Marshall et. al., 1998) an interpretation of the relationships between the three elements is found. This though, differ from the other two mentioned interpretations above in the sense that this is not a work aiming at studying these relationships, but still it pronounce an interpretation about the relationships under consideration.

These three approaches will be further presented and evaluated in Chapter 5.

4.5 Summarizing conclusions

It has appeared that an actual application of UPM on generic data, according to the application guide presented in section 4.2 will not be possible. Based on the performed comparative study of the methodologies it can be concluded that UPM can be disqualified as a quantitative method. This is of particular significance when it comes to application on generic data. When it comes to the impact vector approach it has been shown not being able to provide any qualitative aspects and it can be concluded that there is no generally useful working procedure adopted that captures the qualitative aspects. With these conclusions the matter of interest is: What are the possible ways of moving towards the 'potential models'? In Figure 6 two possible routes are indicated.

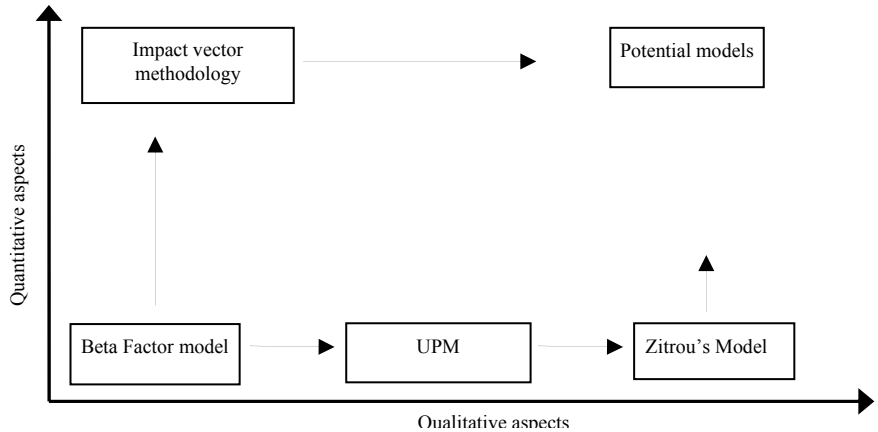

Figure 6. Possible ways of method development.

A possible strategy could be to incorporate UPM into the impact vector approach. This could be made by extending the impact vector approach with a qualitative assessment based on UPM. Some particular desirable feature of UPM has been identified and the next step is therefore to focus on finding a way of enabling application of these on CCF experience data.

A potential way of dealing with this is found in the relationships between root causes, defences and coupling factors. How these relations are configured is therefore to be evaluated, with the intention to develop a 'Relations of Defences, Root causes and Coupling factors' (RDRC) approach. Such an approach would be a qualitative one, which if used as a complement to the impact vector approach could be a possible way of advancing towards the 'potential models'.

5 Qualitative assessment using 'Relations of Defences, Root causes and Coupling factors'-diagrams

In this chapter the matter of subject is the development of the RDRC approach. The goal is to design an interaction diagram, an RDRC-diagram, for the relationships between different categories of root causes, defences and coupling factors. This will be made in the following three main steps. First, the detailed relationships between the three attributes, root causes, coupling factors and defences, are evaluated to develop the structure of the diagram. For this purpose the date set in consideration is presented in section 5.1. This first step is done partially by an assessment of the considered data set and partially by consideration of the approaches by Zitrou (2006), Paula and Parry (1990) and Marshall et. al. (1998). The proceedings of this step are presented in section 5.2. Secondly, the established RDRC-diagram is to be used in an exercise, where it is applied on the considered data set. In section 5.3 the results of this application are provided. Finally, the third step is an assessment is made of the results obtained in the second step. This evaluation is discussed in section 5.4.

5.1 Trial data set

In this thesis the data to be used is limited to ICDE data concerning the component group of emergency diesel generators in Sweden and Finland as of December 2001. The study of these events have included judgements about the interaction between root cause, coupling factor and defence for each separate event for creation of a basis for comparison with earlier work done in this area.

The EDGs are part of the class safety-related electrical power distribution system providing reliable emergency power to electrical buses that supply the emergency core cooling system and other equipments, which demand the availability of a stable source of electrical power, for safe shutdown of the reactor plant. Their configuration ensures that they supply adequate electrical power in case of loss of offsite power, with or without a concurrent large break loss-of-coolant accident (LOCA). These generators provide power only when needed and are normally in standby, whether the plant is at power or shutdown. The EDG system is automatically actuated by signals that sense either a LOCA, or loss of, or degraded, electrical power to its safety bus. Manual initiation of the EDG system is possible from the operator control room if necessary.

The component boundaries, as outlined by Wierman et. al. (2000), are given in the following description and in Figure 7 below. 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 system, 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 system 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 outside the control valves is excluded. The EDG room ventilation is included if the licensee reported ventilation failures that affected EDG functional operability. Included within the EDG system are the circuit breakers that are located at the motor control centres (MCC) and the associated power boards that supply power specifically to any of the EDG equipments. 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 vial electrical loads is considered integral to the EDG function and is therefore considered to be within the boundary of the EDG system. All instrumentation, control logic, and the attendant process detectors for system initiations, trips, and operational control are included.

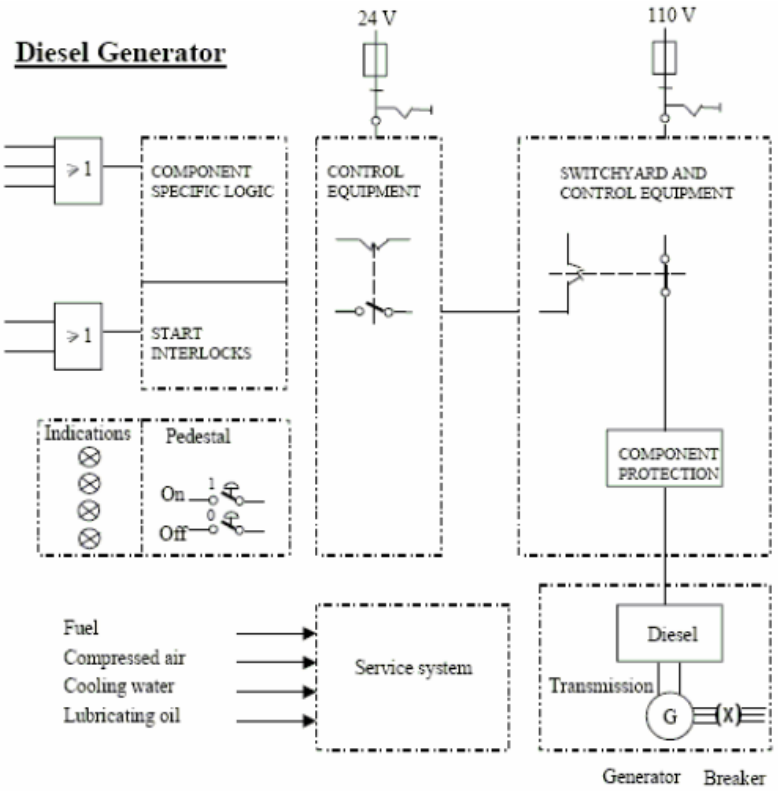

Figure 7. EDG and subsystems.

The data consists of reported CCF events considering EDGs. The events are, in the database, classified concerning root causes and coupling factors. An example of a reported event, although in a concentrated format, together with classified root cause and coupling factor is given in Table 2.

System info:	The diesel system is a four redundant system with trains A, B, C and D. Diesels were in standby during the event. The diesel service water system draws water from the same sea water channel as a four redundant shutdown service water system. Each shutdown service water train is connected to a heat exchanger in a shutdown secondary cooling system and to heat exchangers associated with one diesel. When the shutdown service water system operates the sea water cooling flow goes through exchangers in shutdown secondary cooling system and diesel system.
Brief event description:	Due to sludge movement the heat exchangers in train A, B and D were partially blocked. The event was directly detected (it was a monitored failure) and diesel heat exchangers were taken into clean-up maintenance. In case of an actual demand would exist, the cooling water temperature in trains A, B and D could gradually rise to the trip limit and thus prevent diesel operation. If long run demand would exist during the clean-up of the first heat exchanger there would be some risk for double failure.
Root Cause	Abnormal environmental stress.
Coupling Factor	Environmental, external.

Table 2. Example event.

In Table 3 the data set is presented in terms of root cause and coupling factor for each event. The presented root cause and coupling factor for each event is based on the assessment made within this work, and does not for all events agree with the what is stated in the database.

Event no.	Root cause	Coupling factor group	Coupling factor
01	Internal to component	Environmental	Environmental internal
02	Maintenance	Operational	M/T Procedure
03	Human action	Operational	M/T Procedure
04	Abnormal environmental stress	Environmental	Environmental external
05	Human action	Hardware	System design
06	Abnormal environmental stress	Environmental	Environmental external
07	Abnormal environmental stress	Environmental	Environmental external
08	Internal to component	Environmental	Environmental internal
09	Human action	Operational	M/T Staff
10	Internal to component	Environmental	Environmental internal
11	Abnormal environmental stress	Environmental	Environmental external
12	Abnormal environmental stress	Environmental	Environmental external
13	Design	Hardware	Hardware design
14	Internal to component	Hardware	Hardware design
15	Internal to component	Hardware	Hardware design
16	Internal to component	Hardware	Hardware quality deficiency
17	Human action	Operational	Operation staff
18	Design	Hardware	Hardware design
19	Internal to component	Hardware	Hardware
20	Internal to component	Hardware	Hardware quality deficiency
21	Design	Hardware	Hardware design
22	Human action	Operational	Operational
23	Design	Hardware	Hardware quality deficiency
24	Maintenance	Operational	M/T Procedure
25	Human action	Operational	Operational
26	Design	Hardware	Hardware
27	Design	Hardware	Hardware
28	Design	Hardware	Hardware
29	Design	Hardware	Hardware design

Table 3. Event data.

The data is also presented in graphically in Figure 8, 9 and 10 below. From these figures it becomes obvious that the most frequent root causes are Design and Internal to component, while the most frequent coupling factor is hardware design.

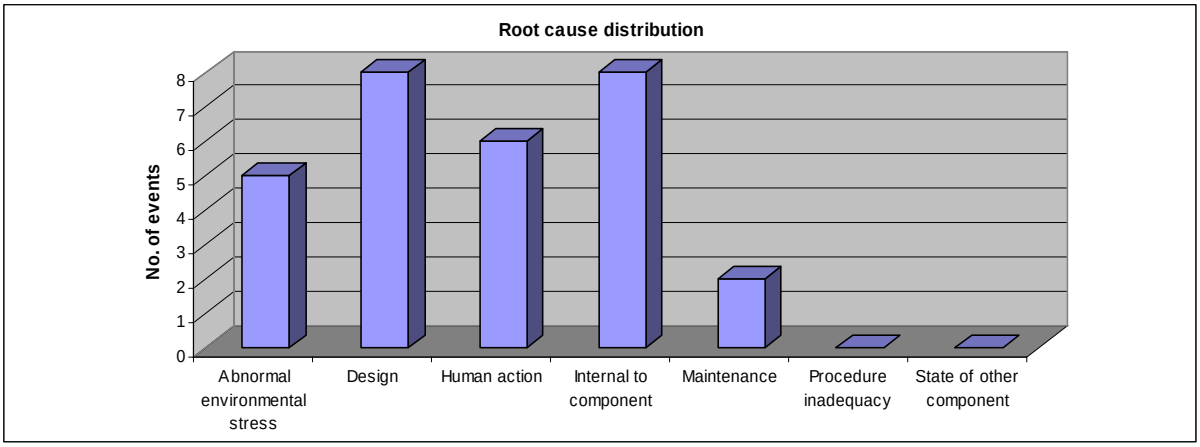

Figure 8. Root cause distribution.

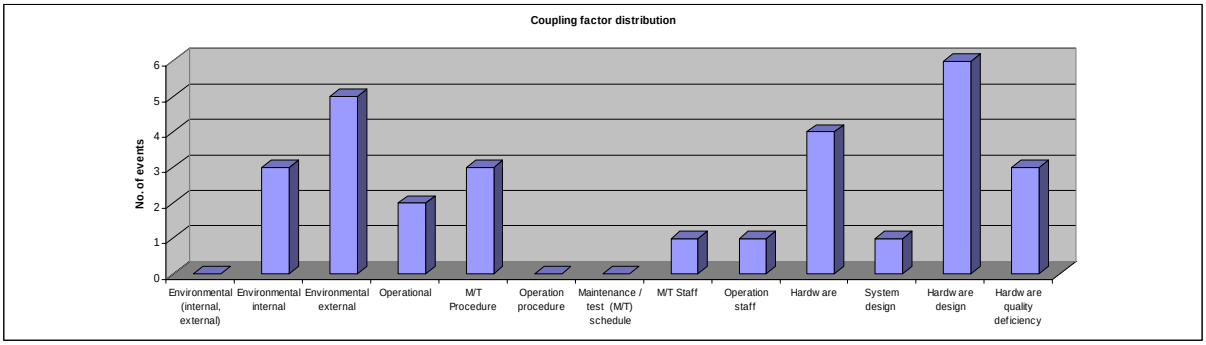

Figure 9. Coupling factor distribution.

When putting the coupling factors in groups it becomes even clearer that the most common coupling factors are the ones related to hardware. This is shown in the Figure 10.

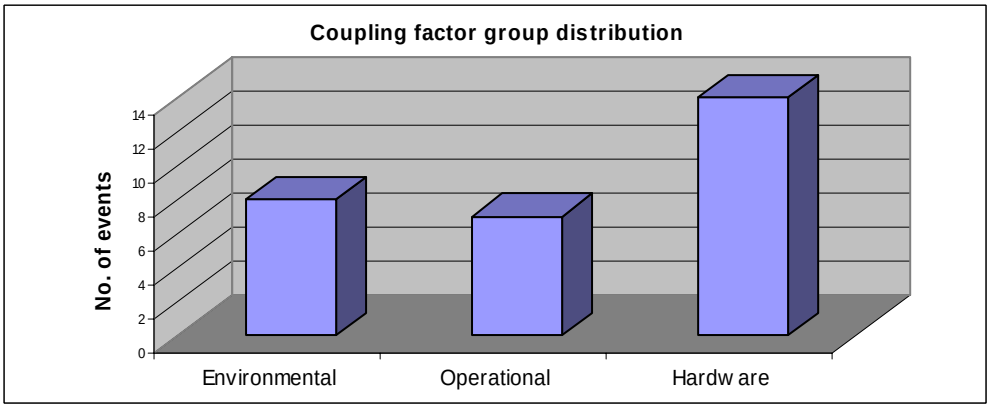

Figure 10. Coupling factor group distribution.

