



**Reliability Analysis of the Reykjavik Area  
Control Center Air Traffic Management System  
-A Case Study -**

by

Unnur Þórleifsdóttir

Thesis  
**Master of Science in Engineering Management**

January 2013



# **Reliability Analysis of the Reykjavík Area Control Center Air Traffic Management – A Case Study**

Unnur Þórleifsdóttir

Thesis submitted to the School of Science and Engineering  
at Reykjavik University in partial fulfillment  
of the requirements for the degree of  
**Master of Science in Engineering Management**

January 2013

Supervisors:

Þorgeir Pálsson, Professor, Reykjavik University

Páll Jensson, Professor, Reykjavik University

Arnór Bergur Kristinsson, Projects Manager (R&D) at Isavia

Examiner:

Ebba Þóra Hvannberg, Professor of Computer Science, University of Iceland

# I. Ágrip

---

## Áreiðanleikakönnun fyrir flugstjórnarkerfi Flugstjórnarmiðstöðvarinnar í Reykjavík

Í heimi stöðugs vaxtar og krafna til flugsamgangna verður æ mikilvægara að þróa nýjar aðferðir til að meta áhættu og öryggi almenningssflugi. Flugstjórnarmiðstöðvar starfrækja flugstjórnarkerfi sem gegna lykilhlutverki og skipta sköpum fyrir flugöryggi. Bilun í flugstjórnarkerfum getur ef illa tekst til leitt til dauða. Það er því afar mikilvægt að gera allt sem hægt er til að bæta áreiðanleika flugstjórnarkerfa til þess að lágmarka líkur á bilunum.

Isavia annast rekstur og uppbyggingu allra flugvalla á Íslandi og stýrir jafnframt flugumferð í íslenska flugstjórnarsvæðinu sem er eitt það stærsta í heiminum (5,4 milljónir ferkílómetrar í Norður-Atlantshafi). Til að geta veitt örugga og öfluga flugstjórnarþjónustu er þörf fyrir flókinn tækjabúnað. Áreiðanleiki slíkra kerfa er gríðarlega mikilvægur og þarf að vega og meta reglulega.

Aðaláhersla þessa verkefnis er að þróa áreiðanleikalíkan sem hægt er að nota til að reikna út áhættu sem tengist tæknilegum búnaði í flugstjórnarkerfi Flugstjórnarmiðstöðvar Reykjavíkur. Almennar áreiðanleikaaðferðir; Greining áhrifa og mikilvægi bilana (FMECA) og Áreiðanleika blokk rit (RBD) eru notaðar ásamt reiknihugbúnaðinum BlockSim til að þróa líkan sem er notað til að meta áhrif sem bilun í rafkerfi flugstjórnarmiðstöðvarinnar hefur á áreiðanleika flugstjórnarkerfisins. Þessi nálgun er fyrsta tilraun til að meta áreiðanleika alls flugstjórnarkerfisins í Flugstjórnarmiðstöðinni í Reykjavík.

Megin niðurstaða þessarar vinnu leiddi í ljós að nálgun verkefnisins og aðferðir eru vel fallnar til að meta áreiðanleika flugstjórnarkerfis. Þannig notast áreiðanleikaútreikningur á flugstjórnarkerfinu við að meta áhrif bilana í rafkerfinu á aðra þætti starfseminnar. Sem dæmi er meðaltími að bilun undir dæmigerðum rekstraraðstæðum um 4,3 ár. Í verkefninu er einnig tekið til skoðunar hvernig auka megi áreiðanleika með því að bæta við aukabúnaði sem leiddi í ljós að áreiðanleikinn eykst mest með því að bæta við auka rafmagnstöflu í tækjasal Isavia. Niðurstöðurnar segja jafnframt til um hvaða áhrif bilun í einstökum þáttum rafkerfisins hefur á flugstjórnarkerfið í heild. Þetta verkefni kynnir til sögunnar mikilvægt verkfæri sem hægt er að nota til að þróa yfirgripsmikið áreiðanleikalíkan fyrir flugstjórnarkerfi Flugstjórnarmiðstöðvar Reykjavíkur, líkan sem hægt er að nota til að meta áreiðanleika kerfisins í heild og um leið meta hugsanlegar breytingar á kerfinu.

**Lykil orð:** Áreiðanleiki, Bilun, Flugstjórnarkerfi, FMECA, RBD.

## II. Abstract

---

### **Reliability Analysis of the Reykjavik Area Control Center Air Traffic Management System**

In a world of continuous growth in the demand for air transport services it has become increasingly important to develop new methods for evaluating risk and safety in civil aviation. Air Traffic Management (ATM) systems represent essential infrastructure that is critical to flight safety. In extreme cases failure of the ATM system can result in loss of life. Consequently it is of utmost importance to make all possible efforts to improve the reliability of the ATM and connected systems by minimizing the probability of failures.

Isavia is the Icelandic Air Navigation Service Provider responsible for providing air navigation services in one of the largest Air Traffic Control regions in the world (5.4 million square kilometers in the North Atlantic). The ability to provide safe and efficient air navigation services is highly dependent on the ATM system located in the Reykjavík Air Traffic Control Center (RACC). The main focus of this research project is on developing a reliability model that can be used to ascertain the risk of technical failure in the ATM system of the RACC ATM system. The Failure Mode Effect and Criticality Analysis (FMECA) and Reliability Block Diagram (RBD) are employed along with a software tool, BlockSim, in order to develop a quantitative model that is used to determine the effect of RACC electrical power system failures on the reliability of the ATM system. This approach is a first attempt at evaluating the overall reliability of the RACC ATM system.

The main conclusion of this work is that the approach and the methods employed are very attractive for evaluating reliability of the RACC ATM system and similar systems. The reliability of the ATM system is computed to determine the effect of electrical failures in various modes of operation. As an example it is found that the Mean Time to Failure is about 4.3 years in a typical operational mode. Also improvements in reliability are considered e.g. by increasing system redundancy. This revealed that adding a fuse board to the electrical power system affects the system reliability the most. The model results also indicate how the system can be improved in terms of electrical power connectivity and what effects failure of certain parts have on the ATM system. This research project provides an important tool that can be used for developing a comprehensive reliability model for the RACC ATM system that could be used to analyze and evaluate the overall reliability of the system as well as providing an important tool to assess any modifications of the ATM system.

**Keywords:** *ATM, Failure, FMECA, RBD, Reliability.*

# **Reliability Analysis of the Reykjavik Area Control Center Air Traffic Management System**

Unnur Þórleifsdóttir

Thesis submitted to the School of Science and Engineering  
at Reykjavík University in partial fulfillment  
of the requirements for the degree of  
**Master of Science in Engineering Management**

January 2013

Student:

---

Unnur Þórleifsdóttir

Supervisors:

---

Þorgeir Pálsson

---

Páll Jensson

---

Arnór Bergur Kristinsson

Examiner:

---

Ebba Þóra Hvannberg

### III. Acknowledgement

---

I would like to express my gratitude to the people that provided assistance during this research project.

Þorger Pálsson supervisor and professor at Reykjavik University for all the work and time he made available, either to read over parts of this paper or help the author with the occasional problems that arose. Páll Jensson professor at Reykjavik University also receives special thanks for his input regarding the subject.

Arnór Bergur Kristinsson, projects manager at Isavia, for acting as a liaison into Isavia, helping to setup meeting with appropriate specialists and for providing information needed for the project. The specialists also receive sincere thanks for providing information about the RACC systems. They are:

- Arnar Sigurðsson, Air Traffic Controller and incident investigator
- Arnar Þórarinnsson, Senior System Administrator – ATM Systems
- Árni Páll Hafsteinsson, Operations Manager – Electrical Services
- Guðmundur Karl Einarsson, Air Traffic Controller
- Guðmundur Kristjánsson, Project Manager – Research & Development
- Hjalti Pálsson, Manager - Research & Development
- Jón Gunnlaugsson, Manager - Safety and Quality
- Kristján Torfason, System Administrator – ATM Systems
- Magnús Ásbjörnsson, Project Manager EATS
- Sigurður Sigurþórsson, Project Manager – Electrical Services
- Steingrímur Hálfðánarson, Deputy Manager
- Steinunn Arna Arnardóttir, ATS Procedure Specialist
- Þorsteinn Jóhannesson, Manager AIS and CNS Systems

Joanna Binka, Sales and Marketing Assistant at Reliasoft, and Krzysztof Kusy, Technical Sales Manager at ReliaSoft, also get special thanks. Joanna Binka for making license for BlockSim 7 available and Krzysztof Kusy for making the time to answer questions about BlockSim that arose.

Finally, Magnús Guðmundur Helgason, Civil Engineer, and Þórleifur Jónsson, Business Administration Cand Oecon, receive special thanks for proof reading the project and helping with the final setup.

## IV. Table of Content

I. ÁGRIP.....	I
II. ABSTRACT.....	II
III. ACKNOWLEDGEMENT.....	IV
IV. TABLE OF CONTENT.....	V
V. TABLE OF FIGURES.....	IX
VI. TABLE OF TABLES.....	XI
<b>1. INTRODUCTIONS .....</b>	<b>1</b>
1.1. <i>Backgrouond</i> .....	1
1.2. <i>State of the problem</i> .....	2
1.3. <i>Research aims and objectives</i> .....	3
1.4. <i>Research questions</i> .....	4
1.5. <i>Research methodology</i> .....	4
1.6. <i>Assumptions and Limitations</i> .....	6
1.7. <i>Structure of the research project</i> .....	8
<b>2. THEORETICAL FRAMEWORK.....</b>	<b>9</b>
2.1. <i>Risk and Safety analysis in air transport</i> .....	9
2.1.1. <i>Technical failure risk</i> .....	10
2.1.1.1. <i>FMECA</i> .....	10
2.1.1.2. <i>RBD</i> .....	11
2.1.2. <i>Human error risk</i> .....	15
2.2.3. <i>Collision risk</i> .....	15
2.2. <i>The inevitability of failures</i> .....	16
<b>3. INTRODUCTION TO RELIABILITY ANALYSIS IN ATM SYSTEMS.....</b>	<b>18</b>
3.1. <i>Safety analysis techniquest and methods evaluation</i> .....	18
3.2. <i>Providing a basis (FMECA)</i> .....	20
3.2.1. <i>FMECA concepts</i> .....	20
3.2.1.1. <i>Failure vs. fault</i> .....	21
3.2.1.2. <i>Failure modes vs. Failure causes</i> .....	21
3.2.1.3. <i>Failure mode classification</i> .....	22
3.2.2. <i>FMECA procedure</i> .....	22
3.2.3. <i>FMECA for the RACC System</i> .....	23
3.2.4. <i>FMECA results</i> .....	25
<b>4. METHODOLOGY.....</b>	<b>27</b>
4.1. <i>Reliability Block Diagrams (RBD)</i> .....	27
4.1.1. <i>Calculating reliability</i> .....	28

4.1.2. Mean Time To Failure.....	29
4.1.3. Component characteristics.....	30
4.1.3.1. Observing failure data and fitting a failure distribution to components.....	31
4.1.3.2. Exponential distribution.....	32
4.1.4. Configuration.....	33
4.1.4.1. Series-Structure.....	33
4.1.4.2. Parallel Structure (Redundancy).....	34
4.1.4.3. k-out-of-n structure.....	35
4.1.4.4. Load sharing construct.....	35
4.1.4.5. Stand-by Construct.....	36
4.2. Analyzing the RBD model.....	37
4.2.1. Sensitivity analysis (Reliability Importance).....	38
4.2.2. Reliability Allocation.....	39
4.2.3. „What-if“ analysis.....	39
<b>5. THE CASE STUDY-REYKJAVÍK ACC SYSTEM.....</b>	<b>40</b>
5.1. The system reliability model.....	40
5.1.1. The electrical power system in Reykjavík ACC.....	40
5.1.1.1. Back-up Power.....	41
5.1.2. The reliability model of the electrical power system.....	42
5.1.2.1. Configurations.....	42
5.1.2.2. Component properties.....	44
5.1.3. Communication, Navigation and Surveillance (CNS) systems in the ATM reliability model.....	45
5.1.4. Reliability model of the Air Traffic Management (ATM) system.....	47
5.2. Assumptions.....	52
5.3. The resulting model of the entire system.....	54
<b>6. RESULTS AND DISCUSSION.....</b>	<b>58</b>
6.1. The RACC Electrical Power System.....	59
6.2. RACC ATM/CNS System Reliability.....	65
6.3. Limitations of results.....	76
6.4. Feasibility of using reliability models for ATM systems.....	77
<b>7. CONCLUSIONS AND RECOMMENDATION.....</b>	<b>79</b>
7.1. Summary.....	79
7.2. Conclusions.....	80
7.3. Further research and development work.....	81
<b>8. REFERENCES.....</b>	<b>84</b>



<b>9. APPENDIXES.....</b>	<b>90</b>
<i>A. Abbreviations.....</i>	<i>90</i>
<i>B. Air Traffic Management.....</i>	<i>92</i>
<i>B.1. Air Traffic Managenent.....</i>	<i>92</i>
<i>B.2. Airspace Management.....</i>	<i>93</i>
<i>B.3. Flow Management.....</i>	<i>96</i>
<i>B.3.1. Capacity Planning.....</i>	<i>97</i>
<i>B.4. Air Traffic Control.....</i>	<i>98</i>
<i>B.5. ATC Planning.....</i>	<i>98</i>
<i>B.6. Separation Service.....</i>	<i>99</i>
<i>C. The Air Traffic Control system at Isavia.....</i>	<i>102</i>
<i>C.1. Surveillance.....</i>	<i>103</i>
<i>C.1.1. Radars.....</i>	<i>103</i>
<i>C.1.1.1. Primary radar.....</i>	<i>104</i>
<i>C.1.1.2. Secondary Surveillance Radar (SSR).....</i>	<i>104</i>
<i>C.1.2. Transponder.....</i>	<i>104</i>
<i>C.1.3. Squawk Allocation System (SPASS).....</i>	<i>104</i>
<i>C.1.4. Automatic Dependent Surveillance Broadcast (ADS-B).....</i>	<i>104</i>
<i>C.1.5. COM Network - Communication network.....</i>	<i>105</i>
<i>C.1.6. Radar Data Processing System (RDPS).....</i>	<i>105</i>
<i>C.1.7. Flight Data.....</i>	<i>105</i>
<i>C.1.8. Flight Data Processing System (FDPS).....</i>	<i>105</i>
<i>C.1.9. Integrated Controller Environment (ICE).....</i>	<i>106</i>
<i>C.1.10. Integrated Situation Display System (ISDS).....</i>	<i>106</i>
<i>C.2. Communication.....</i>	<i>106</i>
<i>C.2.1. High Frequency Radio (HF Radio).....</i>	<i>108</i>
<i>C.2.2. Very High Frequency Radio (VHF Radio).....</i>	<i>108</i>
<i>C.2.3. Satellite Communication (SATCOM).....</i>	<i>108</i>
<i>C.2.4. Controller Pilot Data Link Communication (CPDLC).....</i>	<i>108</i>
<i>C.2.5. Automatic Dependent Surveillance - Contract (ADS-C).....</i>	<i>109</i>
<i>C.2.6. Future Air Navigation System (FANS I/A).....</i>	<i>109</i>
<i>C.2.7. Voice Communication System (VCS).....</i>	<i>109</i>
<i>C.2.8. Aeronautical Fixed Telecommunication Network (AFTN).....</i>	<i>109</i>
<i>C.2.9. Radio Operator Flight Data System (ROFDS).....</i>	<i>109</i>
<i>C.3. Navigation.....</i>	<i>110</i>
<i>C.3.1. Global Navigation Satellite System (GNSS).....</i>	<i>110</i>
<i>C.3.2. Inertial Navigation System (INS).....</i>	<i>110</i>

<i>D. Short overview of Reliability methods for human error ad collision risk.....</i>	<i>111</i>
<i>D.1. Human error risk.....</i>	<i>111</i>
<i>D.2. Collision risk.....</i>	<i>113</i>
<i>E. Additional information on the Electrical Power system at Isavia.....</i>	<i>116</i>
<i>F. Concepts and definitions.....</i>	<i>121</i>
<i>G. The BlockSim terminology.....</i>	<i>126</i>
<i>H. Features of BlockSim.....</i>	<i>131</i>
<i>I. FMECA example.....</i>	<i>140</i>
<i>J. FMECA results.....</i>	<i>141</i>
<i>K. Stand-by construct with three components.....</i>	<i>146</i>
<i>L. First approach.....</i>	<i>147</i>
<i>M. Reliability models.....</i>	<i>148</i>
<i>N. Reliability models.....</i>	<i>150</i>

## V. Table of Figures

Figure 2-1: An example of RBD. The system is functioning if there is a path between start and end point of the diagram. (In this case block number 4 is needed for two of the available paths).....	12
Figure 3-1: Overview of most used analysis techniques (Rouvroye & Bliet, 2002).....	18
Figure 3-2: The relationship between failure and fault (Rausand & Høyland, 2004).....	21
Figure 4-1: An example of RBD. The system is functioning if there is a path between start and end point of the diagram. ....	27
Figure 4-2: Failure rate at time t (“Bathtub Curve” or “Life-Cycle Curve”) (Chandrupatla, 2009).....	31
Figure 4-3: Series structure built with n components (Rausand & Høyland, 2004). ....	33
Figure 4-4: Two components in a series with their constant failure rates.....	33
Figure 4-5: Parallel structure with n components (Rausand & Høyland, 2004). ....	34
Figure 4-6: Two components in parallel with their constant failure rates.....	34
Figure 4-7: A k-out-of-n structure.....	35
Figure 5-1: The electrical system in Reykjavik ACC (Hafsteinsson & Sigurþórsson, 2102).....	41
Figure 5-2: The reliability model of the electrical power system. ....	42
Figure 5-3: The two RBD diagrams both give the same reliability results. Mirrored blocks (same component in more than one location). ....	43
Figure 5-4: The reliability model of the VCS subsystem.....	47
Figure 5-5: The reliability model of the ATM system. ....	51
Figure 5-6: The reliability of a system that is successful if either Q30 or Q31 is functioning.....	55
Figure 5-7: Modeled power outage of RDPS and Operstack switches. ....	56
Figure 5-8: Modeled power outage and human failure of RDPS and Operstack switches. ....	56
Figure 6-1: The reliability function of the electrical power system vs. time. ....	60
Figure 6-2: Shows with red where the components are added.....	64
Figure 6-3: Reliability results when the system has been altered by adding components.....	65
Figure 6-4: The reliability function of the ATM system vs. time. ....	68
Figure 6-5: Overview of the system if fuse boards Q30 and Q32 fail. ....	72
Figure 6-6: Overview of the system if fuse boards Q31 and Q33 fail. ....	73
Figure 6-7: Overview of the system if fuse board Q30 fails. ....	74
Figure 6-8: Overview of the system if fuse board Q31 fails. ....	75
Figure 6-9: Overview of the system if fuse board Q32 fails. ....	75
Figure 6-10: Overview of the system if fuse board Q33 fails. ....	76
Figure B-1: Flow of operational data between Airspace Management, Flow Management, ATC Planning, Separation Service and Aircraft. Adapted from a paper issued 5 <sup>th</sup> US/Europe Air Traffic Management R&D Seminar (Haraldsdottir, Schoemig, Schwab, Singleton, Sipem & van Tulder, 2003).....	93
Figure B-2: Division of Reykjavík control Area into sectors (Isavia, 2012a).....	94

Figure C-1: Information systems and equipment used in Reykjavík ACC.....	102
Figure C-2: Radar stations and radar coverage in the Reykjavík control area at 40 thousand feet.....	103
Figure C-3: The communication between the ATCC and the Aircraft. The path of the voice communication is shown in blue color and the path of data communication is shown in green.....	107
Figure G-1: A graphical representation of important BlockSim terms. ....	126
Figure G-2: Example of PDF and life-stress relationship.....	129
Figure H-1: Block properties window.....	132
Figure H-2: RBD of the electrical power system. ....	134
Figure H-3: The Reliability tab where failure distributions are identified.....	135

## VI. Table of Tables

---

Table 3-1: The criticality ranking used during the FMECA and the associated meaning of each value. ....	25
Table 5-1: MTTF point estimates for the electrical system components. ....	45
Table 5-2: The function of equipment. ....	48
Table 5-3: The operswitch needed for the ATM subsystems and components to function. ....	49
Table 5-4: The main equipment for ATM and CNS systems and whether they have backups. ....	50
Table 5-5: Presents minimum equipment list for each functionality failure mode.....	53
Table 6-1: Probability of successful electrical power system operation. ....	60
Table 6-2: Reliability results when the system has been altered by adding components.....	64
Table 6-3: Minimum equipment list for each functionality Failure Mode. ....	67
Table 6-4: Probability of successful ATM system operation.....	69
Table E-1: Presents the components of the electrical system, their function, detection of failure or tests, effects of failure, MTTF values and risk reducing measures. ....	120

# 1. Introduction

---

This chapter covers a general introduction of the research project; the background of the problem as well as general aims and objectives of the research. Research questions, assumptions and limitations are listed and a short review of the research methodology is summarized. This chapter finally provides the structure of the research project. By the end of this chapter the rationale behind the need for this research should be clear.

## 1.1. Background

Air traffic management (ATM<sup>1</sup>) is the process, procedures and resources used to ensure the safe guidance of aircraft on the ground and in the air<sup>2</sup> (EUROCONTROL, 2012a).

Modern ATM typically consists of a large number of interconnected subsystems and modules containing diverse technical equipment and processes. The subsystems include functions such as communications, navigation and surveillance systems in addition to the data processing and display systems in various air traffic control centers. These are used to receive, process, store and display information about aircraft in the ATM system. The subsystems also generate, transmit and receive flight data, requests, commands, directives and all types of safety related information that is needed to provide efficient and effective air traffic service thus ensuring the safety of air traffic and aircraft.

Safety is considered as one of the most important operational characteristics of ATM (Netjasov & Janic, 2008). In systems where failure can result in injuries or even fatalities, the distinction between reliability and safety becomes blurred (United States Army, 2007). In a narrow sense reliability denotes the probability of success (EUROCONRTOL, 2012b). Clearly the reliability of the ATM system is very important for ensuring flight safety. For this reason a high-level of redundancy is built into these systems to make certain that a minor failure within the system or subsystems does not result in an interruption in the functioning of the ATM system. Thus there exist more than one communication path for all important links in order to prevent a failure of essential system services due to the failure of a single link. Similarly, other essential services are duplicated. Therefore, at least a dual configuration of computer processing systems is installed in all air traffic control centers with an autonomous stand-by system ready to take over from the primary system at any point in time without an interruption. Similarly essential support services, such as electrical power, have multiple back-up systems which are capable of delivering sufficient power to the systems despite breakdown of the electrical power grid or in-house back-up generators.

In the past, reliability studies have been a popular research subject in many fields, especially in the last few years because of increasing risk<sup>3</sup> awareness (Subotic, 2007). Under current circumstances, where permanent and increased pressure on ATM system

---

<sup>1</sup> Abbreviations are listed in appendix A.

<sup>2</sup> An overview of the ATM system will be provided in appendix B.

<sup>3</sup> The risk in this case means the possibility of failure preventing normal system operation.

capacity is driven by continuous growth in air transport demand, it has become especially important to consider these aspects (Janic, 2000).

The need for in-depth analysis of ATM equipment and subsystem failures and reliability is presented briefly above and is discussed in more detail in the remainder of this research.

## **1.2. Statement of the problem**

ATM systems are critical to flight safety and any downtime is typically very costly in terms of economic penalties. In extreme cases failure of the ATM system can result in loss of life (United States Army, 2007). The development of a model to verify that the reliability of the system meets stated requirements is therefore of significant value from safety assurance point of view as well as due to economic aspects. By scrutinizing ATM system design concepts on reliability grounds at an early stage cost overruns of development programs, that sometimes turn out to be ineffective or even fail, can be avoided (Blom H. , Bakker, Blanker, Daams, Everdij, & Klompstra, 2001). Reliability analysis seeking safety assurance is of main concern in this research project.

As the complexity of ATM systems grows it gets increasingly difficult to determine their reliability. Thus reliability of the entire ATM system or even subsystems within ATM is often not known even though there are specifications that have been established by e.g., Eurocontrol<sup>4</sup> relating thereto. Eurocontrol (2012c) specification for ATM surveillance system performance for example states that full radar surveillance data availability shall be no less than 99.5% but availability of essential data shall be no less than 99.999%. Such specifications provide performance measures which reliability and safety calculations can be compared against. Availability and reliability are related concepts and will both be calculated in this research project.

There are many valid reasons for analyzing and calculating system reliability. Analyzing reliability should be an ongoing activity that starts with the initial design and continues through the evaluation of alternate design options, redesigns, and corrective actions (United States Army, 2003). One purpose for reliability analysis is therefore to assess the analysis of modifications that are being contemplated from the point of view of reliability as well as other technical characteristics. In addition, reliability analysis can be used to rank proposed design options.

The estimation of overall reliability is also important to evaluate the need for special measures in order to increase reliability, e.g. to add an extra redundant component of an ATM system in an Air Traffic Control (ATC) Center or to establish a back-up system that is remotely located.

The topic will be focused and formulated more clearly as the aims and objectives of this research are presented. These are presented in the following section.

---

<sup>4</sup>Eurocontrol, also known as the European Organization for the Safety of Air Navigation, is an intergovernmental organization made up of 39 member states and the European community.

### 1.3. Research aims and objectives

The primary aim of the research project is to provide a good understanding of reliability, its importance and how reliability analysis methods may be used to analyze and calculate the reliability of an ATM system. Furthermore, to investigate, select and adapt a recognized general reliability method and apply this method to computing the reliability of the Reykjavík Area Control Center (RACC) ATM system. A commercially available software system, BlockSim 7<sup>5</sup>, was used for this purpose. This software has not been used in Iceland until now. As the ATM system is highly complex system, a software is necessary for calculation of system reliability. Thus this research project also determines whether it is suitable to use the BlockSim software for analyzing and determining the reliability of ATM systems.

