ON SYSTEM SAFETY AND RELIABILITY METHODS IN EARLY DESIGN PHASES

Cost Focused Optimization
Applied on Aircraft Systems

Cristina Johansson
Only those who will risk going too far can possibly find out how far one can go.

– T.S. Eliot 1888
SYSTEM Safety and Reliability are fundamental to system design and involve a quantitative assessment prior to system development. An accurate prediction of reliability and system safety in a new product before it is manufactured and marketed is necessary as it allows us to forecast accurately the support costs, warranty costs, spare parts requirements, etc. On the other hand, it can be argued that an accurate prediction implies knowledge about failures that is rarely there in early design phases. Furthermore, while predictions of system performance can be made with credible precision, within reasonable tolerances, reliability and system safety are seldom predicted with high accuracy and confidence.

How well a product meets its performance requirements depends on various characteristics such as quality, reliability, availability, safety, and efficiency. But to produce a reliable product we may have to incur increased cost of design and manufacturing. Balancing such requirements, that are often contradictory, is also a necessary step in product development. This step can be performed using different optimization techniques.

This thesis is an attempt to develop a methodology for analysis and optimization of system safety and reliability in early design phases. A theoretical framework and context are presented in the first part of the thesis, including system safety and reliability methods and optimization techniques. Each of these topics is presented in its own chapter. The second and third parts are dedicated to contributions and papers. Three papers are included in the third part; the first evaluates the applicability of reliability methods in early design phases, the second is a proposed guideline for how to choose the right reliability method, and the third suggests a method to balance the safety requirements, reliability goals, and costs.


THE work presented in this licentiate thesis was carried out in the form of an industrial PhD project at the Division of Machine Design at the Department of Management and Engineering (IEI) at Linköping University. The research was funded by VINNOVA’s National Aviation Research Programme (NFFP) and Saab Aeronautics.

First of all, I’d like to thank my supervisor Prof. Johan Ölvander for his efforts in reviewing, discussing, and directing the research and for excellent guidance through the academic world. I also want to thank my industrial-supervisor Tech. Lic. Per Persson for always be open to discussions and providing rational advice from an industrial point of view as well as for the effort in reviewing. I thank the senior researcher involved in this project, Dr. Micael Derelöv for the guidance and advice from an academic and industrial point of view.

I want to thank my colleagues at Saab Aeronautics, Division of System Safety and Reliability and Tech. Fellow Lars Holmlund for their support and sharing with me from their field experience within System Safety and the aviation industry.

Special thanks go to my line manager Johan Tengroth for understanding and protecting my academic studies from drowning in industrial assignments.

I also want to thank Dr. Birgitta Lantto for her help and support to start this project. I wouldn’t be here without her advice. Thanks also go to Dr. Hampus Gavel for inspiring me to start this project and letting me know that everything is possible.

I want to give special mention to a mentor and former colleague I had the privilege of working with, Mr. Manfred Stein, who inspired my choice of career.

To my family thanks for believing in me.

Cristina Johansson
May 2013
Appended Papers

The following papers are appended and will be referred to by their Roman numerals. The papers are printed in their originally published state, except for changes in formatting and correction of minor errata.


[III] Johansson, C; Persson, P; Derelöv, M; Ölvander, J (2013), Cost optimization with focus on reliability and system safety, proceeding of ESREL2013, 29 Sep-02 Oct., Amsterdam, Holland.
The following report is not included in the thesis but constitute an important part of the background.

By sharing knowledge you empower [others] to act on their own. Shared knowledge enables people to take a risk to expand an idea and to venture to a new horizon.

– Sheila M. Bethel
PART I:
THEORETICAL CONTEXT
ONCEIVING reliable systems is a strategic issue for any industrial company. System Safety and Reliability can be valuable tools as part of the design process to compare options and highlight critical reliability features of design. Early reliability predictions provide baseline values of reliability and safety that can be used in the development of products and/or systems to compare alternative design approaches. But how well will the methods used for predictions fit when used as early as in the concept development phase? How can reliability and safety predictions of the system be balanced against other aspects of product development such as performance and costs?

This thesis aims to develop a methodology for analysis and optimization of system safety and reliability in early development phases. Optimization should be performed considering requirements that are often contradictory, e.g. high mission reliability, low accident risk contribution value, low cost, etc.

1.1 Background

Reliability is a widely used concept, sometimes without a precise definition, simply summarized as the ability of an item to be functional. The concept of reliability has been used for technical systems for more than 60 years and is a field of research common to mathematics, operational research, informatics, graph theory, physics, etc. According to [113], reliability is defined as

“The ability of an item to perform a required function, under given environmental and operational conditions and for a stated period of time.”

Safety is another widely used concept, mostly as the ability of an item not to cause any kind of injury. According to [31], safety is defined as

“Freedom from those conditions that can cause death, injury, occupational illness, or damage to or loss of equipment or property.”
Both definitions raise several questions, one of which is how these abilities can be engineered into the products and systems. According to standards such as [76], “reliability is an aspect of engineering uncertainty that may be quantified as a probability”. The need to measure and manage uncertainty in reliability analysis involves the use of statistical methods. To apply any statistical methods, data have to be gathered. These data are dependent on the problem to be solved and the type of analyses to be performed. Information can also be captured about factors influencing reliability and included in statistical analysis to measure their impact on performance.

Many reliability and system safety methods and models have been developed in the last decades in order to achieve more reliable and safe systems. However, those methods do not solve all reliability engineering problems. In order to chart some of these problems, in the report [IV], articles published between 2000 and 2010 have been reviewed and compared with those having focus on published articles and books until 2000 [11]. However, comparing those two reviews, all findings are still in the same problems area, some of them influencing the work of this thesis:

- **Systems under development.** The reliability/system safety of systems under development is a major challenge. How to use current information obtained from the field to control system development? How to take into account that with time the system not only changes its structure but also embeds new or modified equipment?

- **Unique system analysis.** There are a number of examples where a single or very few copies of a system are designed: space ships, huge dams, nuclear research equipment, Unmanned Aerial Vehicles (demonstrators and prototypes), etc. These objects must be extremely reliable. But often a prototype or any previous experience is missing. How to evaluate their reliability? In what terms? What is the confidence of such evaluation?

- **Units with several states.** Some systems consist of units with several states, not only on and off. Existing attempts at reliability and system safety evaluation of such systems are by now mostly of theoretical interest: there are no simple constructive results, which can be used in everyday engineering practice.

Even if the last decade has seen many new angles and analyses of those problems, the problems identified in [11] remain.

### 1.2 Product Development

The Product Development Process (PDP) includes numerous steps or phases, described somewhat differently by different authors [26]. Companies have also their own view of how to proceed in the process, although they have great similarities. In this section, the product development process will be briefly described, mainly based on [25]. Staged processes, as illustrated in Figure 1 were popular for decades because of their controlled design structures [26]. These processes methodically follow a series of steps, are characterized by few iterations and rigid reviews, and tend to freeze design specifications early. The generic development process should be divided into the following six phases according to [25].
To manage a product development project, the design company needs to set up a project team with a project leader. The Planning phase has begun. During Conceptual Development numerous design concepts are generated and evaluated, to determine whether a particular set of requirements (in terms of performance, costs, safety, etc) can be met and associated with levels of technology and risks. The key issues of basic configuration layout and performance are addressed and one or two basic concepts will be taken forward to the System-Level Design phase.

After this phase comes System-Level Design where the selected concept(s) start to increase in detail level. Sub-systems begin to take shape while detailed analysis and simulations are carried out. During this phase, the product is defined and the design will be “frozen”. The final step in the design process is the Detailed Design Phase, during which all components and parts are defined in all details and most of the manufacturing documentation is produced.

A system safety and/or reliability study can begin as early as in the Concept Development step, but there are not many suitable methods to apply and the results are mostly qualitative [IV]. Therefore, in this thesis, the author will use the term “early design phases” mean the time span from late Concept Development phase to middle System Level Design phase (Figure 1).

1.3 Objectives

Historically, system reliability and safety analysis are performed relatively late in the development process when a complete design is available on which to evaluate and perform calculations. Incidents and reliability analysis for components and pieces of equipment have also been an important input to improve the current system safety and reliability. The research focus has moved forward in the product development process, but there are great opportunities and a need to develop methods for applying reliability and system safety already in the early design phases. This would reduce the risk of costly redesign late in the process.

Today’s society, nationally and internationally, is characterized by a lower level of tolerance towards accidents, especially due to errors in the technical system, while the requirement for greater accessibility and affordability are being tightened. The use of complex and integrated systems changes the conditions for system safety and reliability work, increasing interest for new techniques and methodologies in these areas. However, beginning a system safety and reliability study as early as in the concept phase is not without its challenges.
A difficult balancing act in the aerospace industry is how to proceed in order to optimize system safety taking into account reliability, cost and weight. There are often conflicting requirements between these areas, for example in terms of redundancies that increase safety but gives rise to higher weight, reduce reliability as more errors can occur and therefore also maintenance requirements and increased costs.

To summarize, the objective of this research project is to increase confidence in the reliability and safety studies in the early design phase, while finding a method to optimize these against the costs of a particular design.

1.4 Research Questions and Method

As indicated above, it is beneficial to start the system reliability and safety studies in early design phases when there is more freedom to choose equipment and components and build in redundancies and/or maintenance policies. However, there are several challenges. Based on the industrial objective and the analysis in report [IV], the following research questions are defined:

RQ1  Which reliability method is best to use in early design phases?

RQ2  a) May a guideline be issued, which shows how to choose the appropriate reliability and/or system safety method in early design phases?
     b) How relevant is it in every day engineering practice?

RQ3  a) Can system reliability and safety be optimized in the concept phase?
     b) Can this help us in the process of choosing the equipment and components in our system?
     c) How can the optimization be done?

The work in this thesis is based on literature studies, prospective inductive observations and participation in courses and conferences. The study of literature is a major activity of this research project, with the purpose of gaining knowledge about methods, techniques and state of the art within system safety, reliability and optimization and a general view about related research areas. Prospective inductive observation have been made over the course of this research project by observing the work within the system safety and reliability areas, in different projects at Saab Aeronautics, as well as discussions with participants in these projects. The author has also attended various courses during this period as well as international conferences with the purpose of gaining a more detailed view into related areas.

Briefly described, the research was performed in an iterative approach including both deductive and inductive research methods [28]. RQ1 is considered to be analyzed according to an inductive approach, starting with a specific application and a specific choice of system reliability and safety methods to form general conclusions. RQ2 and RQ3 rather have a deductive view when the suggested method (general method) is applied and developed.
One fundamental activity when conducting scientific research is verification, as a process of confirming the validity of results [2]. The results presented in this thesis supports logical verification by literature survey, courses and conferences and case studies and verification by acceptance from discussions with colleagues and other researchers and feedbacks and comments on presentations and publications of research work.

1.5 Thesis Outline

The summary of this licentiate thesis is intended to provide a context for the attached papers and summarize the main contributions and essential conclusions. The thesis is divided into three main parts as outlined in Figure 2. The first part offers a theory context for this work, second presents the results and contributions and the third is dedicated to appended papers.

![Figure 2 Thesis Outline](image)

Chapter 1 is the introductory chapter, presenting the background of this thesis. Chapter 2, 3 and 4 are theory reviews, while chapter 5 and 6 are the author contributions. Since one of the papers [III] combines system safety and reliability methods with optimization techniques, a theory basis is provided for each subject in a separate section. Chapter 2, Reliability Engineering, consists of reliability analysis, classification of methods and techniques used and a short description of some of methods. Chapter 3, System Safety, consists of some of the system safety principles, short description of some of methods and a collection of standards regarding safety and reliability. Chapter 4, Optimization, provides a short research review with focus on papers combining the system safety and reliability methods with optimization techniques, and a short description of Genetic Algorithms as another technique.