5.2 RDRC-diagram development

In this section the relationship between defences, root causes and coupling factors will be examined. The classification, as well as definition, of the three elements is for root causes and coupling factors as within ICDE and for defences as within UPM. The assumed categories are given in Table 4.

Defences	Root causes	Coupling factors
-Redundancy/Diversity -Separation -Understanding -Analysis -Operator interaction -Safety culture -Environmental control -Environmental testing	-State of other component -Design, manufacture or construction inadequacy -Internal to component, piece part -Maintenance -Abnormal environmental stress -Procedure inadequacy -Human actions -Other -Unknown	-Environmental (internal, external) -Environmental internal -Environmental external -Hardware -Hardware design -System design -Hardware quality deficiency -Operational -Operation procedure -Operation staff -Maintenance / test (M/T) schedule -M/T Procedure -M/T Staff

Table 4. Categories of defences, root causes and coupling factors.

An exercise has been performed to evaluate these relationships for the experience data presented in the previous section. The result of this is presented in an interaction diagram in Figure 11. This diagram has been created in the following steps; (1) each event has been studied to examine and record root cause and coupling factor, then (2) an interaction diagram has been made for each separate event where assessment of defences of interest against root cause and coupling factor for the specific event provide connections between these elements, and finally (3) these interaction diagrams have been put together to form a data diagram. This is a diagram based on data within the scope of this thesis. In the process of finding the RDRC-diagram the one based on experience data will be studied and compared to other corresponding interpretation of relationships between concerned elements. This is done to enable absorption of interaction of elements that are not present in the studied data. The procedure for this is to study the interpretations by Zitrou (2006), Paula and Parry (1990), Marshall et. al. (1998) in an attempt to harmonize these approaches and incorporate their judgments into the RDRC-diagram. In the design of the RDRC-diagram the interpretation by Zitrou will serve as a starting point, since this is an explicit application of the central method in this procedure, UPM, while the others are developed without consideration of UPM. In this way Zitrou's interpretation will be tested against real experience data and may also be improved by the help of other similar performed research. This is then actually a question of a validation of the diagram by Zitrou by the use of experience data and analysis of corresponding research.

Below are the interpretations of interaction between root causes, coupling factors and defences to be studied presented. An important notice to be made is that in these different interpretations, different definitions of terms are embedded. In the interaction diagram based on experience data the root causes and coupling factors are to be interpreted as within the ICDE project and the defences are as per UPM. This is also the case for the interaction diagram by Zitrou, see Figure 12. In the interpretations by Marshall et. al. (1998), Table 7, and Paula and Parry (1990), Tables 5 and 6, the classification and definition of terms are not the same and must therefore be treated in the light of this circumstance.

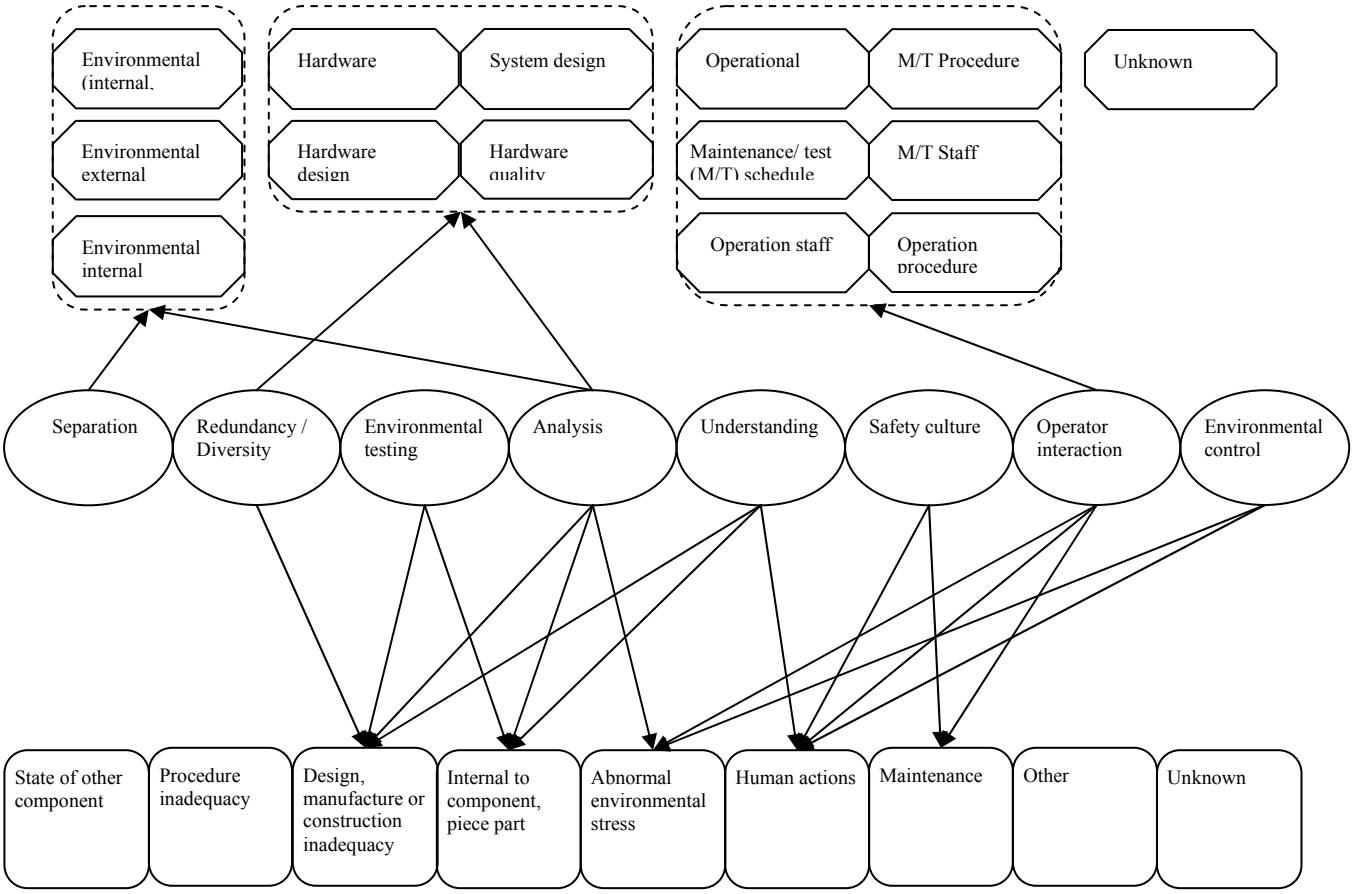

Figure 11. An interaction diagram constructed by the use of ICDE data.

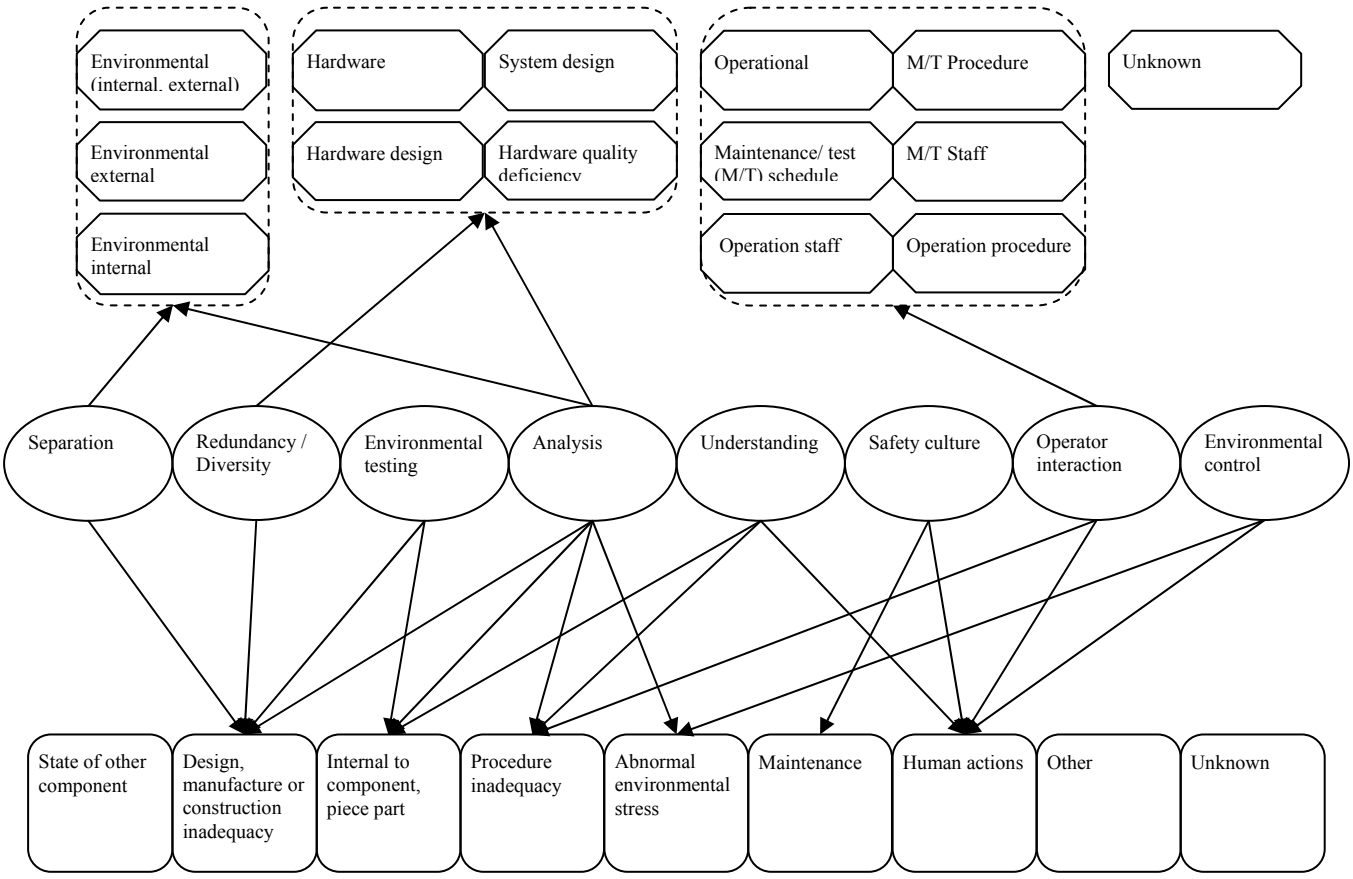

Figure 12. Interaction diagram by Zitrou.

In Table 5 the cause-defence approach by Paula and Parry is presented[7].

Defence	Pre-Operational-Related Causes				Operational-Related Causes						Environmental- Related Causes			
	Systematic Error in Design		Systematic Error in Manufacturing, Construction, Installation and Commissioning		Inadequate Procedure				Inadequate Execution of Procedure					
					Error in Procedure		Ambiguity/ Lack of Clarity		All Crews		Single Crews		Internal Environmental Effect	External Environmental Effect
	Slow-Acting	Fast-Acting	Slow-Acting	Fast-Acting	Slow-Acting	Fast-Acting	Slow-Acting	Fast-Acting	Slow-Acting	Fast-Acting	Slow-Acting	Fast-Acting	Slow-Acting Fast-Acting	Slow-Acting Fast-Acting
Barrier	-	-	-	-	-	-	-	-	-	-	■	■	■	■
Diversity	■	■	■	■	■	■	■	■	■	■	■	■	■ o	■ -
Preventive Maintenance	o	-	o	-	o	-	o	-	o	-	o	-	o -	o -
Procedures Review	-	-	-	-	■	■	■	■	-	-	-	-	o^a o^a	o^a o^a
Personnel training	-	-	-	-	-	-	o	o	■	■	■	■	o^a o^a	o^a o^a
Quality Control (QC)	o^b	o^b	o	o	-	-	-	-	-	-	-	-	- -	- -
Monitoring, surveillance Testing and Inspection	o^c	o^d	o^c	o^d	o^c	-	o^c	-	o^c	-	o^c	-	o^c -	o^c -

[a] Addresses those aspects related to barrier integrity
[b] Design QC and design review
[c] If degradation can be monitored, this may be a strong defence
[d] Proof/acceptance testing

Table 5. Cause-Defence relations by Paula and Parry, root causes and defences.

[7] A solid square (■) represents a strong impact, an open circle (o) represents a weak impact and a dash (-) represents no impact, where impact means beneficial effects of a defence.

Defence tactics against coupling factors for each failure cause group is presented in Paula and Parry (1990). In Table 6[8] their approach is illustrated for operational-related and environmental-related causes[9].

Failure Cause group	Defence Against[a]		
	Conditioning event	Trigger event	Coupling
Inadequate Procedure:			
- Error in procedure	Procedure review		Functional diversity[b] Equipment diveristy[b]
- Inadequate procedure (ambiguity / lack of clarity)	Procedure review Management review	Training	Functional diversity[b] Equipment diveristy[b] Staff diversity[c] Staggered test / maintenance
Inadequate Execution of Procedure:			
- All crews	Management review	Training	Functional diversity[b] Equipment diveristy[b]
- Single crew		Training	Functional diversity[b] Equipment diveristy[b] Staff diversity Staggered test / maintenance
Internal environmental effect (corrosion, etc.)	Ensure internal environment is 'pure' Preventive maintenance	Surveillance testing /condition monitoring (slowly developing only)	Functional diversity Equipment diversity Barrier between inputs to redundant trains Staggered maintenance
External environmental effects:			
- Shock (fast acting)	Barriers		External barriers between redundant trains
- Slow acting			Functional diversity[d] Equipment diversity[d] External barriers between redundant trains

[a] Additionally, surveillance testing/condition monitoring and a preventive maintenance program are defences against persistent (slow-acting) failure mechanisms that show signs of degradation.
[b] Assumes different sets of procedures for redundant equipment.
[c] Staff diversity is here defined as having different persons or different teams for installing, testing, or maintaining redundant components.
[d] Diverse equipment are less likely to be similarly susceptible to the same external environment effects and thus less likely to fail simultaneously from these effects.

Table 6. Defence tactics against coupling factors for each failure cause group by Paula and Parry.

[8] This table is to be understood as for failures causes that concerns 'Error in procedure' beneficial defences against related coupling mechanisms are Functional diversity and Equipment diversity, etc.
[9] Corresponding for pre-operational is not provided explicit in their report.

Below, in Table 7, are the connections between defence mechanisms and coupling factors described, as interpreted by Marshall et. al. (1998).