This will be achieved by developing a quantitative model to determine the reliability of the RACC ATM system operated by Isavia, the Icelandic Air Navigation Service Provider (ANSP) responsible for providing air navigation services in a large region in the North Atlantic. The resulting reliability model will provide the reliability of the ATM system focusing on the role and impact of the electrical power system in the overall system reliability as a logical starting point. The presence of electrical power is absolutely vital to the ATM system as is the case of any safety critical system. Non-availability of electrical power can lead to total system break-down which is unacceptable in systems of this type. Thus it is clearly very important to ensure that all necessary precautions have been made to prevent failures of the electrical power systems in the RACC.

The approach of making this model will be based on a recognized modeling technique that provides a description of how various subsystems interact to deliver the designed functionality of the system. In most cases, constructing a reliability model leads to a better understanding of the system design, including aspects such as component interdependencies, interconnection of equipment/subsystems and reliability weaknesses (Bailey, Frank-Schultz, Lindeque, & Temple III, 2008).

The resulting reliability model will make it possible to compute the overall reliability of the system once all essential subsystems have been included in the model. It will as well enable the analysis of how individual subsystems and subassemblies affect system reliability. Once the reliability has been determined, the model will be used to identify the weak points or the least reliable components in the system in order to improve the system reliability. Thus, the results of the model can be used to justify reliability improvements by generating information that can be used as a basis for decision making regarding possible improvements to increase the systems' reliability.

---

<sup>5</sup> BlockSim 7 is a software tool that provides a comprehensive platform for system reliability, availability, maintainability by generating probability distribution based on data and system configuration. Appendix H presents explanations of features used in the resulting reliability model and how to use BlockSim in future extensions of the model. Underlying principles and theory used in the BlockSim7 will be discussed in chapter 4 about methodology and appendix G.



In order to achieve the aims and objectives the following tasks will be performed:

- Data and documentation of system characteristics and features will be collected.
- A model connecting operational concepts functionality and information flow of the RACC ATM system will be depicted.
- Overview of how technical equipment interacts will be depicted.
- Provide a systematic literature to connect topics of ATM equipment failures and reliability.
- Identify potential failures effects and criticality.
- Develop the system reliability model with special emphasis on the electrical power system.
- Identify the most important components and/or subsystems.
- Perform “what-if” analysis and sensitivity analysis.
- Provide reliability results that can be used to demonstrate if improvements of the electrical system are necessary to increase system reliability.
- Analyze and propose some alternative system configurations in order to investigate what possibilities exist for further increasing the reliability of the ATM system.

In short, the main focus of the research project will be on developing a model, identifying weaknesses and possible improvements in the systems’ design. Improvements can be made by upgrading or replacing existing components or adding an extra redundant component.

A more formal statement of the goals of the research will be presented in the next section.

#### **1.4. Research questions**

While analyzing the ATM system reliability the following research questions will be answered:

1. What is the reliability of the system in terms of probability due to electrical power system failures?
2. How can the reliability of the system be improved? Which components constitute the weak links in the system?
3. How does the failure of certain components of the electrical power system affect the overall ATM system reliability?
4. Is it suitable and convenient to use the method to be selected and for instance the BlockSim software for analyzing and determining the reliability of ATM systems?
5. What further research and development work is needed?

These questions will be discussed in detail and answers provided in chapter 6.

## 1.5. Research methodology

Various approaches are available for modeling system reliability. For this reason it is necessary to provide a survey of the methods that have been successfully employed by other parties for determining the reliability of ATM and similar systems. This is done in Chapter 2. It was determined that the complementary methods **Failure Mode, Effects, and Criticality Analysis** (FMECA) and **Reliability Block Diagram** (RBD) are best suited to reach the identified goals of the research project. These methods are described in chapter 2 and explanations as to why these methods were selected. For detailed description of these methods refer to Rausland and Høyland (2004).

Following the classical approach of modeling large complex systems, the system is broken down into subsystems and components from a top-down point of view. Each component can thereby be looked at individually. Having segmented the system, the next step is to obtain life data (reliability/failure data) concerning each component (Reliasoft, 2007). Then the model is used to obtain the complete mathematical system reliability function that provides the statistical value of probability of success of the system.

The model is used to perform a “what-if” analysis which provides an assessment of the effects failures, of essential electrical power components, have on the overall system performance. The analysis is performed by turning the status of individual components off, to indicate that they are inactive, and then obtain reliability results for the system under those hypothetical conditions (Reliasoft, 2010). In other words, the reliability of the system is calculated given that a certain component within the system has failed. By doing this research question number three<sup>6</sup> can be answered. Finally a sensitivity analysis provides an assessment of the impact of a component on the reliability of the total system which is dependent on components reliability and position in the system.

Once the reliability has been determined, Reliability Allocation calculations are used to identify the weak points and the least reliable components in the system. Then the system reliability can be improved by improving the reliability of the weakest components (Reliasoft, 2007). This can provide the optimum scenario to meet system reliability goals.

This is the first time that an attempt has been made to calculate the reliability of the ATM system on the basis of a reliability model. Therefore an important objective of the research project is to assess if this method and associated software for its implementation is suitable for analyzing the reliability of ATM systems.

Because models of systems can become quite complex the RBD will be applied by using the commercial software tool produced by ReliaSoft Corporation called BlockSim 7. This software has not been used in Iceland until now. However it provides a

---

<sup>6</sup> How does failure of certain components of the electrical power system affect the overall ATM system reliability?

powerful, logical and an easy to use tool which this research project will show is of significant value.

## 1.6. Assumptions and Scope

This project focuses on the analysis of the Isavia ATM system, operated by the Reykjavik ATC Center for provision of air traffic services. Thus it is assumed that remotely located equipment (i.e. outside the center) will not fail e.g. equipment on-board aircraft, communication network and radar stations. The system will be modeled in its present configuration (October 2012) when determining the actual reliability of the system.

The ATM system, as mentioned before, is a large, highly complex system containing software and hardware with multiple functions. It is therefore a major research undertaking to model the system as a whole by including all the functions, features and failure modes available. For this reason **the main focus of this research project will be limited to one of the most important support systems, i.e. the electrical power system**. The presence of electrical power is vital to the ATM system as it would be in the case of any safety critical system. If no electrical power is available to run the system it means that no operation is feasible which can lead to unacceptable risk of accidents or possibly catastrophic failures.

It is assumed that components or subsystems do not fail except in the case of a power outage. Even though the focus is on the electrical power system, the whole ATM system will be modeled in such a manner that only statistical failure data (along with minor adjustments) for the remainder of the subsystems and equipment will be needed to extend the model. This will be discussed further in chapter 5.3.

There are several possible failure causes in ATM systems e.g. technical equipment failure (electrical power failure, software and/or hardware) and human failure. This research addresses technical equipment of the ATM system with respect to electrical power failure. Human error is not considered. For this reason the equipment is assumed correctly connected and properly operated as it is assumed no errors have been made in equipment setup, interconnection or operation. Furthermore the model only contains equipment that is critical for the operation of the system i.e. the equipment necessary to ensure that the ATM functionality for ensuring the safe separation of aircraft is available.

While seeking improvement of systems' reliability, identifying possible failures and preventing these failures from occurring is of main concern (Rausand & Høyland, 2004). To make sure this is performed in a structured way it is important to calculate reliability by modeling the system reliability.

Reliability predictions are only as accurate as the data available for the components of the system. Accurate and readily available statistical data of individual components is needed in order to calculate system reliability. Such data is not always available and in the case of the RACC electrical system there was a scarcity of suitable data on its

components. This lack of data was overcome by including expert judgment. The gathering of information was conducted by interviewing experts within the company. Therefore reliability data is mainly based on the opinion of these experts. Thus significant effort was devoted to defining and documenting the functionality of system components, its interactions and configuration. Even if the absolute values are not very accurate, reliability analysis can be useful for comparing alternative design options and for performing sensitivity analysis (Bailey, Frank-Schultz, Lindeque, & Temple III, 2008).

Systems like the ATM system are always changing and developing. Some criteria, like components failure data or how the system as a whole is connected, keep changing. For this reason it is important to note that the model is based on information gathered in the period September 2011 to October 2012<sup>7</sup>. As changes are made it is important to estimate the reliability of the new arrangement to make sure that the change does not decrease system reliability.

As there is lack of suitable data the reliability of the electrical power system and the ATM system is modeled as non-repairable. This means that the component is studied until the first failure occurs. In actuality the component is repaired after the failure. To make the reliability model reflect the actual system behavior better the average availability of the system is also calculated based on the models including fixed maintenance times i.e. equal to one week, equal to 24 hrs and equal to 1hr. These maintenance values are not based on real data. The value of one week is however meant to provide a reference value for worst case scenario (that in the event of failure it takes a whole week to repair the failed component/s) to be able to calculate availability. The value of 24 hrs is a more realistic maintenance reference value used to calculate the availability of the system. Even more realistic Mean Time To Failure (MTTR) value is one hour as ATM systems are safety critical systems that typically can be repaired quickly.

The most important assumptions made in the research project are listed below:

- The model considers the ATM system in its present configuration.
- The operations not performed by the ATC Center will be ignored i.e. equipment outside the ATC Center will be assumed to function without fault.
- Main focus is on the electrical power system i.e. failure only occurs in the electrical power system.
- Hardware electrical failure only e.g. no human failure, environmental failures nor software failure are taken into account.
- Systems are assumed correctly connected.
- Manual actions will be ignored i.e. only automatic processes are modeled.

---

<sup>7</sup> Appendices B and C are based on information gathered in 2011. The assumptions regarding CNS is based on information gathered in September 2012 and do not consider changes made to the system after that time.

- Operational critical hardware, i.e. only necessary equipment needed to ensure the safe separation of aircraft (to prevent the collision of aircraft).

Other assumptions regarding specific components of subsystems will be stated in the appropriate chapters.

## **1.7. Structure of the research project**

The remainder of this research project is organized into 7 chapters. Chapter 2 explains the importance of safety modeling in air transport and provides a short description of some the methods that have previously been used in the field. In chapter 3 the basis for the reliability analysis is provided along with explanation as to why the RBD approach is selected as the main methodology. In chapter 4 the methodology is explained in detail. Chapter 5 provides the case study of the ATM system. In the 6th chapter the research question will be addressed and results and conclusions based on these questions will be presented and discussed in detail. The 7th chapter presents the summary of the research as well as describing the conclusions and recommendations of the research work.

Additional details are presented in the appendices which are organized as follows. Appendix A contains abbreviations. Appendixes B and C provide insight regarding the Reykjavik ATM system. More specifically Appendix B presents the information flow between four different operational functions of the ATM system and appendix C gives an overview of technical equipment and systems of the ATM system. Appendixes B and C were prepared in cooperation with a fellow student Hulda Ástþórsdóttir. Appendix D provides a short description of reliability methods that have been used successfully in the field of air transport. Appendix E provides information on the electrical system. Appendixes F and G are devoted to terminology, relating to reliability and BlockSim terms respectively. Finally Appendix H provides an introduction to the BlockSim software and its features. Appendixes I and J present an example and the results of the FMECA. Appendixes that follow Appendix J present information and figures explaining the modeling.

The research project was written under the guidance of Professor Þorgeir Pálsson and Professor Páll Jensson. Arnór Bergur Kristinsson Projects manager at Isavia, acted as point of contact establishing connection with system experts within Isavia as well as providing insight into the operation of the system and organizing meetings about various subjects of the research.

## 2. Theoretical framework

---

This chapter focuses on providing an understanding of the importance of safety analysis and modeling in air transport. It also provides a short description of commonly used methods and their associated literature.

In systems where failure can result in injuries or even fatalities, the distinction between reliability and safety becomes blurred. Reliability affects safety i.e. improving reliability of a system results in an improvement of system safety. Appropriate reliability modeling is therefore “...*vital for proper design, dependable operation, and effective maintenance of systems*” (United States Army, 2007) .

### 2.1. Risk and Safety analysis in air transport

It has always been important to analyze and assess risk and safety in civil aviation by application of statistical methods. Under current circumstances where the air transport infrastructure, including ATM systems, is under increased pressure to cope with growth in air traffic it has become increasingly important to adopt statistical methods for ensuring flight safety (Janic, 2000). The following citations are from an article by Netjasov and Janic (2008).

*“For a long time, the interpretation of safety depended on the system involved and the purpose of the analysis” (Kumamoto & Henley, 1996).*

*“For technical systems, risk is related to the probability of failure of components or of an entire system causing exposure to hazard and related consequences. In commercial systems, risk is the chance of being exposed to the hazard of losing business opportunities by making inappropriate decisions when there is a known probability of failure. In terms of safety, risk can be considered as a combination of the probability or frequency of occurrence and the magnitude of consequences or severity of a hazardous event” (Bahr, 1997).*

The process of analyzing risk and safety starts by considering how the components, that are being analyzed, should be assessed in relation to interactions with other system elements. At the same time methods that have been successfully applied by other parties for determining the reliability of ATM and similar systems should be considered in order to find the method best suited for achieving the identified goals of the research project (Everdij, Blom, & Kirwan, 2006).

In general, the problem of accident risk assessment has been widely studied for other complex human controlled safety-critical operations. This includes operations such as those found in the nuclear and chemical industries. Numerous techniques and tools have been developed for these applications (Everdij, Blom, & Kirwan, 2006).

The methods vary from qualitative failure identification methods such as (NLR, 2010):

- Preliminary Hazard Analysis (PHA),
- Common Cause Analysis (CCA),

- Failure Mode and Effect Analysis (FMEA),

through quantitative assessment techniques such as (NLR, 2010):

- Fault Tree Analysis (FTA),
- Event Tree Analysis (ETA),
- Event Sequence Diagrams (ESD),
- Master Logic Diagrams (MLD) and,
- Reliability Block Diagrams (RBD),

to dynamic assessment techniques such as (NLR, 2010):

- Petri net and Markov chain modeling,
- Dynamic event trees.

In air transport, risk and safety are generally related to air traffic accidents and are typically studied from one of three different perspectives: technical failure risk, human error risk and collision risk (Netjasov & Janic, 2008). This categorization is somewhat arbitrary and the dividing lines could have been different.

#### **2.1.1. Technical failure risk. - Risk of failure of technical systems and components that may result in an aircraft accident.**

Technical failure can be caused by failure of the aircraft or its systems or by a failure in the ATM and Communications Navigation and Surveillance (CNS) system e.g. in the surveillance system or communications between aircraft and the ATC Center (Netjasov & Janic, 2008).

This research project focuses on technical failure risks. In fact, the primary objective of this research project is to assess the risk and safety of an ATM system due to failures of particular technical systems that decrease the capacity and functionality of the ATM, increase staff workload and even increase the probability of loss of separation or collision with a focus on the effect of failures of the electrical power system.

It was determined that the **Failure Mode, Effects, and Criticality Analysis (FMECA)** and **Reliability Block Diagram (RBD)** are best suited to reach the identified goals of the research project. Justification as to why these methods were selected is presented in the following subsections.

##### **2.1.1.1. FMECA**

When attempting to model system reliability the system design and functionality needs to be known, and what functionality is vital for operations needs to be specified. Therefore it is important to identify all required functions and their output with respect to the failures, their effects and modes. As systems can be quite complex it is practical to use a structured method for this purpose. FMECA is a known, frequently used method that offers a structured way of getting to know the system design, its features and to understand failures and their consequences. FMECA is an inductive, bottom-up

method to analyze system design for safety and performance. This means that the system is analyzed by focusing on the failures of individual components and working gradually upwards by grouping components into subsystems. The FMECA determines the effects of component and functional failure modes on the system and includes criticality ranking calculations for each failure mode and effect (Testability.com, 2008; ITEM Software, Inc., 2012). The end product is a list of equipment, functionality and the weight of criticality of failure effects.

FMECA is generally used in three different ways, to:

1. Identify the potential failure of each of the functional blocks of a system,
2. study the effects these failures might have on the system and
3. prioritize the significance of different failures (Rausand & Høyland, 2004) (Reliasoft, 2007).

FMECA is primarily a tool for designers but is frequently used as a basis for more detailed reliability analysis e.g. during modifications and for maintenance planning (Rausand & Høyland, 2004).

FMECA is considered suitable for ATM systems since the objective is to study the components of the ATM system and how critical they are to the ATC Centers' operation i.e. what effects will failure of a component have on system performance. Assumptions used during reliability modeling are made based on the information from the FMECA. Thus the FMECA provides a basis for a quantitative reliability analysis, which is in fact one of FMECA's objectives (IEEE Std. 352, 1982). At the same time the analysis provides a valuable document for future reference that can be used to aid in failure analysis (Rausand & Høyland, 2004).

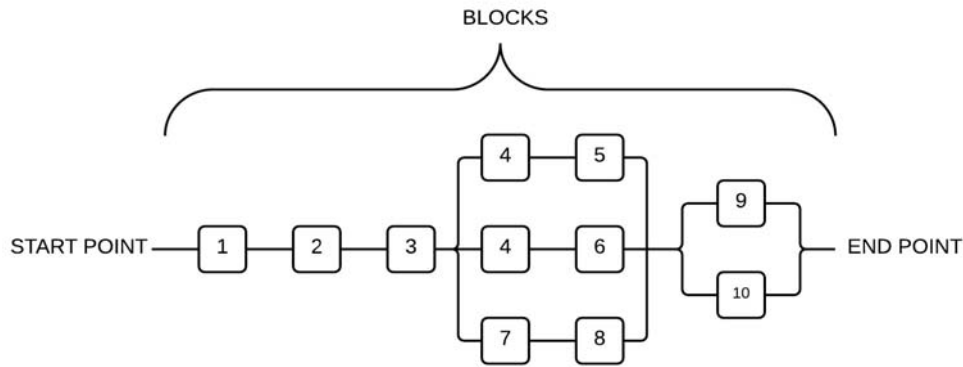
A more detailed description of the FMECA methodology and how it is used in this research project will be provided in chapter 3.

#### **2.1.1.2. RBD**

Reliability block diagram (RBD) is a success-oriented logical diagram for a system, based on its reliability characteristics (Reliasoft, 2007). A system is a collection of components, subsystems and/or assemblies arranged in a specific design in order to achieve desired functionality. The types of components, their quantities, their qualities and the design configuration in which they are arranged have a direct effect on system reliability (Rausand & Høyland, 2004).

The overall structure of the system is illustrated by a functional reliability block diagram describing how various subsystems interact to deliver the designed functionality of the system. The popularity of designing redundancy into systems poses challenges during reliability modeling (United States Army, 2007). An example of RBD is shown in Figure 2-1. For this system components 1, 2 and 3 are always needed for the system to function whereas either component 9 or 10 must be functioning. Furthermore component 4 is needed for four of the available paths through the system.





**Figure 2-1: An example of RBD. The system is functioning if there is a path between start and end point of the diagram. (In this case block number 4 is needed for two of the available paths).**

The RBD modeling starts with the study of the overall design of the system. When systems are large and complex it is a classic approach to break the system into subsystems or components from a top-down point of view until the desired level of detail is obtained. Ideally, the system should be segmented to the lowest actionable level i.e. the lowest level where data is available or can be obtained. However, the level of detail must be specified in each case depending on the objectives of the analysis (United States Army, 2003; Rausand & Høyland, 2004; Bailey, Frank-Schultz, Lindeque, & Temple III, 2008). For example an electrical power system can be segmented into power generators, switches, Uninterruptable Power Supply (UPS), etc. This is the level that this analysis will study. An even lower level could be the parts which make up these components (the power generators, switches and the UPS). Segmentation involves the assumption that components are independent of each other and thus each part can be evaluated separately.

The RBD is supported by a software system that provides a powerful tool for developing models for highly complex systems. A more detailed description of the RBD methodology will be provided in chapter 4.

The following section presents examples of some methods previously applied and related literature concerning technical failure risk. Subsequently an overview and a description of some safety research methods concerning human error risk and collision risk is presented shortly in sections 2.2.3. and 2.2.4. and in more detail in appendix D.

#### **2.1.1.3. Other technical failure research methods**

Other technical failure research methods that have been used successfully in the field of air transport include the following. These are however not used in this research project.

#### **Fault Tree Analysis (FTA)<sup>8</sup>**

FTA was developed by Bell Laboratories (Kumamoto & Henley, 1996) in 1962 and has been used to understand the logic of events that might lead to an unwanted event with serious consequences. FTA can be viewed as the logical inverse of the RBD starting

<sup>8</sup> Former name is CTM (Cause Tree Method).

from the top event proceeding downward rather than from the low level system component as is the case in the application of the RBD method. It is a graphical design technique that could provide an alternative to block diagrams using gates instead of paths. FTA is a top-down, deductive approach structured in terms of events. Starting with an event that would be the immediate cause of the event of interest (the top event), analysis is carried out down a tree path. Combinations of causes are described with logical operators (and, or, etc.). The method is commonly used to assess safety and reliability of aircraft and ATM computer components. Many versions of FTA have been developed e.g. IRP which was developed for ATM risk assessment (Netjasov & Janic, 2008; NLR, 2010). As all causes that could possibly affect the undesired event must be known to be able to use this method, the RBD method was considered more suitable for the purpose of this research project. The RBD is also the main method supported by a software system that provides a powerful tool for developing models for highly complex systems.

### **Event Tree Analysis (ETA)**

ETA “...is used for modeling sequences of events arising from a single hazard and describe the seriousness of the outcomes from these events” (Netjasov & Janic, 2008). ETA was developed in 1980 and is widely used. An event tree analysis (ETA) is an inductive technique and is helpful in understanding the consequences of an initiating event and the expected frequency of each consequential event (Xie, Poh, & Dai, 2004).

*“The hierarchy of presenting a hazard, the sequence of events causing failures of the system components and their state in terms of functioning and failure represent the core of the method. Consequently, a tree with branches of events and functioning and failing components displays probabilities of failures along particular branches. These in combination with the probability of the hazardous event enable quantification of the probability of the system or component failure. This method is applicable in combination with FTA for almost all technical systems including aircraft and ATC/ATM components” (Netjasov & Janic, 2008).*

### **Common Cause Analysis (CCA)<sup>9</sup>**

Identifying common failures or events leading to an aircraft accident is a common usage of the common cause analysis (CCA) This method divides the aircraft into “zones” and therefore implying that the system and components in each zone are ultimately independent. Consequently, it is possible to identify the common causes of failures of particular components of such independent systems. The method also makes it possible to identify and assess hazards from external causes that might compromise independence between particular systems and components and cause their failures due to the same (common) causes.

CCA has been in use since 1987 by The US National Aeronautics and Space Administration (NASA) and it has been recommended for assessment of the risk of failures of aircraft systems and equipment (Netjasov & Janic, 2008). CCA is in general

---

<sup>9</sup> Referred to as Dependent Failure Analysis in the nuclear industry (NLR, 2010).

an extension of the FTA with emphasis on identification of multiple failures that can occur from a single common cause or event CCA offers an advantage over other methods when a single cause results in failure of the system (NASA, 1999). As this research project should provide the option of extending the model for other failure modes the RBD approach is considered a more suitable method for the purpose of the research project.

### **Traffic Organization and Perturbation AnalyZer (TOPAZ)**

TOPAZ is a scenario and Monte Carlo simulation-based accident risk assessment of an ATC/ATM operation. It was developed in the 1990s by the Netherlands National Aerospace Laboratory. The model addresses both nominal and non-nominal events and dynamics including issues such as technical/ technological, organizational, environmental, human-related, other hazards and any of their combinations. TOPAZ facilitates quantitative assessment for new or existing systems, providing safe spacing criticality feedback to developers (Netjasov & Janic, 2008).

The method has been applied to risk assessment of many ATC/ATM operations including converging and parallel landings, assessment of wake vortex induced accident risk, and so on (GAIN Working Group B, 2003).

### **Bayesian Belief Networks (BBN)<sup>10</sup>**

The BBN method strives to provide objective and unambiguous information on the state of system safety for managerial decision-making by capturing the various failures of aircraft systems both qualitatively and quantitatively (Roelen, Wever, Cooke, Lapuhaa, Hale, & Goossens, 2003a; Roelen, et al., 2003b).

BBN are probabilistic networks derived from Bayes theorem, which deduces a conclusion based on prior events. The method was developed to improve understanding of the impacts of different causes of the risk. It may be used to identify and illustrate potential causes for system failures. Probability distribution may be allocated to the various causal factors, and the network may be evaluated quantitatively by a Bayesian approach. BBN are more flexible than fault trees since binary representation and specified logic gates are not needed (Rausand & Høyland, 2004).

The method, which originated in the mid- 1980s, was applied at the beginning of 2000s in the US in the scoping of the Aircraft Separation Risk Analysis Model (ASRM)<sup>11</sup> developed by the FAA and NASA. By using case studies coupled with expert knowledge, 20 specific BBN methods have been developed for CFIT and LOC accidents, runway incursion and engine failures. Causal factors have been identified from accident reports (Luxhoj & Coit, 2006).

---

<sup>10</sup> Also known as Bayesian networks, Bayes networks, Probabilistic cause-effect models and Causal probabilistic networks.

<sup>11</sup> ASRM has been used to provide a systematic, structured approach for understanding the aircraft accident causality as well as performing the assessments of new aviation safety products developed through NASA's Aviation Safety and Security Programme.

**2.1.2. Human error risk.** - The risk of accidents due to human error (by aircraft crew and/or controllers).

One of the most frequent causes of accidents relating to aviation is “Human error” (Boeing Commercial Airplanes, 2006). Human error can include various things. It is defined as an incorrect execution by a human operator of a particular task, which then triggers a series of subsequent reactions in the execution of other tasks, resulting in an undesirable event or possibly an aircraft accident (Netjasov & Janic, 2008). Human error is not of particular interest in this research project.