With input from chapters 2 and 3, papers [I] and [II] are presented in Chapter 5, Application of System Safety and Reliability Methods in Early Design Phases. An evaluation of methods used in early design phases is made and a guideline for choosing a method is presented. For further details, see the attached papers. Chapter 6, Optimizing Reliability and Safety in Early...
Design Phases, uses input from chapters 4 and 5. Paper [III] is also briefly presented in this chapter, but for details see the attached paper. Chapter 7, Discussion & Conclusions, summarizes the contributions of the author of this thesis, the main conclusions, and future work.

What seems to us as bitter trials are often blessings in disguise.

– Oscar Wilde
Reliability Engineering

RELIABILITY modest beginning was in 1816, when the word reliability was first used by the poet Samuel Taylor Coleridge. An early application of reliability relates to the telegraph. By 1915, radios with a few vacuum tubes began to appear in the public. Automobiles came into more common use by 1920 and may represent mechanical applications of reliability [15]. In the 1920s, product improvement through the use of statistical quality control was promoted by Dr. Walter A Shewhart at Bell Labs [30].

On a parallel path with product reliability was the development of statistics in the twentieth century. Statistics as a tool for making measurements would become inseparable from the development of reliability concepts. Wallodie Weibull was working in Sweden during this period and investigated the fatigue of materials. During this time, he created a distribution, which we now call Weibull [28]. By the 1940s, reliability engineering still did not exist. Much of the reliability work of this period also had to do with testing new materials and material fatigue and the first published articles were about this aspect. In 1948 the Reliability Society was formed by the Institute of Electrical and Electronics Engineers (IEEE) [1]. The military was gradually started with cost considerations at the beginning of 1950s. They could not afford to have half of their essential equipment non-functional all of the time. In 1957 Robert Lusser pointed out in a report [13], that 60% of the failures of one Army missile system were due to components and the current methods for obtaining quality and reliability were inadequate and that something more was needed. Papers were being published at conferences showing the growth of this field. Ed Kaplan combined his nonparametric statistics paper on vacuum tube reliability with Paul Meier’s biostatistics paper to publish [9] the nonparametric maximum likelihood estimate (known as Kaplan-Meyer) of reliability functions from censored life data in 1958.

The 1960s saw several events, one of the most important being that a strong commitment to space exploration would turn into the National Aeronautical and Space Administration (NASA), a driving force for improved reliability of components and systems. 1962 was a key year with the first issue of Military Handbook 217 by the Navy and a Failure Modes and Effect Analysis (FMEA) handbook (non-military applications) was issued in 1968 [15].
During the 1970s, work progressed across a variety of fronts, while 1980s and 1990s were decades of great changes. During these decades, the failure rate of many components dropped by a factor of 10. Software became important to the reliability of systems. By the end of 1980s, programs could be purchased for performing FMEAs, Fault Tree Analysis (FTA), reliability predictions, block diagrams and Weibull Analysis [15]. The Challenger disaster caused people to stop and re-evaluate how they estimate risk. This single event spawned a reassessment of probabilistic methods.

New technologies such as micro-electro mechanical systems (MEMS), hand-held GPS, Li-I batteries and hand-held devices that combined cell phones and computers all represent challenges to maintain reliability during the 2000s. Product development time continued to over the decades and what had been done in three years was now done in 18 months or less. Consumers have become more aware of reliability failures and the cost to them [15]. Nowadays, reliability has become part of everyday life and consumer expectations, and the reliability tools and methods must be closely tied to the development process itself.

Some of the questions in this thesis are about reliability methods used in early design. In order to answer these questions, a brief review has been made of the commonly used methods. This section begins with a short description of how a reliability analysis is carried out. The methods and techniques used are classified according to their main purpose and briefly presented. At the end of this section is a description of how the methods fit into a generic product development process.

2.1 Reliability Analysis

During system design, the top-level reliability requirements are usually allocated to subsystems by design engineers and reliability engineers working together. Reliability design begins with the development of a model. Reliability uses models (such as block diagrams and fault trees) to provide a graphical means of evaluating the relationships between different parts of the system, according to [14] and [17]. These models incorporate predictions based on parts-count failure rates taken from historical data. While the predictions are often not accurate in an absolute sense, they are valuable to assess relative differences in design alternatives.

After a system is produced, reliability engineering monitors, assesses, and corrects deficiencies. Monitoring includes electronic and visual surveillance of critical parameters identified during the fault tree analysis design stage. The data should be constantly analyzed using statistical techniques, such as Weibull analysis and linear regression [21], to ensure the system reliability meets requirements. Reliability data and estimates are also key inputs for system logistics. Data collection is highly dependent on the nature of the system and the size of the organization. Most large organizations have quality control groups that collect failure data on vehicles, equipment, and machinery and therefore better data. Consumer product failures are often tracked by the number of returns. For systems in storage or standby, it is necessary to establish a test program to inspect and test random samples. Any changes to the system, such as field upgrades or recall repairs, require additional reliability tasks to ensure the reliability of the modification. Since it is not possible to anticipate all the failure modes of a given system,
Reliability Engineering

especially ones with a human element, failures will occur. The reliability program also includes a systematic root cause analysis that identifies the relationships involved in the failure. Corrective actions may be implemented. When possible, system failures and corrective actions are reported to the reliability engineering organization. One of the most common methods to apply a Reliability Operational Assessment is Failure Reporting, Analysis and Corrective Action Systems (FRACAS) [76].

According to the literature ([14] and [17]), there are three main branches of reliability: hardware, software and human reliability. The following chapter will handle methods and techniques for hardware reliability.

2.2 Methods and Techniques

Within reliability field, many models and methods are used, such as failure models [14], [21] and system analysis methods and models [14], [17]. The methods presented in this thesis are classified into the following categories with regard to their main purpose and according to standard [76]:

a) methods for fault avoidance, e.g.
   • parts derating and selection,
   • stress-strength analysis;
   • part count.

b) methods for architectural analysis and dependability assessment (allocation), e.g.
   1) bottom-up method (mainly dealing with effects of single faults),
      • event tree analysis (ETA),
      • failure mode and effects analysis (FMEA),
      • failure mode, effects and criticality analysis (FMECA).
   2) top-down methods (able to account for effects arising from combination of faults)
      • fault tree analysis (FTA),
      • Markov analysis (MA),
      • Petri net analysis (PNA),
      • truth table (TT),
      • reliability block diagrams (RBD);

c) methods for estimation of measures for basic events, e.g.
   • failure rate prediction,
   • human reliability analysis (HRA)- outside the scope of this thesis,
   • statistical reliability methods,
• software reliability engineering (SRE)- outside the scope of this thesis.

Another distinction is whether these methods work with sequences of events or time dependent properties. If this is taken into account, the following comprehensive categorization results:

• Sequence dependent: ETA, MA, PTA, functional analysis, Dynamic FTA
• Sequence independent: FMEA, FTA, RBD

These analysis methods allow evaluation of qualitative characteristics as well as estimation of quantitative ones, in order to predict long-term operating behaviour. It should be noticed that the validity of any result is clearly dependent on the accuracy and correctness of the input data for the basic events.

The life distributions are not presented in this paper due to their large recurrence in books, articles and studies as for example in the books presented in [14] and [21].

2.2.1 The “Part Count” Approach

The “Part Count” is simplest (and most pessimistic) inductive approach where every component failure is assumed to cause system failure. The Part Count method can be found named or described, by many standards, such as the military US standards [34], [35], [36], [37], [38] and [51] or other standards such as [76]. Under this assumption, obtaining an upper bound on the probability of system failure is especially straightforward. All the components are listed along with their estimated probabilities of failure. The individual component probabilities are then added and this sum provides an upper bound on the probability of system failure. The failure probabilities can be failure rates, un-reliabilities, or un-availabilities depending on the particular application (these more specific terms will be covered later).

For a particular system, the “Part Count” technique can provide a very pessimistic estimate of the system failure probability and the degree of pessimism is generally not quantifiable. It is conservative because if critical components exist, they often appear redundantly, so that no single failure is actually catastrophic for the system. Furthermore, a component can often depart from its normal operating mode in several different ways and these failure modes will not, in general, all have an equally deleterious effect on system operation. If the relevant failure modes for the system operation are not known then it is necessary to sum the failure probabilities for all the possible failure modes.

The principal advantage is that this approach can be used in very early design phases when information is limited or missing. Another advantage of the method is its simplicity.

The analysis provides a very pessimistic estimate of the system failure probability and the degree of pessimism is generally not quantifiable.
2.2.2 Stress-Strength analysis

Stress-Strength analysis is a method to determine the capability of a component or an item to withstand electrical, mechanical, environmental, or other stresses that might be a cause of their failure [76], where reliability is the probabilistic measure of assurance of the component performance. This analysis determines the physical effect of stresses on a component, as well as the mechanical or physical ability of the component. Probability of component failure is directly proportional to the applied stresses. The specific relationship of stresses versus component strength determines component reliability.

Stress-Strength analysis is primarily used in determination of reliability or equivalent failure rate of mechanical components. It is also used in physics of failure to determine likelihood of occurrence of a specific failure mode due to a specific individual cause in a component. Evaluation of stress against strength and resultant reliability of parts depends upon evaluation of the second moments, the mean values and variances of the expected stress and strength random variables. This evaluation is often simplified to one stress variable compared to strength of the component. In general terms, the strength and stress shall be represented by the performance function or the state function, which is a representative of a multitude of design variables including capabilities and stresses. Positive value of this function represents the safe state while negative value represents the failure state. This method is also provided by standards such as [36], [37], and [51].

The advantage of stress-strength analysis is that it can provide accurate representation of component reliability as a function of the expected failure mechanisms. It includes variability of design as well as variability of expected applied stresses, and their mutual correlation. In this sense, the technique provides a more realistic insight into effects of multiple stresses and is more representative of the physics of component failure, as many factors – environmental and mechanical – can be considered, including their mutual interaction [76].

One disadvantage is that, in the case of multiple stresses, and especially when there is an interaction or correlation between two or more stresses present, the mathematics of problem solving can become very involved, requiring professional mathematical computer tools. Another disadvantage is possible wrong assumption concerning distribution of one or more random variables, which, in turn, can lead to erroneous conclusions [76].

2.2.3 Parts derating and selection

Derating can be defined as the practice of limiting electrical, thermal and mechanical stresses on devices to levels below their specified or proven capabilities in order to enhance reliability. If a system is expected to be reliable, one of the major contributing factors must be a conservative design approach incorporating part derating [45]. The allowed stress levels are established as the maximum levels in circuit applications [36], [37]. Parts are selected, taking into account two criteria; a part’s reliability and its ability to withstand the expected environmental and operational stresses when used in a product [76]. Each component type, whether electronic (active or passive) or mechanical, must be evaluated to ensure that its temperature rating,
construction, and other specific attributes (mechanical or other) are adequate for the intended environments.

Derating a part means subjecting it to reduced operational and environmental stresses, the goal being to reduce its failure probability to within the period of time required for proper product operation. When comparing the rated component strength to the expected stress, it is important to allow for a margin, which may be calculated based on the cumulative or fatigue stress and the component strength, or based on other engineering analysis criteria and methods. This margin allows the desired part reliability to be achieved regarding the particular fault modes and the respective causes [76].

The benefit of the part selection and derating practices is the achievement of the product's desired reliability.

The only limitation is when there is no information on part reliability in any of the available databases or from the part manufacturer. In such a case, limitation extends to the part derating, when the derating guidelines involve reliability guidelines.

### 2.2.4 Functional Analysis

Functional Analysis is a qualitative method and an important step in a system reliability analysis. In order to identify all potential failures, the analyst has to understand the various functions of the system, each functional block in the system and the performance criteria related to all those functions. According to literature [14], the objectives of a Functional Analysis are to:

1. Identify all the functions of the system
2. Identify and classify the functions required in different operational modes
3. Provide hierarchical decomposition of the system functions
4. Describe how each function is realized
5. Identify interrelationships between functions
6. Identify interfaces with other systems and with the environment

Functional Trees or Functional Block Diagrams may be needed to illustrate complex systems [31].

Advantages: Functional Analysis provides an understanding of the systems functionality, interconnection between functions, and a base for further reliability and system safety analysis.