Defence mechanism:	Coupling factor:
Functional barrier	Hardware design: component part (internal parts: ease of maintenance and operation)[a] Hardware design: system configuration (physical appearance: identification, size or system layout)[a] Hardware quality: installation construction (initial or modification)[a] Environment: internal fluid
Physical barrier	Hardware quality: installation construction (initial or modification)[a] Environment: external
Monitoring/ Awareness	Hardware quality: installation construction (initial or modification)[a] Operational: maintenance/test schedule[a] Operational: maintenance/test procedure[a] Operational: maintenance/test staff[a]
Maintenance staffing and scheduling	Operational: maintenance/test schedule[a] Operational: maintenance/test procedure[a] Operational: maintenance/test staff[a] Operational: operation procedure Operational: operation staff
Component identification	Hardware design: system configuration (physical appearance: identification, size or system layout) [a]
Diversity	Hardware quality: installation construction (initial or modification) [a] Hardware quality: manufacturing Hardware design: component part (internal parts: ease of maintenance and operation) [a]
No practical defence	Hardware design: component part (internal parts: ease of maintenance and operation) [a]
Unknown	-
[a] More than one defence mechanism can be used against any one of these coupling factors, so judgment is used to select the appropriate defence mechanisms for the specific event.	

Table 7. Defence mechanisms mapping from coupling factors by Marshall et. a1. (1998).

5.2.1 Harmonization of different approaches

As concluded before the interpretations by Marshall et. al. and Paula and Parry need to be considered regarding their respective categorisation. In this section they will be interpreted and to some extent modified to be more comparable with the classification and definitions used in this work, starting with the one by Marshall et. al.

First, the coupling factors by Marshall et. al. are put into three groups, to correspond to the groups found in ICDE terminology. Then the listed defences are categorised to correspond to the defences by UPM. The transformations are presented in Table 8 and 9. The categorisation below is made by interpretation of the classification by Marshall et. al. and the one by ICDE. The definition of different categories might differ between analysts. This has been accounted for in this categorisation, but still it is a question of interpretation.

Marshall et. al. coupling factor groups:		Corresponding ICDE coupling factor groups:
Environmental external Environmental internal	→	Environmental
Hardware design: component part (internal parts) Hardware quality: installation/construction (initial or modification) Hardware design: system configuration (physical appearance) Hardware quality: manufacturing	→	Hardware
Operational: operation procedure Operational: maintenance/test schedule Operational: maintenance/test staff Operational: maintenance/test procedure Operational: operation staff	→	Operational

Table 8. Transformation of coupling factor groups.

Defences by Marshall et. al.:		Corresponding defences by UPM:
Physical barrier	→	Separation
Functional barrier	→	Separation
Maintenance staffing and scheduling	→	Operator interaction and Safety culture
Monitoring / awareness	→	Safety culture
Component identification	→	Understanding
Diversity	→	Redundancy Diversity

Table 9. Transformation of defence categories.

In Figure 13 is an interpretation of the diagram by Marshall et. al. where the coupling factors have been put into groups to agree with the ICDE categorisation and the defences have, under careful consideration, been exchanged to their UPM defence counterpart.

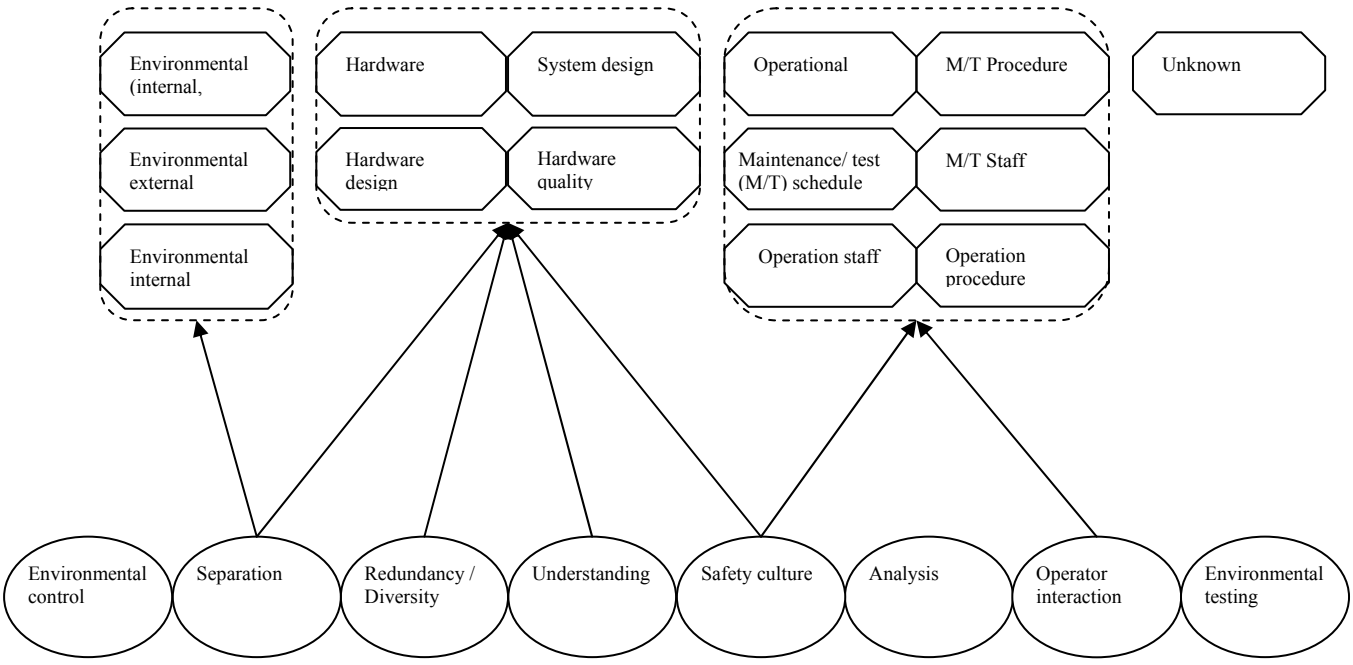

Figure 13. Interaction diagram- interpretation of Marshall et. al.

Now the diagram by Paula and Parry is considered. First the root causes are put into groups, to correspond to the root causes found in ICDE terminology, which is presented in Table 10. Then the listed defence categories are customized to correspond to the defences by UPM. The same is done for the defence tactics against coupling factor for each root cause group although it is worth noting that influence of defence tactics towards coupling factors for pre-operational root causes are not given explicit in the literature. The transformations are presented in Table 11 and 12. Definitions of different defences might differ between analysts. This has been accounted for in this categorisation, but as for the case in the transformation of the diagram by Marshall et. al. it is still a question of interpretation.

Root cause groups by Paula and Parry:		Corresponding Root causes by ICDE:
Operational-inadequate procedure: Error in procedure Operational-inadequate procedure: Ambiguity / Lack of clarity	→	Procedure inadequacy
Operational-inadequate execution of procedure: All crews Operational-inadequate execution of procedure: Single crews	→	Human actions and Maintenance
Environmental: Internal environmental effect	→	Internal to component and State of other component(s)
Environmental: External environmental effect	→	Abnormal environmental stress
Pre-Operational: Systematic error in design Pre-Operational: Systematic error in manufacturing, construction, installation and commissioning	→	Design, manufacture or construction inadequacy

Table 10. Transformation of root cause groups.

Defences against root causes by Paula and Parry:		Corresponding defence by UPM:
Diversity	→	Redundancy / Diversity
Preventive maintenance	→	Environmental testing
Procedures review	→	Operator interaction
Personnel training	→	Safety culture
Quality control	→	Analysis
Monitoring, surveillance, testing and inspection	→	Operator interaction and Environmental testing
Barrier	→	Separation

Table 11. Transformation of defences against root causes.

Defences tactics against coupling factors for each root cause group by Paula and Parry:		Corresponding defence by UPM:
Staggered test / maintenance	→	Operator interaction
Equipment diversity	→	Redundancy / Diversity
Staff diversity	→	Operator interaction
Functional diversity	→	Redundancy / Diversity
Barrier: Between inputs to redundant trains	→	Separation
Barrier: External barriers between redundant trains	→	Separation

Table 12. Transformation of defence tactics against coupling factor groups for root cause groups.

In Figure 14 an interaction diagram by Paula and Parry is presented, where the root causes have been put into groups to agree with the ICDE categorisation and the defences have, under careful consideration, been exchanged to their UPM defence counterpart:

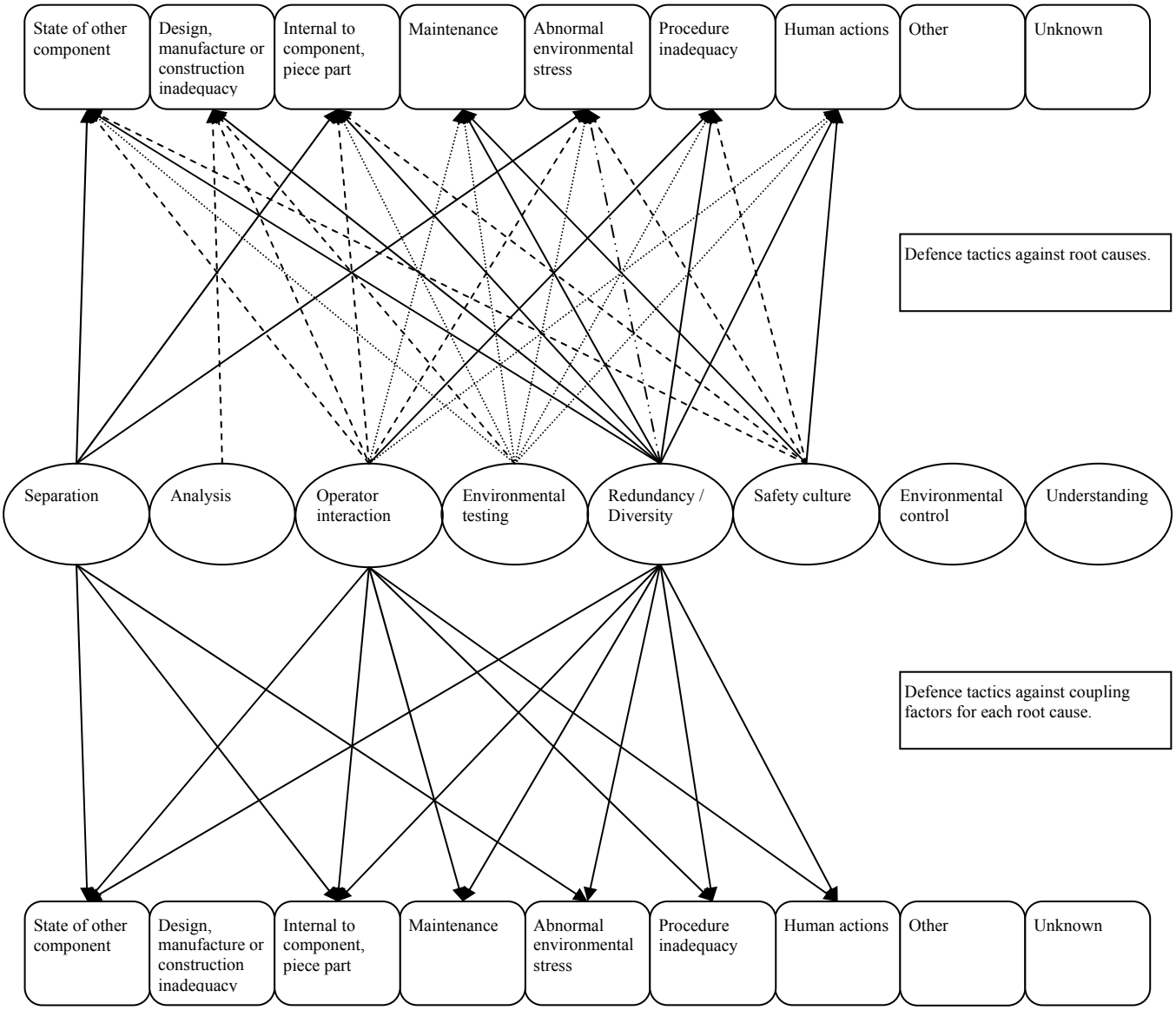

Figure 14. Interaction diagram- interpretation of Paula and Parry.

5.2.2 The RDRC-diagram

When comparing the presented different approaches some differences are revealed. These differences have been evaluated to find the structure of the final interaction diagram. As earlier discussed the diagram by Zitrou is used as a starting point, and some main questions are asked to upgrade this diagram in design of the RDRC-diagram: Are there any interesting relations between these elements that are not present in the diagram by Zitrou, but in some of the others? Are there any relations that is present in Zitrous' interpretation but not in the others? In this way, relations to be added or removed to/from the RDRC-diagram have been found. The final diagram is presented in Figure 15. A more detailed description of the relationships is provided in Appendix B.

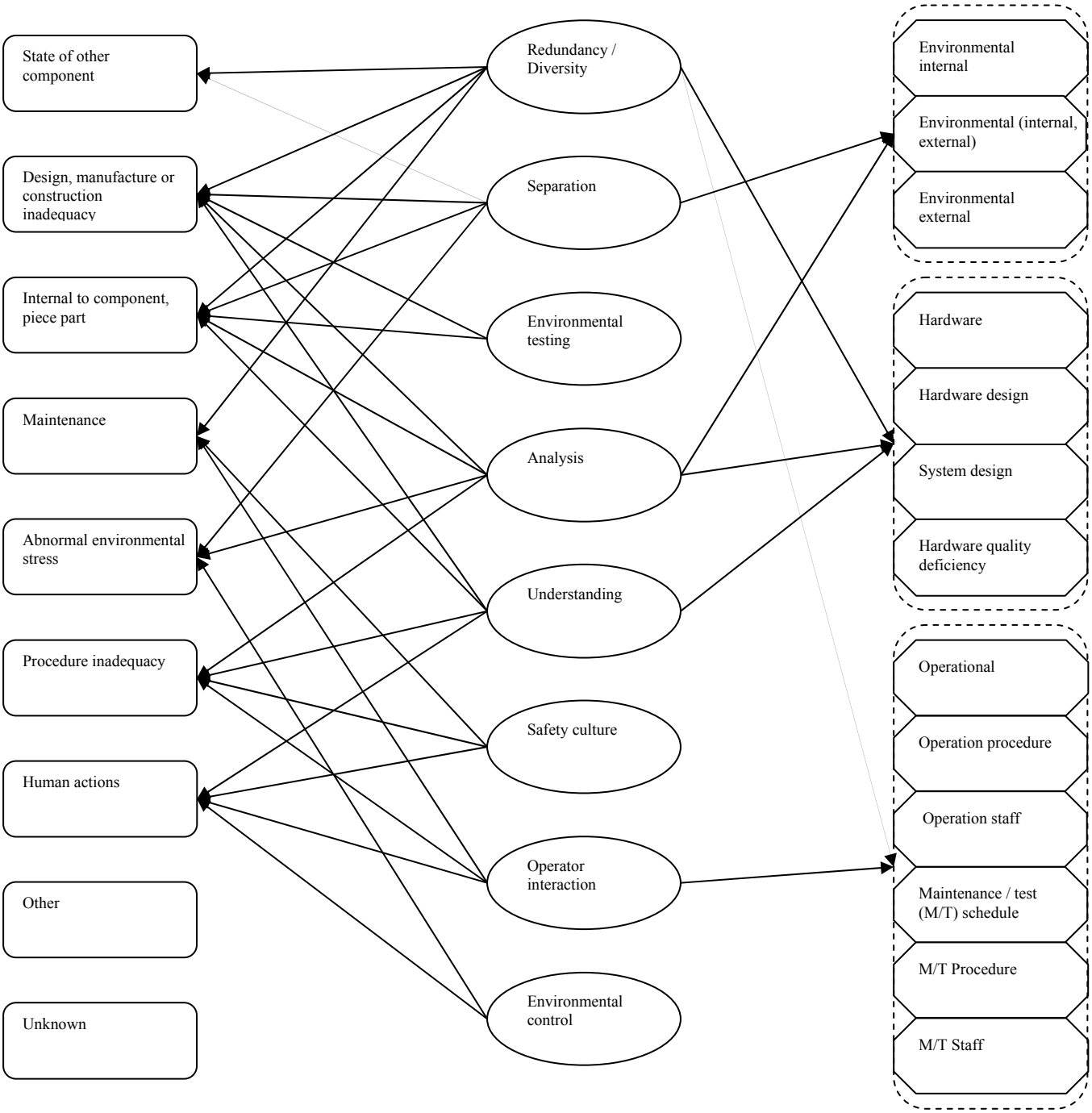

Figure 15. RDRC-diagram

Another feature within UPM is the weighting (Brand, 1996) of the different categories of defences, as stated in section 4.2. This weighting will be accounted for in the same way also in this application, and is structured as shown in Table 13.