The methods that have been developed in order to reduce the probability of Human errors include the following:

- The Hazard and Operability (HAZOP).
- Human Error Assessment and Reduction Technique (HEART).
- Technique for the Retrospective Analysis of Cognitive Errors (TRACER-Lite).
- Human Error in ATM (HERA).
- Human Factor Analysis and Classification System (HFACS).
- Analytic Blunder Risk Model (ABRM).
- Reduced Aircraft Separation Risk Analysis Model (RASRAM).

Further description on these methods is provided in appendix D.

**2.1.3. Collision risk.** - The risk of aircraft collision due to deterioration of separation rules.

ATC is concerned with preventing conflicts that might escalate to a collision of an aircraft with another aircraft during the en route phase<sup>12</sup>, or with fixed obstacles during landing or take-off. In general, separating aircraft using space and time separation standards (minima) has prevented conflicts and collisions. *“It could be observed that the absence of minima separation leads aircraft to a state of high collision probability”* (Vismari & Junior, 2011). Due to reduction of this separation (bringing aircraft closer together) in order to increase airspace capacity, assessment of the risk of conflicts and collisions under such conditions has been a popular research subject (Netjasov & Janic, 2008). The methods that have been developed include the following and are discussed in more details in appendix D:

- Reich-Marks model
- Machol-Reich model
- Intersection and Geometric conflict model
- Generalized Reich model

---

<sup>12</sup> En route phase concentrates on the traffic control while the aircraft is in the air (EUROCONTROL, 2011).

## **2.2. The inevitability of failures**

Technical systems such as electrical power systems are often taken for granted as part of the infrastructure that will always be available on demand. Electrical specialists and system operators, however, are well aware of the costs and effort associated with providing high levels of reliability (Hung & Gough, 1996).

Reliability is a key measure of performance for electrical power systems. Those systems must be active for very long periods of time, providing power to critical systems. Even with robust system design and the best available technology, it is economically impractical, if not technically impossible, to design an electrical power system that never fails. Outages may occur even though the system is designed to minimize the probability of their occurrence. Even the most reliable systems can fail, as no system is perfect. This is also true on the first day of operation. This is very unlikely but still the probability of a failure is not zero (United States Army, 2007).

Since failures are inevitable it makes sense to try to decrease their occurrence and minimize their effects when they occur. Designing with redundancy decreases the chance of a failure, however when any one item fails, it must be repaired or replaced to maintain the intended level of redundancy (United States Army, 2007).

An effective maintenance program can minimize the effects of failures on the availability of repairable systems. A highly maintainable system should be able to be restored to full operation in a minimum amount of time and expenditure of resources (United States Army, 2003).

In spite of these significant efforts, equipment failures still occur and every ATM system eventually fails to perform its intended function or part thereof (Subotic, 2007).

While an equipment outage<sup>13</sup>/failure does not necessarily mean that an ATC Center's ability to safely control aircraft is impaired, certain types of failures could pose a potential risk to air safety. The risk depends on factors such as the type of equipment that fails, traffic load<sup>14</sup> and the timing and duration of the failure.

An example is provided:

A power outage occurred on December 18, 1997 at the Kansas City Air Traffic Control Center, which resulted in the loss of all communications with aircraft for 2 minutes and the loss of radar tracking for 12 minutes before back-up equipment became active. As could be expected aircraft were flying in the airspace during the outage (United States General Accountability Office, 1998). FAA officials noted that this outage greatly affected the center's ability to provide air traffic services, and some controllers expressed a concern that this type of outage could have posed a risk to air safety. In

---

<sup>13</sup> Generally speaking, a "failure" is said to have occurred when a required function is terminated by an unexpected event, but the system remains operational. If the entire system becomes unavailable, the failure is known as an "outage" or complete failure (United States General Accountability Office, 1998).

<sup>14</sup> The manageability of an outage can be different dependant on if aircraft mostly follow tracks or not.

contrast, during another outage on June 1, 1998, when the back-up computer system failed, the center's ability to control aircraft was not impaired because the primary system was actively functioning. This ATC Center experienced 18 outages in a 6 month period during which safety was not compromised because of safety procedures<sup>15</sup>. In fact, the percentage of time that it was operating satisfactorily (available) compared favorably to the national average. (United States General Accountability Office, 1998). From this example it can be seen that failures in ATM systems are not that uncommon.

Total failure of power systems and communications equipment can have very serious consequences; however, they occur infrequently (National Transportation Safety Board, 1996). These outages do not necessarily result in violations in the separation of aircraft; on the other hand, they pose a potential threat to safety as well as causing flight delays, resulting in additional costs to airlines and inconveniencing passengers.

In this chapter an overview of safety methods used in this research project and examples of other methods previously used successfully in the field of air transport. This was given in order to demonstrate the importance and state of application of reliability modeling in air transport.

---

<sup>15</sup> Procedures on how to safely handle air traffic when equipment fails to perform.

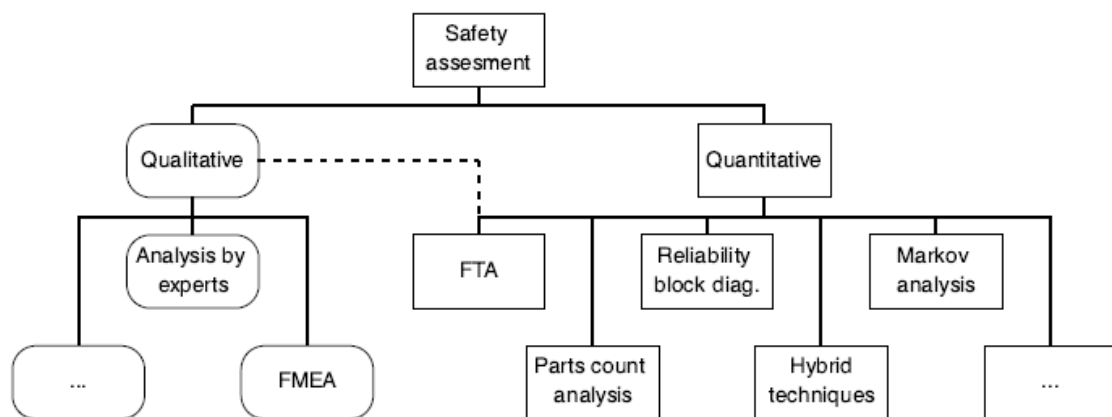
### 3. Introduction to reliability analysis in ATM systems

The purpose of this chapter is to provide an understanding of why the Reliability Block Diagram (RBD) method was selected in this research project and to explain its benefits for studying the reliability of ATM systems. Furthermore this chapter defines the Failure, Mode, Effects and Criticality Analysis (FMECA) method which is used to provide a basis for the reliability analysis.

#### 3.1. Safety analysis techniques and methods evaluation

Many techniques and methods have been developed for reliability analysis in ATM. The analysis techniques can be grouped into qualitative techniques and quantitative techniques depending on the subject matter and availability of data (Rouvroye & Bliet, 2002). Qualitative techniques provide a rank ordering description of the factors that might cause accidents. That can be useful for improving understanding of causes of accidents so they can be avoided. Quantitative techniques estimate the risk of accident by estimating the probability of occurrence of each cause. This can be either pure statistical analysis based on the available data or it can combine such data with expert judgment. They can also estimate the benefits of different solutions aimed at preventing accidents (Spouge, 2004).

Figure 3-1 presents an overview of the most used analysis techniques categorized into quantitative and qualitative groups.



**Figure 3-1: Overview of most used analysis techniques (Rouvroye & Bliet, 2002).**

A formal comprehensive approach to risk assessment that offers a qualitative understanding of ATM system behavior and vulnerability is needed. The approach should be systematic and comprehensive. It should provide a basis for the quantitative analysis of low probability, high severity events, measuring the risk and component importance consistent with analyzed field data. Furthermore, the technique is required to produce lasting benefits for the effort spent and that it can be understood and applied later on by the technical experts within the company. Above all, a method with an established record of success is preferred (Apthorpe, 2001).

To take maximum advantage of the existing body of knowledge, a thorough study of the applicability of previously used techniques should be carried out (Blom H. , Bakker, Blanker, Daams, Everdij, & Klompstra, 2001). According to Everdij, Blom and Kirwan (2006) over 600 methods from various industries are available but only a fraction of them have been used in the field of air transport or in computer based systems that are similar to ATM systems. To narrow down the search, the advantages and disadvantages of some of those methods were examined.

Everdij, Blom and Kirwan (2006) state that the following criteria can be used as reasons for not selecting a method:

- Inappropriate or unsuitable for ATM systems (e.g., methods specifically developed for nuclear or chemical process plants that cannot be easily converted for use in air transport).
- Outdated.
- Superseded by another method.
- Inappropriate scope (Too general or too specific/detailed).
- Emphasis on different aspects (e.g. on human failure as opposed to hardware/software aspects).

It is challenging to find the method that best fits the defined purpose. Since the purpose of the research is to calculate the reliability of a complex computer-based system with a fair degree of redundancy, Reliability Block Diagram (RBD) approach was found very attractive due to the fact that it is the most widely used reliability engineering technique in computing systems (Xie, Poh, & Dai, 2004). After studying and comparing some of the methods that have been successfully used it was concluded that a candidate method for calculating reliability of an ATM system had been found.

In the field of air transport RBDs have mostly been used to assess aircraft avionics<sup>16</sup> (NLR, 2010). RBDs have up until now not been used directly for ATM systems. However, as these are computerized technical systems one can assume that the method will be equally valid in the ATM environment as in other on-line systems.

The RBD method provides a number of benefits. An RBD shows a system graphically from a reliability perspective. Because these diagrams can be nested everything from simple to highly complex systems can be mapped. It can therefore be viewed as being scalable from simple to very complex systems. Components that are critical from a reliability point of view can be identified using the RBD techniques. In particular it can be used to identify Single Points of Failure (SPOF) and to assess the impact that design changes will have on system reliability (Bailey, Frank-Schultz, Lindeque, & Temple III, 2008).

While the RBD approach will be used to present the reliability model of the system, it is practical to use a structured method to study failure effects and to identify which

---

<sup>16</sup> Electronic equipment located on aircraft.



functions are required for successful operation. In this case the Failure Mode Effect and Criticality Analysis (FMECA) is applied.

The RDB method/approach will be defined in further detail in chapter 4. The main concepts of the FMECA method are introduced in following section as well as a description of the general procedure for its application to the Isavia ATM system.

### **3.2. Providing a basis (FMECA)**

FMECA is an inductive, bottom-up method which means approaching with analyzing the failures of individual components of the system and building up gradually. It is used to analyze system design for safety and performance. It determines the effects of component and functional failure modes on the system and includes criticality ranking calculations for each failure mode and effect (Testability.com, 2008; ITEM Software, Inc., 2012).

FMECA is generally used in three different ways, to:

1. Identify the potential failure of each of the functional blocks of a system.
2. Study the effects these failures might have on the system.
3. Prioritize the significance of different failures (Rausand & Høyland, 2004; Reliasoft, 2007).

FMECA is primarily a tool for designers but is frequently used as a basis for more detailed reliability analysis e.g. during modifications and for maintenance planning (Rausand & Høyland, 2004).

FMECA is considered suitable for ATM systems since the objective is to study the components of the ATM/CNS system and how critical they are to the ATC Centers' operation i.e. what effects will failure of a component have on system performance. Assumptions used during the reliability modeling are made based on the information from the FMECA. Thus the FMECA provides a basis for a quantitative reliability analysis, which is in fact one of FMECA's objectives (IEEE Std. 352, 1982). At the same time the analysis provides a valuable document for future reference that can be used to aid in failure analysis (Rausand & Høyland, 2004).

In each case, FMECA is modified to fit the objective of the analysis. Information regarding FMECA adapted to the objective of this analysis<sup>17</sup> is therefore provided in this chapter.

---

<sup>17</sup> More detailed information on FMECA may be found in published guidelines and standards SAE-ARP 5580, SAE J1739, AIAG FMEA-3, IEC 60812, BS 57060-5 and MILSTD-1629A (Rausand & Høyland, 2004).

### 3.2.1. FMECA concepts

The main concepts of FMECA are defined as: failure, fault, failure modes, and failure mode classification. These will now be discussed in more detail.

#### 3.2.1.1. Failure vs. fault

Failure is the occurrence of an undesirable event resulting in termination of a required function of a component, while fault is “...the state of an item characterized by inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources” (IEC 50(191), 1990). An example of external resources could be electrical power.

In other words, fault is a state resulting from a failure. The relationship between these terms is illustrated in Figure 3-2 below (Rausand & Høyland, 2004).

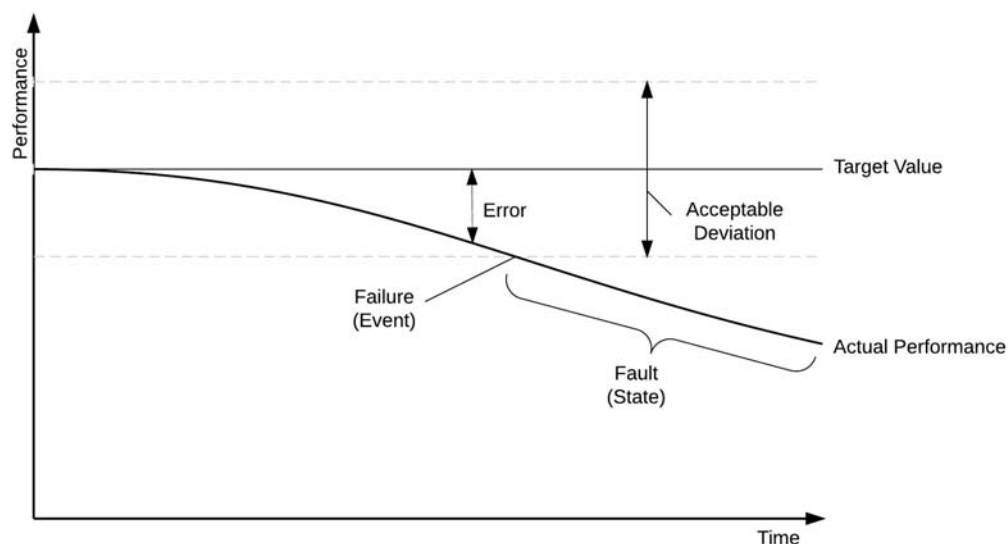


Figure 3-2: The relationship between failure and fault (Rausand & Høyland, 2004).

Failure of a component does not necessarily mean that it has completely broken down. It can fail in two basic ways. First, a component can fail to perform one or more of its' required functions. Second, a component can fail in such a way that no function is impaired e.g. one of two redundant components fails when only one is required for a successful function (United States Army, 2003; Chandrupatla, 2009).

#### 3.2.1.2. Failure modes vs. failure causes

A failure mode is a description of a fault<sup>18</sup> i.e. the state of the component after failure. This is a nonfulfillment of a functional requirement. A failure mode generally describes the way the failure occurs and is the manifestation of failure as seen from the outside. Failure modes occur due to one or many different failure causes i.e. circumstances that have led to failure. One failure mode is power outage, precisely the failure mode being focused on in this research project. This failure mode can occur due to many failure

---

<sup>18</sup> Fault mode would be more descriptive term however failure mode is the term usually used.

causes such as burning of electrical wires, electrical pulses and such events (Rausand & Høyland, 2004; Reliasoft, 2007; Kusy, 2012).

### **3.2.1.3. Failure mode classification**

A failure mode classification has been defined by Blanche and Shirvastava (1994):

1. *“Intermittent failures: Failures that result in a lack of some function only for a very short period of time. The functional block will revert to its full operational standard immediately after the failure.*
2. *Extended failures: Failures that result in a lack of some function that will continue until some part of the functional block is replaced or repaired” (Rausand & Høyland, 2004).*

Extended failures are of main concern in this analysis and may be further divided into:

- a) *“Complete failures: Failures that causes complete lack of a required function.*
- b) *Partial failures: Failures that lead to a lack of some function but do not cause a complete lack of a required function” (Rausand & Høyland, 2004).*
3. Failures in fault tolerant systems: Failures that have no effect on functionality i.e. the system is able to perform its function despite experiencing a failure. This is the case in systems where redundancy is used. Fault tolerance is achieved by one or more redundant components taking over the function previously being performed by another component (United States Army, 2007).

These may be further classified for more detailed description of failure.

As these definitions indicate, the failure mode classification depends on the system function. Thus system function must be clearly defined to be able to categorize the system according to these classifications. As an example, the function of the electrical power system is to deliver power to all four power terminals. So what would be a partial failure? This will be defined with a number of assumptions for each case based on the FMECA.

### **3.2.2. FMECA procedure**

The procedure starts with breaking the system down to subsystems and components. It is often difficult to decide on which component level the analysis should be conducted. The analysis is, however, ideally broken down to a level at which failure data is available or can be obtained. A complete list of all the components at the lowest actionable level is prepared.

For each component, information such as the failure modes and the resulting effects are recorded in a specific FMECA worksheet. There are numerous variations of such worksheets as they are modified to fit the objective of each analysis. An example of an FMECA worksheet is shown in appendix I. In the following bullets the worksheet is gone through column by column as described in Rausand and Høyland (2004):

- Item (column 1). The name of the item that will be the subject of the analysis.
- Function (column 2). The function of the item is described.
- Failure mode classification of the system (column 3). The state of the system after failure of this item.
- Effect of failure on system function (column 4). The main effects that would result from the occurrence of failure of that item. The resulting operating status of the system i.e. whether the system is functioning or not.
- Criticality/severity (column 5). Severity of a failure mode means the worst potential consequence of the failure. Criticality is often a measure of the severity and failure rate combined. In this study failure rate is not known for the ATM equipment and thus criticality represents a measure of how crucial the equipment is considered for system operation. Ranking categories are adopted to describe this.
- Risk reducing measures (column 6). Measures reducing the severity of failure (e.g. maintenance to restore the function) or the likelihood of the failure occurring (e.g. by redundancy).
- Comments (column 7). Other relevant information.

To avoid unnecessary documentation, a few commonly used columns were skipped, namely operational mode, detection of failure, failure causes<sup>19</sup> and failure rate. These were in general considered to be too detailed for the intended purpose of this research project. This information can of course be valuable but is not necessary for this research.

FMECA is a reliability analysis that is straight-forward to conduct even for complex systems. The FMECA technique allows the identification of how the failure of each system component can result in system performance problems (Bailey, Frank-Schultz, Lindeque, & Temple III, 2008). During the analysis, each possible failure is evaluated individually as an independent occurrence with no relation to other failures in the system (Rausand & Høyland, 2004; Bailey, Frank-Schultz, Lindeque, & Temple III, 2008). Multiple component failure can then be analyzed by other techniques such as RBD.

The end product is a list of equipment, functionality and the measure of criticality of failure effects. The FMECA provides valuable systematically summarized information that can be used to decide which components are to be modeled creating the RBD of the system (Bailey, Frank-Schultz, Lindeque, & Temple III, 2008).

---

<sup>19</sup> Failure causes was not needed because in this analysis the failure solely occurs due to loss of electrical power.

### 3.2.3. FMECA for the RACC System

FMECA analysis has not been performed for the RACC System in the past. It can generate valuable information regarding importance of specific components within the system vis-à-vis system reliability. In this research project the FMECA was performed to identify which subsystems and system components are most important and whether failures of these have critical impact on the operation of the ATC Center. It assesses the consequences of failures on the safety of operations within a specified operational environment at the ATC Center.

The FMECA is based on information provided by Isavia specialists<sup>20</sup> in the operation of the ATM system. The analysis consists of the following:

- Explanation of component functions<sup>21</sup>.
- Failure mode of the system.
- Effects of failure on system functionality.
- Criticality/severity ranking.
- Risk reduction methods.
- Comments.

Each part is presented as a column in the FMECA results sheet in appendix J.

The analysis was performed based on the assumption of three failure modes classifications: Complete-, severe partial failure and partial failure. Partial and complete failure are well known classifications of failures used in many prior studies, Severe partial failure is not a predefined classification but is a useful intermediate stage of failure used in this analysis. Failure mode classifications are assumed as follows:

- Complete failure: A failure that causes complete lack of a required function of the system.
- Severe partial failure: A failure that leads to the lack of some functions with severe consequences without causing a complete lack of a required functionality.
- Partial failure: A failure that leads to a lack of some functions but does not cause a complete lack of the required system functionality.

However, when looking at individual components, failure always means complete failure of that component unless noted otherwise. Using the H1<sup>22</sup> radar as an example, partial failure means that the complete failure of the H1 unit leads to a lack of the radar function i.e. partial failure of the ATM system. However, looking at another example, the failure of H1, H2, H3, H4 and KEF radars would result in a severe partial failure of the ATM system which results in an extensive lack of vital functions having severe consequences for the ATC operation.

---

<sup>20</sup> Arnar Sigurðsson and Arnór Bergur Kristinsson Projects Manager at Isavia.

<sup>21</sup> Further explanations of functionality of equipment can be seen in appendix C.

<sup>22</sup> See the results sheet in appendix J.

The criticality of equipment failures can be different depending on the viewpoint. Air transport policies have been aimed at increasing capacity as well as reducing acceptable risk (Netjasov & Janic, 2008). Therefore two factors were considered while assessing the criticality; capacity and workload. Table 3-1 shows the ranking associated with each factor. The event of failure of certain equipment can have severe consequences in terms of capacity, whereas workload is less affected and vice versa. The ranking represents the worst case scenario i.e. when evaluating failure, what is the worst that could happen? The criticality can also depend on the detectability of the failure i.e. the probability of failure being detected as well as recovered. For simplification the failures were considered easily detectable in this preliminary FMECA.

**Table 3-1: The criticality ranking used during the FMECA and the associated meaning of each value.**

<b>Capacity</b>		<b>Workload</b>	
<b>Criticality ranking</b>	<b>Ranking signifies</b>	<b>Criticality ranking</b>	<b>Ranking signifies</b>
<b>0</b>	No affects on capacity	<b>0</b>	No affect on workload
<b>1</b>	Not severe but has some affect on capacity	<b>1</b>	Considerable pressure on the staff on a shift
<b>2</b>	Intermediary severe	<b>2</b>	Increase on staff needed e.g. Staff on a break come to
<b>3</b>	Very severe and has considerable affects on	<b>3</b>	Significant increase in staff needed

### **3.2.4. FMECA results**

The results of the FMECA are presented in appendix J. Based on the results it was determined what subsystems are of most importance for the operation of the air traffic control center. For normal operation it was found that Voice communication system (VCS) and its terminals (iPOS), Flight Data Processing System (FDPS), Radar Data Processing System (RDPS), Integrated Situation Display System (ISDS), Controller Work Station (CWS), Integrated Controller Environment (ICE), the COM network and VHF voice communications system are the main building blocks of the ATM System operation.

From the results in appendix J it can be seen that there are three failure modes that will have the most critical effect on the ATM system and result in a complete failure of the system function. These failure modes are:

- 1) FDPS and VCS fail at the same time.
- 2) FDPS and VHF voice communications system fail at the same time.
- 3) FDPS and the COM network fail at the same time. The COM network transfers all voice communication and radar signals to the ATC Center. This is provided by the telecommunication company Míla

Only the first option is relevant to this analysis since the others take into account VHF and COM networks, neither of which relies on electricity from the electrical power system of the RACC which is analyzed in this research project.

Since these failure modes represent a failure of the system as a whole it goes without saying that if any additional equipment fails along with one of these failure modes, it also results in a complete failure of the system resulting in a complete lack of system functionality. It should be noted that the failure can occur due to some essential support equipment failing not necessarily the component itself such as the Black Boxes that split up the radar lines providing information for the RDPS.

This analysis is also used to make alternative failure modes that are less catastrophic to the systems function which are used as a basis for the reliability analysis (RBD). This will be represented in the form of numerous assumptions made for different functionality failure modes that will be presented in chapter 5.2. For example a failure mode used to calculate the probability that the system can function normally without any disruption of service will be put forward.

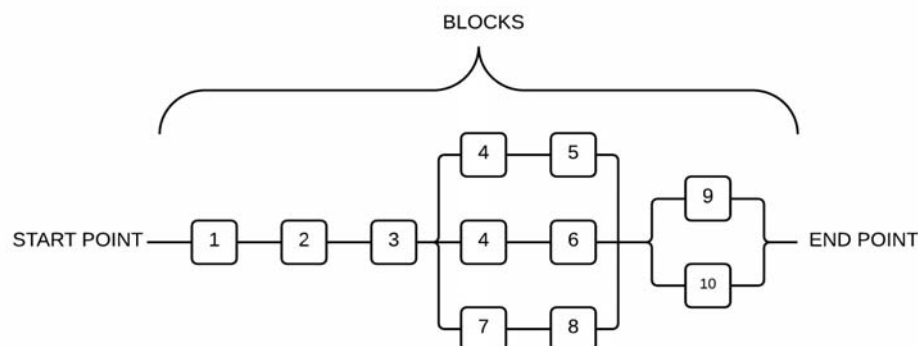
## 4. Methodology

The reliability of the ATM System will be analyzed using the Reliability Block Diagram (RBD) approach. Probability and statistics are the mathematical foundation for the study of reliability (Chandrupatla, 2009). This chapter provides an overview of the RBD approach as well as an overview of the mathematics of reliability theory. This should provide the reader with a practical understanding of the RBD method and how RBD's are used to calculate reliability.

### 4.1. Reliability Block Diagram (RBD)

An RBD is a success-oriented logical model that describes the function of the system from a reliability point of view. The model is configured out of blocks that represent a distinct function or failure mode of the modeled components<sup>23</sup> of the system. This is a graphical representation of how functioning components are connected to sustain successful system operation (Rausand & Høyland, 2004; ITEM Software, Inc., 2007). This reliability configuration may differ from the physical connection of the system (Reliasoft, 2007).