Limitations: Wrong assumptions (for example of performance criteria) can lead to erroneous conclusions.
2.2.5 Failure Modes and Effects Analysis (FMEA)

Failure Mode and Effect Analysis (FMEA) was one of the first systematic techniques for failure analysis according to [14]. It was developed by reliability engineers in the 1950s to study problems that may arise from malfunction of military systems. FMEA is an inductive method or a bottom-up approach. Induction involves reasoning from individual cases to a general conclusion. An FMEA is often the first step in a system reliability study (see [76]). It connects given initiating causes to their end results or consequences. These consequences are often failure of a system or component. It involves reviewing all components, assemblies and sub-systems if possible, in order to identify failure modes and, causes and effects of such failures. For each component, the failure modes and their resulting effects on the rest of the system are recorded in a specific FMEA worksheet [14].

If, in the consideration of a certain system, a particular fault or initiating condition is postulated and an attempt is made to ascertain the effect of that fault or condition on system operation, an inductive system analysis is being conducted. It starts from failure initiators and basic event initiators, and then proceeds upwards to determine the resulting system effects of a given initiator. A set of possible causes are analysed for their effects. There are several standards and procedures providing guidelines for this method, such as older military standard [41] or [49] and [93].

Advantages: An FMEA offers a systematic review of all components, assemblies and sub-systems if possible, in order to identify failure modes and the causes and effects of such failures. It connects single failures with their effects and identifies the causes of those failures. The output of an FMEA is input to other reliability analyses such as Fault Tree, Event Tree, Reliability Block Diagram, etc.

Limitations: The analysis is limited to single failures and is time-consuming.

2.2.6 Reliability Block Diagram (RBD)

A Reliability Block Diagram is a success-oriented network describing the function of the system. RBD is an inductive model wherein a system is divided into blocks that represents distinct elements such as components or subsystems. These elemental blocks are then combined according to system-success pathways as shown in Figure 3. RBDs are generally used to represent active elements in a system, in a manner that allows an exhaustive search for and identification of all pathways for success. Dependencies among elements can be explicitly addressed.

Initially developed top-level RBDs can be successively decomposed until the desired level of detail is obtained. Alternately, series components representing system trains in detailed RBDs can be logically combined, either directly or through the use of Fault Trees, into a super-component that is then linked to other super-components to form a summary model of a system. Such a representation can sometimes result in a more transparent analysis. Separate blocks representing each system element (such as for example fuel supply, block valves, control valves...
and motor) are structurally combined to represent both potential flow paths through the system [14].

The model is solved by enumerating the different success paths through the system and then using the rules of Boolean algebra to continue the blocks into an overall representation of system success. When an element is represented by a block it usually means that the element is functioning (as in Figure 3). Each element has also a probabilistic model of performance, such as Weibull [21], [29], for example. If the system has more than one function, each function must be considered individually according to references [14], [76] and [97].

![Figure 3: Example of an RBD of an Electrical Power System of an aircraft](image)

Some of the advantages of using RBD are:

- Often constructed almost directly from the system functional diagram; this has the further advantage of reducing constructional errors and/or systematic depiction of functional paths relevant to system reliability.
- Deals with most types of system configuration including parallel, redundant, standby and alternative functional paths.
- Capable of complete analysis of variations and trade-offs with regard to changes in system performance parameters.
- Provides (in the two-state application) for fairly easy manipulation of functional (or nonfunctional) paths to give minimal logical models (e.g. by using Boolean algebra).
- Capable of sensitivity analysis to indicate the items dominantly contributing to overall system reliability.
• Capable of setting up models for the evaluation of overall system reliability and availability in probabilistic terms.

• Results in compact and concise diagrams for a total system.

Some of the limitations using RBD are:

• Does not, in itself, provide for a specific fault analysis, i.e. the cause-effect(s) paths or the effect-cause(s) paths are not specifically highlighted.

• Requires a probabilistic model of performance for each element in the diagram.

• Will not show spurious or unintended outputs unless the analyst takes deliberate steps to this end.

• Is primarily directed towards success analysis and does not deal effectively with complex repair and maintenance strategies or general availability analysis.

• Is in general limited to non-repairable systems.

• The analysis is limited to single failures and is time-consuming.

2.2.7 Event Tree Analysis (ETA)

Event Tree Analysis has been used in risk and reliability analyses of a wide range of technological systems. In Reliability Analysis, ETA can be used as a design tool to demonstrate the effectiveness of protective systems in a plant or together with a Success Tree. See chapter 3.1.3 and [111].

2.2.8 Fault Tree Analysis (FTA)

Fault Tree Analysis (FTA) is one of the most important logic and probabilistic techniques used in system reliability and safety assessment [23]. FTA can be simply described as an analytical technique, whereby an undesired state of the system is specified (usually a state that is critical from a safety or reliability standpoint), and the system is then analyzed in the context of its environment and operation to find all realistic ways in which the undesired event (top event) can occur [95].

The FT itself is a graphic model [14], of the various parallel and sequential combinations of faults that will result in the occurrence of the predefined undesired event. A variety of elements are available for building a fault tree, e.g. gates and events, as shown in Figure 4 and described in the literature for example [14] and [23] or standards and handbooks such as [71] and [95].
The faults can be events that are associated with component hardware failures, human errors, software errors, or any other pertinent events which can lead to the undesired event. A FT shows the logical interrelationships of basic events that lead to the undesired event, the top event of the FT. A fault tree is tailored to its top event that corresponds to some particular system failure mode, and the fault tree thus includes only those faults that contribute to this top event. Moreover, these faults are not exhaustive—they cover only the faults that are assessed to be realistic by the analyst. An example of an FT diagram is presented in Figure 5.

Intrinsic to a fault tree is the concept that an outcome is a binary event i.e., either success or failure. A fault tree is composed of a complex of entities known as “gates” that serve to permit or inhibit the passage of fault logic up the tree. The gates show the relationships of events needed for the occurrence of a “higher” event. The “higher” event is the output of the gate; the “lower” events are the “inputs” to the gate. The gate symbol denotes the type of relationship of the input events required for the output event [23].
Figure 5 Example of a FT Diagram from an analysis of an aircraft fuel system. Fuel transfer failure of one fuel tank due to jet pump failure.

The qualitative evaluations basically transform the FT logic into logically equivalent forms that provide more focused information. The principal qualitative results that are obtained are the minimal cut sets (MCSs) of the top event. A cut set is a combination of basic events that can cause the top event. A minimal cut set (MCS) is the smallest combination of basic events that result in the top event. The basic events are the bottom events of the fault tree. Hence, the minimal cut sets relate the top event directly to the basic event causes. The set of MCSs for the top event represent all the ways that the basic events can cause the top event. A more descriptive name for a minimal cut set may be “minimal failure set.” For example, in the Figure 5, one of the MCSs of GATE43 is EVENT82 & EVENT84. Top event frequencies, failure or occurrence rates, and availabilities can also be calculated. These characteristics are particularly applicable if the top event is a system failure. This method is used in System Safety Analysis as well as in System Reliability Analysis. The FT can include basic events of Common Cause. The quantification of those events is made according to Common Cause Failure methods. See section 3.1.4.3.

Some of the advantages of using FTA are:

- Can be started in early stages of a design and further developed in detail concurrently with design development.

Inlet for operational flow plugged Right AT, body fails partially closed
Non return valve drive flow jet pump Right AT1 fails closed
Non return valve drive flow jet pump Right AT2 fails closed
Jet pump failure Right AT
GATE43
O=2.205e-4
EVENT82
\( r=3\times10^{-7} \) tau=300
O=1.950e-5
EVENT83
\( r=7\times10^{-6} \) tau=300
O=1.150e-4
EVENT112
\( r=1.3\times10^{-6} \) tau=300
O=4.500e-5
EVENT84
\( r=3\times10^{-7} \) tau=300
O=1.950e-5
EVENT85
\( r=7\times10^{-6} \) tau=300
O=1.150e-4
EVENT114
\( r=1.3\times10^{-6} \) tau=300
O=4.500e-5
Jet pump failure Right AT
GATE46
O=2.205e-4
GATE43, GATE45, and GATE46 occur
GATE45
O=2.851e-8
\( GATE43 \) = Fuel Transfer through the Jet Pumps, in the right after tank fails if Jet Pump 1 and 2 fail (GATE45 and GATE46 occur)
GATE46
O=2.205e-4
\( AT = \text{After Tank (fuel tank);} \)
\( r = \text{failure rate}; \)
\( \tau = \text{test interval for corrective action}; \)
\( Q = \text{Probability of fault occurrence/Unavailability} \)
• Identifies and records systematically the logical fault paths from a specific effect, back to the prime causes by using Boolean algebra.
• Allows easy conversion of logical models into corresponding probability measures.
• Assists in decision-making as a base and support tool due to variety of information obtained by a FTA.

Some of the disadvantages to using FTA are:
• FTA is not able to represent time or sequence dependency of events correctly.
• FTA has limitations with respect to reconfiguration or state-dependent behavior of systems.

These limitations can compensated for by combining FTA with Markov models, where Markov models are taken as basic events in fault trees.

2.2.9 Markov Chains Models (MA)

The main idea of Markov-chains based models is directly or indirectly (e.g. starting with Petri Network) to build a Markov chain to represent the system behaviour. Markov modeling ([14] and [17]) is a probabilistic method that allows the statistical dependence of the failure or repair characteristics of individual components to be adapted to the state of the system according to [76] and [104]. Hence, Markov modeling can capture the effects of both order-dependent component failures and changing transition rates resulting from stress or other factors. For this reason, Markov analysis is suitable for dependability evaluation of functionally complex system structures and complex repair and maintenance strategies.

The proper field of application of this technique is when the transition (failure or repair) rates depend on the system state or vary with load, stress level, system structure (e.g. stand-by), maintenance policy or other factors. In particular, the system structure and the maintenance policy induce dependencies that cannot be captured by other, less computationally intensive techniques [104]. The size of a Markov model (in terms of the number of states and transitions) grows exponentially with the number of components in the system. For a system with many components, the solution of a system using a Markov model may be infeasible, even if the model is truncated. However, if the system level can be divided into independent modules, and the modules solved separately, then the separate results can be combined to achieve a complete analysis. An example of a state transition diagram is presented in Figure 6. In state 0 all elements are functioning as intended and the state 3 is the absorbent state from where the system cannot recover.
The nomenclature used in Markov Analysis, the types of model used and how to solve them can be found in literature such as [14] and [21] or in standards such as [71], [76] or [104].

Some of the advantages of using Markov model are:

- It provides a flexible probabilistic model for analyzing system behavior.

- It is adaptable to complex redundant configurations, complex maintenance policies, complex fault-error handling models (intermittent faults, fault latency, reconfiguration), degraded modes of operation and common cause failures.

- It provides probabilistic solutions for modules to be plugged into other models such as block diagrams and fault trees.

- It allows accurate modeling of the event sequences with a specific pattern or order of occurrence.

Some of the limitations using Markov model are:

- As the number of system components increases, there is an exponential growth in the number of states resulting in laborious analysis.

- The model can be difficult for users to construct and verify, and requires specific software for the analysis.

- The numerical solution step is available only with constant transition rates.

- Specific measures, such as MTTF and MTTR, are not immediately obtained from the standard solution of the Markov model, but require direct attention.

Figure 6 Example of Markov State Transition Diagram
2.2.10 Petri Nets (PN)

Petri nets (PN) are a graphical tool for the representation and analysis of complex logical interactions between components or events in a system (see [8], [76] and [112]). Typical complex interactions that are naturally included in the Petri net language are concurrency, conflict, synchronization, mutual exclusion and resource limitation. The static structure of the modeled system is represented by a Petri net graph as exemplified in the Figure 7.

A condition is valid in a given situation if the corresponding place is marked, i.e., contains at least one token • (drawn as a blue dot in Figure 7). The dynamics of the system are represented by means of the movement of the tokens in the graph. A transition is enabled if its input places contain at least one token. An enabled transition may fire, and the transition firing removes one token from each input place and puts one token into each output place. The distribution of the tokens into the places is called marking. Starting from an initial marking, the application of the enabling and firing rules produces all the reachable markings called the reachability set. The reachability set provides all the states that the system can reach from an initial state [3], [8].