Defence category	Weighting
Redundancy / Diversity	6
Separation	8
Understanding	6
Analysis	6
Operator interaction	10
Safety culture	5
Environmental control	6
Environmental testing	4

Table 13. Weighting of defences.

In the next chapter an application of the established RDRC-diagram on experience data will be presented.

5.3 Application of RDRC-diagram on trial data set

When the RDRC-diagram is applied on the data set presented in 5.1 the assigned defences are found for each event, since each event is connected to a root cause and coupling factor. The occurrences of the defences are counted and in this way the potential defences for the assessed events can be obtained.[10] Due to the structure of the RDRC-diagram one category of defence can come about more than once for each event, once for the current root cause and once for the current coupling factor. Because a category of defence can take different forms depending on if it is applied against root causes or coupling factors it should in such cases be 'counted twice'. In addition to this the weighting of the different defences has also been accounted for. Finally, the evaluation for each event is summarised to obtain results for the total set of the data. The result of this application will be presented in the following.

In Figure 16 the distribution of the defences is presented. Here it is shown that the most central defence is Analysis, followed by Separation, Understanding and Redundancy/Diversity.

[10] To illustrate how this is done a description of application on the example event in section 5.1 is provided in the following: The identified root cause was "Abnormal environmental stress". When looking at the RDRC-diagram it is found that this root cause is linked with the defence categories "Separation", "Analysis" and "Environmental control". When corresponding is done for the identified coupling factor, "Environmental, external", the associated categories of defence are "Separation" and "Analysis". For this event the occurrences of categories of defences are "Separation" (2), "Analysis" (2) and "Environmental control" (1). When the weighting of the different categories of defence are added it is concluded that "Separation" is counted to (2 x 8 =) 16, "Analysis" is counted to (2 x 6 =) 12 and "Environmental control" is counted to (1 x 6 =) 6.

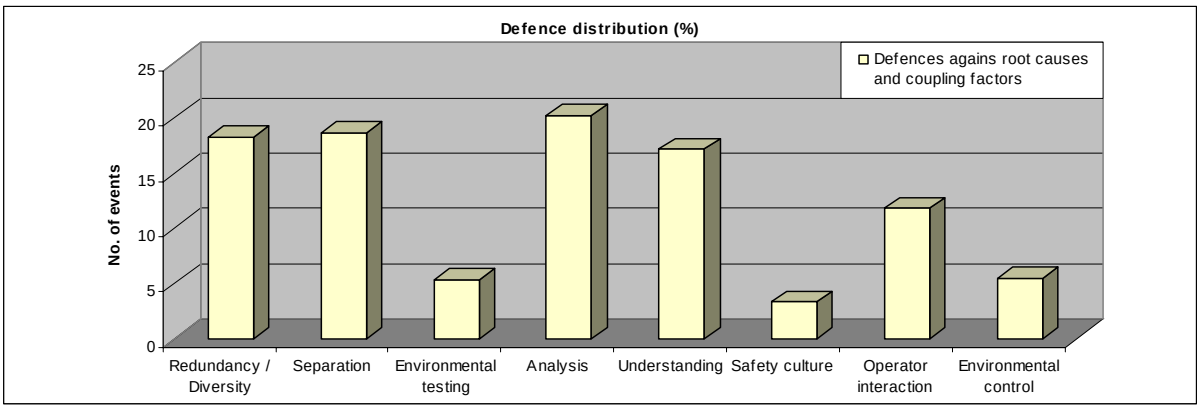

Figure 16. Defence distribution.

However, due to the different characters of a defence depending on whether if it is applied against root causes or coupling factors it can be argued that it is of more interest to look at the distribution when these cases are separated. In Figure 17 the distribution of defences against root causes are presented. From this it can be concluded that the most central defences against root causes are Separation, while other defences of great impact are Understanding and Analysis.

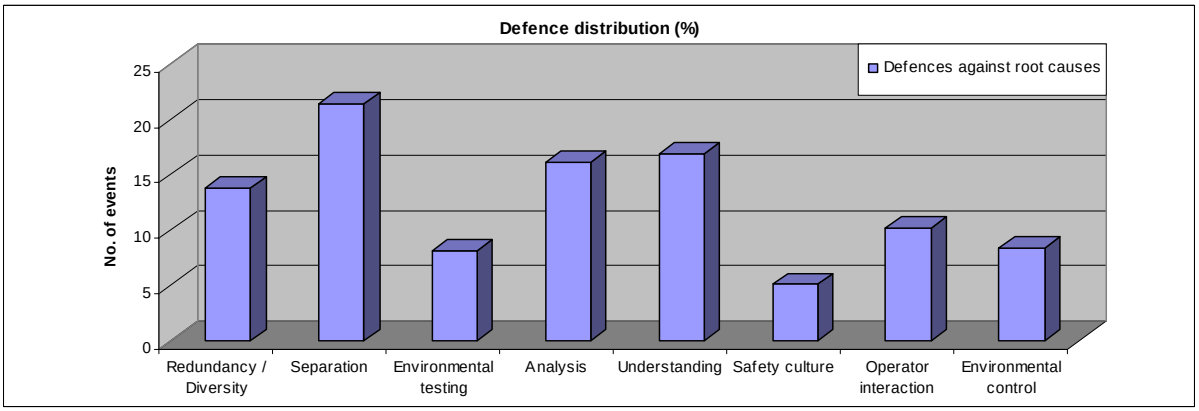

Figure 17. Defence distribution.

In Figure 18 the distribution of defences against coupling factors are given. This shows that the most central defences against coupling factors are Analysis, Redundancy/Diversity.

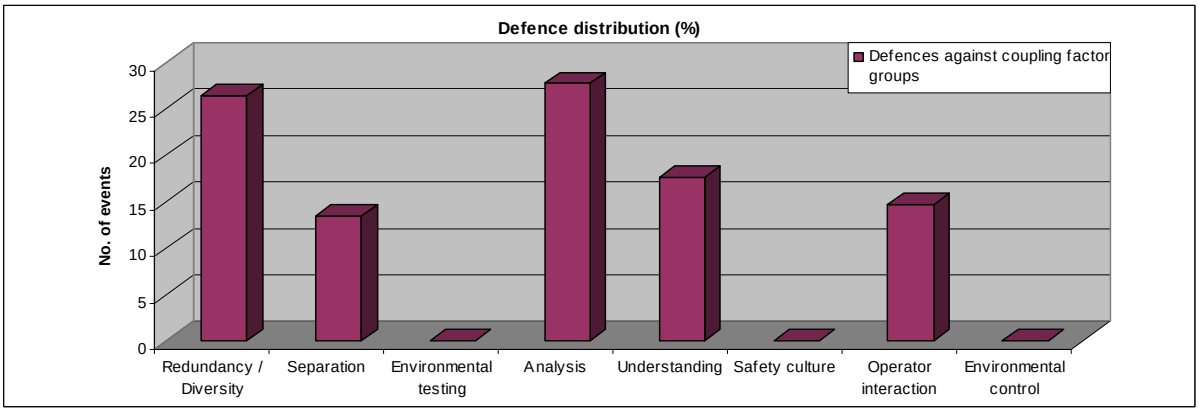

Figure 18. Defence distribution.

Another approach is to consider the different combinations of root causes and coupling factors. This is presented in Figure 19. When this is done the most potential defences are shown to be Analysis, Separation, Redundancy/Diversity and Understanding.

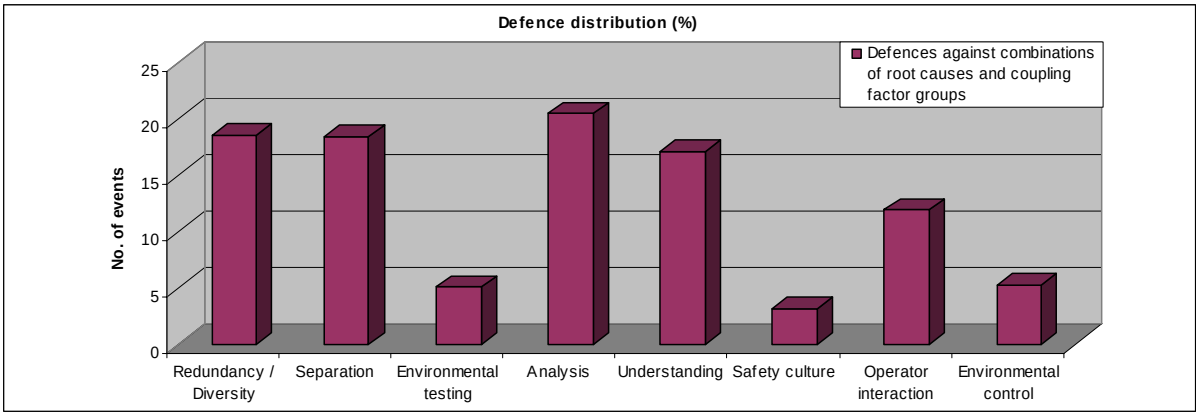

Figure 19. Defence distribution.

5.4 Assessment of the results

There are mainly two subjects to be discussed in this section. One of them concerns the trustworthiness of the results presented in section 5.3, which will be treated first, while the other subject relates to the possible use of such results, which is treated next.

The exact figures obtained in the previous section (5.3) are actually not of any particular interest, but what is of more interest is an evaluation of whether the results actually are reasonable or not. So, that defence X has occurred y times does not really tell us anything, but what is more important is the question of if it is reasonable that defence X is more important to the EDG system than defence Z is when it comes to prevention of CCF events. With such a consideration the credibility of the RDRC-diagram can be evaluated. In Johanson et.al. (2003) a qualitative assessment for Swedish EGDs is made, with which a comparison hopefully will be useful for this purpose. The study made in this reference does have a rather different approach though, since it mainly focuses on MTO-aspects, but still it states some interesting results concerning the general situation. It can be read that

> 'Results from the study indicate that slightly more than 70 % of the hardware CCF – or one third of all the identified CCF events – are related to ageing phenomena. These phenomena encompass both ageing of electronic equipment (electronic cards, EG10 relays, etc.) and of mechanical equipment. For the latter, vibration induced fatigue represents an important factor.'

(Johanson et al., 2003, PR08, p. 10)

Even though the data set considered in this study slightly differs from the one treated in Johanson et.al (2003b) the conclusion regarding the most common causes are the same, since ageing (and wear out) are the most frequent triggers also for the events within this study. When it comes to defences against these kinds of failure it is in the same reference stated that:

> 'Based on these results, it is judged that potential corrective actions should be directed toward:
>
> -Efficient experience feedback (within and between plants, with components manufacturers) for the timely identification, assessment and resolution of ageing phenomena.

-Focussed preventive maintenance programme based on insights from the experience feedback programme.
-Expeditious corrective maintenance programme for the replacement of parts and components sensitive for CCF risks already identified by the plants/industry.'

What appears as certainly interesting is to look at the combinations of root causes and coupling factors, to account for a case being as specific as possible. In Figure 19 it was shown that the category of defence that should be of most importance is Analysis. This was also the result when looking at the total distribution of defences, see Figure 16. Analysis is a defence category that within UPM is associated with checking of design and the experience feedback of this checking. This indicates that the results in the assessment within this work provide the similar conclusions to those made in Johanson et. al. (2003). The main methodological difference between these two assessments is the required input, which in the end makes them each useful for different intentions. This subject will be further discussed in section 6.3.

When it comes to the use of the results an aspect worth some special attention is the diagnostic possibilities of this kind of application. Besides the feature of providing indications about potential defence categories there is actually a way of getting even deeper into this matter. After having performed an analysis where candidate defences have been discovered one could go backwards in the analysis and on a more detailed level discover more specifically the significant defence strategies. By the fact that the procedure of the analysis contains information about which events that contribute to results of one category of defence being shown as more promising than the others these events can be recognized. If these specific events are studied in more detail specific potential defence strategies can be identified. In Johanson et. al. (2006) a list of suggested measures to take against dependency is given. Such a list can be used, beside a RDRC-diagram, to define the appropriate defences on a detailed level. In this way the use of RDRC-diagram can provide a qualitative procedural framework and be used as a diagnostic tool.

Another possible use that would be of particular interest concerns the possibility to in the analysis take account for made improvements, based on previous assessment, in the defences of the system under consideration. As of today, when the analysis is based on experience data, the situation is that before any modifications can be credited in the analysis they have to have had an effect in experience data. This means that a just made modification might not have an effect in the analysis until many years later, when all data needed have been collected and evaluated. Within UPM, modifications in terms of defence improvements are also included since it is the current configuration that is to be assessed. This is a feature that definitely is of great interest and would provide valuable features if it could be incorporated within the parametric field. Perhaps there is a possibility to do this by the use of an applicability factor that in such cases would pave the way for authorization of removal, or decreasing of the impact, of current events in the analysis. In such case the observation time would also have to be considered to reflect the situation. A similar way of using applicability, or transfer, factors can be found in German analysis methodology (Kreuser, Peschke, 2003). Unfortunately this work will not provide a solution to this but it is without doubt a question worth further investigation.

