Proceedings of the 20th

AR² TS

Advances in Risk and Reliability Technology Symposium

21–23 May 2013

Edited by Lisa Jackson and John Andrews

Institution of MECHANICAL ENGINEERS

Safety and Reliability Society

Royal Statistical Society Founded 1834

Loughborough University

Proceedings of the 20th

Advances in Risk and Reliability Technology Symposium

21st – 23rd May 2013

Burleigh Court Conference Centre

Loughborough, Leicestershire, UK

Published by:

Loughborough University
Loughborough
Leicestershire, LE11 3TU
United Kingdom

ISBN 978-1-907382 61 1

CONTENTS

20th Advances in Risk and Reliability Technology Symposium (AR^{2}TS)

Foreword

A warm welcome to Loughborough and the Advances in Risk and Reliability Technology Symposium (AR^{2}TS). These proceedings represent the latest developments in the fields of risk and reliability, covering research as well as industrial case studies. The symposium aims to bring together like minded engineers and scientists striving to push forward the boundaries for implementation, development and improvement of risk and reliability techniques. It is hoped that the symposium will encourage creative discussion of traditional and innovative technologies, enable knowledge sharing and the formation of new collaborative opportunities.

This year's proceedings contain 34 papers, representing the work of authors across the industrial and academic domains. A broad spectrum of techniques are addressed in the areas of systems reliability assessment, hazard and risk analysis, maintenance planning and optimisation, fault diagnostics, data collection, asset management, software reliability, availability modelling and lifecycle costs. The discipline areas covered are power systems, railways, hospitals, road networks, electronics, water industry, design processes, jet engines, wind turbines, renewable heat, aircraft, and bridges.

There is an encouraging mix of academics and industrialists, from both the UK and overseas. This year sees authors from UK Universities in Durham, Edinburgh, Loughborough, Nottingham and Strathclyde. There are also authors from overseas Universities in Canada, Italy, Germany, Sweden, Netherlands and Switzerland. Companies who have contributed to research include Aero Engine Controls, BC Hydro (Canada), GL Noble Denton, the Lithuanian Energy Institute, , the Ministry of Defence, Network Rail, Riyadh Military Hospital (Saudi Arabia), RSSB, SAAB Aeronatics (Sweden), Scottish Water, and TÜV Rheinland InterTraffic GmbH (Germany).

We have the pleasure this year of three key note speakers. Professor Roy Billinton, from the University of Saskatchewan in Canada, will discuss the predictive and past performance assessment of power system reliability. Andy Kirwan, from Network Rail will discuss some of the latest approaches and issues in railway asset management. The final key note speaker will be Sara Goodacre, from the University of Nottingham, who will describe the mechanisms used by nature to enable survival and also touch on how biological means can be used to represent the failures occurring in engineering systems.

It is encouraging to see that young blood is taking on the challenge of research in this area, with a number of young researchers presenting their ideas this year. Prizes will be presented for the IMechE Best Young Researcher paper/poster and an award from the Safety and Reliability Society (SaRS) for the best practical paper.

Thanks go to the Programme Committee for their contributions to this symposium, the administrative support at Nottingham, and of course you the participants, whom we hope will contribute to a friendly and stimulating event. I hope you can join the Committee in the extra curricula activities of a wine reception (sponsored by SAGE) and conference dinner on the respective evenings.

Dr Lisa Jackson
Prof John Andrews

AR2TS Programme		
Tuesday 21st May		
10.00-10.10	**Introduction and Welcome**	John Andrews
10.10-11.00	**Keynote:** Roy Billinton (University of Saskatchewan, Canada) **Predictive and Past Performance Assessment of Power System Reliability**	Chair: John Andrews
11.00-11.15	**Coffee**	
11.15-12.45	Monte Carlo Methods	Chair: Frank Coolen
11.15-11.45	A System-wide Modelling Approach to Railway Infrastructure Asset Management	Dovile Rama and John Andrews
11.45-12.15	Analysis of the Contributions to the Performance of a Functional Product Design using Simulation	Sean Reed, Magnus Löfstrand, Lennart Karlsson, John Andrews
12.15-12.45	Modelling the Deferred Impact of Failures when Considering the Availability of Production Systems	Jelena Borisevic and Mark Rogers
12.45-13.45	**Lunch**	
13.45-15.00	**Poster Presentations**	Chair: Sarah Dunnett
13.45-14.00	A Markov Modelling Approach to Railway Bridge Asset Management	Bryant Le and John Andrews
14.00-14.15	Fault Tree Analysis of Polymer Electrolyte Fuel Cells to Predict Degradation Phenomenon	Mike Whiteley, Lisa Bartlett and Sarah Dunnett
14.15-14.30	Maintenance Planning in a Saudi Arabian Hospital	Hesham Alzaben, Chris McCollin, and Lai Eugene
14.30-14.45	Fault Diagnostics for Railway Point Machines	Marius Vileiniskis, Rasa Remenyte-Prescott, Dovile Rama, and John Andrews
14.45-15.00	Probabilistic Analysis of Renewable Heat Technologies	Adam Thirkill and Paul Rowley
15.00-15.30	**Poster Discussions and Coffee**	
15.30-17.00	**Risk and Safety Assessment**	Chair: John Catchpole
15.30-16.00	Quantifying Technical Risks: Insights into Theory-Practice Tensions in the Elicitation Process and Method	Gillian Anderson, Matthew Revie, Lesley Walls
16.00-16.30	On Combined Data Under Competing Risks	Tahani Coolen-Maturi and Frank P. A. Coolen
16.30-17.00	Towards a Failsafe Flight Envelope Protection: The Recovery Shield	John Stoop
6.00pm	Wine Reception (sponsored by SAGE)	
Wednesday 22nd May		
9.00-9.45	**Keynote:** Andy Kirwan, Julian Williams (Network Rail) **The Art and the Science of Whole Life Costing**	Chair: Lisa Jackson
9.45-11.15	**Rail Risk and Safety Assessment 1**	Chair: Lesley Walls
9.45-10.15	Localising Risk Estimates from the RSSB SRM	Chris Harrison
10.15-10.45	Use of a Generic Hazard List to Support the Development of Re-usable Safety Arguments in the Rail Industry	George Bearfield and Reuben McDonald
10.45-11.15	**Coffee**	
11.15-12.15	**Reliability Estimation 1**	Chair: Darren Prescott
11.15-11.45	Recent Advances in System Reliability using the Survival Signature	Frank Coolen, Tahani Coolen-Maturi, Abdullah H. Al-nefaiee, and Ahmad M. Aboalkhair
11.45-12.15	Degradation Test Analysis: A Case Study	Filippo De Carlo, Orlando Borgia, and Mario Tucci
12.15-13.15	**Lunch**	
13.15-14.30	**Poster Presentations**	Chair: Rasa Remenyte-Prescott
13.15-13.30	A Petri-Net Modelling Approach to Rail Track Geometry Maintenance and Inspection	Matthew Audley and John Andrews
13.30-13.45	Statistical Analysis to Reduce the Risk of Chest Injury for Older Occupants in Frontal Car Crashes	Karthikeyan Ekambaram, Richard Frampton, Lisa Bartlett
13.45-14.00	Asset Management of a Railway Signalling System	Raphaëlle Barbier Saint Hilaire, Darren Prescott and John Andrews