Standard Petri nets do not carry the notion of time [104]. However, many extensions have appeared in which timing is superimposed onto the Petri net. If a (constant) firing rate is assigned to each transition, the dynamics of the Petri nets can be analyzed by means of a continuous Markov time chain whose state space is isomorphic with the reachability set of the corresponding Petri net.

Figure 7 Example of a generic Petri Net Diagram

The key element of the Petri net analysis is a description of the system structure and its dynamic behavior in terms of primitive elements (places, transitions, arcs and tokens) of the Petri net language; this step requires the use of ad hoc software tools:
a) Structural qualitative analysis

b) Quantitative analysis: if constant firing rates are assigned to the Petri net transitions the quantitative analysis can be performed via the numerical solution of the corresponding Markov model, otherwise simulation is the only viable technique.

The Petri net can be utilized as a high level language to generate Markov models, and several tools in performance dependability analysis are based on this methodology. Petri nets provide also a natural environment for simulation. The use of Petri nets is recommended when complex logical interactions need to be taken into account (concurrency, conflict, synchronization, mutual exclusion, resource limitation). Moreover, PN are usually an easier and more natural language to describe a Markov model.

Some of the advantages of using PNs are:

- Petri nets are suitable for representing complex interactions among hardware or software modules that are not easily modeled by other techniques.
- Petri Nets are a viable way of generating Markov models. In general, the description of the system by means of a Petri net requires far fewer elements than the corresponding Markov representation.
- The Markov model is generated automatically from the Petri net representation and the complexity of the analytical solution procedure is hidden to the modeler who interacts only at the Petri net level.
- In addition, the PN allow a qualitative structural analysis based only on the property of the graph. This structural analysis is, in general, less costly than the generation of the Markov model, and provides information useful to validate the consistency of the model.

Since the quantitative analysis is based on the generation and solution of the corresponding Markov model, most of the limitations are shared with the Markov analysis. The PN methodology requires the use of software [104].

During the PDP (Figure 1) of safety critical systems, other properties can be important, e.g. system safety. Some of the methods described in his chapter, e.g. FMEA, FTA, MA, ETA and FMECA are used for both reliability and safety analysis. Other methods are used only for system safety analysis, e.g. CCF, DFM, ZA, CMF, PHA and FHA*. These are described in the next chapter.
A ship in harbor is safe, but that is not what ships are built for.

– John A. Shedd
SYSTEM SAFETY, as we know it today, was introduced in the 1940s. Gaining momentum and support during the 1950s, its value became firmly established during the sixties. The need for system safety was motivated through the analysis and recommendations resulting from different accident investigations. In response to the general dissatisfaction with the trial-and-error or fly-fix-fly approach to aircraft systems design, the early 1960s saw many new developments in system safety [22]. In 1963, the Aerospace System Society was formed in Los Angeles, in California and System Safety had become a recognized field of study. During this time, there were two different driving forces: the Department of Defense (DoD) and the National Aeronautical and Space Administration (NASA).

In July 1969, MIL-STD-882 was published by the DoD. This document sees system safety as a management science and expanded the scope of system safety to apply to all military services within the DoD. This standard, with necessary updates, is still in use. In parallel, NASA developed its own system safety program and requirements. The third driving force in system safety, the Atomic Energy Commission (AEC), began by hiring a retired manager from the National Safety Council to develop a system safety program for the AEC. Unfortunately, the lack of standardization or commonality made effective monitoring, evaluation, and control of safety efforts throughout the organization difficult if not impossible [22].

In the 1980s several non-military, non-flight, and non-nuclear projects with high complexity and high cost, have dictated a more sophisticated upstream safety approach. The system safety experience has also begun to demonstrate that upstream safety efforts lead to better design and the system safety tools and techniques have proven to be cost-effective planning and review tools. The 1990s are characterized by process safety. With the publication in January 1993 of MIL-STD-882C, hardware and software were integrated into system safety efforts. As Jerome Lederer, director of the Flight Safety Foundation for 20 years and NASA’s first director of Manned Flight Safety, put it in 2004:
“Risk management is a more realistic term than safety. It implies that hazards are ever-present, that they must be identified, analyzed, evaluated and controlled or rationally accepted.”

Today, the discipline of system safety is described as an evolving science, consistently increasing its scope to meet an expanding number of system requirements. The underlying principles remain intact, while system safety concepts change and mature through increased knowledge and sparkling advances in technology. Safety is property that arises at the system level, when components are working together. Everything can be viewed as a system at some level, and the unique interconnectedness and complexity of each system presents special challenges for safety. Hazards tend to revolve around systems [22].

Safety has a larger scope than reliability and a safety analysis often starts in early design phases; some of the methods and techniques used in system safety are therefore briefly described in this chapter. These, as well as the ones described in this section, are used further in this thesis as an input for paper [I] and [II], in section 5.

3.1 Methods and Techniques

System safety is a basic requirement of the total system. The goal is to optimize safety by the identification of safety related risks, eliminating or controlling them by design and/or procedures, based on acceptable system safety precedence. According to [5],

“System Safety is a specialty within system engineering that supports program risk management. It is the application of engineering and management principles, criteria and techniques to optimize safety.”

The standard [31] and its updated version [32], uses a similar definition of system safety as:

“Application of engineering and management principles, criteria, and techniques to achieve acceptable mishap risk, within the constraints of operational effectiveness and suitability, time, and cost, throughout all phases of the system life cycle.”

A system safety program includes four main parts according to [5], [31] and [32]:

- Management, including planning and establishing overall requirements;
- Analysis, including breaking down of the overall requirements, identifying and analyzing risks;
- Evaluation, ending with a system safety assessment;
- Verification, including validation and verification of risk mitigation measures.

There are several methods used for analyses of risks within system safety. Some of these methods (such as FTA, FMEA, MA) are also used in reliability analysis and have already been presented in section 2.2. Some of the methods used in system safety analysis are described in the following sections.
3.1.1 Failure Modes, Effects and Criticality Analysis (FMECA)

Failure Modes, Effects and Criticality Analysis (FMECA), is an extension of FMEA (see chapter 2.2.5). An FMEA becomes an FMECA if criticalities or priorities are assigned to the failure mode effects. A Risk Priority Number is introduced in the worksheet ([27] and [41]). The purpose of FMECA is to identify design areas where improvements are needed to meet reliability and/or system safety requirements. FMECA activities vary in different phases of product development, but should be carried out already in the conceptual design phase.

The objectives of an FMECA according to [14] are to:

- Assist in selecting design alternatives with high reliability and safety potential
- Ensure that all conceivable failure modes and their effects have been considered
- List potential failures and their magnitude and effects
- Develop early criteria for test planning
- Provide a basis for quantitative reliability and system safety analyses
- Provide historical documentation for future reference
- Provide input data for trade-off studies
- Provide a basis for establishing corrective actions priorities
- Assist evaluation of design requirement related to redundancy, failure detection systems, fail-safe characteristics, automatic and manual override

The advantages of FMECA are similar to those of FMEA:

- An FMECA offers a systematic review of all components, assemblies and sub-systems, in order to identify failure modes, causes and effects of such failures, ranked according to criticality.
- The output of an FMECA acts as input to other reliability and safety analyses such as Hazard Analysis, Fault Tree, Event Tree, Reliability Block Diagram, etc.
- An FMECA should assist evaluation of design requirements related to redundancy, failure detection systems, fail-safe characteristics, automatic and manual override and test planning.

The analysis is limited at single failures and is time-consuming.

3.1.2 Double Failure Matrix (DFM)

The previous technique (FMECA) is used to analyse the effects of single failures. An inductive technique that also considers the effects of double failures is the Double Failure Matrix (DFM). Its use is feasible for systems with small numbers of redundant components. The DFM approach is useful to discuss since it provides an extension of inductive approaches from single failure causes to multiple failure causes (see [76]). This is a significant enhancement to FMEA and FMECA approaches. To more effectively apply the DFM approach faults,
multiple faults) are first categorized according to the severity of the system effect. A basic categorization originated in [31] and is still used. The categorization will depend on the conditions assumed to exist previously, and the categorizations can change as the assumed conditions change.

The advantages of using DFM are:

- The method offers a systematic review of all components, assemblies and sub-systems if possible, in order to identify failure modes, causes and effects, ranked by criticality.
- DFM handles double failures.
- The output of a DFM acts as input to other reliability and safety analyses such as Hazard Analysis, FTA, ETA, RBD, etc.
- DFM assists evaluation of design requirements related to redundancy, failure detection systems, fail-safe characteristics, automatic and manual override and test planning.

The applicability of DFM is limited to systems with a limited number of components.

### 3.1.3 Event Tree Analysis (ETA)

Event Tree Analysis has been used in risk and reliability analyses of a wide range of technological systems. It is an inductive method and the most common way of analyzing an accident progression ([5], [23], [31], [32] and [110]). An Event Tree is a logic tree diagram, starting from a basic initiating event and provides a systematic coverage of the time sequence of event propagation to its potential outcomes or consequences. The Initiating Event can be identified by FMECA, PHA, HAZOP, etc. In Figure 8, an example of ETA is presented. The analyzed system is an electrical power system of an aircraft. The initiating event is “total loss of AC power supply”. The scenario follows the possible factors that could influence the output (the columns). Each of these factors has an occurrence probability. Every branch shows a possible path and end with a predefined consequence.

The ETA is a natural part of most risk analyses but they can be used as a design tool to demonstrate the effectiveness of protective systems in a plant. In quantitative ET this method can be used independently or, is often combine with fault tree analysis. ET and FT are known as complement to each other. ET can also be used for human reliability assessment [14].

The major benefit of an event tree is the possibility to evaluate consequences of an event, and thus provide for possible mitigation of a highly probable, but unfavorable consequence. The event tree analysis is thus beneficial when performed as a complement to fault tree analysis. An event tree analysis can also be used as a tool in the fault mode analysis. When starting bottom up, the analysis follows possible paths of an event (a failure mode) to determine probable consequences of a failure [23].

The limitations of an event tree: the analyst has to describe the different scenarios and the result will be displayed in chronological development of event chains, which needs detailed system knowledge and understanding of the system.
3.1.4 Common Cause Analysis (CCA)

Common cause analysis (CCA) is a method for identifying sequences of events leading to an accident (e.g. aircraft accident). Following chapters are based on references [5], [31], [32], [71] and [76]. CCA should be carried out to establish the requirements for the elimination of common cause failure between components of the architecture (e.g., a total failure of the communications system, or simultaneous failure of redundant communication nodes. It can be carried out using several qualitative and/or quantitative methods with the purpose of identifying and analyzing dependent failures. According to reference [76], CCA consists of Zonal Analysis (ZA), Common Mode Fault (CMF) and Common Cause Failures (CCF).

3.1.4.1 Zonal (Hazard) Analysis (ZA or ZHA)

In system safety assessment a number of experiential (qualitative) analyses based upon knowledge of the physical structure of the system and arrangement of its components are commonly carried out. Zonal Analysis (ZA) is also known as Zonal Hazard Analysis (ZHA), Zonal Safety Analysis, etc and is typical of these processes; in its usual aerospace domain ZHA considers the interactions of logically unrelated systems in the same physical part (zone) of an aircraft (e.g. nose, wings, etc.). For example, ZHA would consider the effect of a hydraulic leak on electrical connectors in the same zone [71], [76].
Similar approaches have not been applied to software systems. In part this is due to the failure, mentioned above, of many approaches to software Functional Failure Analysis and FMECA, to correctly identify the software components and their failure modes. The failure propagation will not normally respect the logical structure of the design; for example, it may propagate via memory corruption when software is involved, or bird strike. Specifically, it may be used to show that the constraint 'no single point failure shall lead to a catastrophic hazard' is met, even considering the effects of common-mode software failures on the design. However it is unclear how valuable this possibility is as, in many cases, protection against single point failure would be provided by hardware redundancy [71], [76].