There are also two other subjects that need some additional attention. The first one concerns the weighting of the different defences. The second relate to uncertainties that originate from the judged root causes and coupling factors, based on the made categorisations of these attributes. These are two issues that both undoubtedly have a great impact on the results obtained when applying the RDRC-diagram. Further investigation of them is not in the scope

of this thesis, but both issues are brought up when discussing ideas for further research in section 6.3.

6 Discussion

6.1 A brief summary

The far most used tool within the area of CCF analysis is the impact vector method or related methodologies. These are methods providing ‘reliable’ quantitative results, but for obtaining the qualitative counterpart the range of tools are not at all that wide. Due to the lack of diagnostic value of parametric methods, the qualitative analysis is made separately and there is no actual established method for this qualitative part of the total analysis. What has been shown here is that there is a possibility to incorporate a softer factor into the field of the impact vector approach for CCF analysis. This can be done by establishing a method for the qualitative analysis that can be made in parallel to the quantitative one to increase the diagnostic value to the use of parametric methods. By the use of interaction diagram, as the RDRC-diagram presented in this work, a structural working procedure for qualitative assessment that is compatible with impact vector analysis can be obtained.

6.2 Quantitative vs. Qualitative aspects

The aim of this subsection is to discuss the subject of method properties, quantitatively and qualitatively.

In Chapter 3, Figure 3 was provided to illustrate the work by NAFCS. It was already then noted that there is a total separation of quantitative and qualitative analysis. This will be further discussed here as well as the situation of available frameworks for the qualitative part of the analysis.

In section 2.2, a general framework for CCF treatment was illustrated in Figure 2. Currently some difficulties are experienced when it comes to what is indicated as item 4.2, Sensitivity Analysis. To be able to evaluate obtained results from the performed analysis qualitative aspects are required, but as already concluded there is no general framework that is widely adopted for a qualitative analysis. Therefore, it could be argued that a deficiency that has been revealed is that a proper link between item 3.3, Data Classification and Screening, and 4.2, Sensitivity Analysis, is missing. A certainly interesting character of UPM is the possibility of from the assessment results being able to go backwards in the analysis and reconsider issues of interest. By capturing this feature the needed connection from a sensitivity analysis back to the data classification and screening could perhaps be established. What this is also about is avoiding method structures where qualitative and quantitative aspects are not compatible. To overcome this issue the development needs to be directed towards what has been pointed out as ’potential models’ that incorporate both qualitative and quantitative aspects to a sufficient extent. It can be argued that there are two ways of advancing toward this goal, either by development of the model by Zitrou to a model with improved quantitative characteristics or by development of the impact vector approach to one with extended qualitative features. What has been done in this work is the construction of the RDRC-diagram. The question of interest is then of course; how far does this take us? The answer on such a question will obviously not be precise, but it is this matter that is of interest for a discussion at this point.

Within this work information in the ICDE database and its relation to a categorisation of defences has been performed. This has resulted in a structural guide for analysis of these defences, the RDRC approach. The suggested approach has also been used in a trial application in an exercise with Nordic diesel data, so that a first step validation of it has been performed. With these steps taken it can be concluded that with the introduction of RDRC-diagram the main philosophy of UPM can be captured. When the idea of assessing a system in the purpose to find the defences that are most important towards CCF impact is implemented in a structured working procedure that as a matter of fact is compatible with the parametric approach a new dimension of such analysis can be achieved.

The procedure of using RDRC-diagram can provide a structured framework for the qualitative part of the analysis. If this is used as a complement to the impact vector methodology a more comprehensive analysis can be accomplished. It will still be a question of two separated analyses, a quantitative and a qualitative one, but at least there will be two compatible frameworks completing each other. Since there is no approach to be found dealing with both these issues the suggested approach to adopt is an integrated impact vector and RDRC methodology. With such approach the way to move towards the 'potential models' will be along the y-axis with the use of impact vectors. With the complement of RDRC-diagram a movement along the x-axis via the impact vector methodology can be achieved. In this way an RDRC approach could perhaps constitute 'the missing link' in Figure 2. That is, an approach like RDRC, or corresponding, could be useful when it comes to the issue of sensitivity analysis by providing the opportunity of moving backwards in a performed analysis to evaluate the results. Unfortunately not all the desired qualitative aspects of UPM are incorporated, when using the RDRC approach, so a best guess is that the methodology of RDRC-diagram would end up in a position illustrated in Figure 20.

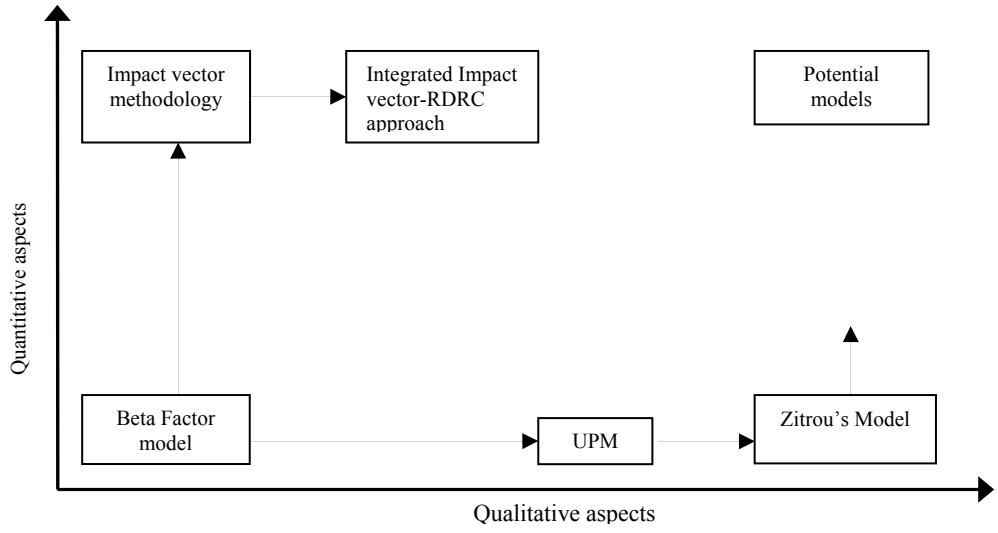

Figure 20. RDRC approach positioning.

6.3 The use of an RDRC approach

Of course it is not the case that qualitative studies are not being performed, even though there is no established approach for this purpose. One example of a thorough qualitative study is found in Johanson et. al. (2003). This kind of study should if illustrated in a chart as the one in Figure 20 be positioned relatively far out along the x-axis, but without reaching any higher level along the y-axis. The main differences between existing qualitative studies and an approach as the RDRC concern the depth of the assessment and the general applicability. In

general, qualitative studies require an analyst that has extremely deep knowledge about the system to be assessed, or at least a very generous availability of data. This makes such a strategy difficult to manage, not least since data availability is often a problem. The RDRC approach is not that demanding in this sense and is therefore more easily applied and has reproducible advantages, but on the other hand it can not provide the same depth in the qualitative results. A pleasant feature of the RDRC approach that needs to be stressed is that it can be applied for defence assessments based solely on the information already available in the ICDE database. This renders the possibility to make the application almost semi-automatic, which is not possible with currently available approaches and is therefore an obvious benefit. A drawback though, as indicated, is its limitations in providing a real depth in the results. Hence, the RDRC approach should be applied for obtaining estimates and indications to be used as basis for a more detailed assessment.

Another feature of the RDRC approach worth considering is its application possibilities. Defence assessment methodologies are usually intended for application on individual plants, and are consequently developed and structured for that purpose. The effect is that the analyst is required to have good knowledge on plant-specific defences and plant-specific system figuration. Such requirements on the analysts understanding makes a method not suited for a more general application, for example application on a generic database, but rather for plant-specific evaluations. The RDRC approach though, is better suited for general applications since it does not have such strict requirements of this kind. For applications on individual plants there are other approaches to defence assessment that is likely to provide more detailed results, but when it comes to general applications the RDRC approach has an advantage.

6.4 Improvements and proposal for further research

Since an integrated impact vector-RDRC approach would still lack qualitative aspects rather than quantitative ones the next question of particular interest will be if, and how, the RDRC methodology can be improved. During this work some major steps have been identified that need to be completed before the ‘potential model’ would be approaching. The recognized deficiencies can be divided into two categories; one that concerns necessary improvements exclusively intended for the RDRC-diagram, presented in item 1-4 in the list below, and one group that concerns more general improvements needed that would have a more indirect impact on the RDRC procedure, presented in item 5-6 below.

1. The RDRC-diagram need to be further validated. This should primarily be done by application on an extended set of data. In this work a trial application was made on Nordic diesel data, but in the same way diagrams need to be designed for more groups of components.
2. The weighting needs to be considered. It is not completely unlikely that this weighting is not optimal, especially different weighting for different groups of components should be considered.
3. The possibility of being able to take credit for made improvements in defences is of great interest and if this feature can be incorporated in the modelling an important step has been taken. This matter should therefore deserve some special attention in a further study.
4. If the RDRC-diagram can not provide fully what is desired, even after required improvements have been made, it needs to be reconsidered. If further developments of this kind of application can not meet the requirements on a ‘potential model’, other

ways need to be explored. The important objective is to direct the development of the methodology in a direction of a 'potential model'.

5. A lot of information is currently provided in the ICDE database. Judgment concerning for example the cause of each event and the extent to which the component(s) was impaired are assessed, but a judgment concerning the failed defence(s) is lacking. Therefore a consideration of extending the set of information provided in the database is suggested. Such an extension would definitely be very useful if applying a RDRC-approach, but also for any other approach for the qualitative analysis.
6. A final subject to be mentioned here is the matter of categorisations in general. The choice of categorisation within this work is for natural reasons based on the ones made within ICDE and UPM. Although, it has shown that it might be questionable whether this is actually the perfect way of classifying these parameters. Other categorisations of defences have been done in other research, for example by Paula and Parry (1990) and Marshall et. al. (1998) and in Johanson et. al. (2003) some doubt concerning the categories of root causes was expressed. It is most likely that these categorisations can be improved and since the made categorisation in fact can have an impact on different types of assessments it should be considered as a critical issue to work on.

6.5 The future possibilities of database use

As of today the ICDE database provides a certain set of information about each event recorded in the database. What seems very interesting though is how this could be modified to in the future constitute an even better tool for CCF analysts. The suggested working process, within this work, is an integrated impact vector and RDRC methodology. The evaluations to be made in this approach consist of construction of partly an impact vector and partly an RDRC-diagram for each event. Under the assumption that agreement is reached concerning methodology to be applied for CCF treatment, the results of such evaluations could actually also be presented in the database. In the case with the integrated approach suggested here it would mean that both an impact vector and an RDRC-diagram would be provided for each event. In a scenario where ideal conditions are assumed, that settlement are made concerning methods to apply and extension of information arrangement is implemented, the database could be used as more extended tool. Such development would render the possibility of easily adding a new level to the assessments, since the first step of the analyses will already be provided and the analyst can more rapidly get into more detailed examinations. Before such modifications can be implemented an important step to take is harmonization of methodologies to apply. This is almost accomplished for the quantitative part of the analysis, but there is still a lot of work to do when it comes to the qualitative part. Since this can be considered as a direction to strive in, the need of harmonization should be highlighted.

6.6 General harmonization problems

In the process of this work some issues has become more evident than other. It was emphasized already in the beginning of this report that the field is thrived with numerous terms and concepts, which has also in the end shown to be one of the biggest challenges to deal with. Beside that fact that judgment is a substantial element in methodologies of CCF treatment, the different methodologies incorporate already themselves various conceptual interpretations. All methodologies are based on some made interpretations of relevant terms, which means that the understanding of these interpretations certainly is of importance. Within this work interpretation has been made of different ways of considering certain aspects, which in a certain sense has resulted in interpretations of interpretations. The most apparent example

of this is found in section 5.2.1 (Harmonization of different approaches). This is of course an issue impossible to solve here, but all the work being done within projects such as NAFCS and EWG is definitely of great importance when it comes to harmonisations about the view of CCF, related methodologies and also the terminology within the area.

7 Conclusions

It has appeared that an actual application of UPM on generic data is not possible, and based on the performed comparative study of the methodologies it can be concluded that UPM can be disqualified as a quantification method. When it comes to qualitative aspects though, UPM has appeared to possess some great advantages. When considering the impact vector approach it has been shown not being able to provide any qualitative aspects and it was concluded that there is no generally useful working procedure adopted that captures the qualitative aspects. Based on these insights a harmonization of certain approaches has been performed for development of a new procedure, namely the RDRC approach. A trial application of the RDRC-diagram has been made, showing that the approach can be used as a defence importance indicator. A first validation of these results has also been performed with sufficiently satisfying results. An integrated impact vector and RDRC methodology is suggested for progress towards a methodology incorporating both qualitative and quantitative aspects.

Further it has been concluded that the structure of the RDRC-diagram presented at this point might not be the most appropriate one though and is most likely to need additional adjustments. Therefore some potential ways for further developments of this approach has also been provided. It is important to note that the intention here is not to present a complete diagram that is the solution to the actual problem, but rather to show that it is actually possible to establish a method for the qualitative part of the analysis that can be applied in parallel to the quantitative one. The use of an established method for the qualitative analysis would hopefully in the long run provide a better knowledge of the system and the defences needed for protection against CCF. The use of an RDRC approach could be one possible way of dealing with this.

8 References

Apostolakis, G., (1986). “On the use of judgment in probabilistic risk analysis.” Nuclear Engineering and Design, Vol.93, Issue 2-3, 161-166.

Bourne, A.J., Edwards, G.T., Hunns, D.M., Poulter, D.R., Watson, I.A., (1981). Defences against common-mode failures in redundancy systems: A guide for management, designers and operators. UKAEA, SRD R 196.

Brand, V.P., (1996). UPM 3.1: A pragmatic approach to dependent failures assessment for standard systems. AEA Technology plc (Warrington), SRDA-R13.

Fleming K.N., Mosleh, A., Worledge, H., (1987). “Development of a systematic approach for the analysis of system level dependent failures.” PSA ‘87, Proceedings of International topical conference on probabilistic safety assessment and risk management, Vol. 1, Verlag TÜV Rheinland (Köln), ISBN 3-88585-417-1.

Hellström, P., Johanson, G., Bento, J-P., (2004). ”Dependency Defence – How to protect against dependent failures.” PSAM 7 – ESREL ’04, Proceedings of International conference on Probabilistic Safety Assessment and Risk Management (Berlin).