Consider a system consisting of n number of components. In an RBD each of the n components is represented by blocks which are structurally configured to represent all potential flow paths through the system. An example of an RBD is shown in Figure 4-1. When there is a path between the start and end points the system is considered functioning i.e. successfully operational (Rausand & Høyland, 2004; ITEM Software, Inc., 2007). For this system components 1, 2 and 3 are always needed for the system to function whereas either component 9 or 10 must be functioning. Furthermore component 4 is needed for four of the available paths through the system. It must be specified in each case what is needed for a system to be considered functioning or successfully operational, depending on the objectives of the analysis. These conditions of operation must be clearly defined with a number of key assumptions (Rausand & Høyland, 2004; Bailey, Frank-Schultz, Lindeque, & Temple III, 2008; Chandrupatla, 2009).



**Figure 4-1: An example of RBD. The system is functioning if there is a path between start and end point of the diagram.**

<sup>23</sup> Blocks can represent subsystems, subassemblies, components, parts, units, equipment and so forth.



The RBD modeling starts with the study of the overall design of the system. When systems are large and complex it is a classic approach to break the system into subsystems or components from a top-down point of view until the desired level of detail is obtained. Ideally, the system should be segmented to the lowest actionable level i.e. the lowest level where data is available or can be obtained. However, the level of detail must be specified in each case depending on the objectives of the analysis (United States Army, 2003; Rausand & Høyland, 2004; Bailey, Frank-Schultz, Lindeque, & Temple III, 2008). For example an electrical power system can be segmented into power generators, switches, UPS, etc. This is the level that this analysis will study. An even lower level could be the parts which make up these components (the power generators, switches and the UPS). Segmentation involves the assumption that components are independent of each other and thus each part can be evaluated separately. The next step is to obtain suitable data concerning each component.

RBD diagrams depend on:

1. Component properties<sup>24</sup>.
2. Configuration<sup>25</sup>.

Once the data has been provided and components have been combined at a system level the RBD model is ready for calculation of the reliability of the system. The RBD is used to obtain the complete mathematical system reliability function which can be used to obtain exact reliability results (Reliasoft, 2010).

Now, the mathematics behind reliability analysis will be considered.

#### 4.1.1. Calculating reliability

A commonly used definition of reliability is the following:

**Definition 1.** *Reliability*  $R(t)$  is defined as the probability that the system (or a component) can perform its intended function under stated working conditions for a specified period of time (Xie, Poh, & Dai, 2004; Chandrupatla, 2009). In other words, reliability is a design characteristic that indicates a system's ability to function without failure in a specific time interval.

The reliability function<sup>26</sup> of an item is defined by (Rausand & Høyland, 2004):

$$R(t) = 1 - F(t) = \Pr(T > t) \text{ for } t > 0 \quad (4.1)$$

Where  $T$  is a random variable presenting the failure time or time-to-failure,  $F(t)$  is the probability of failure and  $t$  is operating time.

Or equivalently if  $T$  has a Probability Density Function (PDF)<sup>27</sup>  $f(t)$ .

---

<sup>24</sup> Also referred to as life data, reliability data, failure data or component characteristics.

<sup>25</sup> Component arrangement or construct.

<sup>26</sup> Also referred to as success or survival function.

$$R(t) = 1 - \int_0^t f(u)du = \int_t^{\infty} f(u)du \quad (4.2)$$

*“Hence  $R(t)$  is the probability that the item does not fail in the time interval  $(0,t]$ , or, in other words the probability that the item survives the time interval  $(0,t]$ , and is still functioning at time  $t$ ” (Rausand & Høyland, 2004).*

Consequently, the  $f(t)$  of the items needs to be known to be able to calculate their reliability. As equation (4.1) shows the complement<sup>28</sup> of reliability is the probability of failure. As a result, being able to characterize the component properties is one of the most important aspects of reliability engineering activities (Sararakis, Gerokostopoulos, & Mettas, 2011).

According to Rausand and Høyland (2004) reliability can be measured in different ways depending on the analysis:

1. Mean time to failure ( $MTTF$ ).
2. Failure rate.
3. Probability that the component does not fail in a time interval  $(0,t]$  (reliability).
4. Probability that the component is available to operate at time  $t$  (availability<sup>29</sup>).

In this study the first of these measures will be used to represent the reliability of components within the electrical power system. The  $MTTF$  values are used to calculate the reliability of the system (third measurement) as these are relatively easy to obtain or estimate.

When the system is non-repairable, reliability is equal to availability (Reliasoft, 2007). This means that the unit is under consideration until the first failure occurs. In actuality all units of the ATM system are repaired after the failure.

#### 4.1.2. Mean Time To Failure (MTTF)

A commonly used definition of MTTF is the following:

**Definition 2.** The *mean time to failure (MTTF)* is defined as the expected lifetime before a failure occurs (Xie, Poh, & Dai, 2004).

Suppose that the reliability function for a system is given by  $R(t)$ , the  $MTTF$  of an item is defined by:

$$MTTF = \int_0^{\infty} t \cdot f(t)dt = \int_0^{\infty} R(t)dt \quad (4.3)$$

---

<sup>27</sup> The Probability Density Function (PDF) is the differential of the cumulated density function  $F(t)$  which is the probability of failure i.e.  $f(t)=F'(t)=-R'(t)$ . Thus if any of  $R(t)$ ,  $F(t)$  and  $f(t)$  is known, the others can be determined (Xie, Poh, & Dai, 2004).

<sup>28</sup> The complement of an event  $A$  is the event that  $A$  does not occur i.e. probability of failure is the complement of probability of success and vice versa.

<sup>29</sup> Availability is defined in more detail later in this chapter and in appendix F.

Ideally, the *MTTF* represents a statistical value of large number of identical components. The interval to failure may be measured in time (years, hours and minutes) or in number of cycles depending on the analysis (Chandrupatla, 2009).

*MTTF* is a measure of reliability for non-repairable systems. Another important measure is used for repairable systems, Mean Time Between Failures (*MTBF*). This implies that the system can be repaired in the event of failure and it takes a Mean Time To Repair (*MTTR*) the system. Mathematical relationship between these measures is given by (Xie, Poh, & Dai, 2004):

$$MTBF = MTTF + MTTR \quad (4.4)$$

When *MTTR* is small in comparison to the other values, the *MTBF* is approximately equal to the *MTTR*.

The component characteristics and the configuration in which they are arranged in the system have a direct effect on the system's reliability (Reliasoft, 2007). These aspects are discussed more closely in the following sections.

#### **4.1.3. Component characteristics**

Having segmented the system into components, the first step in evaluating the reliability of a system is to obtain reliability data concerning each component i.e. each block.

Time-to-failure data can be gathered from different sources, including:

1. In-house reliability tests.
2. Accelerated life tests.
3. Field data such as operator shift reports, monitoring system logs.
4. Warranty data.
5. Engineering knowledge or specialist insight.
6. Comparable to prior system designs (assumes that failure data from one system can be used to predict the reliability of a comparable system).
7. Manufacturer, supplier or vendor information (Reliasoft, 2007).

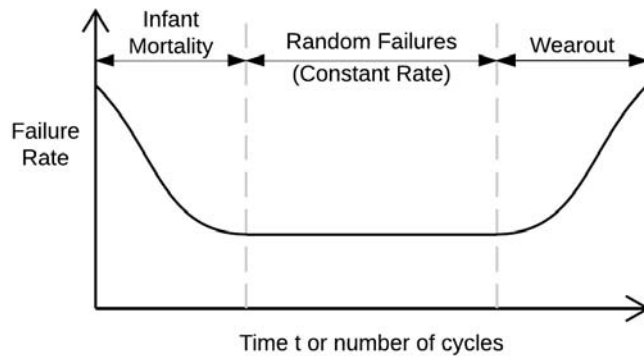
This information will allow determination of the life distribution of each component (Reliasoft, 2007). The analysis of time-to-failure data includes various data analysis techniques. The life distribution<sup>30</sup> that best fits to the data can be estimated using Reliasoft's Weibull++ life data analysis software and ReliaSoft's ALTA accelerated life testing analysis software (Reliasoft, 2007).

---

<sup>30</sup> Also referred to as failure/reliability distribution.

#### 4.1.3.1. Observing failure data and fitting a failure distribution to components

Failure rate is a function that describes the number of failures experienced or expected per time unit or cycles (Rausand & Høyland, 2004; Testability.com, 2008). Failure rate generally varies over the life cycle of the system. The plot of failure rate versus time (or number of cycles) typically has a bathtub shape as shown in Figure 4-2.



**Figure 4-2: Failure rate at time t (“Bathtub Curve” or “Life-Cycle Curve”) (Chandrupatla, 2009).**

There are three life stages known as:

1. The ‘infant-mortality’ or ‘burn-in’ stage.
2. The ‘Steady-life’ stage (nearly constant failure rate).
3. The ‘wear-out’ stage (the failure rate increases as components degrade due to wear) (Apthorpe, 2001).

A mathematical function model that describes the probability of failure (or the probability of success – reliability) of the component at different ages then was used to quantify component reliability. This is referred to as a failure or reliability distribution of the component (Reliasoft, 2007).

A number of probability distributions may be used to model the probability of failure, e.g.:

- Exponential distribution.
- The Weibull distribution.
- The lognormal distribution.
- The normal distribution.
- The gamma distribution.

The most widely used distributions in reliability studies are the exponential distribution, the Weibull distribution and the lognormal distribution (Chandrupatla, 2009).

When modeling component failure rates, the component type (software, hardware, mechanical, electrical) must be considered<sup>31</sup>. The times to failure of electronic components, for example, often follow the exponential distribution because it is often assumed that they do not wear out (memory loss property). On the other hand, the failure of mechanical components is often represented by the Weibull distribution (Apthorpe, 2001; United States Army, 2003)

---

<sup>31</sup> Other factors must be considered such as operation characteristics (active or stand-by unit), maintenance frequency, test frequency, operating environment and so on.

#### 4.1.3.2. Exponential distribution

The underlying statistical distribution of the time to failure for components is often assumed to be exponential. Where *MTTF* relies on the exponential distribution it is sometimes referred to as “point estimate”. Point estimate involves the use of sample data to calculate a single statistical value that represents a best estimate of an unknown parameter (Gnedenko & Khichin, 1962). These estimates give the average *MTTF* (i.e. one point). The exponential distribution implies a constant failure rate equal to  $\lambda$ . This does not capture changes in failure rate over time i.e. exponential distribution does not take into account the infant-mortality and wear-out failures. This can result in overly optimistic reliability estimates (Sarakakis, Gerokostopoulos, & Mettas, 2011). With point estimates, the data collector only needs to count operational hours and failure events for a component. Other distributions require more precise time-to-failure data (United States Army, 2007).

In this analysis the data was built on specialist insight and vendor-supplied *MTTF*. Because of lack of suitable data and the memory loss property commonly attributed to electrical systems, the exponential distribution was assumed.

Consider an item, with an exponential distribution, that is put into operation at time  $t=0$ . The time to failure  $T$  of the item has a Probability Density Function (PDF).

$$f(t) = \begin{cases} \lambda e^{-\lambda t} & \text{for } t > 0, \lambda > 0 \\ 0 & \text{otherwise} \end{cases}$$

This distribution is called the exponential distribution with failure rate parameter  $\lambda$ , and is sometimes written as  $T \sim \exp(\lambda)$ . In this case  $T$  is a random variable that has an exponential distribution.

The reliability function is:

$$R(t) = PR(T > t) = \int_t^{\infty} f(u) du = e^{-\lambda t} \text{ for } t > 0 \quad (4.5)$$

The *MTTF* is:

$$MTTF = \int_0^{\infty} R(t) dt = \int_0^{\infty} e^{-\lambda t} dt = \frac{1}{\lambda} \quad (4.6)$$

The failure rate function is defined as:

$$z(t) = \frac{f(t)}{R(t)} = \frac{\lambda e^{-\lambda t}}{e^{-\lambda t}} = \lambda \quad (4.7)$$

If the underlying failure distribution is exponential, the reliability function of the item is:

$$R(t) = e^{-\lambda t} \quad (4.8)$$

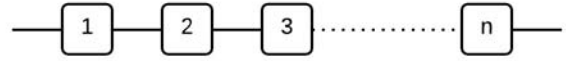
Where  $R(t)$  is reliability in the time interval  $(0, t]$ ,  $t$  is the time period the system must function,  $e$  is the base of natural logarithms and  $\lambda$  is the failure rate (inverse of  $MTTF$ ).

#### 4.1.4. Configuration

An RBD is made up of individual blocks that are connected to other blocks making up a system. Each block corresponds to a component (failure mode/cause) or a function that can fail. Those blocks can be configured (i.e. interconnected) in several ways i.e. by series structures, parallel structures, k-out-of-n structures, load sharing structures and stand-by structures. A mathematical definition of each of these will be presented below.

##### 4.1.4.1. Series Structure

The system is functioning if all of its  $n$  components are functioning i.e. if one component fails, the system fails. In other words the system is functioning if and only if there is a path from the



**Figure 4-3: Series structure built with  $n$  components (Rausand & Høyland, 2004).**

start point through all the  $n$  blocks to the end block (Rausand & Høyland, 2004). The total system reliability is less than the reliability of the least reliable component which is therefore often referred to as weakest link. The system reliability decreases as more components are added. The series structure reliability block diagram is shown in Figure 4-3 (United States Army, 2003; Rausand & Høyland, 2004; Reliasoft, 2007).

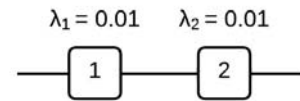
The reliability function is:

$$R_s = R_1 \cdot R_2 \cdots R_n = \prod_{i=1}^n x_i \quad (4.9)$$

*Example 4-1: Two components in series.*

Suppose that  $\lambda_1 = 0.01$  and  $\lambda_2 = 0.02$  are constant failure rates for an exponential model. Reliability of those components can be calculated:

$$\begin{aligned} R_1(t) &= e^{-\lambda_1 t} = 0.99005 \\ R_2(t) &= e^{-\lambda_2 t} = 0.98020 \end{aligned} \quad \text{where } t = 1 \text{ time units}$$



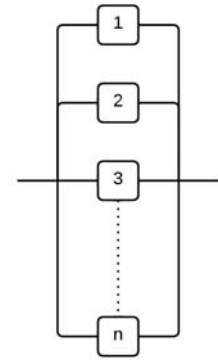
**Figure 4-4: Two components in a series with their constant failure rates.**

Then the reliabilities of a block 1 and 2 are known to be  $R_1(t) = 0.99005$  and  $R_2(t) = 0.98020$ . Assuming that the blocks are independent from a reliability point of view, the reliability of a system consisting of these two serially connected blocks can be calculated by multiplying the reliabilities of the two components:

$$R_s(t) = R_1(t) \cdot R_2(t) = 0.99005 \cdot 0.98020 = 0.97045$$

#### 4.1.4.2. Parallel Structure (Redundancy)

As systems become more critical to an organization, more emphasis is placed on reliability (Leveson, 1992). In order to provide continuous air traffic services, redundancy is designed into systems to prevent or mitigate the occurrence of subsystem failures i.e. the system does not fail due to failure of a single subsystem that has built in redundancy (Subotic, 2007). Redundancy increases availability by allowing the system to operate despite the event of component failure. In general, redundancy means that there is an active master component and a backup component that is not



**Figure 4-5:** Parallel structure with n components (Rausand & Høyland, 2004).

actively participating within the system during normal operation. Thus failure of the first unit (master) does not result in failure of the required function. Redundancy poses challenges during reliability modeling as increased redundancy results in increased complexity of the system (United States Army, 2003).

A parallel structure is used to show redundancy (ITEM Software, Inc., 2007). The system is functioning if at least one of its n components is functioning i.e. system fails only if all components fail. The system is functioning if there is at least one path between the start and endpoints. The system reliability increases as more components are added. A parallel structure reliability block diagram is shown in Figure 4-5 (United States Army, 2003; Rausand & Høyland, 2004; Reliasoft, 2007).

The reliability function is:

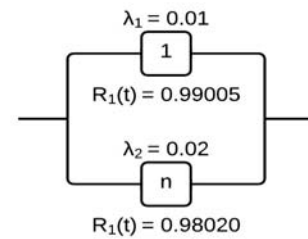
$$R_s = 1 - (1 - R_1)(1 - R_2) \cdots (1 - R_n) = \prod_{i=1}^n (1 - R_i) \quad (4.10)$$

#### Example 4-2: Two components in parallel

One of the two possible paths is sufficient for the system to be successfully operational. The reliability of the system can be calculated by the reliability function by calculating the probability of failure ( $1 - R(t)$ ) for each path, multiplying the probabilities of failure and then subtracting the result from 1.

Using the reliability of each component that was found in the previous example,  $R_1(t) = 0.99005$  and  $R_2(t) = 0.98020$ , the reliability of the system is:

$$R_s = 1 - (1 - R_1(t)) \cdot (1 - R_2(t)) = 1 - (1 - 0.99005) \cdot (1 - 0.98020) = 0.99980$$



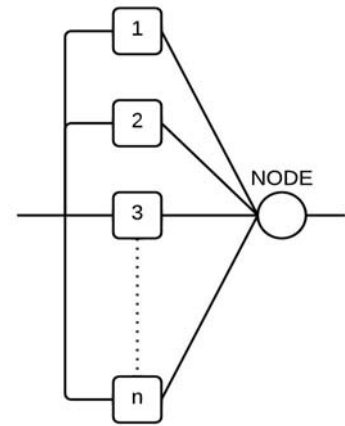
**Figure 4-6:** Two components in parallel with their constant failure rates.

#### 4.1.4.3. *k-out-of-n structure*

A system is considered functioning if at least  $k$  out of a total of  $n$  components are functioning. A series structure is an  $n$ -out-of- $n$  and parallel structure is a  $1$ -out-of- $n$  structure (Rausand & Høyland, 2004).

A node<sup>32</sup> (voter) is used to specify the number of components needed for the system to be successfully operational (Xie, Poh, & Dai, 2004).

A  $k$ -out-of- $n$  structure reliability block diagram is shown in Figure 4-7.



**Figure 4-7: A  $k$ -out-of- $n$  structure.**

The node fails if there are less than  $k$  components functioning. If the node does not fail and all the components have the same failure distribution and reliability  $R$ , the reliability of the structure can be calculated using the binomial distribution (Xie, Poh, & Dai, 2004; Reliasoft, 2007):

$$R_s = \sum_{i=k}^n \binom{n}{i} R^i (1-R)^{n-i} = \sum_{i=k}^n \frac{n!}{i!(n-i)!} R^i (1-R)^{n-i} \quad (4.11)$$

Where  $n$  is the total number of units in parallel,  $k$  is the minimum number of units required for the system to function and  $R$  is the reliability of each unit.

In series, parallel and  $k$ -out-of- $n$  configurations the components are assumed to be independent. These structures can be merged into one block by calculating the reliability using the reliability functions of the configurations and then the system reliability can be easily computed.

Next constructs with dependant units are considered. The components within these structures can be in series, parallel or  $k$ -out-of- $n$  configurations.

#### 4.1.4.4. *Load sharing construct*

The previously defined reliability of parallel units is based on the assumption that when a redundant unit fails it has no influence on the reliability of the surviving units. There will however be situations when this will not prevail and the reliability of the surviving units will change. Then there are dependencies between the units. Usually the reliability will decrease because their share of the load increases (Kececioglu, 2002).

In a *load sharing configuration*, there is a dependency upon the redundant components<sup>33</sup>. In the event a component fails, the other components compensate for the failure by taking on an increased load to keep the system operating.

<sup>32</sup> A node is defined in Appendix G.

<sup>33</sup> Independence was assumed for simple parallel configurations.



When dealing with load sharing, the reliability function has to take into account all possible combinations of failure and survival. Thus a container<sup>34</sup> with  $n$  components would result in having  $n-1$  integral level (Kusy, 2012). Hence, formulating load sharing can be very complex and for the purpose of this research project only two- unit load sharing needs to be considered<sup>35</sup>.

The reliability of a two-unit load sharing container (as for example the Uninterruptable Power Supplies in our system) at some time  $t$ , can be calculated with the following general equation<sup>36</sup>.

$$R(t, S) = R_1(t, S_1) \cdot R_2(t, S_2) + \int_0^t f_1(x, S_1) \cdot R_2(x, S_2) \cdot \left( \frac{R_2(t_{1e} + (t-x), S)}{R_2(t_{1e}, S)} \right) dx + \int_0^t f_2(x, S_2) \cdot R_1(x, S_1) \cdot \left( \frac{R_1(t_{2e} + (t-x), S)}{R_1(t_{2e}, S)} \right) dx \quad (4.12)$$

Where  $S_1 = P_1 S$ ,  $S_2 = P_2 S$  and  $S$  is the total load.  $P_1$  and  $P_2$  are the portion of the total load that each unit supports when both units are operational.  $S_1$  and  $S_2$  represent the load that Unit 1 and Unit 2 must support when both units are operational.  $R_1$  and  $R_2$  are the reliability of corresponding components.  $f_1$  is the *PDF* of component 1 and  $t_{1e}$  is the equivalent operating time for Unit 1 if it had been operating at  $S$  instead of  $S_1$ .

#### 4.1.4.5. Stand-by Construct

The previously defined reliability of parallel units is based on the assumption that all units are operating simultaneously. However, components in parallel may always be operating (active redundancy) or some may be off (stand-by redundancy). In the latter case, back-up units stand idly by in cold, warm or hot stand-by mode until called upon by a switching system when the active unit fails. The function of the switching system is to detect a failure in the active unit and activate the stand-by unit. Stand-by redundancy may be necessary to avoid interference between the components. Since the redundant component is normally off it is less used and is only in use from the time when the active component fails (Kececioglu, 2002; United States Army, 2003).

As in load sharing, the reliability function has to take into account all possible combinations of failure and survival. Thus a container with  $n$  components would result in having  $n-1$  integral level e.g. a container with four components would result in a triple integral (Kusy, 2012). For simplification an example the reliability function of a two-unit stand-by system will be considered. A two-unit stand-by system succeeds when:

---

<sup>34</sup> A container is defined in appendix G.

<sup>35</sup> An example demonstrating how fast the formulation becomes complex is demonstrated by looking at a load sharing construct with 3 units. This is presented in appendix K.

<sup>36</sup> BlockSim implementation of the load sharing can be seen in appendix H.

1. The active unit does not fail and the switching system does not fail.
2. The active unit fails, the switching system does not fail and the stand-by unit hasn't already failed (at time  $x$ ) and succeeds until time  $t$  (Kececioglu, 2002; Reliasoft, 2007).

The reliability of a two-unit stand-by container at some time  $t$ , can be calculated with the following general equation<sup>37</sup>:

$$R(t) = R_1(t) + \int_0^t f_1(x) \cdot R_{2;SB}(x) \cdot \frac{R_{2;A}(t_e + t - x)}{R_{2;A}(t_e)} \cdot R_{SW;Q}(x) \cdot R_{SW;REQ} dx \quad (4.13)$$

Or if there is no switching action:

$$R(t) = R_1(t) + \int_0^t f_1(x) \cdot R_{2;SB}(x) \cdot \frac{R_{2;A}(t_e + t - x)}{R_{2;A}(t_e)} dx \quad (4.14)$$

where  $R_1$  is the reliability of the active component and  $f_1$  is the *PDF* of the active component.  $R_{2;SB}$  is the reliability of the stand-by component when in stand-by mode (quiescent reliability),  $R_{2;A}$  is the reliability of the stand-by component when in active mode and  $R_{SW;Q}$  is the quiescent reliability of the switch. Finally  $R_{SW;REQ}$  is the switch probability per request and  $t_e$  is the equivalent operating time for the stand-by unit if it has been operating in an active mode.

A detailed case study using the RBD software system, BlockSim, is presented in chapter 5.

## 4.2. Analyzing the RBD model

An overall system reliability calculation can be made by looking at the reliabilities of the components within the system. This can be performed either by an analytical approach or simulation. The analytical approach will be used here because it generates exact reliability results whereas simulation generates random failure times for each component. The analytical approach produces a mathematical expression that describes the reliability of the system i.e. it generates the Cumulative Density Function ( $CDF^{38}$ ) for the system. The systems' *CDF* can be used to obtain exact reliability results (Reliasoft, 2007; Reliasoft, 2010). Simulation is however suitable when calculating the reliability of repairable systems including maintenance actions. Then availability of the system is analyzed.

**Availability  $A(t)$ :** Availability of a system is defined as the probability ( $Pr$ ) that the system is available to perform its required function at time  $t$  (Xie, Poh, & Dai, 2004). Mathematically:

---

<sup>37</sup> Contained block properties can be seen in appendix H.

<sup>38</sup> See analytical approach and *CDF* definitions in appendix F.

$A(t) = Pr(\text{System is functioning/available at time instant } t)$

The availability function is a complex function of time but has a simple “steady-state” or average availability that is given by (Xie, Poh, & Dai, 2004):

$$A_{av} = \lim_{t \rightarrow \infty} A(t) = \frac{\text{System uptime}}{\text{System uptime} + \text{System downtime}} = \frac{MTTF}{MTTF + MTTR}$$

This gives the percentage of time that a system is available to perform its required functions (United States Army, 2003).

Availability accounts for both failures and repairs of the system. When the system is non-repairable, availability is equal to reliability (Reliasoft, 2007).

#### **4.2.1. Sensitivity analysis (Reliability Importance)**

The results obtained from the reliability model are sensitive to factors such as the change in choice of distribution and availability of reliability data. Sensitivity analysis assesses the impact that certain changes in components parameters have on the model’s reliability results.