14.00-14.15	Modelling Railway Service Reliability	Claudia Fecarotti, Rasa-Remenyte-Prescott and John Andrews
14.15-14.30	Automatic Construction of a Reliability Model for a Phased Mission System	Kathryn Stockwell and Sarah Dunnett
14.30-15.00	**Poster Discussions and Coffee**	
15.00-17.00	**Analysis using Belief Network Approaches**	Chair: Jake Ansell
15.00-15.30	Using Deep Belief Networks for Predicting Railway Operations Failures	Olga Fink and Ulrich Weidmann
15.30-16.00	Bayesian Analysis of Electric Transmission Network Outages	Tomas Lešmantas and Robertas Alzbutas
16.00-16.30	Predictive and Diagnostic Analysis of a Holdup Tank by means of Dynamic Bayesian Networks	Daniele Codetta-Raiteri and Luigi Portinale
16.30-17.00	Condition Monitoring Data in the Study of Offshore Wind Turbines' Risk of Failure	Maria Segovia, Matthew Revie and Francis Quail
7.30pm	**Conference Dinner**	
Thursday 23rd May		
9.00-9.45	**Keynote:** Sara Goodacre (University of Nottingham) **Risk and Reliability: An Evolutionary Biologist's Perspective**	Chair: Lisa Jackson
9.45-10.45	**Asset Management**	Chair: Richard Denning
9.45-10.15	Long-term Asset Maintenance Optimization at Scottish Water	Travis Poole, Tom Archibald, Robert Murray and Jake Ansell
10.15-10.45	Road Network Flow Modelling for Maintenance	Chao Yang, Rasa Remenyte-Prescott and John Andrews
10.45-11.15	**Coffee**	
11.15-12.15	**Reliability Estimation 2**	Chair: John Andrews
11.15-11.45	Probabilistic Reliability and Risk Analysis for Systems of Fusion Device	Roman Voronov and Robertas Alzbutas
11.45-12.15	Aleatory Uncertainty in Power System Reliability Index Assessment	Roy Billinton and W Wangdee
12.15-13.15	**Lunch**	
13.15-14.45	**Reliability Case**	Chair: Lisa Jackson
13.15-13.45	Choosing the Reliability Approach – A Guideline for Selecting the Appropriate Reliability Method in the Design Process	Cristina Johansson, Per Persson, Michael Derelöv, and Johan Ölvander
13.45-14.15	Investigating Electronics Reliability in Business Jet Applications	Ian James
14.15-14.45	The Dependability Case is it Achievable	Richard Denning
14.45-15.15	**Coffee**	
15.15-16.15	**Railway Asset Management**	Chair: Luis Neves
15.15-15.45	Onboard, Real-Time Detection of Adhesion Levels in the Rail/Wheel Contact	Pete Hubbard, Chris Ward, Roger Dixon and Roger Goodall
15.45-16.15	Use of Bayesian Updating to Combine Experts' Opinion and Results of Inspection in Bridge Management	Luis Neves and Dan Frangopol
16.15-16.45	Stochastic State Space Methods for Railway Network Asset Management Modelling	Darren Prescott and John Andrews
16.45-17.00	**Awards and Close**	Richard Denning Lisa Jackson

Posters: 12 min presentation, 3 min change over
Presentations: 30 min slot - 25 min presentation, 5 min questions

Predictive and Past Performance Assessment of Power System Reliability

Roy Billinton, Power System Research Group
University of Saskatchewan, Canada

Electric power utilities collect considerable data on the past performance of individual system components and on how well the overall system performed it intended function. These data are also used to predict how the system will perform in the future and to evaluate the reliability of alternate expansion plans. This presentation will discuss a range of past reliability performance indices for bulk transmission and distribution systems and briefly illustrate the calculation of similar indices for predictive reliability assessment of future systems.

The Art and the Science of Whole Life Costing

Andy Kirwan and Julian Williams
Network Rail

Network Rail is one of the biggest asset management companies in the UK. In railway terms, we have the oldest system in the world and one of the busiest networks in Europe, with more train services than France, and more than Spain, Switzerland, The Netherlands, Portugal and Norway combined. We also have one of the safest rail networks, second only to Luxembourg in Europe, and one of the fastest growing, with a 50% increase in passenger journeys over the past decade and 30% more freight expected in the next five years.