IAEA, (1992). Procedures for conducting common cause failure analysis in probabilistic safety assessment (Vienna), TECDOC 648.

Johanson et.al, (2003a). Dependency Defence and Dependency Analysis Guidance. SKI, Report 2004:4, Volyme 1.

Johanson et.al, (2003b). Dependency Defence and Dependency Analysis Guidance. SKI, Report 2004:4, Volyme 2.

Johanson, G., Hellström, P., Knochenhauer, M., (2006). Skydd mot beroenden och beroendefel, Bli kvitt beroendet. NPSAG, educational material. English summary published in: PSAM 8, Proceedings of the Eight International Conference on Probabilistic Safety Assessment and Risk Management (New Orleans), 0364.

Kreuser, A., Peschke, J., (2003). Kopplungsmodell, Modell zur Berechnung fon GVA-Wahrscheinlichkeiten. Gesellschaft für Anlagen- und Reaktorsicherheit mbH (Köln), GVA-Seminar.

Marshall, F.M., Mosleh, A., Rasmuson, D.M., (1998). Common-Cause Failure Database and Analysis System: Data collection and Event Coding. U.S. Nuclear Regulatory Commission, NUREG/CR-6268, Vol. 3.

Mosleh, A., Parry, G.W., Zikria, A.F., (1994). “An approach to the analysis of common cause failure data for plant-specific application.” Nuclear Engineering and Design, Vol.150, Issue 1, 25-47.

Mosleh, A., Rasmuson, D.M., Marshall, F.M., (1998). Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment. U.S. Nuclear Regulatory Commission, NUREG/CR-5485.

Mosleh, A., Siu, O., (1987). "On the use of uncertain data in common cause failure analysis." PSA '87, Proceedings of International topical conference on probabilistic safety assessment and risk management, Vol. 1, Verlag TÜV Rheinland (Köln), ISBN 3-88585-417-1.

OECD/NEA, (2002). The Use and Development of Probabilistic Safety Assessment in NEA Member Countries. OECD/NEA report NEA/CSNI/R(2002)18.

OECD/NEA, (2004). International Common-cause Failure Data Exchange, ICDE General Coding Guidelines. Technical Note NEA/CSNI/R(2004)4.

Parry, G.W., (1991). "Common Cause Failure Analysis: A Critique and Some Suggestions." Reliability Engineering and System Safety, Vol.34, Issue 3, 309-326.

Paula, M., Parry, W,(1990). A cause-defense approach to the understanding and analysis of common cause failures. U.S. Nuclear Regulatory Commission, NUREG/CR-5460.

Rasmuson, D.M., (1991). "Some Practical Considerations in Treating Dependencies in PRAs." Reliability Engineering and System Safety, Vol. 34, Issue, 327-343.

Vaurio, J.K., (2002). "Extensions of the uncertainty quantification of common cause failure rates." Reliability Engineering and System Safety, Vol. 78, Issue 1, 63-69.

VGB/NPSAG, (2006). "European Working Group for assessment of CCF". Project program, PM.

Wierman, T.E, Rasmuson, D.M., Marshall, R.M., (2000).ICDE Project Report on Collection and Analysis of Common-Cause Failures of Emergency Diesel Generators. OECD/NEA report NEA/CSNI/R(2000)20.

Zitrou A., (2006). Exploring a bayesian approach for structural modelling of common cause failures. University of Strathclyde, Department of management science.

9 Appendices

Appendix A: Survey of CCF methodologies

This survey is to be considered as an extension of the main report and Chapter 4 in particular, to provide a more detailed background on the considered CCF methods. The CCF methods considered here are parametric methods, in section A-1, and the Unified Partial Method (UPM), in section A-2.

A-1 Parametric methods

In the sections below the most common parametric methods will be presented. These are methods used for applications of the impact vector approach.

For quantification of probabilities for multiple failures with Common Cause Component Group (CCCG) there are different concepts. Some of the models use the concept of Common Cause Basic Events (CCBEs) and corresponding probabilities,

Q(m|n) = P{specific m components fail due to CCF, other n-m not affected in a CCCG of size n},

while others use probabilities for multiple failures with CCCG with Subgroup Failure Probability (SGFP) entitites. One of these SGFP entities, close to the CCBE probability is

Peg(m|n) = P{Specific m components fail while other n-m not affected in a CCCG of size n}.

The difference between these two entities is that Peg(m|n) covers any multiple failure of order m, also due to combination of different causes, while Q(m|n) is restricted to actual CCFs of order m, exactly, and due to a clear shared cause. In practice the two entities are numerically close, i.e

$Q(m|n) \approx Peg(m|n)$.

Usually CCCGs are assumed internally homogeneous, which means also internal symmetry[11]. This means that the probability of a CCBE is not dependent of the specific combination of components, only the multiplicity affects and the same Q(m|n) or Peg(m|n) applies to all CCBEs of order m, although the size of CCCG is significant. When instead considering another SGFP entity,

Psg(m|n) = P{specific m components fail in a CCCG of size n},

this no longer have the same impact since Psg(m|n) is subgroup invariant[12], i.e. if considering two mutually homogenous CCCGs of different size $Psg(m|n_A) = Psg(m|n_B)$ applies when assuming internal homogeneity. This makes this entity very practical for data comparisons. The Psg entity can be obtained from the following transformation:

$$Psg(k|n) = \sum_{m=k}^{n} \binom{n-k}{m-k} Peg(m|n).$$

(Johanson et.al., 2003b)

[11] Homogeneity of a CCCG means that the probability entities in the subgroups of any given size are mutually identical, i.e. homogeneity means also symmetry.

[12] Subgroup invariance denotes that the probability entity or parameter is the same in a subgroup and in the whole CCCG. Hence, a subgroup invariant probability entity or parameter is the same in mutually homogeneous CCCGs of different size.

These concepts (CCBEs and SGFP entities) are both used in different models for definition and presentation of results. Thus, they can be considered as constituting a basis for all the methods and understanding of them is necessary for use or evaluation of the methods. For comparability within in this report though the SGFP entities will not be used in the presentation of some methods below, even if the mathematical expressions are in some cases made less complex if these entities are introduced.

A-1.1 Direct estimation method

The Direct estimation method is also referred to as the Basic Parameter (BP) model. This model is one of the most straightforward models. The model parameters are defined in terms of basic events and are directly estimated from the data and is expressed as the already defined Q(m|n). The total failure probability, QT, of a component in a CCCG of 'n' components is:

$$Q_T = \sum_{m=1}^{n} \binom{n-1}{m-1} Q(m|n).$$

(Fleming et. al., 1986)

A-1.2 Alpha Factor (AF) method

The method is sometimes referred to as a 'ratio' model since the alpha parameters are defined in terms of conditional probabilities or ratios of failure rates. (Vaurio, 1994) Alpha Factor Method is basically defined by using CCBE probabilities:

$$\alpha(m|n) = \frac{\binom{n}{m} Q(m|n)}{\sum_{k=1}^{n} \binom{n}{k} Q(k|n)} .$$

The interpretation of this method is that for a redundant system of 'm' identical components the k-th alpha factor is the probability that a CCF event fails exactly 'k' components, given that a failure event occurs. The alpha factors are not subgroup invariant. (Mosleh et. al., 1998)

A-1.3 Beta factor (BF) method

The beta factor method is a single parameter method, i.e. it uses one parameter in addition to the total component failure probability to calculate the common cause failure probabilities. The method assumes that a constant fraction, β, of the component failure probability is associated with CCFs where the β-factor is a conditional probability, i.e. that β is defined as the conditional probability that a specific component fails dependently, given that it fails. (Fleming et. al., 1981)

Since the BF parameters describe the failure behaviour of a specific component the method is said to be component-oriented. The BF method was first developed only for application on two redundant components but has been extended to CCCG sizes above two and is then described by the following:

$$Q(1|n) = (1-\beta)\, Q_T$$
$$Q(m|n) = 0 \quad \text{for } 1 < m < n \ ,$$
$$Q(n|n) = \beta\ Q_T$$

where Q_T represent the total failure probability of one component, i.e. $Q_T = Q(1|n)+Q(n|n)$. (Mosleh et. al., 1998)

A-1.4 Multiple Greek Letter (MGL) Method

The MGL method is an extension of the BF method, developed in an attempt to take into account CCF events of different multiplicities, which occur to systems comprised by more than two components. Mathematically, the method is equivalent to the BF method. The main difference is that a different set of parameters are used and the requirements are thereby different. The set of parameters included in the MGL method consist of total component level failure rates that include the effects of all independent and common cause contributions to that component failure. Also a set of failure rate fractions are included that are used to quantify the conditional probabilities of all the possible ways the component failure can be shared with other components within its CCCG, given that failure has occurred. The parameters describe the failure behaviour of a specific component in relation to the rest of the components in the considered CCCG and are defined in terms of conditional probabilities. (Fleming et. al., 1986) The parameters are:

β = conditional probability that the cause of a component failure will be shared by one or more additional components, given that a specific component has failed.

γ = conditional probability that the cause of a component failure that is shared by one or more components will be shared by two or some additional components, given that two specific components have failed.

δ = conditional probability that the cause of a component failure that is shared by two or more components will be shared by three or more additional components given that three specific components have failed.

The CCBE probabilities in terms of MGL parameters are obtained though the following generalized expression:

$$Q(m|n) = \frac{1}{\binom{n-1}{m-1}} \cdot \prod_{k=1}^{m} g(k|n) \cdot (1 - g(m+1|n)) \cdot Q_T$$

,

where

$g(1|n) = 1$

$g(n+1|n) = 0$

For other g(n|n) one parameter for each order of multiplicity, i.e. up to the size of the considered component group, is to be introduced:

$g(2|n) = \beta^{(n)}$

$g(3|n) = \gamma^{(n)}$

$g(4|n) = \delta^{(n)}$

…

If for instance the considered group is of size 2 the following will apply:

$g(1|n) = 1$

$g(2|n) = \beta^{(n)}$

$g(3|n) = g(n+1|n) = 0.$

(Mosleh et. al., 1998)

A-1.5 Common Load Model (CLM)

The Common Load Model (CLM) was developed for treatment of high redundant cases, and is the recommended method for such applications. (Johanson et. al., 2006) In the model the failure condition is expressed by a stress-resistance analogy. The components in a considered group are loaded with a common stress and their failure is described by their resistances to

this stress. Both the common stress and the component resistances are assumed as stochastic distributed variables. The occurrence of multiple failures is then to take place when the common load exceeds the resistances of the components. The model has been extended to also include a base load part for failure probability and dependence at low order and an extreme load part for corresponding high order. Parameters used are:

p_tot : Total single failure probability,

p_xtr : Extreme load part as contribution to the single failure probability,

c_co : Correlation coefficient of the base load part,

c_cx : Correlation coefficient of the extreme load part.

It is not possible to present simple point estimation expressions for these parameters, except for p_tot. Another illustration of the model is provided by the failure conditions that corresponds to

$$Psg(m|n) = \int_{x=-\infty}^{+\infty} dx(f_S(x)[F_R(x)]^m),$$

where,

$f_s(x)$ = Probability density function of the common stress.

$F_R(x)$ = Cumulative probability distribution of the component resistances.

This is also illustrated in Figure A-1, illustrating that at a demand the components are loaded with a common stress, S, and their failure is described by component resistances, R_i.

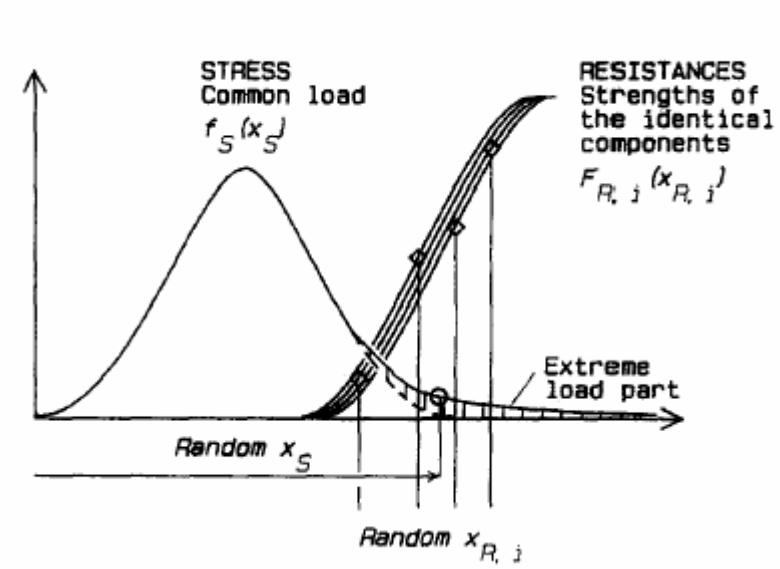

Figure A-1. Illustration of the concept of CLM.
(Mankamo, Kosonen, 1992)

A-2 UPM

A-2.1 An introduction to the method

Unfortunately there is not much literature to be found dealing with UPM, although, it is the current approach towards modelling of CCF in the UK. Due to this shortage of literature a significant part of the study of UPM as a method will be based on a UPM-manual (Brand, 1996) that is one of very few publications of the structure of the methodology. This is a manual not exclusive for a specific industry, but it is developed for assessments within civil

nuclear industry and is not suited for systems, or plants, not comparable with those in this industry unless re-calibrated for other conditions (Brand, 1996).

UPM was developed on expert judgment basis – not actual experience data. This applies also for further developments, or extensions, of the method. An example of this is found in Zitrou (2006).

UPM is a predictive reliability analysis tool for obtaining an estimation of a factor, for the vulnerability of the system to dependent failures, which is to be used as a complement to the independent failure analysis result[13]. The foundation of the method is *defences* against dependent failure and this is also what forms the structure of the method. Another important gist of the method is judgment. The estimation of the dependent failure factor is made essentially based on the analyst's judgment of the involved defences against dependent failure. These judgments are made transparent by being recorded throughout the analysis. A characteristic feature of the method is subsequently the ability of making use, with an explicit acceptance, of the judgment element.

Brand (1996, p.3) describes UPM as being, not a complete method for dependent failure assessment, but a useful methodology mainly for 'standard systems'[14]. This can be understood as one limitation of the method, but Brand also defines the following three other limitations.

- -Human factors: The method excludes specific assessment of dependencies between human actions, even if it intends to consider human factor in dependency between hardware items.
- -Functional dependencies: Functioning of some common service system or component, on which the operability of redundant hardware trains is dependent, is considered to be modelled without specific dependent failure methods such as UPM.
- -Software: Systems where software is incorporated are not included in the extent of UPM.