3.1.4.2 Common Mode Fault (CMF)

A common-mode fault occurs when multiple copies of a redundant system suffer faults almost simultaneously, generally due to a single cause. According to [71], Common Mode Fault (CMF) is used to verify the redundancy/independency of failures assumed in other analysis such as FTA or independent of other analysis. The faults that affect more than one fault containment region at the same time, generally due to a common cause have to be investigated.

There is no single theory on which to base a solution to CMF's, and redundancy is of little help or any utility in tolerating CMF. Design diversity and formal methods have been proposed as two ways to deal with this problem. A broader perspective shows that there is a three-pronged approach to CMF's: fault avoidance by using formal methods, for example; fault removal through test and evaluation or via fault insertion; and fault tolerance in real time via exception handlers and program check-pointing and restart. All the safety-critical systems have had to use one or more of these techniques [71], [76].

Two phases are important in the CMF: identification and classification of common mode faults and common mode faults avoidance, removal and/or tolerance. The most cost effective phase of the total design and development process for reducing the likelihood of CMF is the earliest part of the program. Avoidance techniques and tools can be used from the requirements specifications phase to the design and implementation phase, and result in fewer permanent and intermittent design CMFs being introduced into the computer system and/or hardware [71].

3.1.4.3 Common Cause Failures (CCF)

The purpose of Common Cause Failures (CCF) is to identify and quantify the common cause failures and eliminate/improve the protection against dependent failures. Dependent Failures may be classified as Common Cause Failures or Cascading Failures [23]. Common Cause Failures are multiple failures sharing a root cause (fire, earthquake, human error, etc.). They are not a failure of another component in the system. Explicit methods such as Event Tree and Fault Tree are used to identify and treat the root causes.

Cascading failures are multiple failures initiated by the failure of a component in the system. Implicit methods using parametric models (e.g. RBD) are used to identify and analyze intersystem or/and inter-component dependency. Explicit methods such as Event Tree and Fault Tree are also used. The treatment of CCF ([23], [71]) within a probabilistic safety assessment requires four phases:
a. **System logic model development.** The aim of this phase is to identify and understand the physical and functional links in the system, functional dependencies and interfaces and develop the corresponding logic models of the system (FT/ET).

b. **Identification of common cause (CC) component groups.** The purpose of this phase is a definition of components with common cause failures to be included in the model, and determination of which root causes and coupling mechanisms should be included in the common cause events for the purpose of quantification.

c. **CC modeling and data analysis.** The objective of this phase is to complete the system quantification by incorporating the effects of common cause events for component groups. This includes choice of basic event failure model.

d. **System quantification and interpretation of results.** The results will show the weaknesses of the design and allows us to improve the protection against the unwanted events caused by CCF.

Some of the advantages using the presented CCA methods, according to [71] are:

- CCF and CMF reduce design errors and human errors in the system, increasing the fault tolerance of the system.
- Zonal Analysis identifies failures missed by other approaches in the safety analysis and verifies the physical separation requirements.

Some limitations are related to competence issues, and lack of information about the system or/and components. CCA methods are time-consuming.

### 3.1.5 Hazard Analysis

When evaluating risk, contributory hazards are important. According to [32], the definition of hazard is

“A real or potential condition that could lead to an unplanned event or series of events (i.e. mishap) resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment”.

Briefly put, hazards are **unsafe acts** and **unsafe conditions** with the potential for harm. Unsafe acts are human errors that can occur at any time throughout the system life cycle. Human reliability addresses human error or human failure. Unsafe conditions can be failures, malfunctions, faults, and anomalies that are contributory hazards. An unreliable system is not automatically hazardous; systems can be designed to be fail-safe ([31] and [32], [71], [76]).

#### 3.1.5.1 Functional Hazard Assessment (FHA)

Functional Hazard Assessment (FHA) is a predictive, qualitative technique that attempts to identify and mitigate the effects of functional failures of part of a system. The primary aim of conducting FHA is to identify hazardous function failure conditions. According to [5] and [71] an FHA
• Identify all functions of a system
• Identify and describe failure conditions,
• Determine the effect of each failure condition,
• Classify failure condition effects,
• Assign the requirements to a lower level,
• Identify supporting material and
• Identify methods to verify requirement compliance.

The advantages of FHA are that can be started in very early development phases, can be based on existing functional analysis, breaks down the overall safety requirements and gaining a better understanding of the effect and failures of intended system.

The limitations are related to difficulties of applying in a meaningful way. Identifying and defining functions at the right level of abstraction as well as extracting functions from requirement documentation is not an easy task. Another limitation is the size of an FHA.

### 3.1.5.2 Preliminary Hazard Analysis (PHA)

Preliminary Hazard Analysis (PHA) is the initial effort in hazard analysis during the system design phase or the programming and requirements development phase for facilities acquisition. It may also be used on an operational system for the initial examination of the state of safety. The purpose of the PHA is not to affect control of all risks but to fully recognize the hazardous states with all of the accompanying system implications [5].

The objectives of a PHA are to identify potential hazardous conditions inherent within the system and to determine the significance or criticality of potential accidents that might arise. The first step in a PHA is to identify potentially hazardous elements or components within the system. This process is facilitated by engineering experience, the exercise of engineering judgement, and the use of numerous checklists that have been developed from time to time. The second step in a PHA is the identification of those events that could possibly transform specific hazardous conditions into potential accidents. Then the seriousness of these potential accidents is assessed to determine whether preventive measures should be taken. The tasks and necessary input when performing PHA, are described by standards and handbooks such as [5], [31], [32] and [71]. The output of the PHA may be used in developing system safety requirements and in preparing performance and design specifications. In addition, the PHA is the basic hazard analysis that establishes the framework for other hazard analyses that may be performed [5].

### 3.1.5.3 Fault Hazard Analysis (FHA)

Another method, Fault Hazard Analysis (FHA), was developed as a special purpose tool for use in projects involving many organizations, one of which is supposed to act as integrator. This technique is especially valuable for detecting faults that cross organizational interfaces. Even though FHA is generally not used now per se, FHA concepts and approaches are used in certain extended FMEAs and FMECAs [76]. The FHA approach considers the following basic causes and effects, which can be arranged in columns and which characterize this form of inductive approach.
Column (1) Component identification
Column (2) Failure probability
Column (3) Failure modes (identify all possible modes)
Column (4) Percent failures by mode
Column (5) Effect of failure (traced up to some relevant interface)
Column (6) Identification of upstream component that could command or initiate the fault in question
Column (7) Factors that could cause secondary failures (including threshold levels). This column should contain a listing of those operational or environmental variables to which the component is sensitive.
Column (8) Remarks

What is different for FHA is the consideration of the extra information given in columns 6 and 7. Column 6 identifies possible command or interface failures. Column 7 identifies secondary failures that are failures outside the design envelope. As will become apparent in later chapters, Columns 6 and 7 have special significance for the fault tree analyst [76].

One advantage of this method is that can be used in very early design phases and allows events that could possibly transform specific hazardous conditions into potential accidents to be identified. Another advantage is the possibility to prevent these potential accidents by developing procedures and preventive measures. This will permit the early development of design and procedural safety requirements for controlling these hazardous conditions, thus eliminating costly design changes later on.

Some of the limitations are related to competence issues and, depending of the complexity of the analyzed system, can be time consuming, and need to be complemented with another analysis.

3.2 Standards and Regulations

A collection of standards for the use of practitioners, handling methods and methodologies within reliability and system safety are presented in this chapter and included in reference section from [31] to [112].

US military standards and handbooks are presented in references [31] to [44]. Some are more than 20 years old but are still in use. Other standards, handbooks and specification issued by different organizations such as IEEE, NASA, etc are referenced between [46] to [51]. In the UK, there are more up to date standards maintained under the sponsorship of the UK MOD, as Defense Standards (see references [52] to [71]).

There are also numerous commercial standards, produced by various organizations including the SAE, MSG, ARP, and IEE. An example of a French standard is the FIDES [72] methodology and is based on the physics of failures and supported by the analysis of test data, field returns and existing modeling. The IEC (International Electro-technical Commission) standards, is one
of three global sister organizations (IEC, ISO, ITU) that develop international standards. IEC standards (from [73] to [112]) cover methods and procedures within reliability and system safety for a vast range of technologies from power generation, transmission and distribution to home appliances and office equipment, semiconductors, fibre optics, batteries, solar energy, nanotechnology and marine energy as well as many others.

*Knowledge is an unending adventure at the edge of uncertainty.*

– Jacob Bronowski
Optimization is an important tool in decision science and in the analysis of physical systems. To make use of this tool, we must first identify some objectives, a quantitative measure of the performance of the system under study. This objective can be profit, time, potential energy, reliability, etc. The objectives depend on certain characteristics of the system, called variables. The goal is to find values of the variables that optimize the objective. Often the variables are restricted, or constrained, in some way. The process of identifying objective, variables and constraints for a given problem is known as modeling [16].

Over years of development, optimization theory and methods have grown in their ability to handle various practical problems. In light of advances in computing systems, optimization approaches have become one of the most promising techniques for engineering applications. To close the gap between optimization theory and the practice of engineering, paper [6] intends to provide the details of recent advances in optimization sciences and promote the applications of optimization methods in engineering.

There are many trends within the research of optimization, some of them including different reliability or safety features. For example, paper [4] deals with the design and optimization for crashworthiness of a vehicle bumper subsystem, a key scenario in vehicle component design. Passive safety has a central attention during a vehicle development process. Paper [7] presents an approach to calculate optimal reliability characteristics of mechatronic system components with unknown fault histories in the application, provided that both the system topology (structure) is given and the reliability characteristics of the remaining components of the system are known. Genetic Algorithms, and pattern search are applied in this paper, to solve contradictions with a given objective function.

In paper [12] the authors present a way of optimizing the reliability of the system in the concept phase. Paper [17] propose a design process in which techniques for semi-automatic safety and reliability analysis of systems models are combined with multi-objective optimization techniques to assist the gradual development of designs that can meet reliability and safety requirements and maximize profit within pragmatic development cost constraints.
However, the author of this thesis did not found a generally applicable method of optimization, capable of balancing system safety and reliability against performance parameters and costs, regardless of the system analyzed. All methods found are applicable for one type of system (inductive research method) and it is difficult to generalize.

The purpose of an optimization algorithm is to let the computer automatically explore the design space of a mathematical problem and present an optimal solution to it [20]. Many algorithms have been purposed over the years, one of which is the Genetic Algorithm (GA), used further in this thesis. In the next section GAs are briefly described, and are used in paper [III] and commented in chapter 6.

4.1 Genetic Algorithm

Genetic Algorithms (GAs) were inspired by the optimization procedure that exists in nature, the biological phenomenon of evolution.

![GA working principle](image)

Figure 9 GA working principle
A GA maintains a population of different solutions, allowing them to mate, produce offspring, mutate, and fight for survival. GAs have become popular tools for solving various optimization problems [10]. The working principle of a GA is described by Figure 9. It basically begins by generating a predefined number of generations, consisting of a constant number of individuals. First, it spreads an initial population randomly in the design space and each individual is given a fitness value by calling the objective function. The individuals with the best fitness values are selected for mating and a new generation with the same number of individuals is created. Each generation is better than its precedent. GA progresses until a predefined number of generations is reached. The best individuals can be let to survive several generations, or mutation can be enabled, where the individuals may change randomly [20].

One drawback is that GAs usually converged slowly and requires many objective function evaluations since the values of all individuals in each generation needs to be calculated. This makes GAs computationally rather expensive. Another potential drawback is that GAs are heuristic methods that do not guarantee finding a global optimum [18]. In practice this is not a major issue as it is often not possible to prove optimality in the general case for the problem studied in this thesis.