The welcome increase in the demand for rail services presents a major challenge to asset managers – the people who plan and deliver work on the infrastructure. Additional trains increase the rate of asset degradation, restrict the time for access to the track to undertake preventive or restorative work, and exacerbate delays when failures occur. In parallel, there is a relentless drive for cost efficiencies, meaning the extra work needs to be done by fewer people.

To meet these challenges, we have had to rethink the way we prioritise work, to implement technological solutions that identify potential failures before they occur, and to devolve decisions to teams with a local understanding of the assets and close proximity to customers. To support this shift, we have introduced a whole life costing framework that puts customer service at the centre of decision making and provides consistency across asset disciplines and between business functions.

In this presentation, we will describe the approach taken, explain how it has been practically implemented, and show how the results have informed our investment plans for the next five years. Emphasis will be given to the models we have developed, the influence of uncertainties on decision making, and the compromises that are necessary to integrate ‘top down’ forecasts with ‘bottom up’ real world plans.

Risk and Reliability: An Evolutionary Biologist’s Perspective

Sara Goodacre
University of Nottingham

Evolutionary biologists study the process through which organisms adapt and survive. At the core of this process lies the generation of variation upon which natural selection acts. This can be viewed as an exploration of the different solutions that are possible for the same challenge (*i. e.* survival in a particular environment). The range

of solutions that is explored is rarely if ever exhaustive, being constrained by the time that an organism has had to adapt, and by the starting point, which is itself a product of previous evolutionary processes.

There are parallels between the evolutionary process described above and the search for optimum solutions in engineering designs. Survival (ie. non-failure of an engineered design) is maximised by searching for the optimal solution given known parameters. The search may or may not have been exhaustive and the 'solution' adopted is the best set of conditions found from those searched. There is a difference, however, in that evolution can and regularly does explore options of high risk whereas engineered solutions may not.

A study has been made of the literature on the evolution of bacterial and invertebrate genomes to ask to what extent the most successful solutions found by evolution to the challenge of survival favour redundancy, diversity or repair, or a combination of each of these.

Choosing the reliability approach - A guideline for selecting the appropriate reliability method in the design process

Cristina Johansson[1,2], Per Persson[2], Michael Derelöv[1], Johan Ölvander[1]
Department of Management and Engineering, Linköping University, Sweden
SAAB Aeronautics, Bröderna Uggla Gatan, Linköping, Sweden

Abstract
The main objective of a reliability study should always be to provide information as a basis for decisions e.g. concept choice, design requirements, investment, choice of suppliers, design changes or guaranty claim. The choice of reliability method depends on the time allocated for the reliability study, the design stage, the problem at hand and the competence and resources available.

During a reliability study the engineer focuses on providing a graphical means of evaluating the relationships between different parts of the system, gather or assess the reliability data for the components and interpret the results of the analyses. Even though the commercial software tools available claim to provide answers to most reliability questions, the choice of which method that is best suited is not an easy task. Often several methods can be applied and none of them will fit the purpose perfectly.

This paper presents a guideline for choosing the best suited reliability method in early design phases, from two aspects: objective and system characteristics. The methods studied are the most common methods available in commercial software tools: Reliability Block Diagram (RBD), Fault Tree (FT), Event Tree (ET), Markov Analysis (MA) and Stochastic Petri Network (SPN). The guideline considers two aspects, the characteristics of the system studied, and the scope of the analysis. The applicability of each of the five chosen methods is assessed for all possible combinations of system characteristics and objective. A study has been done on Saab Aeronautics in order to evaluate the practical use of the analysed methods and how this guideline can improve the selection of appropriate reliability method in early design phases.

1. Background and Scope

The main objective of a reliability study should always be to provide information as a basis for decision making e.g. concept choice from a reliability point of view, design requirements such as redundancy, functional redundancy, protections, warnings, choice of suppliers, design changes in order to meet the safety and reliability requirements, guaranty claim, maintenance strategies and investments etc. Traditionally, reliability engineering focuses on critical hardware parts of the system and most of the reliability methods have been developed accordingly. 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 (IEEE, 1998) and (IEC 60300-3-1, 2003), or standards issued by organizations like International Standardization Organization (ISO) and European Commission for Space Standardization (ECSS), procedures and guidelines as for example (NASA, 1990) and (FAA, 2000) are available, in order to outline a standard practice for conducting reliability studies. Even though there are standards and handbooks available, the choice of the best fitting reliability method is still not an easy task. Often several methods can be applied and none of them will fit perfectly.

Several traditional reliability methods are available, and are incorporated in commercial software tools as well as “in house” tools. The commercial software tools developers claim to give you answers to most questions while the researchers try to solve complex reliability problems by using new mathematical methods or new methodologies. But from an engineering point of view, the study must give reasonable answers as quick as possible with a minimum effort and invested time.

While the research focus within the reliability field is on the mathematical modelling, during a reliability study, the engineer focuses on providing a graphical means of evaluating the relationships between different parts of the system. The confidence of the answers he gets, depend 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.