A-2.2 Reliability Cut-Off Method and the Partial Beta Factor Method

Two common techniques applied for dependent failure assessment are the Reliability Cut-Off method and the Partial Beta Factor (PBF) method. The Reliability Cut-Off method is usually applied in system level assessment, while the PBF method usually is applied to component level assessments. (Brand, 1996)

Like the Beta Factor method the PBF method has been developed for component level application. It defines the beta (β) factor in the same way as the BF method, i.e. as the conditional probability that a specific component fails dependently, given that it fails. Furthermore it assumes that the β-factor is decomposed into a number of partial β-factors, representing contributions from different features of the system (sub-factors) according to

$$\beta = \sum_j \beta_j \ .$$

The analyst is required to make judgments, based on a set of criteria, to assign a level to each sub-factor. The levels are related to scores, which are then used to obtain the overall β-factor. The scores are determined so that overall β-factor is constrained to stay within the limits of generally accepted values and to agree with observations. (Brand and Matthews, 1993)

[13] Independent failure analysis is assumed to be obtained directly by standard fault tree analysis. Methods and analysis for independent failure are not included in the scope of this thesis.

[14] Standard systems meaning safety systems consisting of 2, 3 or 4 redundant trains which possibly include some diversity assuming the equipment, technology and environments involved are mostly well understood even if the configuration or context is novel.

The Reliability Cut-Off method is a system level approach and does not consider partial groups of components that are subjects to CCFs. It is used to assess the reliability of the target system and it directly yields an estimate of the overall system failure probability on demands, including both dependent and independent ones. This is done with the assumption that the results are dominated by dependent failures. Like the PBF model it requires the analyst to make judgments concerning a number of features of the system. An assumption is made that a systems' unreliability, caused by CCF, is limited by certain baseline values that are determined by the design of the system. These baseline values are set, according the redundancy/diversity structures, which are to reflect the accepted values for certain basic system types. For the simplest systems lacking presence of all 'good' characteristics the baseline value is set to 10^{-3} failure per demand. For systems incorporating all the good characteristics while avoiding all the bad ones, an improvement of the probability can be achieved resulting in a value of 10^{-5}. It should be noted though that these baseline values apply to whole systems and not to each set of redundant components within systems. (Brand and Matthews, 1993) 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. (Zitrou, 2006)

Both the PBF method and the cut-off method are based on the principle of decomposition of an overall assessment into judgments relating to different features of the system and determination of the respective factor by an additive scheme. The difference is that while the cut-off method is a holistic approach the PBF method is component oriented, and subsequently the definitions of the factors are different and they need to be calibrated differently. The set of features of the system to be assessed and the related criteria are the same though. This subject will be further explored in section A-2.4.

A-2.3 UPM application guide

Brand's (1996) workbook gives a step by step user guide for application of UPM. Figure A-2 illustrates this guide. A summary of the workbook is given in the following subsections, which is intended to provide a brief introduction to the methodology.

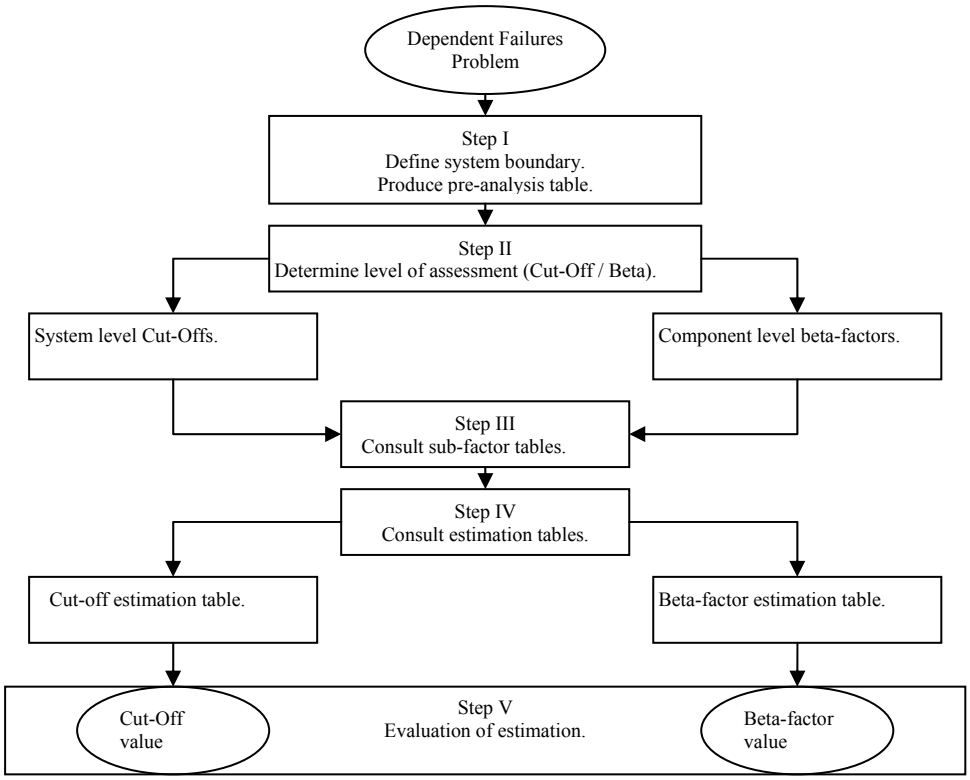

Figure A-2. Illustration of UPM application guide.

A-2.3.1 Step I

The analyst is to define the physical boundary of the system in interest. This includes for example decision of whether service systems should be included or not. (Worth noting is that design boundary definitions might not be appropriate in this matter.) In this first stage a pre-analysis table is to be produced. The pre-analysis table is to be used for assessing the work that is to be done but also to provide a quality rating on the assessment.

A-2.3.2 Step II

A choice is to be made between Cut-Off and β-factor method, i.e. assessment on system or component level.

A-2.3.3 Step III

A review of the Sub-Factor tables is to be done. Each aspect, or sub-factor, of system design, operation or environment is presented represented by a table. The sub-factors, D_i, to be considered are: Redundancy (and Diversity), Separation, Understanding, Analysis, M.M.I (Man Machine Interface), Safety Culture, Environmental Control and Environmental Testing. These will all be given in further detail in section A-2.4. The sub-factor tables should be completed, by the analyst, with each sub-factor's effectiveness in defending against dependent failures. This is to be done by choosing the system description, out of five alternatives, that best matches the system to be assessed for each sub-factor. The five alternative system descriptions are different for the eight sub-factors, each adapted to the considered sub-factor. In this way a judgment table is created where each sub-factor is categorized concerning its judgment. The judgments categories are A, B, C, D and E, where A is the worst defence and E the best defence against dependent failures, x_i ($x_i \in \{1,...,5\}$).

A-2.4 Sub-factors

In this section the sub-factors, as defined Brand (1996), will be outlined together with the judgment criteria for each sub-factor.

A-2.4.1 Redundancy (and diversity)

How vulnerable a system is to dependent failure depends on how many parallel trains there is, and to which extent they are alike. These factors should be considered for the system under assessment and the appropriate category, A-E, is to be chosen from Table A-1. The notation used is 1 out of 2 (1oo2), 2 out of 4 (2oo4) etc.

A	Minimum identical redundancy (e.g. 1oo2, 2oo3, 3oo4 for success).
A+	Enhanced identical redundancy (e.g. 1oo3, 2oo4 for success).
B	Robust identical redundancy (e.g. 1oo4, 1oo5, 2oo5 etc.).
B+	Unusually high identical redundancy (1oo≥8).
C	Enhanced identical redundancy (e.g. 1oo3) with functional diversity OR Robust identical redundancy (e.g. 1oo≥4) with operational diversity. OR Unusually high identical redundancy (1oo≥8) in a passive system.
D	Robust identical redundancy (1oo≥4) with functional diversity.
E	Two entirely diverse independent redundant sub-systems.

Table A-1. Redundancy (and diversity) criteria.

A-2.4.2 Separation

Physical separation and segregation by barriers influences the degree to which redundant parallel trains of a system can be affected by environmental events. These factors should be considered for the system under assessment and the appropriate category, A-E, is to be chosen from Table A-2, based the different separation levels illustrated in Figure A-3.

A	Redundant items, separation less than level 1 (se fig A-2).
B	Redundant items, separation level 1 (se fig A-2).
C	Redundant items, separation level 2 (se fig A-2).
D	Redundant items, separation level 3 (se fig A-2).
E	Redundant items, separation greater than level 3 (se fig A-2).

Table A-2. Separation criteria.

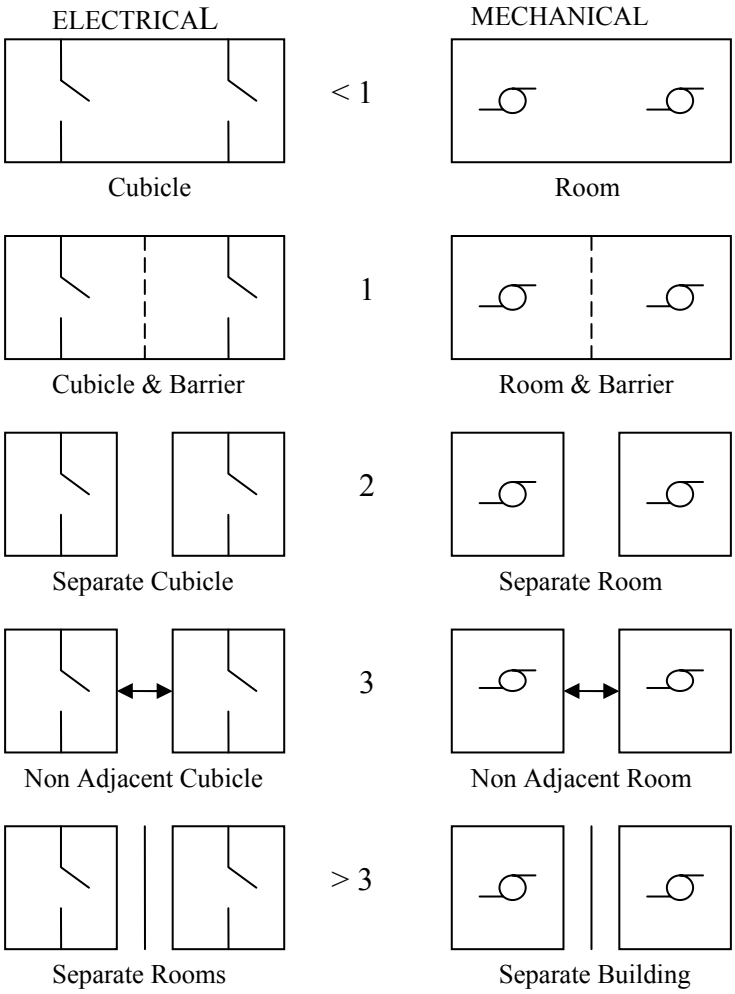

Figure A-3. Separation levels for electrical and mechanical systems

A-2.4.3 Understanding

Under the category of understanding there are four aspects to be considered: experience, novelty, complexity and misfit (where misfit is intended to be a measure of the 'gap' in understanding which can exist where equipment has not been designed to fit the application, but rather has been selected 'off the shelf'). These factors should be considered for the system under assessment and the appropriate category, A-E, is to be chosen from Table A-3, based on a two-stage assessment: First (1), the experience is to be evaluated. If an extensive experience can be demonstrated, where a threshold of > 10 years of operational experience of the particular system is suggested, Table A-3 should be used. Table A-3 can also be applied if experience with other systems can be demonstrated, if these systems are sufficiently similar in terms of equipment, design and operational characteristics. Otherwise the option is reduced to Table A-4. Secondly (2), the existence of novelty, complexity and misfit is to be assessed. Optional categories for these three factors are Small (or Average) or Big (or greater than average). Based on this analysis an appropriate category is to be chosen from those described in Table A-3 and Table A-4.

Extensive experience (> 10 years)	
A	Software in system
B	All 3 Big
C	2 Big, 1 Small
D	1 Big, 2 Small
E	All 3 Small

Table. A-3. Understanding criteria for extensive experience.

Limited experience (< 10 years)	
A	Software is present in system OR All 3 Big
B	2 Big, 1 Small
C	1 Big, 2 Small
D	All 3 Small
E	Not permitted for limited experience

Table A-4. Understanding criteria for limited experience.

A-2.4.4 Analysis

For safety assessments an independent check of the design of the system in consideration can be obtained by the use of fault analysis. For example, the detection of failures and the adequacy of testing can be evaluated in this way. Results of such analyses must be fed back into the design, or operation, for them to have an effect. It can also be a question of an assessment on a future design, and then the designers' knowledge about the dependent failure issue is a very important factor. The two factors to consider under this category of defence are (1) how much analysis has been done on the design/system and (2) to what extent the designers are aware of the dependent failures issue. The criteria to choose between are the ones provide in Table A-5.

A	No formal safety assessment. No design knowledge of dependent failure issues.
B	High level study (perhaps Failure Mode and Effect Analysis, FMEA) or designer has general knowledge of dependent failure issues (demonstrated in the design).
C	Previous reliability assessment and evidence of feedback or designer has specific guidelines and knowledge of dependent failure issues (demonstrated in the design).
D	As C 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 (demonstrated in the design).

Table A-5. Analysis criteria.

A-2.4.5 Man Machine Interface (MMI)

The probability of human error does not only depend on the detailed understanding of the procedures but also on the number and complexity of operator and maintenance action. In this category the operator actions and maintenance actions are to be considered. Considering the factor of operator actions judgments are required regarding the presence of written procedures and how much human interaction there is in the operation of the item to be assessed. The

suggested levels of this category are provided in Table A-6. The maintenance actions factor is to be judged concerning the presence of certain elements with influence on the effectiveness of the factor. The suggested levels and corresponding requirements, which are based on the Accident Sequence Evaluation Programme (ASEP) technique, are provided in Table A-6. The overall MMI category is then assumed to be the more pessimistic of these two factors, according the criteria in Table A-7.

Operator Actions	
Level 1	Written procedures and normal interaction. OR No procedures and minimal interaction.
Level 2	Checklist and normal interaction. OR Written procedures and minimal interactions.
Level 3	Checklist with evidence of use and normal interaction. OR Checklist and minimal interaction.
Maintenance Actions	
Level 1	Supervisor check. (The check may be by another person at the site of maintenance or by the same operator, post maintenance, remote from the site maintenance.)
Level 2	Post-maintenance proof test.
Level 3	Test and check.
> 3	Error Alarmed.

Table A-6. Suggested levels of operator and maintenance interaction.

A	Procedures and human interaction poorer than level 1.
B	Procedures and human interaction level 1.
C	Procedures and human interaction level 2.
D	Procedures and human interaction level 3.
E	Procedures and human interaction better than level 3.

Table A-7. MMI criteria.