In literature they are often used to solve problems of the type addressed in this thesis. GAs are appropriate for high-dimension, stochastic problems, with many nonlinearities and discontinuities. They are suited to the characteristics of reliability design problems: multi-modal domains with some epistasis (one part of the solution or structure is affected by another) [18], but can also be applied to a deterministic, combinatorial reliability problem. In chapter 6, the GA is used to find the optimal vendor for each piece of equipment in order to maximize system safety and reliability and minimize the development cost. The problem considered is multi-objective to its nature with objectives such as system cost, system reliability and system safety (or the probability of unwanted events).
PART II:
RESULTS AND
CONTRIBUTIONS
Experience is the name everyone gives to their mistakes.

- Oscar Wilde
Application of System Safety and Reliability Methods in Early Design Phases

RELIABILITY theory is a general theory about systems failure. Failures are related to development work, production or use. A reliability analysis will normally include an evaluation of some kind of random value characterizing the system behavior.

5.1 Usage of Reliability Methods in Early Design Phases

During a product development process like the one presented in Figure 1, the reliability methods can be used in several product development steps. One method can be used in several PDP phases, the detail level increasing concomitant with the settlement of the design. Figure 10 presents a visualization of how the reliability and safety methods presented can be used during a Generic PDP. For example, a Functional Hazard Assessment (FHA) can be started in the concept development phase with a set of requirements of overall system functions. Like most of the reliability and safety analysis, this is an iterative process and in the system-level development step, FHA will handle all the functional requirements derived from the breaking down of main functions.
Methods like FTA, ETA, RBD, etc can also start being used in the concept phase but they are qualitative at such an early stage in PDP. They can also be used in order to break down the system safety overall requirements and reliability goals. In the system-level development step, quantitative information is added about failures and at the end of detailed development all the

---

1CCF   Common Cause Failure (3.1.4.3)
FMEA   Failure Mode and Effect Analysis (2.2.5)
FME(C)A Failure Mode, Effect and Criticality Analysis (3.1.1)
DFM   Double Failure Matrix (3.1.2)
ETA   Event Tree Analysis (3.1.3)
FTA   Fault Tree Analysis (2.2.8)
ZA   Zonal Analysis (3.1.4.1)
CMF   Common Mode Fault (3.1.4.2)
PHA   Preliminary Hazard Analysis (3.1.5.2)
FHA   Functional Hazard Assessment (3.1.5.1)
FHA*   Fault Hazard Analysis (3.1.5.3)
MA   Markov Analysis (2.2.9)
PNA   Petri Net Analysis (2.2.10)
RBD   Reliability Block Diagram (2.2.6)
details about systems are known. Figure 10 is further used in chapter 5 (paper [I] and [II]), when choosing between methods available in early design phases.

5.2 Research versus Industry

No one can dispute the need for a product to be reliable. But do the researchers and engineers really have the same focus during a reliability study? While the research focus within the reliability field is on the mathematical modeling, during a reliability study, the industry focuses on providing a graphical means of evaluating the relationships between different parts of the system. The confidence of the answers depends on the assumptions, quality of input data and the applicability of the reliability method used. The quality of input data often depends on the vendor and it is difficult for the reliability engineer to influence. The choice of methods can on the other hand increase the confidence of the answers [II].

5.3 Choosing the Reliability Approach

Reliability design begins with the development of a model. Reliability uses models (such as RBD and FTA) to provide a graphical means of evaluating the relationships between different parts of the system. These models incorporate predictions based on parts-count failure rates taken from historical data. The methods for architectural analysis and dependability assessment, possible to use in the conceptual design are, according to Figure 10, Functional Analysis, ET, FT, MA, PN, PHA and RBD. The choice of methods in paper [I] and [II] is selected from these methods.

5.3.1 Applying reliability methods in early design phases

Paper [I] evaluates some commonly used reliability methods and their applicability to an overall concept of a system. Based on Figure 10 from section 5.1, only three methods are used in this analysis: a static method (RBD), a dynamic method (MA), and a method currently commonly used in system safety today (FTA). First, all three methods are applied on an electrical power system concept to analyze what may be gained by applying these methods in early design phases. Do all three methods give the same kind of answers? The second part evaluates the three methods. Three criteria, including a set of questions, are considered in order to evaluate the practical use of the methods in early design phases (from concept): usefulness, modeling of the system, and applicability. The choice of these criteria is based on the author’s experience from questions asked in everyday engineering practice.

A grading system from 1 to 3 is used to quantify every answer for a set of questions used to evaluate the methods, where 3 is the maximum result. The advantages and weaknesses of the methods are presented and discussed. The evaluation matrix does not take into consideration the importance of each question, each being considered equally important. The application case studied in this paper is an overall concept of an aircraft’s electrical power system. Preliminary system architecture and the main sub-systems are established.
The conclusions for the application case analyzed with the three methods are:

- In order to achieve the highest system reliability, the design focus must be on the installation part of the system (AC and DC). This can be done, for example, by design requirements concerning transformer rectifier unit 3 and failure rate and single failures causing total loss of function.
- Attention must also be paid to the requirement specification for the vendors when choosing system equipment and components with failure rates higher than $1 \cdot 10^6$ failures/hour.

The conclusions for the method evaluation part are:

- None of the evaluated methods was able to answer all questions related to reliability that are relevant in early design phases.
- Their applicability also shifts depending on the system analyzed.
- FTA can be a powerful tool when breaking down the safety requirements of the system, while MA is appropriate when modeling the states of a system. RBD is best for communicating reliability within the project with team members who are not reliability engineers.
- The time consumed when working with a certain method also depends on the software tool that is used.
- The choice of which reliability methods to use during the concept phase should be taken after weighting several factors, e.g.
  - the type of system being analyzed,
  - questions to be answered,
  - the component and equipment data that can be collected and
  - modeling possibilities in the software tools available.

### 5.3.2 Choosing the right reliability method

The choice of method for reliability depends on the design schedule, the problem to solve and competence and resources allocated. Depending on the industry, several standards such as those presented in references, or standards issued by organizations like International Standardization Organization (ISO) and the European Commission for Space Standardization (ECSS), procedures and guidelines such as for example [5] are available, to outline a standard practice for conducting reliability studies. Even though there are standards and handbooks available, choosing the best fitting reliability method is still not an easy task. Often several methods can be applied and none of them will fit perfectly. The aim of paper [II] is to create a short guideline for choosing the best fitting reliability method, based on the combination of system characteristics and the objective.

Like in the paper [I], according to Figure 10, the methods studied are also the most common methods available in commercial software tools: RBD, FT, ET, MA and PN (or Stochastic Petri Network - SPN). The first aspect taken into consideration in order to determine the choice of method is the system characteristics. Five general categories A to E are considered in this guideline, each of them with two mutually exclusive answers: system behaviour: static or
dynamic, type of system: prototype or serial, the system parts type: mostly mechanical/electromechanical or electronic parts, repairable or un-repairable system, safety or non-safety critical system. Due to possibility of several methods to fit a certain system characteristic, the suitability of each method is graded from 1 to 3 points, where 3 points means that the method fits well, 2 points means that the method fits well with some exceptions and one point means that the method does not fit very well but it is possible to apply, or when used as qualitative method it fits well, but not when used as quantitative method.

The second aspect taken into consideration is the scope of the analysis and is defined by means of six categories 1 to 6 as questions with regard to: system or mission reliability/unreliability, states probabilities, failure scenarios and system behaviour/qualitative analysis. The same fitting method as for system characteristics is also used for scope of analysis as well. The applicability of each of the five chosen methods is assessed for all possible combinations of system characteristics (32 scenarios) and scope of analysis (6 scenarios) giving a total of 192 answers concerning the method and its applicability. An example of scenarios is presented in the Table 1. A complete list of scenarios and how they can be used can be found in paper [II].

<table>
<thead>
<tr>
<th>Scenario no.</th>
<th>System Reliability/Unreliability</th>
<th>State Probabilities</th>
<th>Failure Scenarios/Probability of an unwanted event</th>
<th>Failure Scenarios/Consequences for given events</th>
<th>Mission Reliability/Unreliability</th>
<th>System behaviour Qualitative analysis (barrier efficacy, sequence dependent failure scenario, etc)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>MA(*) 12</td>
<td>MA(*) 12</td>
<td>FT(<em>) 10, MA(</em>) 12</td>
<td>ET(*) 9</td>
<td>MA(*) 12</td>
<td>MA(<em>) 12, FT(</em>) 10, ET(<em>) 9, SPN(</em>) 11</td>
</tr>
<tr>
<td>2</td>
<td>MA(*) 12</td>
<td>MA(*) 12</td>
<td>MA(*) 12</td>
<td>ET(*) 7</td>
<td>MA(*) 12</td>
<td>MA(<em>) 12, ET(</em>) 7, SPN(*) 11</td>
</tr>
<tr>
<td>3</td>
<td>MA(*) 12</td>
<td>MA(*) 12</td>
<td>FT(<em>) 12, MA(</em>) 12</td>
<td>ET(*) 10</td>
<td>MA(*) 12</td>
<td>MA(<em>) 12, FT(</em>) 12, ET(<em>) 10, SPN(</em>) 9</td>
</tr>
<tr>
<td>4</td>
<td>MA(*) 12</td>
<td>MA(*) 12</td>
<td>MA(*) 12</td>
<td>ET(*) 8</td>
<td>MA(*) 12</td>
<td>MA(<em>) 12, ET(</em>) 8, SPN(*) 9</td>
</tr>
<tr>
<td>5</td>
<td>MA(*) 13</td>
<td>MA(*) 13</td>
<td>MA(<em>) 13, FT(</em>) 9</td>
<td>ET(*) 9</td>
<td>MA(*) 13</td>
<td>MA(<em>) 13, ET(</em>) 9, FT(<em>) 9, SPN(</em>) 13</td>
</tr>
</tbody>
</table>

Table 1 Choice of method considering both scope of analyses and system characteristics

If two methods are equal qualified to answer one category of questions depending on system characteristics (see for example Table 1, scenario no. 3, questions about failure scenarios/
probability of an unwanted event), the points grading the methods (paper [II], table 2) are added to each method and the final result will be different. In chosen example the scenario no.3 from Table 1 becomes as bellow.

<table>
<thead>
<tr>
<th>Scenario no.</th>
<th>System Reliability/Unreliability</th>
<th>State Probabilities</th>
<th>Failure Scenarios/Probability of an unwanted event</th>
<th>Failure Scenarios/Consequences for given events</th>
<th>Mission Reliability/Unreliability</th>
<th>System behaviour Qualitative analysis (barrier efficacy, sequence dependent failure scenario, etc)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>MA(*) 15</td>
<td>MA(*) 15</td>
<td>FT(<em>) 15, MA(</em>) 14</td>
<td>ET(*) 13</td>
<td>MA(*) 15</td>
<td>MA(<em>) 15, FT(</em>) 15, ET(<em>) 13, SPN(</em>) 12</td>
</tr>
</tbody>
</table>

Table 2 Extension of Table 1

The aspects analyzed here have been chosen to be as general as possible and tested on different systems in order to verify the applicability of the guideline. This guideline can improve the selection of appropriate reliability method in early design phases, but its practical use it is still to be demonstrated.

There are some drawbacks such as the limited number of methods considered (only five), and considerations regarding system knowledge. Software reliability is not considered and neither is the failure data source and relevance. In future work, several methods will be considered as well as a possible connection to the failure data.

_We are all in the gutter, but some of us are looking at the stars._

– Oscar Wilde
Optimizing Reliability and Safety in Early Design Phases

One challenge for the engineer is to design a system that will achieve the desired reliability of the system and meet the system safety requirements while performing all of the system’s intended functions at a minimum cost. Can system safety, reliability and costs be balanced against each other? When a choice has to be made between different vendors, an optimization involving objectives such as reliability, system safety and costs is seldom performed to rate the systems.

The aim of paper [III] is to find out if it is possible to find a set of promising design alternatives by optimizing the system safety, reliability and costs of the system in early design phases. A method is suggested and applied on an overall concept of a basic aircraft system (electrical power system), the same concept used in paper [I].