The scope of this paper is to create a short guideline for choosing the best fitting reliability method, based on the combination of *system characteristics* and the *objective.*

2. Method and Analysis

There are many reliability methods and models (Rausand & Hoyland, 2004) developed in order to achieve more reliable and safe systems, and described in international standards and handbooks. According to (IEC 60300-3-1, 2003) one way of the methods to be classified is with regard to their main purpose: *methods for fault avoidance* (such as *Parts derating and selection*, *Stress-Strength Analysis* and *Part Count*), *methods for estimation of measures for basic events* (such as *failure rate prediction, human reliability analysis HRA, statistical reliability methods* or *software reliability engineering*) and *methods for architectural analysis and dependability assessment (allocation)*. The last category includes Failure Mode and Effect (and Criticality) Analysis (U.S. Department of Defence, 1980) or (IEC 60812, u.d.), Event Tree Analysis (IEC 62502, 2010), Fault Tree Analysis (IEC 61025, u.d.) or (Stamatelatos, et al., 2002), Zonal Analysis and Common Mode Fault (Federal Aviation Administration, 2000), Preliminary Hazard Analysis and Fault Hazard Analysis (MIL-STD-882D, 2000), Markov Analysis (IEC 61165, u.d.) and (International Electro-technical Commision, 2003), Petri Net Analysis (IEC 62551, 2012) or (ISO/IEC 15909, u.d.), Reliability Block Diagram (IEC 61078, u.d.), Common Cause Failure (Federal Aviation Administration, 2000) and (International Electro-technical Commision, 2003), and the list can continue.

The reliability methods considered in this paper are classical *methods for architectural analysis and dependability assessment* and the most common implemented in commercial software tools, such as: Reliability Block Diagram (RBD)- adopted for example to evaluate the reliability of three designs at both the functional and component level (O'Halloran, 2011), Fault Tree (FT)- one of the most popular method, used in many different applications, for example recently used to develop and analyse safety/security requirements for a gateway software (Kornecki & Liu, 2013), Event Tree (ET)- used often in early design phase in many applications, as for example to highlight common hazards arising from hydrogen storage and distribution systems, as well as to reveal potential accidents that hydrogen may yield under certain conditions (Rigas & Sklavounos, 2005), Markov Analysis (MA) and Stochastic Petri Network (SPN)- used for example to calculate the availability of safety critical on-demand systems (Kleyner & Volovoi, 2010) . The chosen methods can be used in conceptual design as well as all other design phases of a product development.

The variables taken into consideration in this paper in order to determine the choice of method (RBD, FT, ET, MA or SPN) are the *system characteristics* and the *goal of analysis*. These variables are chosen by the author from every day engineering practice, with regard to the impact on a reliability study.

The *system characteristics* are general in order for the method to be applicable to technical systems from many different fields such as the automotive and the aircraft industry (military and commercial). The proposed guideline considers six characteristics where each characteristic could have two mutually exclusive properties.

- The system behaviour: static or dynamic. Direct, explicit relationships among components (data path, workflow, feedback, etc.) creates a static behaviour, while load-sharing, standby redundancy, interferences, dependencies, on-demand, cascade, and/or common cause failures, human factor, fault-coverage, growth, phased-mission systems, time dependent sequences or several states systems and components qualifies for dynamic behaviour.
- Type of system: prototype or serial. A prototype system is unique and used for gathering information for future use while in the case of a serial system there are several identical individuals. The reliability models incorporate predictions based on parts-count failure rates taken from historical data. If the system analysed is unique, there is very little or no failure data information that can be used. Performing a reliability study on a prototype system is one of the challenges within the reliability field and therefore always important to specify the type of the system analysed.
- The system parts type: mostly mechanical/electromechanical or electronic parts. The electronic parts are considered well defined by exponential distribution (no aging) while the electromechanical and mechanical parts may have a different distribution (aging). Hence systems of a more mechanical nature (valves, pumps, rotors, generators, etc.) will show different behaviour (non-constant failure rate) from the electronic parts (constant failure rate) such as sensors, protection devices, inductors, capacitors, etc.
- Repairable or un-repairable system: Repairable systems receive maintenance actions to renew or restore the failed components when the system fails. These actions have to be taken into consideration when assessing the system behaviour. When the system fails during operation and the components that fail are not restored, the system is considered un-repairable.
- Safety or non-safety critical system: A safety-critical system is a system whose failure or malfunction may result in severe damages or injuries of persons, environment or equipment. Those systems will require not only a classical reliability study but sometimes extended risk analysis with event and consequence analyse. The analysis of such a system follows standards and handbooks such as for example (Federal Aviation Administration, 2000), (National Aeronautics and Space Administration Jet Propulsion Laboratory, 1990), (MIL-STD-882D, 2000), etc.

The different reliability questions that could arise during product development are addressed as *objective.* By contrast with the *system characteristics* (mutual exclusive choices), the *objective* can have several answer in the same time. In the proposed method the different questions have been grouped into the following six areas.

- System Reliability/ Unreliability: Usually calculated as the probability over the systems life time, the system reliability is a quality question and therefore has to be answered for any type of product from a large range of industries (automotive, aeronautics, space, manufacturing,

etc.). In early design phases can assure a more effective requirement selection, cost- performance trade off and a base for decisions regarding redundancies and maintenance, while in later design phases will help in guarantee issues. The system can have several phases/states and all of them should be accounted when analysing system reliability.