Sensitivity analysis is generally defined as the analysis of how uncertainty in the output of a model can be assigned to different sources of uncertainty in the model input (Saltelli, et al., 2008). In other words, sensitivity analysis is the process of determining the effects on the output of a model through systematic changes in the input.

Sensitivity analysis is commonly used for three purposes:

- 1) To guide system optimization.
- 2) To find reliability/ performance bottlenecks in the system.
- 3) To identify the key components i.e. identify which components have the greatest influence on model’s results (Blake, Reibman, & Trivedi, 1988).

The sensitivity analysis provides an assessment of how change in one components’ reliability affects the reliability of the system as a whole. This generates a wider range of scenarios and can therefore increase the level of confidence in the result generated by the model (Taylor, 2009).

Sensitivity analysis is normally performed by changing one value in the model by a specific amount, and examining the impact that the change has on the model’s results. Thus the task of identifying the least reliable components in a system is rather easy for simple systems. However in case of complex systems a mathematical model is needed. For this purpose it is useful to define the Reliability Importance which is an indicator of the contribution of any given component to the overall system reliability in a certain time period. In other words Reliability Importance represents the impact of a component on the reliability of the total system which is dependent on components reliability and position in the system. The Reliability Importance can be calculated by using BlockSim (Reliasoft, 2007).

The value of Reliability Importance given mathematically by:

$$I_{R_i} = \frac{\partial R_s}{\partial R_i} \quad (4.15)$$

Where  $R_s$  is the system reliability and  $R_i$  is the component reliability (Leemis, 1995).

Reliability Importance changes with time but if the goal is  $R$  at time  $t$  for the system, then the most critical components can be indentified and focused on. If improving this components' reliability is not sufficient to reach the reliability goal of the system as a whole, even if the components reliability is improved to 100%, then the focus is shifted to the next component and so on. This is a trial and error process (Kusy, 2012).

#### 4.2.2. Reliability Allocation

Once the reliability has been determined, **Reliability Allocation calculations** are used to identify the weak points and the least reliable components in the system. Then the system reliability can be improved by improving the reliability of the weakest components (Reliasoft, 2007).

The Reliability Allocation calculations provide an optimum configuration by presenting the so called Number of Equivalent Parallel Units (NEPU) which indicates the number of blocks that would be required to meet system reliability goals. The results suggest which units to add in order to increase the reliability of the system. Furthermore, if a component is to be replaced rather than adding redundancy, the Reliability Allocation calculations show how reliable the new component is needed to meet the system reliability goal.

Now the methodology should be clear then the next step is to see how it is applied to the ATM system of the Reykjavik Area Control Center (RACC).

#### 4.2.3. “What-if” analysis

“What-if” analysis is used when calculating conditional probability. It assesses the effects that failures of certain electrical power components have on the overall system performance. “What-if” questions that are believed to result in a problem of interest are generated.

For example: “What-if” a specific electrical component fails? Then the model responds with a different reliability value given that this component has failed. The analysis is performed by changing the status of individual components to off, to indicate that they are inactive, and then by obtaining reliability results for the system under those hypothetical conditions (Reliasoft, 2010).

## **5. The case study–Reykjavík ACC System**

---

Chapter 4 provides a detailed discussion of the methodology used to calculate system reliability. The next step is to see how the RACC system can be modeled based on this methodology. First a more thorough description of the electrical power system at the Reykjavik Center is provided. The purpose of this chapter is to provide a functional understanding of the system and how it carries out its control mission in order to ensure orderly and safe air traffic. Subsequently, a reliability model of the RACC system, that describes the effect of subsystem and component failures on the overall system reliability, is presented.

### **5.1. The system reliability model**

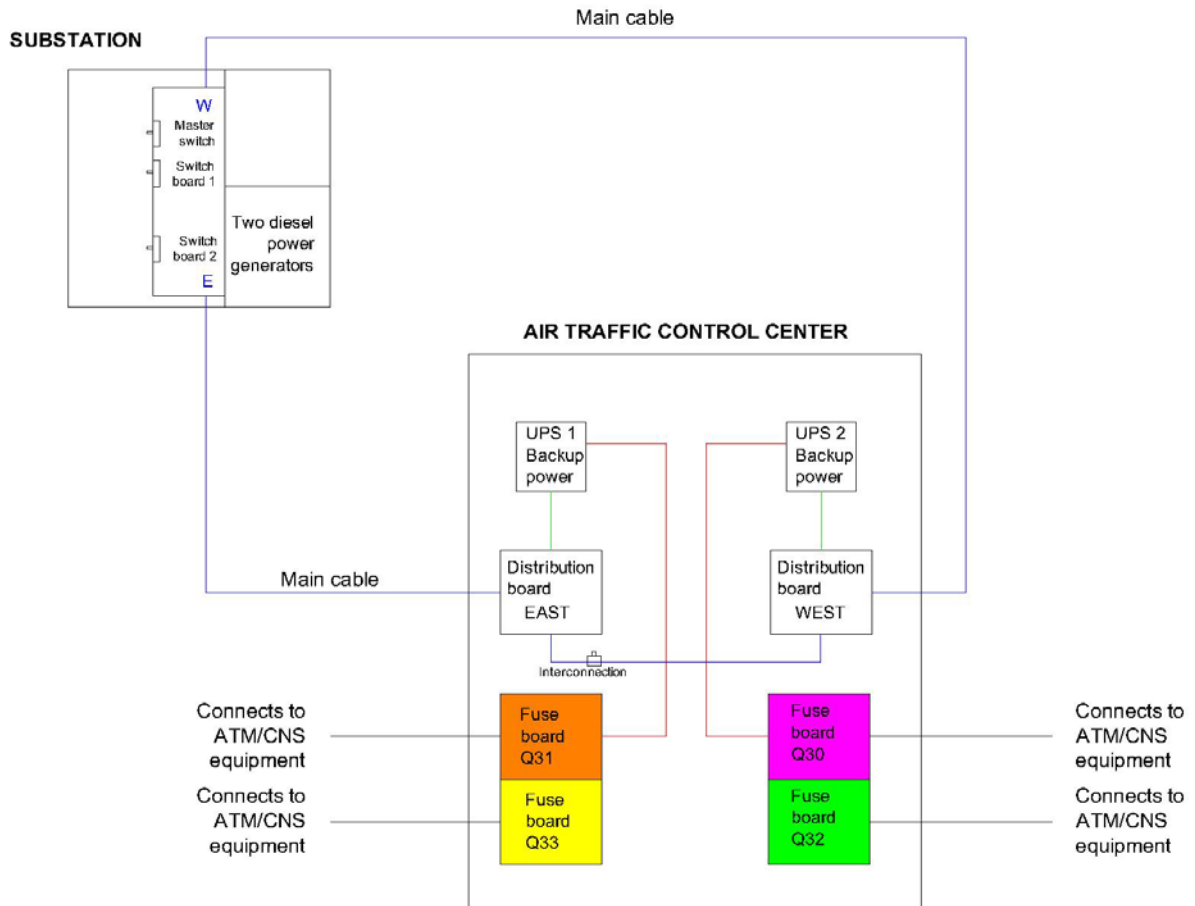
The Reykjavik Area Control Center consists of three major system groups; the ATM processing systems, Communications Navigation and Surveillance (CNS) systems, and the Electrical Power Systems. This chapter contains a description of the main subsystems/components of the RACC systems and how they are connected to represent the reliability model. The subsystems/components of the ATM and CNS systems and their interrelationships are described in further detail in appendix C. Assumptions made while modeling the system as well as some essential equipment will be discussed in the following sections. This equipment includes multiplexers, switches, splitters, optical fiber terminals and so on.

As noted before, only systems and equipment that are critical to the normal operation of the overall system are modeled in this research project. Various support equipment that may be used for testing and monitoring purposes are not considered.

#### **5.1.1. The electrical power system in Reykjavík ACC**

The availability of stable and ultra-reliable electrical power systems is essential in an environment that is totally dependent on the continuous availability of computer systems, such as an ATC Center. Electrical power is obtained from a public utility, but in case of interruptions or non-availability, the ATC Center has its own electrical back-power. This is provided by diesel driven power generators in addition to uninterruptable power supply (UPS) subsystems. These are required to prevent a system shut down due to electrical failure (Subotic, 2007).

The main components of the electrical power system are switch boards, diesel powered generators, cables and wires, distribution boards, UPSs and fuse boards (called Q30, Q31, Q32 and Q33). Figure 5-1 shows how these system components are physically connected.



**Figure 5-1: The electrical system in Reykjavik ACC (Hafsteinsson & Sigurþórsson, 2012).**

The normal path of electrical power is as follows: The feed for the master switch in a transformer substation comes from the power utility company. Power transfer to the distribution boards in the basement of the RACC follows two routes from the transformer substation, where there are two back-up generators. One of the two main cables goes into the west distribution board and the other goes into the east. These two distribution boards distribute electricity throughout the center, to other fuse boards and UPSs. A branch goes to the fuse boards in the equipment room from each of the UPSs. The fuse boards finally feed electrical power to individual equipment.

#### **5.1.1.1. Back-up Power**

In the event that the feed of electricity from the grid fails for some reason there is an automatic switch-over to the backup generators. There are two of these provided. Generator 1 takes over if the power utility is disconnected. If this fails generator 2 takes over. Similarly generator 1 can serve as a back-up for the generator 2. When the automatic transfer system detects that back-up power is needed it activates the switch-boards for the diesel powered generators. The activation takes a few milliseconds. The generators on the other hand need about 10 seconds to start up. These seconds do not result in a system interruption because the UPSs, that are constantly online filtering electrical interferences, provide the system with the needed electricity in the meantime.

If both diesel powered generators fail the UPS and their batteries can provide the system with electricity for at least one hour according to specifications. However, tests performed by Isavia have revealed that sufficient power can be expected up to two hours.

To sum up, if electricity from the grid fails the back-up is provided by two redundant diesel powered generators. If these fail as well the UPS systems provide back-up for at least an hour. This raises an important question: are two back-up generators enough or is a third back-up generator needed? The reliability of the electrical power system having two and tree back-up systems is calculated in chapter 6.

The back-up systems are fully tested once a year by turning off the service lines from the electrical grid. The test reveals whether the automatic transfer system detects that there is no electricity available from the grid and automatically switches function to the diesel powered generators. The test also shows whether the generators start up normally. Furthermore, the generators are also started biweekly to maintain motor oil and to check whether they start.

### 5.1.2. The reliability model of the electrical power system

The components, their properties, and the configuration of the electrical distribution network have a direct effect on the system's reliability (Reliasoft, 2007). Information on the electrical power system configuration and component properties were gathered in meetings with three specialists<sup>39</sup> within Isavia. Thus the expected time between failures of the electrical power components are based on RACC specialists' judgment and experience of failure in electrical power system components.

#### 5.1.2.1. Configurations

The configuration of the electrical distribution system (system connectivity) plays an important part in the calculation of reliability. The system RBD configuration is illustrated in Figure 5-2 below.

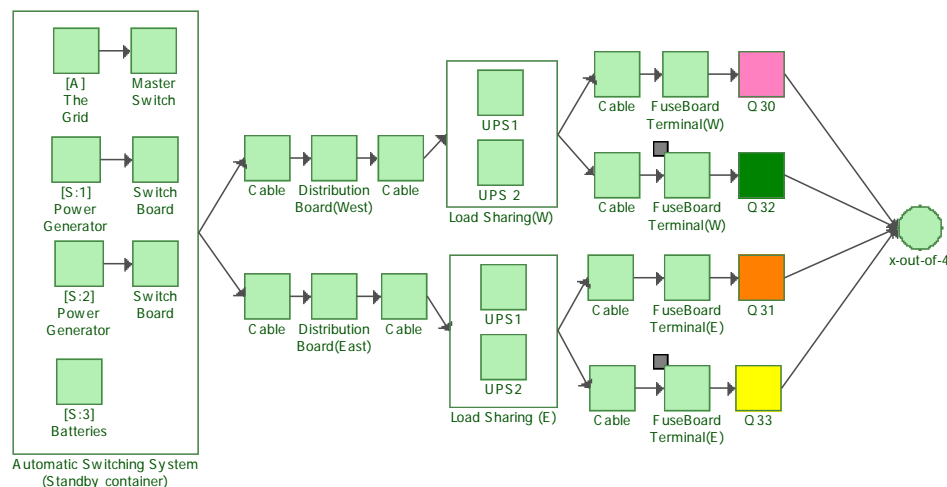


Figure 5-2: The reliability model of the electrical power system.

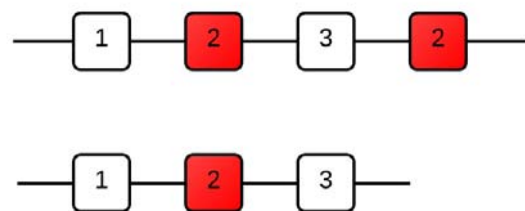
<sup>39</sup> Arnór Bergur Kristinsson, Árni Páll Hafsteinsson and Sigurður Sigurþórsson.

The automatic switching system is a stand-by container<sup>40</sup> that contains the backups of the system. A stand-by container is a system configuration that allows specification of active components (A), stand-by components (S) and a switching system. The container has Mean Time To Failure (*MTTF*) properties (representing the *MTTF* of the switching system) as well as the contained blocks. The *MTTF* values are presented in the next section.

In the event of failure of either the grid or the master switch the container switches to a back-up power generator. Since failure of either the grid or the master switch results in switching to a back-up power generator, the components are modeled in a series. The same happens if either the back-up power generator 1 or the switch board associated with that generator fails, then the container switches to the back-up power generator 2. Finally if the back-up generator 2 or the associated switch fails the batteries provide the backup. The location of the batteries within the model is not obvious since physically they are connected to the UPS components only. UPS systems present a unique challenge to the analysis because modeling the effects on availability from the added battery backup can be difficult (United States Army, 2003). The concept of operation for a UPS is limited to the fact that the battery has a limited life time. If, as in this case, the UPS has at least one hour of ride-through time, then any upstream interruption of less than one hour will be avoided. However, if an interruption lasts longer than one hour, the total interruption time is shortened by one hour before failure of the system occurs (United States Army, 2003). The batteries do however provide a back-up and thus it was considered logical to model the batteries within the backup container.

The reliability-wise configuration of the system does not always align with or represent the physical connections of the system. The distribution boards are physically connected to the UPSs on both sides. However since we are looking at the same component twice in the system it is enough to represent that component's reliability model only once in the diagram. The mirrored component completely correlates with the component it represents. A simple example demonstrates the way in which a mirrored block is applied.

If there are three blocks that are all needed for operational success of a system they are modeled in series. If the system is physically connected in such a way that one of those components is needed twice for successful operation the physical connection would look like that of the first RBD diagram in Figure 5-3.



**Figure 5-3: The two RBD diagrams both give the same reliability results. Mirrored blocks (same component in more than one location).**

However since the mirrored blocks (the red blocks number 2) are one and the same component it is sufficient to have the component only appear once in the reliability model (as depicted in the second RBD diagram in the figure). This means that the

<sup>40</sup> A stand-by container and other terminology containing to BlockSim are explained in appendix G.



reliability of the three component system can be modeled as either the first RBD diagram (by using mirrored blocks) or the second diagram in the Figure 5.3. It is preferred to use mirrored blocks when showing the component in multiple places displays the functionality of the system better.

Next the load sharing container is used because the UPS units share the load i.e. in the event of one failing the other takes on an increased load to keep the system operating.

When all components are needed to provide system functionality the components are modeled in series. The components that have not been mentioned (cables, distribution boards, fuse board input terminals and fuse boards) are modeled in the same configuration as the physical connections.

#### **5.1.2.2. Component properties**

In order to compute the reliability of a system the reliability distribution and its parameters must be known or assessed for each component (Reliasoft, 2007). According to reliability specialists the exponential distribution<sup>41</sup> describes best the reliability of electrical and electronic equipment. Therefore exponential distribution is used for all components except for the batteries (Kusy, 2012). The batteries can only provide back-up for a specific amount of time. Thus the reliability is presented with a normal distribution. Then if the system would be modeled in hours the parameters would be, mean 1hr. and std. 0.000000001 hrs. The normal distribution is used instead of exponential distribution because this component is modeled as working for one hour but then it fails. The std. should be 0 in this case but as the normal distribution needs a std. greater than 0 a very small value is used to be able to use the normal distribution. Entered this way, means that the batteries can support the system by exactly one hour. After one hour the batteries are empty and the system will fail if other electrical power sources have not been restored. In this analysis the time is presented in years and hence the values need to be converted into years. This is easy to do. In one year there are 8760 hours and then we simply divide the hourly parameters by 8760, and then we get the mean of 0.000114 yrs.

The parameter of an exponential distribution is *MTTF*. *MTTF* represents the mean time the electrical power equipment is expected to operate before failing<sup>42</sup>. The *MTTF* values are based on judgments of three RACC specialists<sup>43</sup> and considers the usage of each individual component within the electrical power system. The *MTTF* values are presented in Table 5-1 below. For more information on the electrical power system see appendix E.

Load-sharing requires a life-stress relationship to model the effect of load on probability of failure. The inverse power law relationship was used as it applies to most mechanical

---

<sup>41</sup> Reasons for selecting exponential distribution were explained in chapter 4.

<sup>42</sup> *MTTF* was discussed in more detail in chapter 4.1.2.

<sup>43</sup> Arnór Bergur Kristinsson, Árni Páll Hafsteinsson and Sigurður Sigurþórsson

and non-thermal stressing of components. This relationship can be defined in the BlockSim software.

**Table 5-1: *MTTF* values for the electrical system components based on RACC specialists' judgment.**

<b>Item</b>	<b>MTTF</b>
<b>Electrical grid</b>	1 year
<b>Transforming station/ transformer substation</b>	
Master switch/switch board	25 years
Automatic transfer system	25 years
Switch board for diesel powered generators	25 years
Diesel - powered generators	30 years
<b>ATC center</b>	
Distribution board (East/West)	50 years
Uninterrupted Power Supply (UPS)	15 years
Fuse board input terminal	15 years
Fuse boards	20 years
<b>Cables/wires and connectors</b>	
Main cables	1,000 years
Branches	1,000 years

### **5.1.3. Communication, Navigation and Surveillance (CNS) systems in the ATM reliability model.**

This section contains the assumptions and information used to model the CNS systems that are a part of the ATC Center. The CNS system operated by Isavia contains the path from the aircraft or other information sources to routers within the system that provide the connectivity of these systems to the ATM system of the Area Control Center. In other words the CNS process from aircraft to the ATC Center involves: radios, radio stations, communication network, optical fiber terminals, multiplexers, Balun (devices that connect lines with different impedances.), cables, Voice Communication System (VCS) and VCS terminals or operator position (iPOS). Balun and cables is not connected to the electrical power system and is therefore not modeled in this research project.

Navigation equipment is for most part located on aircraft, however a small part of navigation systems are located within the ATC Center. Since the navigation systems are not a direct critical part of ATC Centers' operations the navigation part of the CNS system is excluded from the analysis.

Data arrives through many different channels e.g. through various channels of the radio network, submarine communication cables (DANICE<sup>44</sup>, FARICE<sup>45</sup>) and so on. How Isavia receives the data is however not important to this research as it does not depend

<sup>44</sup> A submarine communication cable connecting Iceland and Denmark.

<sup>45</sup> A submarine communication cable connecting Iceland, Scotland and Fareo Islands.

on electrical power from the ATC Center as it is remotely located. Thus the modeling starting point is at the optical fiber terminals within Isavia.

The main part of operational voice and data communications are received through two optical fiber terminal units, where both are active at the same time and one is considered a backup for the other. Thus these components are modeled in a parallel configuration. These physical terminals are connected to multiplexers.

A multiplexer<sup>46</sup> (MUX) is equipment that can receive many input signals from other remotely located multiplexers and forwards the selected input via a single line, for instance with compression. Multiplexers are used for voice, radio, data and radar connections. These connections are very important for ATM system operation and thus there are four parallel multiplexers providing four available data paths through the system.

There is a predetermined order of data into the optical fiber terminals and then into multiplexers i.e. there is a specific multiplexer that receives data from each optic fiber terminal. That means that optical fiber terminals A and B cannot share the load. If one optical fiber terminal fails the system loses redundancy.

VCS is a telecommunication control system used for establishing access to the various radio channels that are used for voice communications with the aircraft and telephone lines to adjacent control units, in particular adjacent area control centers and airport towers. The reliability model contains a simplified version of the VCS system which is modeled as two independent components A and B. However, in reality each component is a complicated combination of many interfaces, switches, Communication Interface (CIF) cards and so on. Component A and B are not independent. Thus B can control an interface in component A and vice versa. This functionality will not be discussed in further detail in this analysis; it could however be an interesting topic for another study.

Both VCS A and VCS B need to be functioning during a normal system operation because they do not provide a complete backup for one another. In the event of one unit failing the consequences to the ATC Center is mainly a loss of half of the communications services. This means that air traffic controllers can still communicate with all parties but they have to share phone lines with others i.e. they no longer have dedicated telephone channels. Furthermore it means that the system loses its redundancy i.e. where normally main and stand-by sets are available only one set of radios is up and running. In short, failure of a VCS component leads to increased workload for controllers.

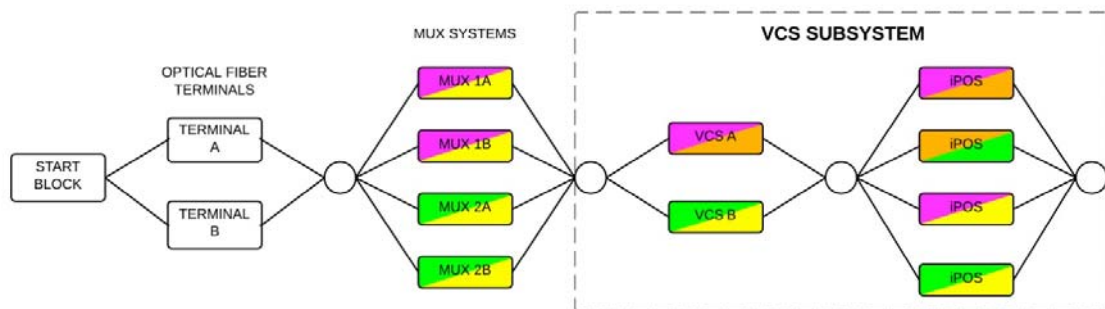
For the VCS to work its terminals (called iPOS), that are located at each Controller Work Station (CWS) must be operational. The iPOSes are connected to electrical power in 4 ways, creating 4 independent sets of iPOSes which provide back-up for one another. Each set is connected to two fuse boards i.e. one set connects to Q30 and Q31,

---

<sup>46</sup> Often referred to as MUX, Newbridge equipment or Mainstreet equipment within Isavia.

one to Q31 and Q32 and so on, where Q30, Q31, Q32 and Q33 represent the 4 fuse boards of the electrical system.

In short the model components of the CNS system that are needed for successful functioning of the VCS are: optical fiber terminals, multiplexers, VCS and iPOS terminals. The reliability model is illustrated in Figure 5-4. This will be referred to as the VCS submodel from now on (where as VCS A and B are two of the components of the VCS submodel). The colors of the component represent how the equipment is connected to electricity. Pink represents that the component is connected to Q30, orange represents Q31, green represents Q32 and yellow represents Q33. The optical fiber terminals are not colored in the reliability model because they are not connected to the fuse boards of the electrical power system as they receive power directly from the UPS systems. The nodes represent voters that are used to specify how many paths are needed for a successful function. These are based on a set of assumptions and a few failure modes which will be presented in chapter 5.2.



**Figure 5-4: The reliability model of the VCS subsystem.**

As can be seen in the Figure 5-4 a starting block has been added. This is done because BlockSim diagrams must have exactly one starting and one end point. If, as in this case, the system contains more than one starting points, a single block that does not fail, and thus does not impact reliability, must be introduced<sup>47</sup>.

#### **5.1.4. Reliability model of the Air Traffic Management (ATM) system**

This section contains the assumptions and information used to model the ATM system within the ATC Center. The ATM system contains all equipment from the routers of the telecommunications network to the displays and terminal equipment that the air traffic controllers use in their workstations. The ATM process from router to the terminal equipment involves two submodels; the Radar Data Processing system (RDPS) submodel and the Flight Data Processing system (FDPS) submodel (this can be seen in Figure 5-5).

FDPS is a complicated system that consists of many processes working together. It receives and distributes all flight information other than radar data. It automatically processes all the information related to all flights in the system, most notably aircraft

<sup>47</sup> See how these properties are specified in Appendix H.

position, into electronic progress strips<sup>48</sup>. These strips are vital for operation and contains the most up-to-date known information about each flight. CWS/IOT are the user interface that allows the air traffic controller to access the information of the FDPS systems.

The FDPS receives data through different data connections; Aeronautical fixed communication network (AFTN), submarine communication cables (DANICE and FARICE) and OLDI. Where these names are used in the model it refers to the equipment used to receive data through these connections. AFTN is a ground-to-ground communication system for transmitting flight data messages. The system is a part of a worldwide network for transmitting messages between ANSPs, the CFMU, airlines, etc.. OLDI, stands for On-Line Data Interchange,. This component is used to receive data similar to the data that go through the AFTN system. AFTN needs a splitter, operational switch stack (operswitch) and Nport to operate. The function this of equipment is listed in Table 5-2. In short the FDPS submodel needs communication and data connections (AFTN/OLDI/FARICE/ DANICE), operswitch, splitters, N-port, FDPS, CWS and IOT to be considered successfully operational.

Table 5-2 lists the function of equipment.