A-2.4.6 Safety culture

The probability of human error is affected by the training of the staff, particular for in situations with emergency operations. This matter is related to both the level of training and the level of experience by the operator or the person managing the operation of the system. Another issue to consider is the presence of an active safety culture and dedication by the staff. It should be emphasized that a distinction is made here between the general culture in which operators and plant managers are working, and the nature of the support given for performing specific tasks. The latter is covered in the category of MMI, while the general safety culture is to be judged under this category. A combination of the considerations of training and experience is to be made according the criteria in Table A-8.

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.

Table A-8. Safety culture criteria.

A-2.4.7 Environmental control

Under this category the control exercised on the environment around the system under assessment is to be considered. This includes judgments on the presence of other processes, not related to the system, and how the access by personnel is limited. The different criteria to consider are provided in Table A-9. It should be noted also that the highest category can only be achieved if everything and everyone is controlled, i.e. even factors like cleaners, drains, cables and air supplies unless the site is isolated.

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 authorized personnel only – all activities related (e.g. laboratory).
D	Limited access area, trained personnel only, except under close supervision. All equipment and services are subject to design control (e.g. remote sub-station).
E	As D but a smaller scale with closely related activities (e.g. flight deck of aircraft, power station control room).

Table A-9. Environmental control criteria.

A-2.4.8 Environmental testing

The design of the system is made for it to withstand a number of environmental effects such as shock, vibration, temperature, humidity, etc. In practice, testing of such parameters can reveal some susceptibilities of dependent failure. It is therefore required to evaluate the variety, type and range of such environmental testing at manufacturing, construction, installation and commissioning stages. The optional categories are provided in Table A-10.

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 it is required to, i.e. shock, vibrations, 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 it will withstand all excess fault conditions that it is required to.
E	Example unit run in parallel with the existing unit for a period (e.g. 1 year) before it is brought on line.

Table A-10. Environmental testing criteria.

A-2.5 Feature Factors

When treating systems incorporating diversity or in system level assessment the option of using Feature Factors in the judgment is provided. By using feature factor it is possible to consider individual element in a train of equipment[15], resulting in an overall judgment.

A-2.6 The final steps

In this stage the judgments at hand are brought together and a Cut-Off or Beta sub-factor, based on these judgments, is achieved by consulting either the provided Cut-Off or β-Factor estimation table, depending on the choice made in step II (see subsection 5.1.2). A sub-factor value, s_i, is selected from these estimation tables, illustrated in Table A-11 and A-12, for each of the eight sub-factors and their judged level of defence, x_i. Each sub-factor value is then given by $s_k(x_k)$.

	A	A+	B	B+	C	D	E
Design:							
Redundancy (& Diversity), see subsection 2.4.1	60000	30000	6000	3000	600	60	6
Separation, see subsection 2.4.2	80000		8000		800	80	8
Understanding, see subsection 2.4.3	60000		6000		600	60	6
Analysis, see subsection 2.4.4	60000		6000		600	60	6
Operation:							
MMI, see subsection 2.4.5	100000		10000		1000	100	10
Safety Culture, see subsection 2.4.6	50000		5000		500	50	5
Environment:							
Control, see subsection 2.4.7	60000		6000		600	60	6
Tests, see subsection 2.4.8	40000		4000		400	40	4

Table A-11. Partial Cut-Off estimation table.

[15] This might be useful if for example the analyst find that separation is good in some parts of the system, but poor in others.

	A	A+	B	B+	C	D	E
Design							
Redundancy (& Diversity)	1750	875	425	213	100	25	6
Separation	2400		580		140	35	8
Understanding	1750		425		100	25	6
Analysis	1750		425		100	25	6
Operation							
M.M.I.	3000		720		175	40	10
Safety Culture	1500		360		90	20	5
Environment							
Control	1750		425		100	25	6
Tests	1200		290		70	15	4

Table A-12. Partial β factor estimation table.

In the final step the overall estimation of the system Cut-Off-factor ($\hat{Q}$) or Beta factor ($\hat{\beta}$) is obtained by summarizing the numerical value of the sub-factors and dividing this by a denominator that is a scaling constant depending on choice between cut-off or PBF method:

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

Hence, the procedures for system and component level assessment are identical. The only structural difference concerning Cut-Off and Beta Factor are the assigned sub-factor values and scaling factors.

A-3 References

Brand, V.P., (1996). UPM 3.1: A pragmatic approach to dependent failures assessment for standard systems. AEA Technology plc (Warrington), SRDA-R13.

Brand, V. P., Matthews, R. H., (1993). ”Dependent failures-’when it all goes wrong at once’.” Nuclear Energy, Vol. 32, no. 3, 155-63. (Also included in Brand (1996), Appendix A1.)

Fleming, K.N., Mosleh, A., Deremer, (1986). ”A systematic procedure for the incorporation of common cause events into risk and reliability models.” Nuclear Engineering and Design, Vol. 93, Issue 2-3, 245-273.

Fleming, K.N., Houghton, W.J., Hannaman, G.W., Joksimovic. V., (1981). “Probabilistic risk assessment of HTGRs.” Reliability Engineering, Vol. 2, Issue 1, 17-25.

Johanson et.al, (2003b). Dependency Defence and Dependency Analysis Guidance. SKI, Report 2004:4, Volyme 2.

Johanson, G., Hellström, P., Knochenhauer, M., (2006). Skydd mot beroenden och beroendefel, Bli kvitt beroendet. NPSAG, educational material. English summary published in: PSAM 8, Proceedings of the Eight International Conference on Probabilistic Safety Assessment and Risk Management (New Orleans), 0364.

Mankamo, T., Kosonen, M., (1992). “Dependent failure modelling in highly redundant structure – Application to BWR safety valves.” Reliability Engineering and System Safety, Vol. 35, Issue 3, 235-244.

Mosleh, A., Rasmuson, D.M., Marshall, F.M., (1998). Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment. U.S. Nuclear Regulatory Commission, NUREG/CR-5485.

Vaurio, J.K., (1994). "The theory and quantification of common cause shock events for redundant standby systems." Reliability Engineering and System Safety, Vol. 43, Issue 3, 289-305.

Zitrou A., (2006). Exploring a bayesian approach for structural modelling of common cause failures. University of Strathclyde, Department of management science.

Appendix B: Description of relations in the RDRC-diagram

In the main report the 'Relations of Defences, Root causes and Coupling factors' (RDRC) diagram was illustrated. In the section below the indicated relationships between defences, root causes and coupling factors are described in more detail.

B-1 Relationships between defences, root causes and coupling factors

Descriptions of the relationships in the RDRC-diagram are provided in Table B-1 below.

Relations between defences and root causes		
Defence	*Root cause*	*Relation description*
Environmental Testing	Design	During the environmental testing process, issues that could lead to failures related to design aspects 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. (Zitrou, 2006)
Analysis	Design	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. (Zitrou, 2006)
Redundancy / Diversity	Design	Diversity is a design characteristic of the system (redundant group) and influences the occurrence of (total) design failures. (Zitrou, 2006)
Separation	Design	Separation is a design characteristic of the system (redundant group) and its use or absence may lead to design failures. (Zitrou, 2006)
Understanding	Design	Existing experience of design features, i.e. a good level of understanding of the systems design, can provide knowledge on how to protect against design, manufacture or construction inadequacy. (Experience compensating for systems design complexity.)
Environmental Control	Human	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. (Zitrou, 2006)
Safety Culture	Human	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. (Zitrou, 2006)
Operator Interaction	Human	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, Operator Interaction does influence the Human root cause. (Zitrou, 2006)
Understanding	Human	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. (Zitrou, 2006)
Environmental Testing	Internal to Component	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. (Zitrou, 2006)
Analysis	Internal to Component	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 Analysis on the Design root cause), however, a proportion of these failures are related to internal failures. (Zitrou, 2006)
Understanding	Internal to Component	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. (Zitrou, 2006)
Redundancy / Diversity	Internal to Component	Failure due to internal to component root cause can possible be avoided by having redundant/diversified component(s).
Separation	Internal to Component	Improved Separation can in some cases reduce the likelihood of events due to the internal to component root cause. Bad fluid chemistry is one example of mechanism whose impact can be prevented or limited by separation.
Safety Culture	Maintenance	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. (Zitrou, 2006)
Redundancy / Diversity	Maintenance	Failure due to maintenance root cause can in some cases be avoided by having diversified staff.
Operator interaction	Maintenance	The level/nature of support given to operators and plant managers influence their capability of performing specific maintenance tasks. If they are provided with good support they are more likely to perform their maintenance work adequate. Operator interaction as an UPM defence addresses issues concerning operator and maintenance action. An important feature of operator interaction defence, in defence against dependency, is its possibilities to influence the likelihood that a maintenance error may be made in a second redundant item, or a third, fourth etc.
Operator Interaction	Procedures	The Operator Interaction defence 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. (Zitrou, 2006)
Analysis	Procedures	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. (Zitrou, 2006)
Understanding	Procedures	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 that exists, the more likely the procedures are to be honed. (Zitrou, 2006)
Safety culture	Procedures	If considering the level of feedback and in view of procedures review the safety culture can perhaps have a considerable impact.
Environmental Control	Abnormal environmental stress	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. (Zitrou, 2006)
Analysis	Abnormal environmental stress	The higher the level of analysis, the more prepared the system is to sustain environmental shocks. (Zitrou, 2006)
Separation	Abnormal environmental stress	Separation is a defence with possibilities to reduce the likelihood of events due to the abnormal environmental stress root cause. Fire and floods are two examples of mechanisms whose impact can be prevented or limited by separation.
Redundancy / Diversity	State of other component	Redundancy/Diversity of component(s) can reduce the likelihood of failure of other component that relies on it (reduce the probability of failure since a redundant component can take its place).
Separation	State of other component	Failure of a component caused by the state of another component can be avoided by assuring these components being sufficiently separated by distance or by physical barriers, i.e. a good level of Separation is applied.
Relations between defences and coupling factor groups		
Defence	*Coupling factor group*	*Relation description*
Analysis	Environmental	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. (Zitrou, 2006)
Separation	Environmental	In principle, separation is a defence targeted against removing the common environmental characteristics from the system, which propagate a failure mechanism amongst several components. (Zitrou, 2006)
Analysis	Hardware	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. (Zitrou, 2006)
Redundancy / Diversity	Hardware	Functional diversity is oriented towards reducing the effect of coupling (due to hardware similarities) amongst failures. (Zitrou, 2006)
Understanding	Hardware	Understanding/Experience of how to design system configuration (perhaps to avoid misfit) can prevent CCF events from occurring. For example, better physical appearance (equipment identification, colour, coding etc.) can improve the identifying equipment and thereby prevent a CCF event.
Operator Interaction	Operational	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. Moreover, well-written procedures would cater for procedural mistakes being propagated amongst several components. (Zitrou, 2006)
Redundancy / Diversity	Operational	Staff diversity can be a useful measure to defend against failures being coupled by having the same staff for installation, testing or maintaining redundant component.

Table B-1. Description of relations in the RDRC-diagram.

B-2 References

Zitrou A., (2006). Exploring a bayesian approach for structural modelling of common cause failures. University of Strathclyde, Department of management science.

Appendix C: Terminology

In the main report, Chapter 2, some concepts of certain significance were brought up. Of these, the different categories of defences were further explained in Appendix A. This appendix is devoted to the different categories of root causes and coupling factors listed in the main report.

C-1 Definitions of categories of root causes and coupling factors

A *root cause* is the most basic reason for the component's failure, representing the common cause. The suggested coding within ICDE (OECD/NEA, 2004) is:

- State of other component(s), if not modelled in PSA: The cause of the state of the component under consideration is due to the state of another component. Examples are loss of power and loss of cooling.
- Design, manufacture or construction inadequacy: 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.
- Abnormal environmental stress: Represents causes related to a harsh environment that is not within component design specifications. Specific mechanisms include chemical reactions, electromagnetic interference, fire/smoke, impact loads, moisture (sprays, floods, etc.) radiation, abnormally high or low temperature, vibration load, and severe natural events.
- Human actions: Represents causes related to errors of omission or commission on the part of plant staff or contractor staff. An example is a 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, piece part: 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 of the component. Specific mechanisms include erosion/corrosion, internal contamination, fatigue, and wear out/end of life.
- Procedure inadequacy: 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: All maintenance not captured by Human actions or Procedure inadequacy.
- Other: The cause of events is known, but does not fit in one of the other categories in the classification scheme.
- Unknown: This cause category is used when the cause of the component state cannot be identified.

A *coupling factor* describes the mechanism that ties multiple impairments together and identifies the influences that created the conditions for multiple components to be affected. This means that a coupling factor is a property of a group of components or piece parts that identifies them as being susceptible to the same mechanisms of failure. Within ICDE (OECD/NEA, 2004) the following coding is suggested:

- Hardware design: Components share the same design and internal parts
- System design: The CCF event is the result of design features within the system in which the components are located.
- Hardware quality deficiency: Components share hardware quality deficiencies from the manufacturing process. Components share installation or construction features, from initial installation, construction, or subsequent modifications.
- Hardware (component, system configuration, manufacturing quality, installation configuration quality): Coded if none of or more than one of Hardware design, System design or Hardware quality deficiency applies, or if there is not enough information to identify the specific 'hardware' coupling factor.
- Maintenance/test (M/T) schedule (OMS): Components share maintenance and test schedules. For example, the component failed because maintenance was delayed until failure.
- M/T procedure (OMP): Components are affected by the same inadequate maintenance or test procedure. For example, the component failed because the maintenance procedure was incorrect or a calibration set point was incorrectly specified.
- M/T staff (OMF): Components are affected by a maintenance staff error.
- Operation procedure (OP): Components are affected by an inadequate operations procedure. For example, the component failed because the operational procedure was incorrect and the pump was operated with the discharge valve closed.
- Operation staff (OF): Components are affected by the same operations staff personnel error.
- Operational (maintenance/test (M/T) schedule, M/T procedures, M/T staff, operation procedure, operation staff): Coded if none of or more than one of OMS, OMP, OMF, OP or OF applies, or if there is not enough information to identify the specific 'maintenance or operation' coupling factor.
- Environmental internal (EI): Components share the same internal environment. For example, the process fluid flowing through the component was too hot.
- Environmental external (EE): Components share the same external environment. For example, the room that contains the components was too hot.
- Unknown (U): Sufficient information was not available in the event report to determine a definitive coupling factor.
- Environmental (internal, external): Coded if none of or more than one of Environmental external or Environmental internal applies, or if there is not enough information to identify the specific 'environmental' coupling factor.

C-2 References

OECD/NEA, (2004). International Common-cause Failure Data Exchange, ICDE General Coding Guidelines. Technical Note NEA/CSNI/R(2004)4.