6.1 Proposed Method

In the method suggested in Figure 12, the overall system safety requirements are taken into consideration as well as reliability goal and the analysis is performed bottom-up, using the vendor provided preliminary failure data. A dynamic method for calculation of probabilities and the existing failure data (such as failure intensities), and the associated costs for every part included in the system, are used to find the optimal solutions for the design.
The desired solution is the one with the lowest probabilities of occurrence for the system safety states, the highest probabilities of occurrence for reliability states and the lowest costs. As these objectives are naturally contradictory, one design seldom meets these goals.

During Step 1, models for System Safety, Reliability and Cost are created. Given the usually known failure information and architecture of the system, the states of the system such as full functionality, degraded or partial loss, loss of redundancy or total loss of the system are usually known already in the concept phase. Some of the states are considered system safety states and have certain quantitative requirements, while others may relate to reliability with associated reliability goals. The suggested method when modeling both system reliability and safety is therefore Markov analysis [104]. The cost of system development can vary depending on the application and a generic model is therefore used in paper [III]. After the models are established, the question is if our models really serve their purpose.

In Step 2, the models built for system safety, reliability and costs are validated and verified. Both the reliability and system safety model and the design cost model are validated by solving the models, one by one, for one set of parameters. The results, obtained by solving each model, will be compared with previous results from similar designs and field experience. If the results are considered to reflect reality, all models will be linked together and solved. If the results are still considered to reflect reality, move to the next step, optimization.

Step 3 is allocated to the optimization. The problem considered is multi-objective in character with objectives such as system cost ($f_1$), system reliability ($f_2$), and system safety (or the probability of unwanted events) ($f_3$). The problem is to find the optimal vendor for each piece of equipment in order to maximize system safety and reliability and minimize the development cost. There may also be constraints that need to be considered as well, for example on the probabilities for different system states or costs.

The mathematical nature of the different objectives differs. The most simple is the cost objective, which is deterministic and linear. However, both the system safety and the reliability objectives are stochastic and non-linear and the overall problem is thus a stochastic non-linear integer problem, which is a challenging optimization problem to solve.

The mathematical nature of the different objectives differs. The most simple is the cost objective, which is deterministic and linear. However both the system safety and the reliability
objectives are stochastic and non-linear. Hence the overall problem is a stochastic non-linear integer problem, which is a challenging optimization problem to solve.

6.2 Application

One question regarding choice of case study is how advanced the design must be in order for the results to be relevant? How early in the development process according to Figure 10 may, the method described in sections 2 and 3, be applied? A functional model has been determined as well as a preliminary system architecture. The established functions (the same as used in paper [1]) can be realized by equipment that can be purchased from different vendors. Depending on the vendor, the equipment has different costs, and different uncertainty data or failure data information such as failure rates or Mean Time Between Failures (MTBF).

The method used to model reliability and safety is MA. When a functional model, as well as preliminary system architecture, has been determined, there is also knowledge about possible states of the system. The analyzed states in this application are presented in Table 2 and used to build the Markov time-continuous model for system safety and reliability, according to Figure 12.

<table>
<thead>
<tr>
<th>State</th>
<th>Type of State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>success</td>
<td>electrical power supply to all a/c systems (AC/DC)</td>
</tr>
<tr>
<td>b</td>
<td>degraded</td>
<td>loss of main power supply (MGen fault)</td>
</tr>
<tr>
<td>c</td>
<td>degraded, safety critical state</td>
<td>total loss of AC</td>
</tr>
<tr>
<td>d</td>
<td>failed (absorbing state)</td>
<td>no electrical power supply to a/c systems to sustain flight</td>
</tr>
<tr>
<td>e</td>
<td>redundancy loss</td>
<td>loss of emergency power supply</td>
</tr>
<tr>
<td>f</td>
<td>degraded</td>
<td>double rectifier loss</td>
</tr>
<tr>
<td>g</td>
<td>redundancy loss</td>
<td>loss of auxiliary power supply</td>
</tr>
<tr>
<td>h</td>
<td>degraded</td>
<td>loss of main power supply (PTS, AGB fault)</td>
</tr>
<tr>
<td>l</td>
<td>redundancy loss</td>
<td>loss of TRU 1 or 2</td>
</tr>
<tr>
<td>m</td>
<td>redundancy loss</td>
<td>loss of all redundancy (auxiliary and emergency)</td>
</tr>
</tbody>
</table>

Table 3 State Description for the chosen Case Studied

A state transition diagram is built as presented in paper [III] and the transition matrix associated with it has the form:

\[
\begin{bmatrix}
1 - \lambda_{ab} - \lambda_{ah} - \lambda_{ac} - \lambda_{af} - \lambda_{ag} & \lambda_{ab} & \lambda_{ac} & \lambda_{ah} & \lambda_{af} & 0 & 0 & 0 & 0 \\
0 & 0 & 1 - \lambda_{bc} & \lambda_{bc} & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 - \lambda_{cd} & \lambda_{cd} & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 - \lambda_{em} & \lambda_{em} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 - \lambda_{fg} - \lambda_{pf} & \lambda_{fg} & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 - \lambda_{gm} - \lambda_{mg} & \lambda_{gm} & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 - \lambda_{mf} & \lambda_{mf} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0
\end{bmatrix}
\]
The elements of transition matrix consist of the departure rates from state $i$ to state $j$ (such as $\lambda_{ab}$, $\lambda_{bc}$, etc) and the diagonal elements denote the rate of the system remaining in state $i$ through the time interval $\Delta t$.

The notations used in the cost model are presented in Table 3 and a simplified cost model taking into consideration the basic costs for a design is given by

$$ C = C_{eq} + C_{comp} + C_{pers} \quad (1) $$

where $C_{eq} = \text{costs of equipment purchase}$, $C_{comp} = \text{costs for components/installation purchase}$ and $C_{pers} = \text{costs for personnel (hours needed for integration work)}$.

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
<th>Notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$C_{AGB}$</td>
<td>costs for a/c Gear Box</td>
<td>$C_{spec}$</td>
<td>costs for specialists</td>
</tr>
<tr>
<td>$C_{PTS}$</td>
<td>costs for PTS</td>
<td>$C_{tec}$</td>
<td>costs for technicians,</td>
</tr>
<tr>
<td>$C_{MGen}$</td>
<td>costs for MGen</td>
<td>$C_{ost}$</td>
<td>costs for other personnel</td>
</tr>
<tr>
<td>$C_{AuxGen}$</td>
<td>costs for AuxGen</td>
<td>$C_{eng}$</td>
<td>costs for engineers</td>
</tr>
<tr>
<td>$C_{AuxGB}$</td>
<td>costs for AuxGB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$C_{TB}$</td>
<td>costs for TB</td>
<td>$h_1$</td>
<td>engineers hours</td>
</tr>
<tr>
<td>$C_{TRU}$</td>
<td>costs for TRU</td>
<td>$h_2$</td>
<td>specialist hours</td>
</tr>
<tr>
<td>$C_{batt}$</td>
<td>costs for a/c Battery</td>
<td>$h_3$</td>
<td>technicians hours</td>
</tr>
<tr>
<td>$C_{MLC}$</td>
<td>costs for MLC</td>
<td>$q_{bus}$</td>
<td>no. of fuses</td>
</tr>
<tr>
<td>$C_{rel}$</td>
<td>costs for relays</td>
<td>$h_4$</td>
<td>administration hours</td>
</tr>
<tr>
<td>$C_{swi}$</td>
<td>costs for switches</td>
<td>$h_5$</td>
<td>time for other personal</td>
</tr>
<tr>
<td>$C_{bus}$</td>
<td>costs for fuses</td>
<td>$q_{bus}$</td>
<td>meter of bus bar</td>
</tr>
<tr>
<td>$C_{fus}$</td>
<td>costs for bus bar</td>
<td>$q_{rel}$</td>
<td>no. of relays</td>
</tr>
<tr>
<td>$C_{con}$</td>
<td>costs for contactors</td>
<td>$q_{swi}$</td>
<td>no. of switches</td>
</tr>
<tr>
<td>$C_{adm}$</td>
<td>costs for administration personal</td>
<td>$q_{adm}$</td>
<td>no. of contactors</td>
</tr>
</tbody>
</table>

Table 4 Notations used in the cost model

The optimization problem has been formulated in different ways, one being to find the optimal solution that will balance the cost against the probability of occurrence of some chosen states. The objective function can be stated as:

$$ \min f(x) = \alpha \cdot f_1(x) + \beta_2 \cdot \text{probability}_2(x) \quad (2) $$

where $\alpha$ and $\beta$ are weighting factors according to the designer requirements and $z$ is the analyzed state(s), $f_1(x)$ is the cost function for a design vector $x$, $\text{probability}_2(x)$ = probability of given state (such as $f_2(x)$ for state $a$, $f_3(x)$ for state $d$) for the given design vector $x$, and $x$ has the form $x = [x_1 \ x_2 \ \ldots \ x_n]$ where $x_i$ represent the choice of vendor for a particular equipment.
Due to the nature of the optimization problem, the optimization technique used in paper [III] is based on a Genetic Algorithm (GA). Some of the results are presented in the Table 4 bellow and for more details about the results, see paper [III].

The first solution (row 1 in Table 4) is the one with the lowest costs. However, this solution is not acceptable from a system safety and reliability point of view. The second solution (row 2 in Table 4) is the most expensive one (almost double the cost). Also solutions no.3 and 4 are too expensive. The best solution from a system safety and reliability point of view is no. 4. The design cost, however, is unacceptable. Solutions no. 5, 7, 8 and 9 are totally unacceptable from a safety point of view (too high probability of total loss of AC power supply). Solution no. 6 is acceptable from a safety point of view and also from a cost point of view. The reliability goal is not met. However, due to the low difference in probability (7e-04), it is still the best choice for the design. The slight difference can be overcome during the detailed design stage, for ex-ample by reviewing the maintenance policies and/or the operational profile.

The advantages of the suggested method are:

- The combination of one model for reliability and system safety with one model for cost and one optimization algorithm provides an overview of the problem with all its aspects.
- A handful of good solutions are obtained for this trade-off, helping the designer with a good base for decision making.

The drawbacks are related to the practical implementation and integration with the existent design processes and tools and are a subject for future study.

<table>
<thead>
<tr>
<th>No</th>
<th>Cost [millions SEK]</th>
<th>State a probability</th>
<th>State c probability</th>
<th>State d probability</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5.912</td>
<td>0.9940</td>
<td>3.99e-04</td>
<td>1.52e-07</td>
<td>[2 3 3 4 2 1 4 3 2]</td>
</tr>
<tr>
<td>2</td>
<td>10.14</td>
<td>0.9983</td>
<td>8.12e-06</td>
<td>2.02e-08</td>
<td>[3 3 1 1 1 2 4 4 1]</td>
</tr>
<tr>
<td>3</td>
<td>8.754</td>
<td>0.9978</td>
<td>8.04e-06</td>
<td>6.72e-08</td>
<td>[3 2 1 4 4 4 3 1]</td>
</tr>
<tr>
<td>4</td>
<td>7.872</td>
<td>0.9988</td>
<td>8.04e-06</td>
<td>2.02e-08</td>
<td>[4 3 1 4 1 4 4 1]</td>
</tr>
<tr>
<td>5</td>
<td>6.197</td>
<td>0.9942</td>
<td>3.99e-04</td>
<td>6.54e-08</td>
<td>[2 3 4 4 2 1 4 1 2]</td>
</tr>
<tr>
<td>6</td>
<td>6.247</td>
<td>0.9943</td>
<td>8.07e-06</td>
<td>8.36e-08</td>
<td>[2 3 4 4 2 1 4 3 1]</td>
</tr>
<tr>
<td>7</td>
<td>6.217</td>
<td>0.9977</td>
<td>3.99e-04</td>
<td>6.40e-08</td>
<td>[1 3 4 4 2 1 4 1 2]</td>
</tr>
<tr>
<td>8</td>
<td>6.238</td>
<td>0.9972</td>
<td>3.99e-04</td>
<td>6.02e-08</td>
<td>[1 2 3 4 2 1 4 1 2]</td>
</tr>
<tr>
<td>9</td>
<td>6.236</td>
<td>0.9980</td>
<td>3.99e-04</td>
<td>6.39e-08</td>
<td>[3 3 4 4 2 1 4 1 2]</td>
</tr>
</tbody>
</table>

Table 5 Selection of results
Creativity requires the courage to let go of certainties.