**Table 5-2: The function of equipment.**

Item	Function
APC Switch	A device that provides multiple small devices with redundant power, i.e. for devices that only have a single power supply.
Black Boxes	A device that splits up the radar data line. Also reffered to as Serial Sharer.
Oper Switch	A stack of network switches made to look and work as a single large switch. This enables the Etherchannel functionality.
Router	A device that forwards data packets between different computer networks.
AFTN Splitter	A device that splits a serial stream input to serveral outputs without loosing signal strength (similar to Black boxes).
N-port	A device that converts serial input into TCP/IP or UDP/IP connection.

The ATM system needs an Ether Channel (EC) network also known as link bonding or link aggregation to operate. EC is a port-channel architecture used to group several physical links to create one logic Ethernet providing fault-tolerance between switches, routers and servers. The network is built up with operational switch stacks, which are stacks of network switches made to look and work as a single large switch. This enables the Etherchannel functionality, which is commonly used for redundant networks. Specific operswitches are needed for each of the ATM subsystems and components to be successfully operational. This information is displayed in Table 5-3 below. The operswitches are needed for operation of both the FDPS submodel discussed above and the RDPS submodel that will now be discussed.

---

<sup>48</sup> A strip contains updated information from the flight plan displayed in a specific format.

**Table 5-3: The operswitch needed for the ATM subsystems and components to function.**

Switch	Operational Switch Stack		
	1	2	3
1	FDPS A	FDPS C	RDPS A
	CWS/IOT	FDPS D	RDPS B
	AFTN 1		
	OLDI		
2	FDPS A	FDPS C	RDPS A
	CWS/IOT	FDPS D	RDPS B
	AFTN 2		
	OLDI		
3	FDPS B		
	CWS/IOT		
	ICE 1		
	DANICE		
4	FDPS B		
	CWS/IOT		
	ICE 1		
	FARICE		

Other equipment used in the RDPS submodel are APC switches and Black Boxes. The Black Boxes represent the radars that the ATC Center is connected to. The ATC Center is connected via a communications network to 8 radars; in Keflavik (two radars –KFM and H-1), Bolafjall (H4), Gunnólfsvíkurfjall (H2), Stokksnes (H3), two in bFaroe Islands (FAE) and Sumburgh (SUM) in the Shetland Islands (Scotland). A Black Box is a device that splits up the radar data line. The APC switches provide multiple small devices with redundant power, i.e. for the Black Boxes that only have a single power supply.

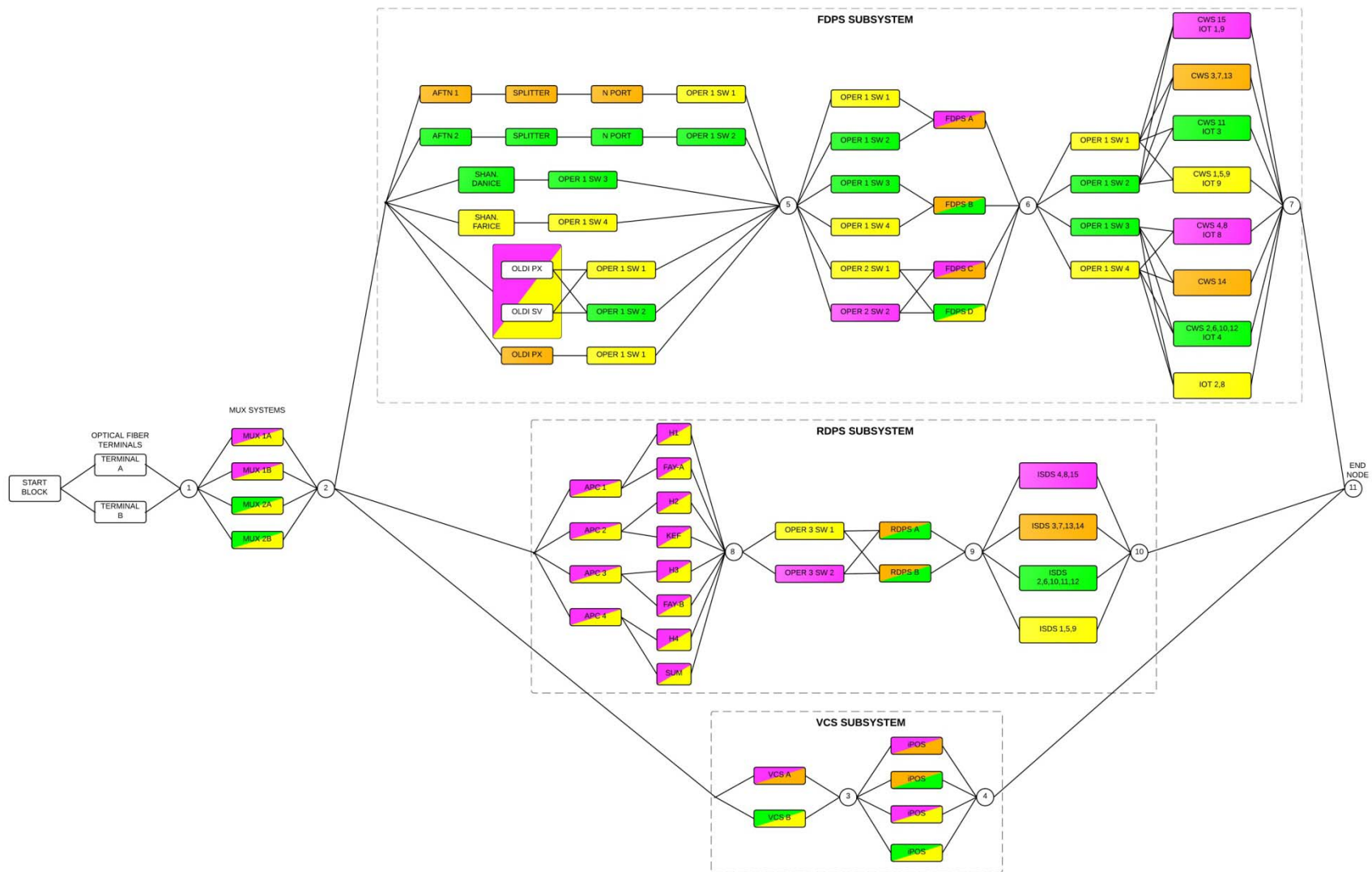
The RDPS system provides simultaneous data processing from radar data while performing real-time monitoring and data extrapolation. ISDS is a display system that provides a visual representation of flight profiles, flight estimates, crossing times etc. ISDS integrates two fundamental systems in the Reykjavik Oceanic Area Control; the RDPS and FDPS. ISDS combines information from the different systems into one situation display for the air traffic controllers. In short the RDPS submodel needs APC switches, the Black Boxes, operswitches, RDPS and ISDSes to be considered successfully operational.

The most important information needed for modeling is regarding backups and which functions are needed to stay operational. The former will be presented in Table 5-4 whereas the latter will be covered in chapter 5.2.

**Table 5-4: The main equipment for ATM and CNS systems and whether they have backups.**

<b>Item</b>	<b>Redundancy</b>
<b>ATM components</b>	
AFTN path	2 paths
Shanwick DANICE/FARICE	2 paths
OLDI router	2 paths
FDPS	2 times redundant system or 4 units
CWS	There are 16 CWS for ATCOs in the ATC center and can be divided up to 4 independent sets of CWS
Black Box	There are 8 independent units with complex relationship as to which provide backups for each other. Assumptions are made regarding which ones are needed
RDPS	2 items
ICE	2 items
ISDS	There are 16 number of ISDS in the ATC center and can be divided up to 4 independent sets of ISDS
<b>CNS components</b>	
Optic Fiber Terminals	2 items
Multiplexers	4 paths
VCS	both units are needed for operation
iPOS	There are 30 iPOSs in the ATC center and can be divided up to 4 independent sets of iPOSs

The model is illustrated in Figure 5-5. This includes two new subsystems the RDPS submodel and the FDPS submodel (where RDPS A and B as well as FDPS A, B, C and D are components of these functions). The colors of the component represent how the equipment is connected to electricity. Pink represents that the component is connected to Q30, orange represents Q31, green represents Q32 and yellow represents Q33. The terminals are not colored in the reliability model because they are not connected to the fuse boards of the electrical power system as they receive power directly from the UPS systems. The nodes represent voters that are used to specify how many paths are needed for a successful function. These are based on a set of assumptions and a few failure modes will be presented in chapter 5.2.





## 5.2. Assumptions

When analyzing reliability the system functionality must be clearly defined in terms of what is needed for the system to be considered successfully operational. This analysis considers three operational success or failure modes i.e. three sets of assumptions pertaining to functions needed for the system to be considered successfully operational. Two extreme failure modes were analyzed along with one more realistic failure mode in between. These functionality failure modes are:

- Failure Mode 1: Most demanding case: The system is operational and there is absolutely **no tolerance of failure** in the system. All paths are needed for a successful operation and thus there is no redundancy in the system.
- Failure Mode 2: A normal function: The minimum equipment needed for the system to **function normally** without any disruption of service. No influence on operational staff or ATC center capacity. The system has increased redundancy as fewer paths are required.
- Failure Mode 3: The system is considered functional as long as there is not a complete failure of the system, i.e. the system is considered to be functional as long as both the Flight Data Processing System (FDPS) submodel and Voice Communication System (VCS) submodel are operational. This has significant influence on operational staff and ATC Center capacity and would be unacceptable for extended periods and at peak times.

Since the functionality of the system is dependent on various subsystems and equipment a few questions were defined to determine how many successful (minimum) paths are needed from each subsystem or equipment, for the system to be operating properly in each failure mode. The questions are listed below, each of them corresponding to the node with the same number in Figure 5-5.

### CNS equipment:

- Question/ Node 1: How many paths are needed from the Optical fiber terminals? (max available paths 2).
- Question/ Node 2: How many paths are needed through the MUX system? (max available paths 4).
- Question/ Node 3: How many paths are needed from the VCS system? (max available paths 2).
- Question/ Node 4: How many paths are needed from the iPOS? (max available paths 4).

### ATM equipment:

- Question/ Node 5: How many data paths are needed (AFTN/OLDI/DANICE/FARICE)? (max available paths 7).
- Question/ Node 6: How many paths are needed from the FDPS? (max available paths 4).

- Question/ Node 7: How many paths are needed from the Black Boxes? (max available paths 8).
- Question/ Node 8: How many paths are needed from the RDPS? (max available paths 2)
- Question/ Node 9: How many paths are needed from the CWS/IOT? (max available paths 4).
- Question/ Node 10: How many paths are needed from the ISDS? (max available paths 4).
- Question/ Node 11: How many paths are needed through the whole system? Is FDPS, RDPS and VCS needed? (max available paths 3).

These questions were answered with respect to each failure mode. The answers are listed in Table 5-5 below and are based on the FMECA analysis conducted as a part of this research project (results are discussed in chapter 3.2.3. and the overall analysis is presented in appendix J). The numbers denote how many paths are needed for a specific equipment for a specific failure mode. Max paths are needed for failure mode 0.

**Table 5-5: Presents minimum equipment list for each functionality failure mode.**

Question/ Node	Equipment	Failure Mode 1	Failure Mode 2	Failure Mode 3
1	Optical fiber terminals	2	1	1
2	MUX	4	2	2
3	VCS	2	2	1
4	iPOS	4	2	2
5	AFTN/OLDI/FARIC/DANICE	7	3	2
6	FDPS	4	1	1
7	Black Boxes	8	8	0
8	RDPS	2	1	0
9	CWS/IOT	8	4	1
10	ISDS	4	2	0
11	Subsystems (FDPS,RDPS,VCS)	3	3	2

Voice and data communications are received through two optical fiber terminals that are connected to four multiplexers that receive many input signals and forward the selected input via a single line.

From this point forward the multiplexers are connected to various equipment needed for the main submodels of the ATM system reliability model (i.e. FDPS, RDPS and VCS) to be operational. Each subsystem can be modeled individually or as done here all are modeled in one RBD with one node (number 11) at the end indicating which those submodels are needed for the system to be considered successfully operational. All three subsystems are needed for normal operation. However for Failure Mode 3 only FDPS and VCS are needed for the system to be considered functional as RDPS is considered less important. When the RDPS is missing larger aircraft separation minima have to be used. This has a major influence on the number of operational staff and on

ATC Center capacity. This is the main difference between Failure Mode 2 and 3. Failure Mode 1 however is the most demanding case which assumes that no equipment may fail i.e. it assumes that there is no redundancy in the system. Thus less functionality is required in Failure Mode 2 than in Failure Mode 1 and even less functionality is required in Failure Mode 3 than in Failure Mode 2.

These failure modes and assumptions are not carved in stone; they do however reflect the FMECA results and specialists perception of system functionality. The reliability calculations are based on these assumptions

### **5.3. The resulting model of the entire system**

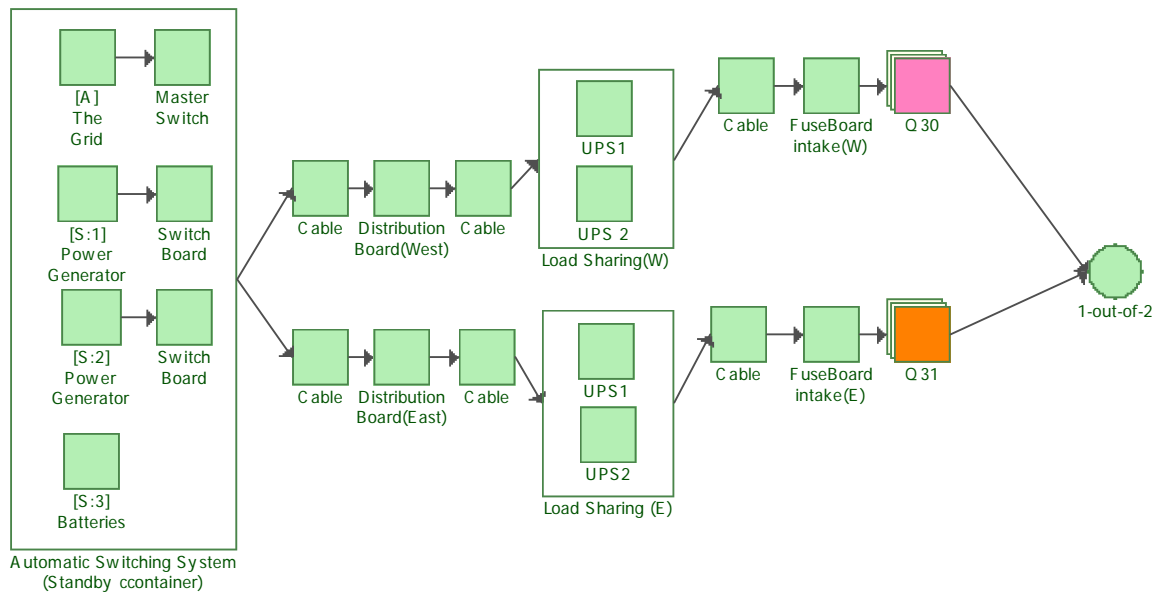
The resulting reliability model of the entire system includes all the information and assumptions made earlier in this chapter. At first it was attempted to develop one model for the entire system, by modeling the electrical power system, and then connecting each piece of equipment to the corresponding fuse boards. This resulted in a spider web of connection lines and nodes making it difficult or even impossible to read the path of any desired functionality. Thus it was very difficult to see what equipment was needed for a specific function. This approach was considered unacceptable for this reason. An example that models only the VCS submodel by using this approach can be seen in appendix L.

For this reason an alternate approach was developed for modeling of the entire system. This approach uses specific failure modes to calculate the reliability. This was performed by defining two models, one for the electrical power system and another for the ATM systems. The electrical power system model is used to describe failure characteristics of the components of the ATM model, i.e. the component reliability characteristics represent the failure mode caused by power outage.

As an example the FDPS A system needs electrical power from Q30 or Q31. Thus the probability of failure of FDPS A due to power outage is the probability of Q30 and Q31 both failing to provide the unit with electrical power. Thus the FDPS A reliability distribution is the same as a reliability distribution of an RBD that contains the success of Q30 or Q31 as shown in the 5-6 below<sup>49</sup>.

---

<sup>49</sup> This is performed by encapsulation in BlockSim, see appendix G for a definition and appendix H for further details of how it is performed in BlockSim



**Figure 5-6: The reliability of a system that is successful if either Q30 or Q31 is functioning.**

In the event of failure of Q31 and Q30 the FDPS A component would fail as well as all the other components that are connected to the electrical power system in that way. For this reason all equipment that is connected in the same way is treated as one and the same (because they fail in the same way). This is achieved by mirroring the components in BlockSim. Mirrored blocks are used to model either common cause failures or to represent exactly same component which in this case results in common cause failures in the ATM system. As in this case the component of the FDPS A system (and any other component connected to electrical power in this way) is pink and orange in the ATM reliability model.

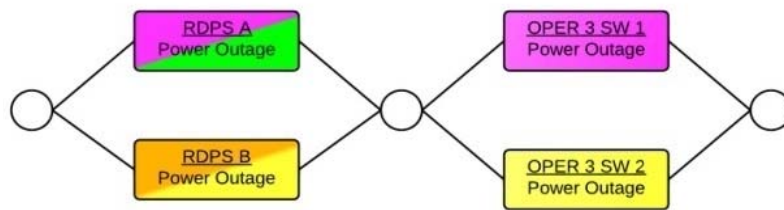
As no component or subsystem is connected to three fuse boards, there are 10 different ways to connect a component to electricity. Either the equipment is connected to one fuse board and thus fails if that fuse board fails or the equipment is connected to two fuse boards as in Figure 5-6 above. Since there are 4 fuse boards there are 6 different ways that a component could be connected to two fuse boards. Hence, there are 10 different ways that any given equipment can be connected. However, two of these are not used because that would connect the equipment twice to the same UPS source. Clearly a better back-up is achieved by connecting it to separate UPS sources. Therefore there are 8 different building blocks of the ATM model.

1. Q30 fails/succeeds.
2. Q31 fails/succeeds.
3. Q32 fails/succeeds.
4. Q33 fails/succeeds.
5. Q30&Q31 fail/succeed.
6. Q30&Q33 fail/succeed.
7. Q31&Q32 fail/succeed.
8. Q32&Q33 fail/succeed.

This provides a fully satisfactory model of the effect of electrical power outage on the ATM system.

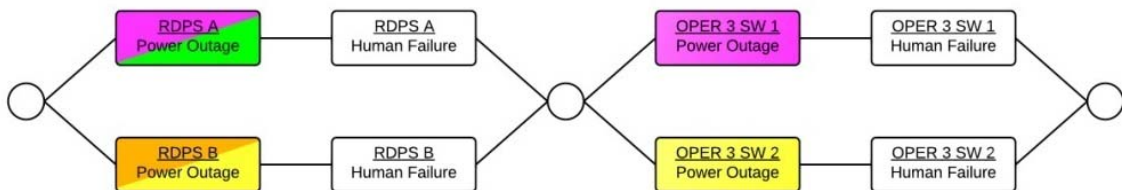
It is assumed here that components or subsystems do not fail except in the case of a power outage. The model can easily be extended to account for other failure causes such as failure of the component itself. This is done by adding another block in series<sup>50</sup> with the block that is already in the model representing the electrical power failure mode. This is explained further by the following example from the ATM model.

In this study the power outage for RDPS and operswitches needed are modeled as follows:



**Figure 5-7: Modeled power outage of RDPS and Operstack switches.**

When the analysis is extended to include e.g human failure, the model would look like this:



**Figure 5-8: Modeled power outage and human failure of RDPS and Operstack switches.**

Extending the model for other failures such as failures caused by hardware and software failures is performed in the same manner i.e. by adding blocks in series.

In the RBD there is no distinction made between failure causes and failure modes. Individual blocks can be used to represent failure modes/causes with independent probability of occurrence. There is one probability of power outage and there is another for human failure (Kusy, 2012).

One of the major assumptions made during the analysis is that the system is not repairable. This of course does not reflect the operation of the real system, as it is repairable. However, modeling a repairable system requires *MTTR* data related to each failure mode for each component. As this data regarding maintenance is not available it was decided look at the system as being non-repairable for this research. The model can

<sup>50</sup> Then the reliability distribution can be added by using Weibull or by inserting values in the block properties, depending on the data available. To see how this is done refer to H.

easily be changed to a repairable system when the maintenance data has been gathered by adding this into the existing model<sup>51</sup>.

The component properties and system configuration is based on numerous assumptions that are based on specialist opinions and the FMECA conclusions. However, it is fairly simple to change the model to adapt it to reflect new assumptions. The nodes<sup>52</sup> in the model indicate how many paths are needed for the system to be operational. The model is flexible with regards to node value and it can be changed easily.

It may be interesting to model the CNS system and the ATM system separately to get separate reliability for each one. However as they use some of the same components e.g. multiplexers and optical fiber terminal equipment, they are modeled in the same diagram i.e. by using BlockSim mirrored blocks which must appear in the same diagram.

By now, a success-oriented logical reliability model of the RACC ATM system has been developed. The reliability models put forward in this chapter (in Figures 5-2, 5-4 and 5-5) are also presented in appendix M. These will be used to determine the reliability of the system and perform all the calculations needed to answer the research questions of this research project. The reliability results will be discussed in the next chapter.

---

<sup>51</sup> Reference is made to Appendix H.

<sup>52</sup> A node and other terminology containing to BlockSim are explained in appendix G.

## 6. Results and discussion

---

The previous chapter provided a discussion of the component properties and how the reliability models of systems are configured. This is an important step towards the overall objective of this research project, i.e. to develop a quantitative model for determining the reliability of the Reykjavík Area Control Center (RACC) ATM system with special emphasis on the electrical power system.

The purpose of this chapter is to present and discuss the reliability results of the models. This will be achieved by performing model calculations to answer the research questions put forward in the introduction. Thus in this chapter the following questions will be answered:

1. What is the reliability of the system in terms of probability due to electrical power system failures?
2. How can the reliability of the system be improved? Which components constitute the weak links in the system?
3. How does the failure of certain components of the electrical power system affect the overall ATM system reliability?
4. Is it suitable and convenient to use the method to be selected and for instance the BlockSim software for analyzing and determining the reliability of ATM systems?

The results consider various failure modes based on clearly defined assumptions regarding the functionality of the system. There are four separate failure modes considered in analysis of the electrical power system. Three additional failure modes are then considered for determining the effect of electrical power on the RACC ATM system. These failure modes were introduced in chapter 5.2.

All failure statistics are calculated for a time interval of one year. Performing calculations for a longer period of time would not be practical as the reliability analysis at this point does not take system maintainability into account i.e. the system is so far assumed to be non-repairable. Based on that assumption, reliability of the system after a system failure drops to zero. Thus the model represents the reliability of the system i.e. the probability that the system does not fail within a year. Availability is in many ways a more suitable measurement as it accounts for maintenance and gives the percentage of time that a system is available to perform its required functions.

To make the reliability model reflect the actual system behavior better the average availability of the system was also calculated by simulation based on the models including fixed maintenance times i.e. Mean Time To Repair (MTTR) equal to one week, equal to 24 hrs and equal to 1hr. These maintenance values are not based on real data. The value of one week is however meant to provide a reference value for worst case scenario (that in the event of failure it takes a whole week to repair the failed component/s) to be able to calculate availability. The value of 24 hrs is a more realistic maintenance reference value used to calculate the availability of the system. Even more

realistic MTTR value is one hour as ATM systems are safety critical systems that typically can be repaired quickly. The reliability is the probability that the system does not fail in a time interval whereas the availability is the probability that the system is functioning at a given point in time. Average availability gives the percentage of time that a system is available to perform its required functions.

In the following section the electrical power system is analyzed separately with respect to reliability and in order to identify which components are the “weakest links” in the electrical power system. Subsequently in section 6.2 the overall ATM system is analyzed with respect to the first three research questions listed at the beginning of this chapter. Research question four is answered in chapter 6.3.

### **6.1. The RACC Electrical Power System**

The reliability of the electrical power system or the probability of successful functioning of the system is calculated based on four different EP (Electrical Power) Failure Modes:

- EP Failure Mode 1: No path can fail. All paths are required for the system to be considered functional.
- EP Failure Mode 2: 1 path can fail. 3 paths are required for the system to be considered functional.
- EP Failure Mode 3: 2 paths can fail. 2 paths are required for the system to be considered functional.
- EP Failure Mode 4: 3 paths can fail. 1 path is required for the system to be considered functional.

These paths are depicted in the reliability model of the electrical power system which can be seen in Figure 5-2.

**Research question 1:** What is the reliability of the system in terms of probability?

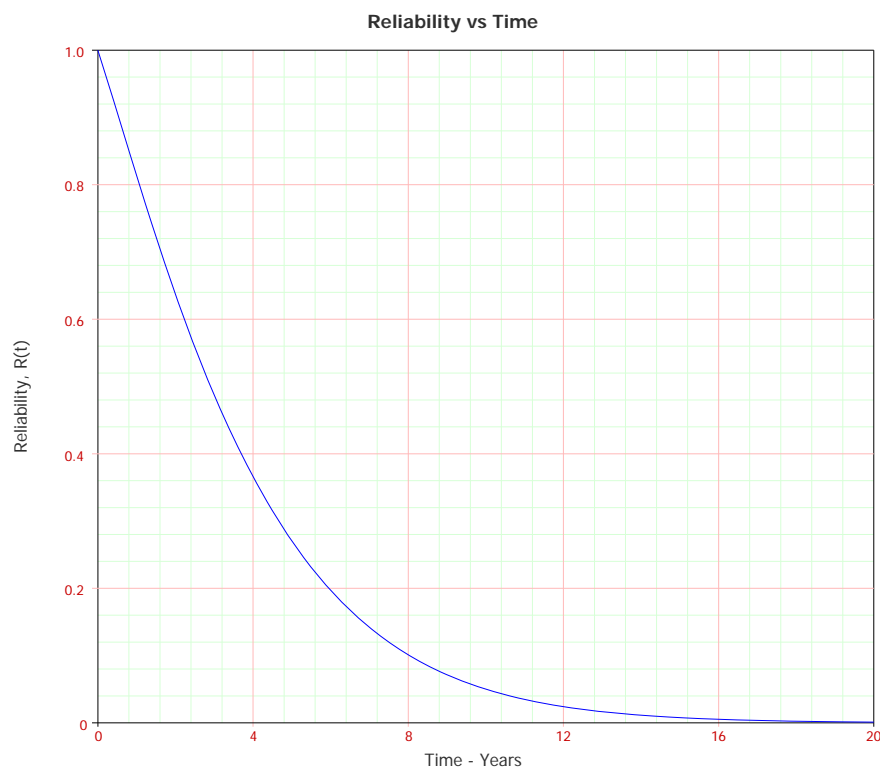
The reliability of the electrical power system is presented in Table 6-1 for the four EP Failure Modes in terms of the reliability of a non-repairable system, Mean Time To Failure (MTTF) and availability given three different values for the Mean Time To Repair (MTTR).