- States Probabilities: A system can have several degraded states (graceful degradation) and can be of interest to calculate depending of the customer, mission, etc. The reliability definition can be different for customers as well as mission performed and therefore a system with the same states (and state probability of occurrence) can have different output for reliability. These questions are important to answer for products within the manufacturing industry, automotive, aeronautics, etc at least in early design phases.
- Failure Scenarios/ Probability of an unwanted event: This question applies when the unwanted event is identified (usually with other analysis techniques such as Preliminary Hazard Analysis, Functional Hazard Assessment (Federal Aviation Administration, 2000), (International Electro-technical Commision, 2003), (MIL-STD-882D, 2000), (Rausand & Hoyland, 2004), etc.) and the calculation of the probability of occurrence is wanted. In those cases analysis are done in order to break down the faults causing the occurrence of the unwanted event until the root causes of these faults are identified. The failure scenarios analysis are performed from early design phases to detailed design in order to eliminate, avoid or mitigate failures and mandatory for system safety critical systems.
- Failure Scenarios/ Consequences for given events: This question applies when the unwanted event is identified (usually with other analysis techniques such as Preliminary Hazard Analysis, Functional Hazard Assessment (Federal Aviation Administration, 2000), (International Electro-technical Commision, 2003), (MIL-STD-882D, 2000), (Rausand & Hoyland, 2004), etc.) and probabilities of occurrence for consequences are wanted. In those cases failure scenarios causing certain outcomes of the given unwanted event are followed and probabilities of occurrence can be calculated. These failure scenarios analyses are performed from early design phases to detailed design in order to justify the fulfilment of safety requirements, test the efficiency of the mitigations, barriers, etc.
- Mission Reliability/ Unreliability: The same product (for example an airplane, a car, an industrial robot, etc) can require different functions depending of the mission. Usually calculated as the probability over the mission time is important for a mission planning (in any field this concept is used such as aeronautics, space, automotive, etc). Performed in early design phases can assure a more effective equipment selection, cost- performance trade off and a base for decisions regarding redundancies and maintenance, while in later design phases will help in guarantee issues.
- System Behaviour or Qualitative Analysis: In early design phases, when very little or no failure data is available, the reliability (and safety) study is qualitative. Reliability methods can be applied in order to

gather information about the system behaviour or to break down the safety (and reliability) requirements. System weaknesses (like single failures causing occurrence of a hazard or certain cut sets) can be discovered from such analysis.

Each of the five classical methods chosen in this guideline (RBD, FT, MA, ET, SPN) are analysed in order to determine how well the method can be used with regard to the different *objective* and *system characteristics* listed above. This analysis is presented in Table 1 and Table 2.

The applicability of each method is graded from one to three points, where:

*** means that the method fits well,
** means that the method fits well, with some exceptions and
* means that the method does not fit very well but it is possible to apply, or when using as a qualitative method it fits well, but not when used as quantitative method.

Where the method is not recommended for certain *system characteristic* (Table 1), no point is accounted in the respective table. This will exclude the respective method from analysed scenarios.

For example, if the system analysed has a static behaviour, the application of Stochastic Petri Network will be a waste of time but other methods such as Reliability Block Diagram are easier to apply and fit better. In this case no scenario with SPN for a system with static behaviour will be analysed. However, if the system analysed has a dynamic or dependent behaviour, the RBD is not able to model the relationship between components (see Table 1) and this scenario is excluded from this analyse.

If the analysed system is a prototype system (see Table 1) none of the methods will fit very well. The reason for this is that historical data and field experience are missing, leading to uncertainty in the result of the analysis.

In order to decide what kind of system we are dealing with, we have to go through all the *system characteristics* from A to E (Table 1) as follows:

A. Have the system static or dynamic behaviour?
B. Is the analysed system a prototype or a serial system?
C. Is the system composed mostly by electromechanical/mechanical or electronic parts?
D. Are we dealing with a repairable or non-repairable system?
E. Is the system safety or non-safety critical?

In order to analyze all the scenario combinations for system characteristics, a tree structure is used, see Figure 1. A method is qualified to use if it is qualified for every single characteristic of the system. For example, in scenario number 2 in Figure 1, RBD is not qualified because it is not recommended for systems with dynamic behaviour, while FT is not qualified because it is not recommended for non-safety critical systems.

Characteristic (mutual exclusive) [1]		RBD	ET	FT	SPN	MA
A	Static behaviour	***	**	***		*
	Dynamic dependent behaviour		**	**	***	***
B	Prototype System	*	*	*	*	*
	Serial System	***	***	***	**	***
C	Mostly electromechanical/ mechanical parts	***	**	***	**	**
	Mostly electronic parts	*	**	**	***	***
D	Repairable system		*	*	***	***
	Un-repairable system	***	**	***	*	***
E	Safety Critical	*	***	***	***	***
	Non-safety Critical	***	*		***	***

Table 1: Choice of method considering different *System Characteristics*

A measure to grade the methods applicability for a certain system is defined by the cumulated points for all system characteristics for each method. This measure will have a minimum value of 5 points (considered poor fitting) and a maximum value of 15 points (excellent fitting). The following intervals are used to determine the quality of fit:

- 5 to 7 for poor fitting
- 8 to 12 for good fitting
- 13 to 15 for very good fitting.

In the Table 2 the choice of method is performed following the *objective* of the analysis. Where the method is not recommended for certain system characteristic (Table 2), no point is accounted in the respective table. This will exclude the respective method from analyzed scenarios, in the same way as in Table 1.

Objective	RBD	ET	FT	SPN	MA
System Reliability/ Unreliability	***				***
States Probabilities	*		*		***
Failure Scenarios/ Probability of an unwanted event			***		**
Failure Scenarios/ Consequences for given events		***			
Mission Reliability/ Unreliability	***				***
System behaviour- Qualitative analysis		***	***	***	***

Table 2: Choice of method considering different *Objective*

The *objective* can include several questions included in the question categories presented in the Table 2. The same reasoning about the points used in Table 1 is used as well in Table 2.