– Erich Fromm
Discussion & Conclusions

This thesis has aimed to develop a methodology for analysis and optimization of system safety and reliability in early design phases. Performing optimization considering requirements that are often contradictory, e.g. high mission reliability, low accident risk, contribution value and low cost have also been included in the scope of this thesis.

The contributions of this work (including papers [I], [II] and [III]) are described in this section, as well as conclusions including answers to research questions (from section 1.4) and future work.

7.1 Contributions

In general, this work has contributed by increasing focus on using system safety and reliability methods and models in early design phases as well as combining them with optimization techniques. Several commonly used methods have been evaluated. In an attempt to overcome the differences between the researchers focus and respective industry focus on reliability studies, a guideline for how to choose between different methods has been proposed. The system safety requirements, reliability goals and costs have been balanced against each other and a method has been suggested. Contributions per paper are listed below.

Paper [I]: The main contribution of this paper is to evaluate the applicability of different reliability methods for analyzing an overall system concept in early development stages. Furthermore, the paper constitutes the first step in a methodology intended to address the issues outlined above from a practical point of view. Two static methods (RBD and FTA), and one dynamic method (MA), have been applied to conceptual design of an aircraft electrical system. These three methods have been evaluated regarding usefulness, modeling possibilities and applicability in early design phases.

Paper [II]: This paper presents a guideline for choosing the best suited reliability method in early design phases, from two aspects: objective and system characteristics. The main
contribution of this paper is the guideline itself and how it can improve the selection of appropriate reliability method in early design phases. The applicability should be on any technical system, but is tested only on basic aircraft systems. The methods studied are the most common methods available in commercial software tools: RBD, FT, ET, MA and SPN. The applicability of each of the five chosen methods is assessed for all possible combinations of system characteristics and objective.

Paper [III]: The main contribution of this paper is the suggested method to find a set of promising design alternatives (represented by choosing different equipment suppliers), by optimizing the system safety, reliability and costs of the system in early design phases. The method is thought to be general, applicable on any technical system which in itself is a contribution. This paper proposes an approach capable of investigating the trade-offs described above, combining the techniques for system safety and reliability analysis with optimization methods. Markov analysis is employed for modeling the system safety and reliability characteristics and a Genetic Algorithm is used for optimization. The result is the selection of suppliers for each component in the system in order to achieve a balance between system safety, reliability and other design objectives.

7.2 Conclusions

The research questions defined in section 1.4 have been investigated during this project and answers are discussed below.

RQ1 Which reliability method is best to use in early design phases?

Answer RQ1: There is no single method able to give all the relevant answers in early design phases. Different methods will address different questions.

In paper [I], the evaluated methods are RBD, FT and MA. None was able to answer all questions related to reliability that are relevant in early design phases. FTA can be a powerful tool when breaking down the safety requirements of the system, while MA is appropriate when modeling the states of a system and RBD is best for communicating reliability within the project with team members who are not reliability engineers. Their applicability also shifts depending on the system analyzed. The time consumed when working with a certain method also depends on the software tool that is used. The reliability methods to use during the concept phase should be chosen after weighing several factors, e.g. type of system being analyzed, questions to be answered, the component and equipment data that can be collected and modeling possibilities in the software tools available.

RQ2 a) May a guideline be issued, which shows how to choose the appropriate reliability and/or system safety method in early design phases?

   b) How relevant is it in every day engineering practice?
Answer RQ2: a) Paper [II] is one such example. However, this guideline is issued to analyze five different methods, considering the systems characteristics and the analysis objective. There are some drawbacks such as the limited number of methods considered (only five), and considerations regarding system knowledge. Software reliability is not considered and neither is the failure data source and relevance.

b) The aspects analyzed here were chosen to be as general as possible and tested on different systems in order to verify the applicability of the guideline. However, the engineer will sometimes be forced to consider other aspects than those analyzed, such as the capability of the reliability tool used, field experience, time and resources allocated, etc.

RQ3 a) Can system reliability and safety be optimized in the concept phase?

b) Can this help us in the process of choosing the equipment and components of our system?

c) How can the optimization be done?

Answer RQ3: a) Yes, it can. However, in order to find more relevant answers, the author has chosen in paper [III] to analyze an early design phase. A functional model have been determined as well as a preliminary system architecture. The established functions can be realized by equipment that can be purchased from different vendors in order to analyze the next part of the RQ3.

b) Yes, this aspect has been considered in the analysis. The result of the optimization is the selection of suppliers for each component in the analyzed system, in order to achieve a balance between system safety, reliability and costs.

c) A method (paper [III]) has been suggested to find a set of promising design alternatives by optimizing system safety, reliability and cost of the system in early design phases. This method has three steps:

- Model building for cost and system reliability and safety;
- Validation and verification of model
- Optimization

The suggested method has been applied to the case studied of the overall concept of an aircraft’s electrical power system. Markov analysis is employed for modeling the system safety and reliability characteristics and a Genetic Algorithm is used for optimization. The result obtained is the selection of suppliers for each component in the system.
7.3 Future Work

There are two ideas rising different questions:

**FW1:** The methodology proved applicable but must mature viewed from two aspects:
- **Modeling and validation**
  The cost model must be robust and linked to the company’s IT systems. More emphasis should also be placed on life-cycle costs. If possible uncertainties in input data can also be added to the analysis. An alternative to Markov analysis to model system reliability should be investigated, eg. FTA and RBD. The link between the cost model and the reliability of the model is also of interest to investigate further in order to improve the methodology.
- **Optimization - studying different ways to formulate the optimization problem.**
  Within this project, it has been shown that it is possible to formulate and solve this problem with the help of optimization but can it be done in a more efficient way? What should be optimized and what should be the constraints? How to treat the multi-objective nature of the problem? What compromises should be considered and how should the problem be formulated mathematically in the most efficient way possible? Within this project one type of algorithm is used, but it needs to be streamlined and refined to be integrated in the company’s development process.

**FW2:** Evaluate the ability of the methodology to be integrated / connected to the tools used for system security in the industry today.
This part aims to ensure that the developed methodology can be implemented in industry and that it can be integrated with or connected to the tools used in industry today. In order to ensure that the developed methodology answers the right questions and properly implemented, new case studies should be analyzed. Also the computational aspects of the optimization problem need to be addressed when solving large industrial problems. Care need to be taken in order to be able to formulate the problem and solve it in a time efficient manner.
References


[7]. Kazeminia, A, Junglas, M., Söffker, D., (2010). Optimization of system component reliability characteristics at early design stage with economically reasonable uncertainty level, Taylor& Francis, s. 5.


[30]. Walter A Shewhart, 1924 and the Hawthorne factory (2006) at

http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2464836/

**US Standards, Handbooks and Procedures**


**UK Standards**

[52]. DEF STAN 00-40 *Reliability and Maintainability (R&M)*

[53]. DEF STAN 00-40 PART 1: Issue 5: *Management Responsibilities and Requirements for Programmes and Plans*

[54]. DEF STAN 00-40 PART 4: (ARMP-4) Issue 2: *Guidance for Writing NATO R&M Requirements Documents*

[55]. DEF STAN 00-40 PART 6: Issue 1: *In-service R & M*

[56]. DEF STAN 00-40 PART 7 (ARMP-7) Issue 1: *NATO R&M Terminology Applicable to ARMP’s*

[57]. DEF STAN 00-42 *Reliability and maintainability assurance guides*

[58]. DEF STAN 00-42 PART 1: Issue 1: *One-shot devices/systems*

[59]. DEF STAN 00-42 PART 2: Issue 1: *Software*

[60]. DEF STAN 00-42 PART 3: Issue 2: *R&M Case*

[61]. DEF STAN 00-42 PART 4: Issue 1: *Testability*

[62]. DEF STAN 00-42 PART 5: Issue 1: *In-service reliability demonstrations*

[63]. DEF STAN 00-43 *Reliability and maintainability assurance activity*

[64]. DEF STAN 00-43 PART 2: Issue 1: *In-service maintainability demonstrations*

[65]. DEF STAN 00-44 *Reliability and maintainability data collection and classification*

[66]. DEF STAN 00-44 PART 1: Issue 2: *Maintenance data & defect reporting in the royal navy, the army and the royal air force*

[67]. DEF STAN 00-44 PART 2: Issue 1: *Data classification and incident sentencing - general*

[68]. DEF STAN 00-44 PART 3: Issue 1: *Incident sentencing - sea*
[69]. DEF STAN 00-44 PART 4: Issue 1: *Incident sentencing - land*

[70]. DEF STAN 00-49 Issue 1: *Reliability and maintainability mod guide to terminology definitions*

[71]. SAE ARP4761, *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*

**French Standards**


**International Electro-Technical Commission Standards**

[73]. IEC 60300 *Dependability management*

[74]. IEC 60300 -1 *Dependability management. Dependability management systems*

[75]. IEC 60300 -2 *Dependability management. Guidelines for dependability management*

[76]. IEC 60300 -3-1 *Dependability management. Application guide - Analysis techniques for dependability*

[77]. IEC 60300-3 -3 *Dependability management. Application Guide*

[78]. IEC 60300-3 -10 *Dependability management. Maintainability*

[79]. IEC 60300 -3-11 *Dependability management. Reliability centred maintenance*

[80]. IEC 60300 -3-12 *Dependability management. Integrated logistic support*

[81]. IEC 60300 -3-2 *Dependability management. Collection of dependability data from the field*

[82]. IEC 60300 -3-3 *Dependability management. Life cycle costing*

[83]. IEC 60300 -3-4 *Dependability management. Guide to specification of dependability*

[84]. IEC 60300 -3-5 *Dependability management. Reliability test conditions and statistical principles*

[85]. IEC 60319 *Presentation of reliability data for electronic components*
[86]. IEC 60410 Sampling plans and procedures for inspection by attributes

[87]. IEC 60605 Equipment reliability testing

[88]. IEC 60706 Maintainability of equipment

[89]. IEC 60706-1 Maintainability of equipment Introduction, requirements and maintainability program

[90]. IEC 60706-2 Maintainability of equipment Maintainability requirements and studies during the design and development phase

[91]. IEC 60706-3 Maintainability of equipment Verification and collection, analysis and presentation of data

[92]. IEC 60706-5 Maintainability of equipment Diagnostic testing

[93]. IEC 60812 Analysis Techniques for system reliability - Procedure for FMEA

[94]. IEC 61014 Programs for reliability growth

[95]. IEC 61025 Fault Tree Analysis (FTA)

[96]. IEC 61070 Compliance test for steady-state availability

[97]. IEC 61078 Analysis techniques for dependability - Reliability block diagrams and boolean methods

[98]. IEC 61124 Reliability testing - Compliance test for constant failure rate and constant failure intensity

[99]. IEC 61050 Design Review

[100]. IEC 61163 Reliability stress screening

[101]. IEC 61163-1 Reliability stress screening. Repairable assemblies manufactured in lots

[102]. IEC 61163-2 Reliability stress screening. Electronic components

[103]. IEC 61164, Reliability growth - Statistical test and estimation methods

[104]. IEC 61165, Application of Markov techniques

[105]. IEC 61649, Goodness-of-fit tests, confidence intervals and lower confidence limits for Weibull distributed data

[106]. IEC 61650, Reliability data analysis techniques - Procedures for comparison of two
constant failure rates and two constant failure (event) intensities.

[107]. IEC 61703, Mathematical expressions for reliability, availability, maintainability and maintenance support terms

[108]. IEC 61713, Power law model - Goodness-of-fit tests and estimation methods

[109]. IEC 61882, Hazard and operability studies (HAZOP) - Application Guide

[110]. IEC 62198, Project risk management - Application guide

[111]. IEC 62502, Analysis techniques for dependability – Event Tree Analysis

[112]. IEC 62551, Analysis Techniques for Dependability-Petri Net techniques

International Standards Organization

[113]. ISO 8402, (1986). Quality Vocabulary