The reliability of the system is described by a mathematical expression. The BlockSim software generates different equations for each failure mode. As an example the software provided the following equation for EP Failure Mode 2:



$$\begin{aligned}
R_S = & R_{\text{Automatic Switching System (Standby container)}} \cdot R_{\text{x-out-of-4}} (-3R_{Q32} \cdot R_{\text{FuseBoard terminal(E)}} \cdot R_{Q33} \cdot R_{\text{Cable}}^8 \cdot R_{\text{Load Sharing(W)}} \cdot R_{Q31} \\
& \cdot R_{\text{Load Sharing(E)}} \cdot R_{\text{Distribution Board(West)}} \cdot R_{\text{Distribution Board(East)}} \cdot R_{\text{FuseBoard terminal(W)}} \cdot R_{Q30} + R_{Q32} \cdot R_{\text{FuseBoard terminal(E)}} \\
& \cdot R_{Q33} \cdot R_{\text{Cable}}^7 \cdot R_{\text{Load Sharing(W)}} \cdot R_{Q31} \cdot R_{\text{Load Sharing(E)}} \cdot R_{\text{Distribution Board(East)}} \cdot R_{\text{FuseBoard terminal(W)}} + R_{Q32} \cdot R_{\text{FuseBoard terminal(E)}} \\
& \cdot R_{Q33} \cdot R_{\text{Cable}}^7 \cdot R_{\text{Load Sharing(W)}} \cdot R_{\text{Load Sharing(E)}} \cdot R_{\text{Distribution Board(West)}} \cdot R_{\text{Distribution Board(East)}} \cdot R_{\text{FuseBoard terminal(W)}} \cdot R_{Q30} \\
& + R_{Q32} \cdot R_{\text{FuseBoard terminal(E)}} \cdot R_{\text{Cable}}^7 \cdot R_{\text{Load Sharing(W)}} \cdot R_{Q31} \cdot R_{\text{Load Sharing(E)}} \cdot R_{\text{Distribution Board(West)}} \cdot R_{\text{Distribution Board(East)}} \\
& \cdot R_{\text{FuseBoard terminal(W)}} \cdot R_{Q30} + R_{\text{FuseBoard terminal(E)}} \cdot R_{Q33} \cdot R_{\text{Cable}}^7 \cdot R_{\text{Load Sharing(W)}} \cdot R_{Q31} \cdot R_{\text{Load Sharing(E)}} \cdot R_{\text{Distribution Board(West)}} \\
& \cdot R_{\text{Distribution Board(East)}} \cdot R_{\text{FuseBoard terminal(W)}} \cdot R_{Q30} ))
\end{aligned}$$

A plot of the reliability function is presented next in Figure 6-1. For further information about the results provided by the BlockSim refer to appendix N.



**Figure 6-1: The reliability function of the electrical power system vs. time.**

**Table 6-1: Probability of successful electrical power system operation.**

Failure Mode	Reliability Non-repairable	MTTF of the system	Availability (MTTR=1 week)	Availability (MTTR=24 hrs)	Availability (MTTR=1 hr)
1	0.67263704	2.4 years	0.9934248	0.99899786	0.99995785
2	0.81341431	3.7 years	0.99732917	0.99954964	0.99998121
3	0.96339205	6.7 years	0.99997366	0.99999919	0.99999999
4	0.97831578	9.2 years	0.99998749	0.99999971	0.99999999

As can be seen from Table 6-1 the availability of the system is on average in the interval from 0.9934 to 0.9999 depending on MTTR values and the specific failure mode. The reliability does not consider the effect of maintenance. The reliability is in the interval

from 0.6726 to 0.9783 depending on the failure mode. Reliability of 0.6726 for instance is not high but EP Failure Mode 1 dictates that all fuse boards must be functioning in order for the system to be considered functional. The RACC ATM system is designed in such a way that important subsystems have connections to two fuse boards. In other cases multiple paths exist through equipment needed for the functioning of these subsystems. This strict functionality requirement is therefore not necessary for a successful ATM operation. Later on it will be shown in fact that the reliability of the ATM system in normal operation, while considering electrical power system failures, is higher than the reliability of the first two EP Failure Modes<sup>53</sup>.

The failure mode that is of most interest is EP Failure Mode 3 because of the dual connection of the ATM subsystems. EP Failure Mode 3 assumes that the system is functional if two fuse boards are operational. The results for this failure mode reveal a reliability of 0.9634 and availability of 0.999974-0.999999 depending on the value of the MTTR. This means that the system has decreased functionality for 13.8 minutes pr. year in the worst case (1 week), 26 seconds/year when maintenance takes 24 hours and 0.3 seconds/year when maintenance takes only one hour

These kinds of results raise an important question as to whether the reliability and availability of the system are acceptable or whether improvements are necessary. The answer depends on the goal that is set for the RACC electrical power system. This question and reliability goal should be considered by the system owner.

**Research question 2:** How can the system reliability be improved? Which components constitute the weak links in the system? (**Reliability Importance and Reliability Allocation**).

Orkuveita Reykjavíkur provides three power lines to the Reykjavik ACC. However, only one master switch is used to select one of these sources of electrical power. Thus if this switch breaks down the system has to switch over to back-up power generators even though the grid serving the RACC is up and running. The probability of failure of the master switch component is 3.92% based on exponential distribution with MTTF of 25 years. In order to make the system even more reliable Isavia could add another main power switch decreasing the failure probability down to 0.15%. This is one option of improving reliability of the system. The question remains how the reliability model can be used to find out which components of the electrical power system should be improved?

The task of identifying the least reliable components in a system is rather easy for simple systems. However in case of complex systems a mathematical model is needed. For this purpose it is useful to define the Reliability Importance which can be easily calculated by the BlockSim software. Reliability Importance is an indicator of the contribution of any given component to the overall system reliability in a certain time

---

<sup>53</sup> This will be discussed further in Section 6.2 when the total ATM system is examined with respect to failures in the electrical power system.

period. In other words Reliability Importance represents the sensitivity of the total system reliability to changes in the reliability of the individual system components. The rate of increase of the system reliability is greatest when the least reliable component is improved. The value of Reliability Importance is given mathematically by:

$$I_{R_i} = \frac{\partial R_s}{\partial R_i}$$

Where  $R_s$  is the system reliability and  $R_i$  is the component reliability (Leemis, 1995).

Thus the most critical components can be identified and ranked (Reliasoft, 2007). The BlockSim software has the facility for computing the Reliability Importance values of the RACC electrical power components. The components that could potentially be added to the system are listed in the following order, from highest Reliability Importance to the lowest:

1. Fuse board input terminal 0.72.
2. Fuse boards 0.71.
3. Distribution board 0.69.
4. Automatic transfer system (the whole stand-by container) 0.68.
5. Uninterrupted Power Supply (UPS) system (a load sharing container) 0.67.
6. Automatic transfer system (switch) 0.49.
7. Switch board 0.03.
8. Power generator 0.03.
9. Batteries 0.002.
10. Master switch 0.001.

The configuration of the system and component reliability influence Reliability Importance. Thus components that may be important from a functional point of view but are very reliable can have low Reliability Importance. This is an indicator of which components to focus on when attempting to improve the system. As an example the value for the power generators is fairly low which would indicate that there is less need of improving the generators or add another one. However, it should be noted that the model does not take into account important operational aspects such as prolonged maintenance of essential equipment.

Fuse board input terminal has the largest Reliability Importance in the electrical power system relative to the other components of the system and thus constitutes the weakest link in the system.

Using Reliability Importance measures is a powerful method of identifying the relative importance of each component in a system with respect to the overall reliability of the system. Another useful method used when attempting to find out how to improve a system is Reliability Allocation calculations. Reliability Allocation involves a balancing act of determining how to allocate reliability to the components in the system so the

system meets the desired reliability while ensuring that the system meets all other associated performance specifications (Reliasoft, 2007).

Reliability Allocation calculations determine the best way to achieve a system reliability goal by improving the reliability of individual components (Reliasoft, 2010). Reliability goals for a certain time period (one year in this case) and which components are to be considered can be specified when searching for the optimum configurations for meeting these goals. Then, decisions can be taken based on technical feasibility<sup>54</sup> (e.g. cost and technology) of improving the reliability of each individual component, BlockSim calculates the optimum configuration for increasing component reliability in order to achieve a system reliability goal. There is no data available for this research project regarding feasibility and therefore all components are considered equally attractive. The optimum configuration results are presented with so-called Number of Equivalent Parallel Units (NEPU). This factor indicates how many blocks would be required in a parallel configuration to reach a reliability goal (Reliasoft, 2007; 2010).

For the RACC electrical power system the NEPU had a value between one and two for all the system components. The Reliability Allocation results give the same ranking of components as expressed by Reliability Importance i.e. the highest NEPU value is found for the component with highest Reliability Importance. When using Reliability Allocation, no component stands out as being the least reliable component needing multiple parallel back-up units. Thus it was decided to use trial and error method to add a few different components one at a time to see how that would affect the reliability. Once the reliability has been calculated for the system with an added component, the model is changed back to its previous configuration and the process is repeated for another component. The reliability was calculated for each of the following cases of additional components:

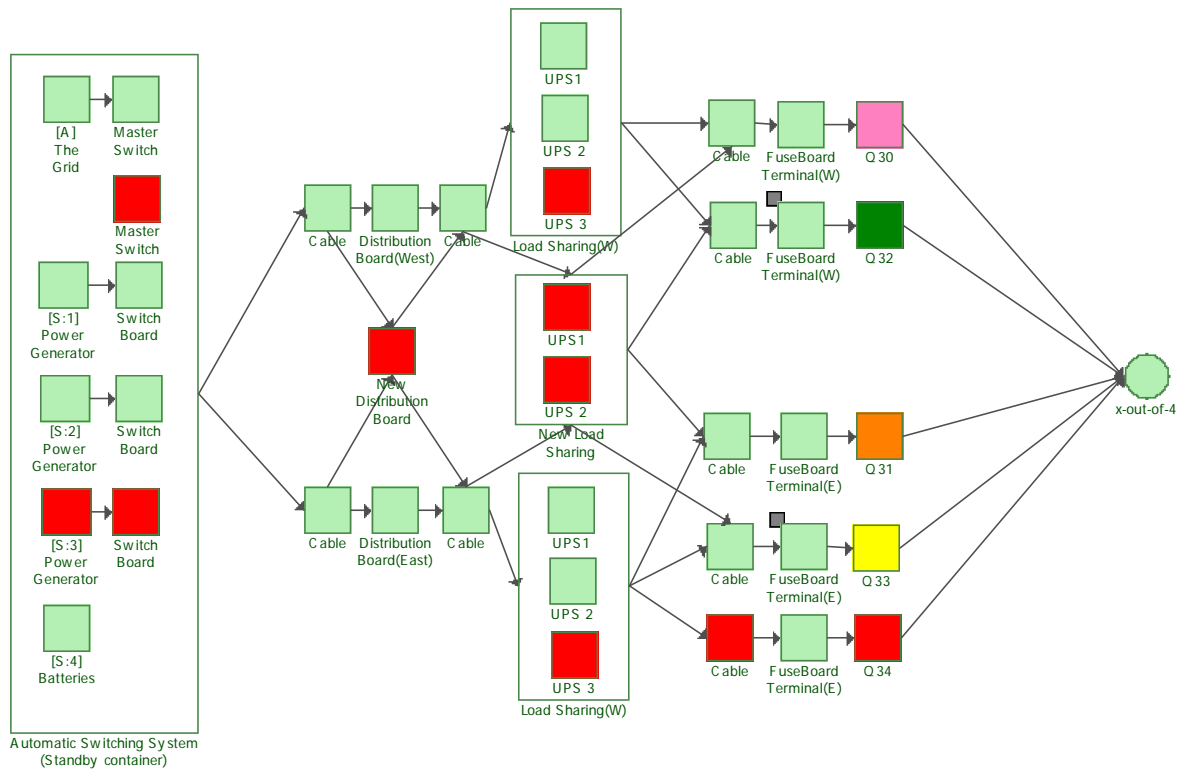
- Master switch.
- A power generator and switch board.
- Distribution board.
- A third UPS within the load sharing containers (on both sides).
- A third UPS on one side of the system.
- A third UPS load sharing container.
- Fuse board.

Figure 6-2 shows where these units were added into the model. The components were added one at a time and they are displayed in red<sup>55</sup>.

---

<sup>54</sup> How difficult it is to improve with regards to e.g. cost or availability of technology.

<sup>55</sup> There should be an arrow from the grid to the new master switch. This is not an option because it is inside a container and BlockSim does not allow complex configurations within a container. However by using a feature of BlockSim (subdiagrams) the reliability distribution for 2 master switches in parallel was imbedded in the master switch component.



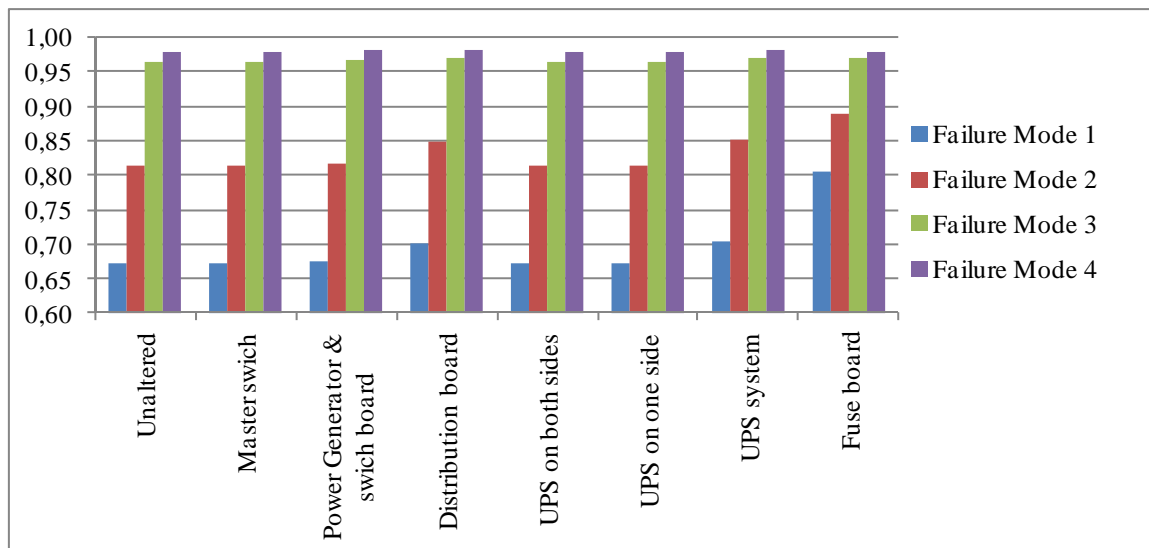
**Figure 6-2: Shows with red where the components are added.**

As these units are added one at a time the configuration of the block diagram changes. Accordingly, the results of the calculations change to reflect the additional new component. The reliability results are presented in Table 6-2.

**Table 6-2: Reliability results when the system has been altered by adding components.**

Failure Mode	Unaltered	Master swich	Power diesel & swich board	Distribution board	UPS on both sides	UPS on one side	UPS system	Fuse board
1	0.672637	0.672790	0.67462835	0.70091745	0.6733	0.67297	0.70324	0.8064146
2	0.813414	0.813600	0.81582237	0.84761357	0.81421	0.81381	0.85042	0.8899243
3	0.963392	0.963612	0.96624412	0.96929887	0.96353	0.96346	0.96936	0.9706660
4	0.978315	0.978539	0.98121203	0.98122951	0.97839	0.97835	0.98100	0.9785012

These results are in harmony with previous results of Reliability Importance ranking of components and the Reliability Allocation results. Now it can be seen numerically how much each change affects the reliability of the electrical power system. These reliability results can also be seen in Figure 6-3 and are in many cases quite close for different additional components (especially for EP Failure Mode 3 and 4). Thus in those cases adding an additional component has a small effects on system reliability. This is explained by redundancy i.e. the system becomes less sensitive to changes when fewer paths are required for the system to be considered operational.



**Figure 6-3: Reliability results when the system has been altered by adding components.**

Figure 6-3 shows that the reliability of the electrical power system increases most by adding an extra fuse board to the system. Hence the fuse boards constitute the weakest links in the model. According to Reliability Importance the next best thing should have been to add a distribution board. However, by using trial and error it can be seen that adding an extra UPS system gives better results. The difference occurs because reliability importance only accounts for adding one extra UPS component to the system not a whole UPS system. A UPS system includes two UPS components in a load sharing unit, i.e. in the event of one failing the other takes on an increased load to keep the system operating. Thus in the next section, it will be determined how modifying the electrical system by adding a UPS system will affect the reliability of the ATM system.

By now research questions 1 and 2 have been answered *with respect to the electrical power system*. In the next subchapter these questions along with research question 3 is discussed *with respect to the RACC ATM/CNS system*.

## 6.2. RACC ATM/CNS System Reliability

The reliability of the ATM/CNS system or the probability of proper functioning of the system is calculated based on three different Failure Modes:

- Failure Mode 1: Most demanding case: The system is operational and there is absolutely **no tolerance of failure** in the system. All paths are needed for a successful operation and thus there is no redundancy in the system.
- Failure Mode 2: A normal function: The minimum equipment needed for the system to **function “normally”** without any disruption of service. No influence on operational staff or ATC Center capacity. The system has increased redundancy as fewer paths are required.
- Failure Mode 3: The system is considered functional as long as there is not a complete failure of the system, i.e. the system is considered to be functional as long as both the Flight Data Processing System (FDPS) submodel and Voice

Communication System (VCS) submodels are operational. This has significant influence on operational staff and ATC Center capacity and would be unacceptable for extended periods and at peak times.

Since the functionality of the system is dependent on various subsystems and equipment a few questions were defined to determine how many successful (minimum) paths are needed from each subsystem or equipment, for the system to be operating properly in each failure mode. The questions are listed below, each of them corresponding to the node with the same number in Figure 5-5.

**CNS equipment:**

- Question/Node 1: How many paths are needed from the Optical fiber terminals? (max available paths 2).
- Question/Node 2: How many paths are needed through the MUX system? (max available paths 4).
- Question/Node 3: How many paths are needed from the VCS system? (max available paths 2).
- Question/Node 4: How many paths are needed from the iPOS? (max available paths 4).

**ATM equipment:**

- Question/Node 5: How many data paths are needed (AFTN/OLDI/DANICE/FARICE)? (max available paths 7).
- Question/Node 6: How many paths are needed from the FDPS? (max available paths 4).
- Question/Node 7: How many paths are needed from the Black Boxes? (max available paths 8).
- Question/Node 8: How many paths are needed from the RDPS? (max available paths 2).
- Question/Node 9: How many paths are needed from the CWS/IOT? (max available paths 4).
- Question/Node 10: How many paths are needed from the ISDS? (max available paths 4).
- Question/Node 11: How many paths are needed through the whole system? Is FDPS, RDPS and VCS needed? (max available paths 3).

Each of those questions was discussed in chapter 5. The answers to these questions are provided in Table 6-3 for each of the three Failure Modes.

**Table 6-3: Minimum equipment list for each functionality Failure Mode.**

Question/ Node	Equipment	Failure Mode 1	Failure Mode 2	Failure Mode 3
1	Optical fiber terminals	2	1	1
2	MUX	4	2	2
3	VCS	2	2	1
4	iPOS	4	2	2
5	AFTN/OLDI/FARIC/DANICE	7	3	2
6	FDPS	4	1	1
7	Black Boxes	8	8	0
8	RDPS	2	1	0
9	CWS/IOT	8	4	1
10	ISDS	4	2	0
11	Subsystems (FDPS,RDPS,VCS)	3	3	2

The values are assumptions regarding the minimum paths needed for a successful functioning of the system. The assumptions were made based on specialist opinions and the FMECA analysis conducted in cooperation with Isavia specialists for this analysis (FMECA was discussed in chapter 3.2.3.).

The values that draw attention are the values for mux, iPOS and the Black Boxes as the required functionality may not require this many paths. The Black Boxes are used to split up radar data lines. Looking at the Black Boxes as an example, it may be excessive to require that all of the radars are needed for normal operation. However, here it is assumed that all of them are needed for normal operation because the Black Boxes are all connected the same way, i.e. to Q30 (pink) and Q33 (yellow). As they are all connected to electrical power in the same manner it is not necessary to specify which ones are needed for each Failure Mode as either all or none are working. The multiplexers are connected to the electrical power system in such a way that either all four, two or none receive electrical power.

By looking at the reliability model in Figure 5-5 it can be seen that if one VCS is operational there are at least two sets of iPOSeS that are also operational. Further more if two VCSs are operational there are at least 3 sets of iPOSeS (if Q31<sup>56</sup> (orange) and Q32 (green) have failed and if Q30 (pink) and Q33 (yellow) have failed at the same time). In all other cases the whole four sets are available.

Any failure that does not violate the specifications of required minimum equipment needed for each Failure Mode only results in a lower level of redundancy.

---

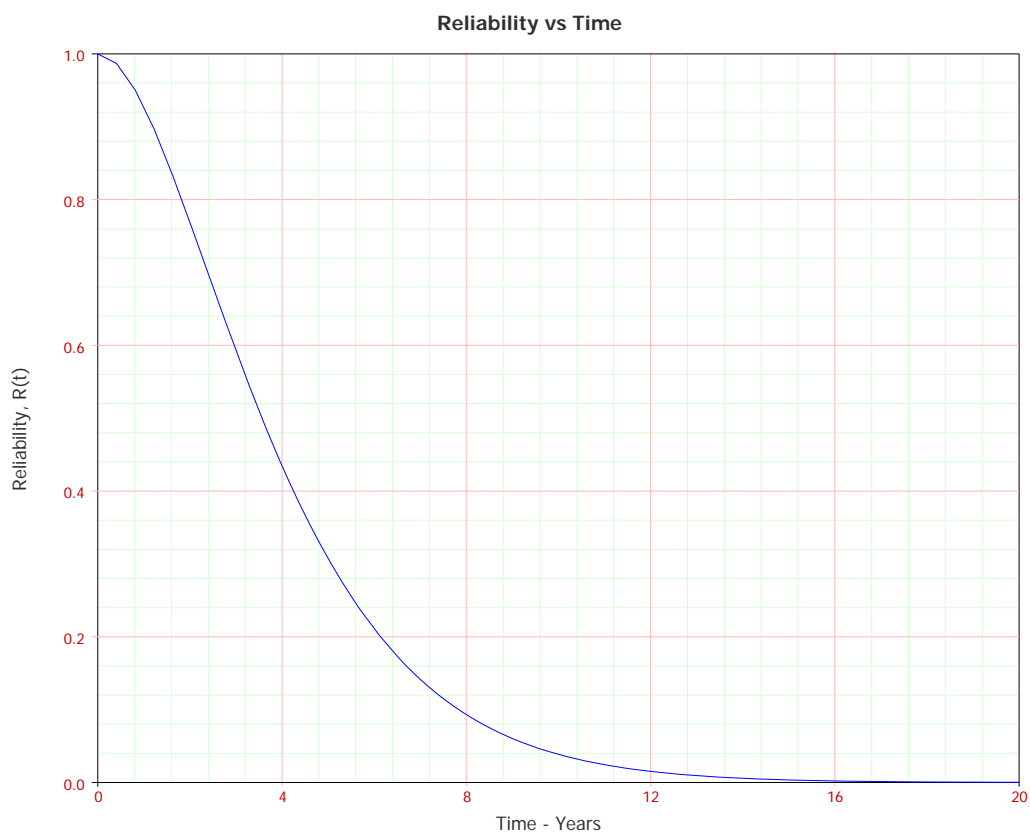
<sup>56</sup> Q30-Q33 represents fuse boards. Each equipment is connected to at least one fuse board which provides it with electrical power.



**Research question 1:** What is the reliability of the overall ATM system in terms of probability due to electrical power system failures?

As the reliability of the ATM subsystems and components are dependent on the electrical power system the maximum reliability of the ATM system is 0.99957423 when only failures of the electrical power system are considered. As already noted the model is sensitive to the data that is put into the electrical power system model. Other MTTF values may generate different reliability results. However the analysis and evaluation of different design options and what units could be added to improve overall system reliability does not change.

A plot of the reliability function of Failure Mode 2 is presented next in Figure 6-4.



**Figure 6-4: The reliability function of the ATM system vs. time.**

The reliability of the ATM system is presented in Table 6-4 for the three Failure Modes in terms of the reliability of a non-repairable system, MTTF and availability given three different MTTR values for the components of the electrical power system. The probability that the ATM system does not fail over a period of one year is given in the reliability column of the table.