[1] The System is defined by Characteristics A to E, every each of them with two mutual exclusive possibilities

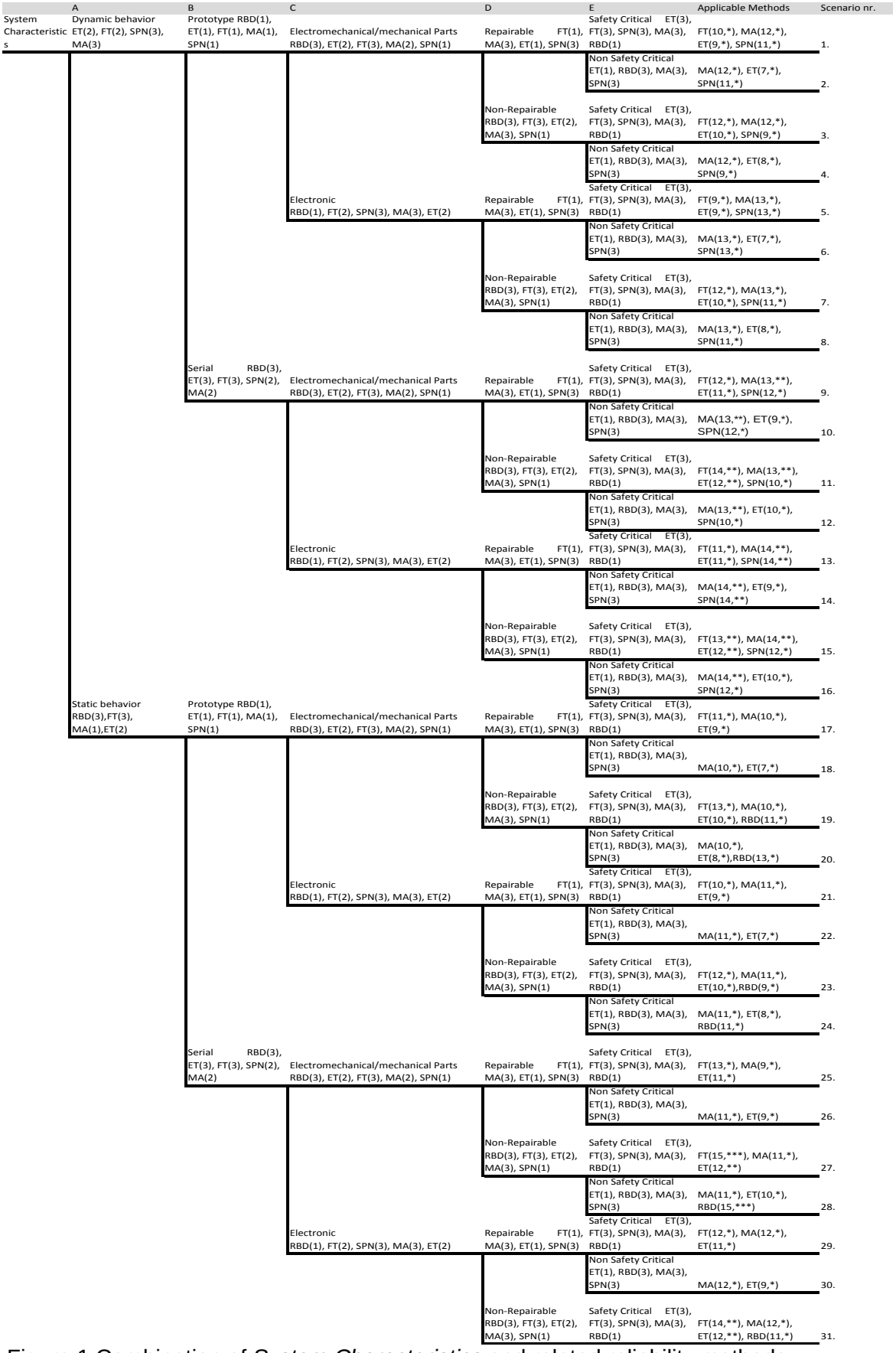

Figure 1 Combination of *System Characteristics* and related reliability methods

For example, if the *objective* is a question about system reliability (such as what is the reliability of the General Electronic Computer Unit), only two paths are available to the study, corresponding to RBD and MA methods. However, we have to ask all six questions listed in the Table 2 with answers of yes or no.

All the possible system scenarios derived from the matrix presented in Table 1 and analyzed in Figure 1, are combined with the objectives of the reliability/ system safety analysis from Table 2. Table 3 presents the fit of each reliability method for a certain objective and a system with certain characteristics. The engineer has to choose the scenario (1 to 32) describing the system to be analyzed and the objective of the analysis. One or more methods are suggested for use.

For example, if the engineer wants to know the System reliability or unreliability, for a safety critical, repairable, prototype system with dynamic behaviour, composed mostly of electromechanical/mechanical parts (row 1- first scenario in the Table 3), the recommended method is Markov Analysis which has a good fitting.

Scenario no. according to the Figure 1	**System Reliability / Unreliability**	**State Probabilities**	**Failure Scenarios / Probability of an unwanted event**	**Failure Scenarios / Consequences for given events**	**Mission Reliability/ Unreliability**	**System behaviour Qualitative analysis (barrier efficacy, sequence dependent failure scenario, etc)**
1	MA(*) 12	MA(*) 12	FT(*) 10, MA(*) 12	ET(*) 9	MA(*) 12	MA(*) 12, FT(*) 10, ET(*) 9, SPN(*) 11
2	MA(*) 12	MA(*) 12	MA(*) 12	ET(*) 7	MA(*) 12	MA(*) 12, ET(*) 7, SPN(*) 11
3	MA(*) 12	MA(*) 12	FT(*) 12, MA(*) 12	ET(*) 10	MA(*) 12	MA(*) 12, FT(*) 12, ET(*) 10, SPN(*) 9
4	MA(*) 12	MA(*) 12	MA(*) 12	ET(*) 8	MA(*) 12	MA(*) 12, ET(*) 8, SPN(*) 9
5	MA(*) 13	MA(*) 13	MA(*) 13, FT(*) 9	ET(*) 9	MA(*) 13	MA(*) 13, ET(*) 9, FT(*) 9, SPN(*) 13
6	MA(*) 13	MA(*) 13	MA(*) 13	ET(*) 7	MA(*) 13	MA(*) 13, ET(*) 7, SPN(*) 13
7	MA(*) 13	MA(*) 13	MA(*) 13, FT(*) 12	ET(*) 10	MA(*) 13	MA(*) 13, ET(*) 10, FT(*) 12, SPN(*) 11
8	MA(*) 13	MA(*) 13	MA(*) 13	ET(*) 8	MA(*) 13	MA(*) 13, ET(*) 8, SPN(*) 11
9	MA(**) 13	MA(**) 13	MA(**) 13, FT(*) 12	ET(*) 11	MA(**) 13	MA(**) 13, ET(*) 11, FT(*) 12, SPN(**) 12
10	MA(**) 13	MA(**) 13	MA(**) 13	ET(*) 9	MA(**) 13	MA(**) 13, ET(*) 9, SPN(**) 12

11	MA(**) 13	MA(**) 13	MA(**) 13, FT(**) 14	ET(**) 12	MA(**) 13	MA(**) 13, ET(**) 12, FT(**) 14, SPN(*) 10
12	MA(**) 13	MA(**) 13	MA(**) 13	ET(*) 10	MA(**) 13	MA(**) 13, ET(*) 10, SPN(*) 10
13	MA(**) 14	MA(**) 14	MA(**) 14, FT(*) 11	ET(*) 11	MA(**) 14	MA(**) 14 ET(*) 11, FT(*) 11, SPN(**) 14
14	MA(**) 14	MA(**) 14	MA(**) 14	ET(*) 9	MA(**) 14	MA(**) 14, ET(*) 9, SPN(**) 14
15	MA(**) 14	MA(**) 14	MA(**) 14, FT(**) 13	ET(**) 12	MA(**) 14	MA(**) 14, ET(**) 12, FT(**) 13, SPN(*) 12
16	MA(**) 14	MA(**) 14	MA(**) 14	ET(*) 10	MA(**) 14	MA(**) 14, ET(*) 10, SPN(*) 12
17	MA(*) 10	MA(*) 10	MA(*) 10, FT(*) 11	ET(*) 9	MA(*) 10	MA(*) 10, ET(*) 9, FT(*) 11
18	MA(*) 10	MA(*) 10	MA(*) 10	ET(*) 7	MA(*) 10	MA(*) 10, ET(*) 7
19	MA(*) 10, RBD(*) 11	MA(*) 10, RBD(*) 11	MA(*) 10, FT(*) 13	ET(*) 10	MA(*) 10 RBD(*) 11	MA(*) 10, ET(*) 10, FT(*) 13
20	RBD(*) 13, MA(*) 10	RBD(*) 13, MA(*) 10	MA(*) 10	ET(*) 8	RBD(*) 13, MA(*) 10	MA(*) 10, ET(*) 8
21	MA(*) 11	MA(*) 11	MA(*) 11, FT(*) 10	ET(*) 9	MA(*) 11	MA(*) 11, ET(*) 9, FT(*) 10
22	MA(*) 11	MA(*) 11	MA(*) 11	ET(*) 7	MA(*) 11	MA(*) 11, ET(*) 7
23	MA(*) 11, RBD(*) 9	MA(*) 11 RBD(*) 9	MA(*) 11, FT(*) 12	ET(*) 10	MA(*) 11 RBD(*) 9	MA(*) 11, ET(*) 10, FT(*) 12
24	RBD(*) 11, MA(*) 11	RBD(*) 11, MA(*) 11	MA(*) 11	ET(*) 8	RBD(*) 11, MA(*) 11	MA(*) 11, ET(*) 8
25	MA(*) 9	MA(*) 9	MA(*) 9, FT(*) 13	ET(*) 11	MA(*) 9	MA(*) 9, ET(*) 11, FT(*) 13
26	MA(*) 11	MA(*) 11	MA(*) 11	ET(*) 9	MA(*) 11	MA(*) 11, ET(*) 9
27	MA(*) 11, RBD(*) 13	MA(*) 11, RBD(*) 13	MA(*) 11, FT(***) 15	ET(**) 12	MA(*) 11, RBD(*) 13	MA(*) 11, ET(**) 12, FT(***) 15
28	RBD(***) 15, MA(*) 11	RBD(***) 15, MA(*) 11	MA(*) 11	ET(*) 10	RBD(***) 15, MA(*) 11	MA(*) 11, ET(*) 10
29	MA(*) 11	MA(*) 12	MA(*) 12, FT(*) 12	ET(*) 11	MA(*) 12	MA(*) 12, ET(*) 11, FT(*) 12
30	MA(*) 12	MA(*) 12	MA(*) 12	ET(*) 9	MA(*) 12	MA(*) 12, ET(*) 9
31	MA(*) 12, RBD(*) 11	MA(*) 12, RBD(*) 11	MA(*) 12, FT(**) 14	ET(**) 12	MA(*) 12, RBD(*) 11	MA(*) 12, ET(**) 12,FT(**) 14
32	RBD(*) 13, MA(*) 12	RBD(*) 13, MA(*) 12	MA(*) 12	ET(*) 10	RBD(*) 13, MA(*) 12	MA(*) 12, ET(*) 10

Table 3: Choice of method considering both *Scope of analyses* and *System Characteristics*

If several methods are recommended for the same scope of the analysis, the analyst can chose between the methods depending on fitting points, experience or if one of the methods can give the answers for several objectives. If the aim of the reliability study is the system behaviour, several methods can be chosen.

3. Application

As an example, the following questions are relevant to answer for a reliability study for an Electrical Power Supply System of an aircraft:

1. What is the mission reliability for the Electrical Power Supply function? Several phases need to be considered such as taxing, take off, flight and landing.
2. What are the probabilities of failure (failure rate) of safety critical functions? For example Emergency Power Supply, Auxiliary Power Supply, etc.
3. What are the probabilities of an initiating event to result in certain consequences? For example loss of aircraft due to total loss of AC power.
4. What is the probability of electrical power supply failure for certain consumers? For example loss of power supply to General Electronic Control Unit, loss of power supply to cockpit displays, etc.

The characteristics of the system according to Table 1 are:

A-dynamic, dependent behaviour;
B-serial system;
C- mostly electromechanical/ mechanical parts;
D- non repairable during flight;
E- safety critical.

The *objectives* are according to Table 2:

1. Mission Reliability/ Unreliability
2. Failure Scenarios/ Probability of an unwanted event,
3. Failure Scenarios/ Consequences for given events,
4. States Probabilities.

In Table 3 the scenario for the Electrical Power System is presented on row 11. The recommended methods are:

- Markov Analysis for question 1 and 4,
- Fault Tree or Markov Analysis for question 2 and
- Event Tree for question 3.

When the recommended methods are Fault Tree and/or Markov Analysis, the possibility of using dynamic fault tree gates for modeling certain dynamic behaviour should be investigated. This depends on what level of detail that is relevant for the questions asked and which design phase that is considered. The majority of commercial reliability software will support such dynamic gates.

When the choice is between two methods with the same fitting points, the choice will depend on other factors such as for example if a quick answer is more important than the accuracy of the answer (typical for concept phase).

4. Conclusions

This paper presents a guideline for choosing the best suited reliability method in early design phases, from two aspects: *system characteristics and objective*.

The guideline is deliberately written as general as possible to be applicable to many fields. Questions from the daily engineering practise are summarized in the Table 1 and Table 2. A decision tree (Figure 1) combines all the *system characteristics* (Table 1) in a number of possible systems, with respective fitted method to analyse. Finally, in the Table 3 these scenarios are combined with the *objective* from the Table 2. In the Table 3 at list one reliability method will be suggested to use, depending on what question is asked for the system to analyse.

The aspects analysed here has been 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 analysed, such as the capability of used reliability tool, field experience, time and resources allocated, etc.

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

References

1. Institute of Electrical and Electronics Engineers, 1998. *IEEE Standard Reliability Program for the Development and Production of Electronic Systems and Equipment.* s.l.:s.n.
2. Federal Aviation Administration, 2000. *FAA System Safety Handbook.* s.l.:s.n.
3. IEC 60812, n.d. *Analysis Techniques for system reliability - Procedure for FMEA.* s.l.:s.n.
4. IEC 61025, n.d. *Fault Tree Analysis (FTA).* s.l.:s.n.
5. IEC 61078, n.d. *Analysis techniques for dependability - Reliability block diagrams and boolean methods.* s.l.:s.n.
6. IEC 61165, n.d. *Application of Markov Techniques.* s.l.:s.n.
7. IEC 62502, 2010. *Analysis techniques for dependability – Event tree analysis (ETA).* s.l.:s.n.
8. IEC 60300-3-1, 2003. *Application Guide- Analysis techniques for dependability- Guide on methodology.* s.l.:s.n.
9. ISO/IEC 15909, n.d. *High-level Petri Nets - Concepts, Definitions and Graphical Notation.* s.l.:s.n.

10. Johansson, C., Persson, P. & Ölvander, J., 2011. *On the Usage of Reliability Methods in Early Design Phases.* Helsinki, PSAM11 & ESREL 2012.
11. Kleyner, A. & Volovoi, V., 2010. Application of Petri nets to reliability prediction of occupant safety systems with partial detection and repair. *ELSEVIER*, June.
12. Kornecki, A. & Liu, M., 2013. Fault Tree Analysis for Safety/Security Verification in Aviation Software. *Electronics,* Volume 2, pp. 41-56.
13. Lough, K., Stone, R. & Tumer, I., 2005. *THE RISK IN EARLY DESIGN (RED) METHOD: LIKELIHOOD AND CONSEQUENCE FORMULATIONS.* Philadelphia, ASME 2005 International Design Engineering Technical Conferences.
14. MIL-STD-882D, 2000. *Department of Defense Standard Practice For System Safety.* s.l.:s.n.
15. National Aeronautics and Space Administration Jet Propulsion Laboratory, 1990. *JPLD-5703 Reliability Analysis Handbook.* s.l.:s.n.
16. O'Halloran, B., 2011. *EARLY DESIGN STAGE RELIABILITY ANALYSIS USING FUNCTION-FLOW FAILURE RATES.* s.l., ASME 2011 International Design Engineering Technical Conferences .
17. Rausand, M. & Hoyland, A., 2004. *System Reliability Theory, Models, Statistical Methods and Applications.* Second ed. s.l.:Wiley.
18. Rigas, F. & Sklavounos, S., 2005. Evaluation of hazards associated with hydrogen storage facilities. *International Journal of Hydrogen Energy,* 30(13-14), p. 1501–1510.
19. Stamatelatos, D. M. et al., 2002. *Fault Tree Handbook with Aerospace Applications.* s.l.:s.n.
20. U.S. Department of Defence, 1980. *MIL-STD-1629A Procedures for Performing a Failure Mode Effects and Criticality Analysis.* s.l.:s.n.
21. IEC 62551, 2012. Analysis Techniques for Dependability-Petri Net techniques. s.I s.n

PUBLISHED BY:
Loughborough University, Loughborough, Leicestershire, LE11 3TU.

FOR FURTHER INFORMATION CONTACT:
Kate Sanderson, Nottingham Transportation Engineering Centre, University of Nottingham
University Park, Nottingham, NG7 2RD

Tel: +44 (0)115 9513953 Email: Kathryn.Sanderson@nottingham.ac.uk

ISBN 978 1 907382 61 1