**Table 6-4: Probability of successful ATM system operation.**

<b>Failure Mode</b>	<b>Reliability Non-repairable</b>	<b>MTTF of the system</b>	<b>Availability (MTTR=1 week)</b>	<b>Availability (MTTR=24 hrs)</b>	<b>Availability (MTTR=1 hr)</b>
1	0.53779079	1.5 years	0.98729239	0.99815579	0.9999228
2	0.92889362	4.3 years	0.99997042	0.99999927	0.9999999
3	0.99703598	9.8 years	0.99998343	0.99999934	0.9999999

Failure Mode 1 is not very realistic as it is based on the assumption that the system is considered to be dysfunctional even if a single subsystem or component fails. However the system has built in redundancy and consequently continues to operate normally. This failure mode is included to see the most demanding case of system operation. In this failure mode the availability of the system can be very high although the reliability is low as is to be expected if only one simple failure is considered to be the cause of a system failure. The availability is high because the availability is only affected by down-time due to corrective maintenance. It is assumed that corrective maintenance of the RACC electrical power system takes up to a week which is a rather low value compared to the MTTF. However, a week is meant to present a reference value for worst case scenario.

Failure Mode 2 represents a successful normal operation where failure has no influence on operational staff or ATC Center capacity. Hence it is the Failure Mode of most interest. The results obtained from the model for this Failure Mode reveal a reliability of 0.9289 and availability of 0.999970-0.999999 for a time period of one year. This means that there is 7.11% probability of failure of the system within one year period. Availability on the other hand suggests that the system has decreased functionality for 15.5 minutes pr. year in the worst case, 23 seconds/year when maintenance takes 24 hours and 0.3 seconds/year when maintenance takes only one hour.

Failure Mode 3 assumes that the system is functioning with less functionality than in Failure Mode 2. The primary difference is that the RDPS system is assumed to be non-operational. This means that the MTTF of the system more than doubles. Thus it has significantly higher reliability than Failure Mode 2 and almost perfect availability. The availability being almost perfect can perhaps be explained by very high redundancy in the system configuration. Thus when failure occurs (which does happen) another path can be used in the interim period (until repairs have been performed) which means that the failure does not contribute to system down-time.

**Research question 2:** How can the system reliability be improved? Which components constitute the weak links in the system?

This question was answered earlier in this chapter for the electrical power system. It is interesting to see how improving the system by adding an extra component affects the ATM system reliability. In the previous section 6.1 it was found that adding an extra fuse board to the system would result in the most increase in reliability of the electrical

power system. As the ATM system is made up of subsystems and components that are directly linked to the electrical power system, adding an extra fuse board would also result in the highest increase in the ATM system reliability. The question however becomes, how much does this change affect the overall system reliability? The first option would be to add a new fuse board. However as the reliability depends on which equipment would be connected to the new component this option will not be considered. Instead, the next best option is looked at; adding a third UPS system as was done in previous section 6-1.

When answering research question 1 it was found that the reliability of the ATM system is 0.92889362. If a third UPS system would be added to the electrical power system, the reliability of the ATM system assuming Failure Mode 2 (Normal operation) would become 0.94412355. Thus the reliability would increase by approximately 1.52% adding half a year to MTTF. Failure Mode 1 (the most demanding case) would however increase by 4.57%. The reason why reliability increases more for Failure Mode 1 is because it has no redundancy so that the reliability increase of each component has more value.

Reliability Allocation and Reliability Importance were used to answer this research question for the electrical power system. Reliability Allocation cannot be used for the ATM system as the BlockSim software cannot perform Reliability Allocation on mirrored components. The Reliability Importance measurement also provides limited information in this case since it only considers the importance of each fuse board connection but not the importance of ATM components.

The ATM system has three main submodels; the FDPS, RDPS and VCS submodel. Each function was analyzed by trial and error, by either trying different electrical power connections on the existing components in the ATM or by adding extra ATM components in parallel to see how these additions effect system reliability. As an example the reliability of the system is calculated were another VCS component is added. These calculations were performed for Failure Mode 2 as it is of most interest.

As only one FDPS component (A, B, C or D) is needed for a successful FDPS submodel in normal operation and FDPS components are connected to all fuse boards, the FDPS submodel cannot fail due to failure of FDPS components without the whole electrical power system having failed, i.e. all FDPS components do not fail unless none of the electrical fuse boards are operating (which would result in total system failure anyway). The FDPS submodel is however dependent on data connections. This is where the weakest link of the FDPS submodel lies. By adding a third AFTN terminal connected to Q30 (and Oper2 sw2) the reliability of the FDPS submodel would increase from 0.96169568 (MTTF: 6.4 years) to 0.97682759 (MTTF: 6.9 years). To increase reliability even further a submarine communications cable that is also connected to Q30 can be added resulting in reliability of 0.99449774 (MTTF: 8.6 years). Thus adding these components has significant affects on system reliability.

The reliability of the RDPS submodel can be improved as the Black Boxes (devices needed to split up radar signals) are all connected to electricity the same way (to Q30 and Q33). Thus either all are functioning or all have failed. Connecting the Black Boxes to different electrical sources would create redundancy as the radars provide partial back-up for one another. Both the dual RDPS systems are connected to Q31 and Q32. If one RDPS would be connected to Q30 and Q33 the reliability for the RDPS submodel in normal operation would increase from 0.95915743 (MTTF: 5.2 years) to 0.97936583 (MTTF: 8.1 years). Then, by adding only Q32 to the Black Boxes connection and oper1 sw2 or 3 to the Black Boxes connection the reliability would increase to 0.99703598 (MTTF:9.8 years).

The VCS submodel seems to be rather reliable with respect to electrical power as it is connected to all four fuse boards. If it is assumed that only one of VCS A or B is needed for full operation the VCS submodel is as reliable as it can get with respect to electrical power. On the other hand if both units are needed (as is assumed for normal operation in Failure Mode 2) adding an extra VCS unit that is connected to both UPS systems would increase the reliability of the VCS submodel from 0.95915743 to 0.99449774. This meant that the MTTF would increase from 5.2 years to 8.6 years.

As increasing the MTTF of the system is very important it goes without saying that these are significant results. Thus these values can be used as bases for decision making regarding improvements of the ATM system.

**Research question 3:** How does the failure of certain parts of the electrical power system affect the overall system reliability? (“**What-if**” analysis).

“What-if” analysis is used when calculating conditional probability. This is used here to assess the effects that failures of certain electrical power components have on the overall system performance. The reliability of the ATM system is calculated with respect to what-if questions that are believed to result in a situation (problem) that is of interest with respect to system performance. The questions that were generated are listed below:

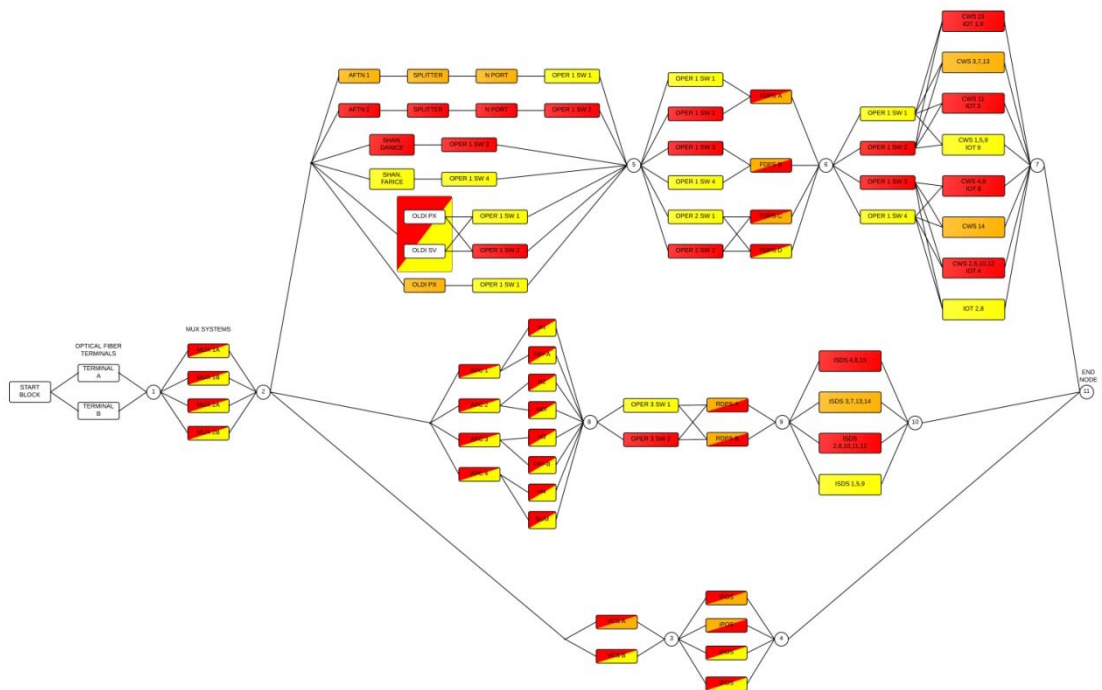
1. “What-if” one diesel power generator fails?
2. “What-if” one of the two UPS components in a UPS system fails?
3. “What-if” one distribution board fails?
4. “What-if” East or West UPS system fails?
5. “What-if” a fuse board input terminal fails?
6. “What-if” one fuse board (Q30 – Q33) fails?

As there is no room for error in Failure Mode 1 the reliability drops to 0 if a single component fails. This failure mode is therefore not examined in the what-if analysis.

If one diesel power generator fails the reliability of the RACC ATM system in normal operation drops approximately 5% (“what-if” question 1). One UPS failing on either side has a lesser effect as it is in load-sharing and the other component would take over

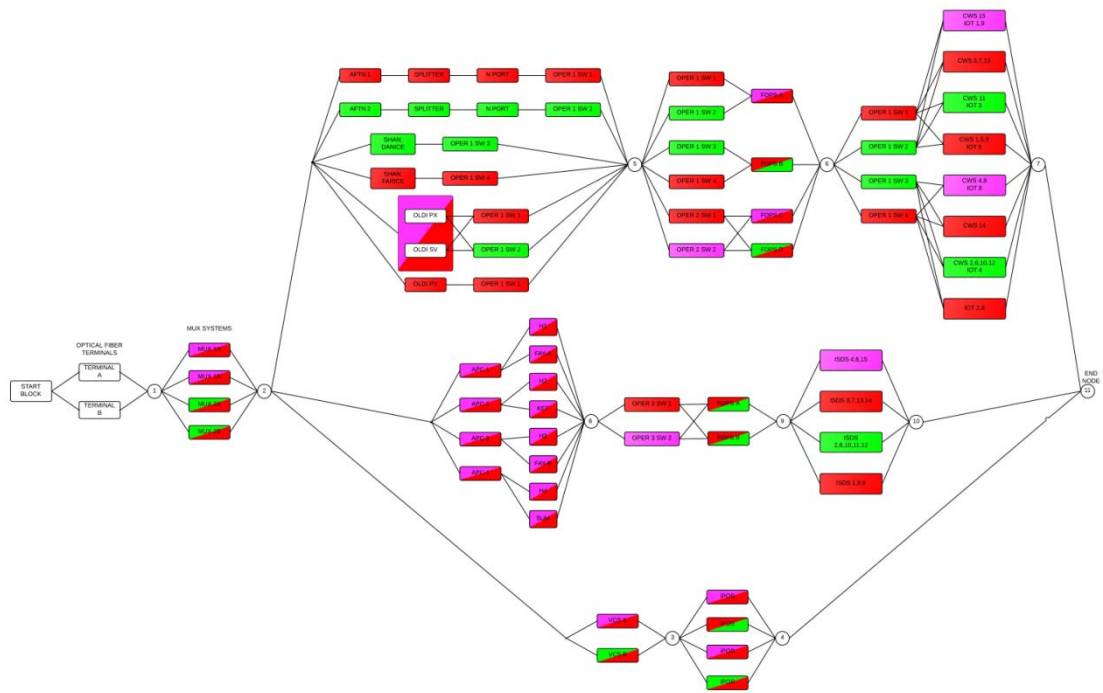
the load. This would decrease the reliability of the system approximately 1.66% for normal operations (“what-if” question 2). The effect on Failure Mode 3 are less than 1% for both questions but there is consistency in the reliability decrease i.e. failure of the diesel power generator results in a more significant decrease in reliability than if one UPS fails.

If one distribution board fails it would result in the failure of two fuse boards, either both Q30 and Q32 (pink and green) or both Q31 and Q33 (orange and yellow). The same applies if East or West UPS systems or if a fuse board input terminal fail. This can be seen in the reliability model (Figure 5-2) by the fact that these are modeled in series which means that all of these are needed for the path to succeed. Thus what-if questions 3,4 and 5 all have the same answer which is *either Q30 and Q32 (pink and green) or Q31 and Q33 (orange and yellow) fail*. These would result in the most serious decrease in the system reliability or approximately 20% for both Failure Modes (1 and 3). The failure modes are depicted in Figure 6-5 and Figure 6-6. When these are compared to the original model (Figure 5-5) it can be seen that there are fewer redundancy paths available for the system. Next the figures depicting failure of one UPS will be discussed. When the components in a path have been colored red it means that the path fails in the event of failure of the UPS.



**Figure 6-5: Overview of the system if fuse boards Q30 and Q32 fail.**

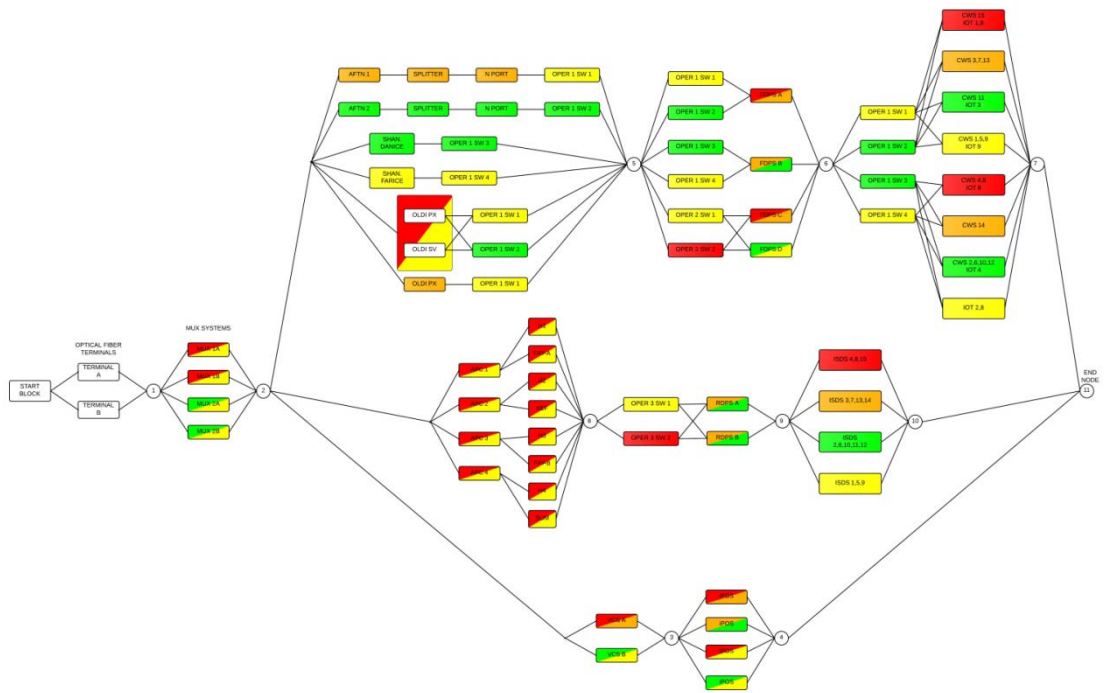
When fuse boards Q30 and Q32 fail (pink and green) half of CWS/IOT and ISDS fail. In addition one AFTN path and the DANICE path are missing. Thus there are only 4 data and communication paths available instead of 7 paths when nothing has failed.



**Figure 6-6: Overview of the system if fuse boards Q31 and Q33 fail.**

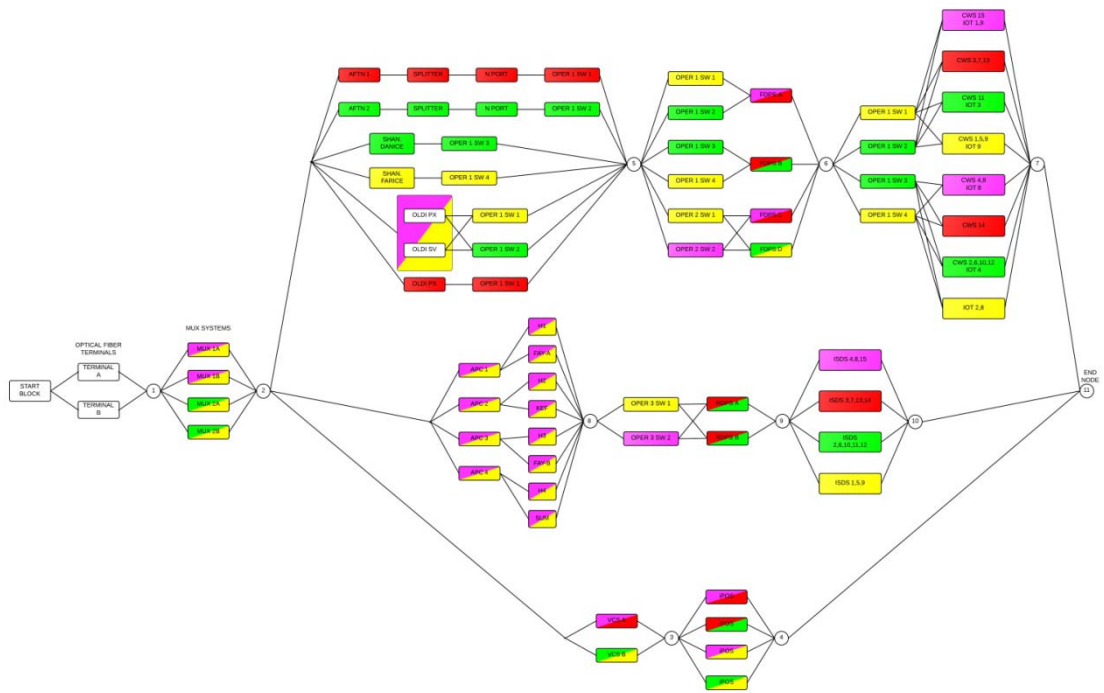
When fuse boards Q31 and Q33 fail (orange and yellow) the same thing happens as when Q30 and Q32 fail (pink and green) except instead of DANICE failing the FARICE path fails. In addition the data path OLDI fails. Thus there are only 3 data and communication paths available instead of 7 paths when no failure has occurred. As there are only 3 available paths when Q31 and Q33 fail this has the most effects on system functionality.

“What-if” question 6, i.e. that one fuse board (Q30 – Q33) fails, can be addressed by considering failure mode Figures 6-7, 6-8, 6-9 and 6-10. The figures present the ATM reliability model in the event that one of the fuse boards has failed. When the components in a path have been colored red it means that the path fails in the event of failure of the fuse board.



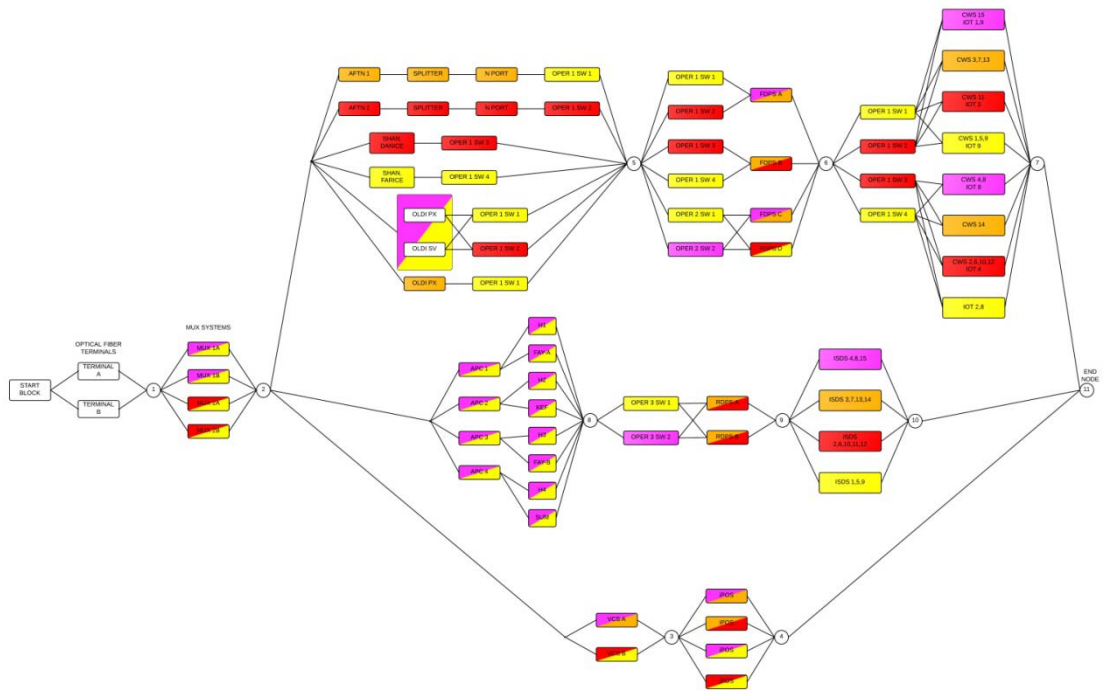
**Figure 6-7: Overview of the system if fuse board Q30 fails.**

The effects of failure of Q30 can be seen in Figure 6-7. When Q30 fails it has a minor effect on the system as only those components of the CWS/IOT and the ISDS that are connected to that fuse board fail. Fortunately, the system has redundant components connected to other fuse boards. This is also the case if one of the other fuse boards fails. Another component that fails is the operswitch needed for the FDPS system. There are four other back-up operswitch components so that this failure has no effect on the system. Other effects are that the system loses redundancy and thus the probability of failure increases.



**Figure 6-8: Overview of the system if fuse board Q31 fails.**

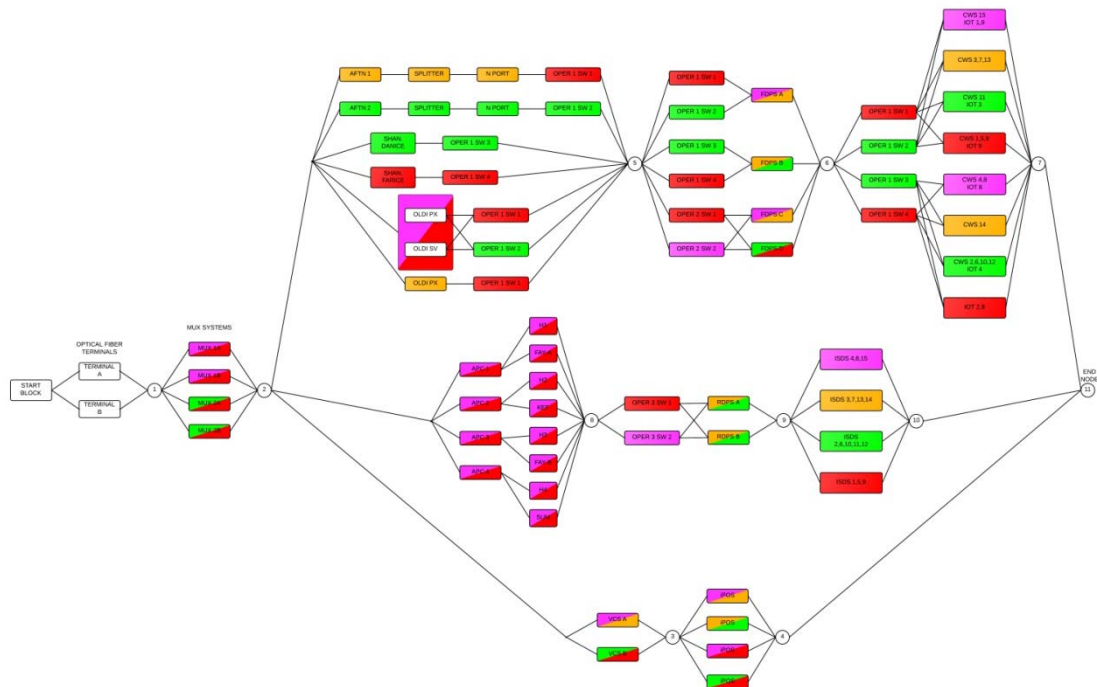
The effects of failure of Q31 can be seen in Figure 6-8. When Q31 fails the same thing happens as when Q30 fails. In addition one AFTN path and one OLDI path are missing. Thus there are only 5 data and communication paths available instead of 7 paths when nothing has failed.



**Figure 6-9: Overview of the system if fuse board Q32 fails.**



The effects of failure of Q32 can be seen in Figure 6-9. When Q32 fails the same thing happens as when Q31 fails except instead of OLDI path failing a DANICE path fails.



**Figure 6-10: Overview of the system if fuse board Q33 fails.**

The effects of failure of Q33 can be seen in Figure 6-10. When Q33 fails the same thing happens as when Q30 fails. In addition one AFTN path, one OLDI path and the FARICE path are missing. Thus there are only 3 data and communication paths available instead of 7 paths when nothing has failed. When Q33 fails the system loses more paths than any of the other fuse boards. Thus failure of Q33 has the most influence on system functionality. The failing of Q30 on the other hand has the least influence on system functionality. The system also loses the most redundancy if Q33 fails, after that if Q32 fails, Q30 and then Q31.

It can be seen in these figures that the system loses most redundancy when Q33 (yellow) fails (Figure 6-10), then Q32 (green) (Figure 6-9), then Q30 (pink) (Figure 6-7) and finally Q31 (orange) (Figure 6-8). Furthermore the figures demonstrate that there is no single point of failure in the system.

### 6.3. Limitations of results

All results are limited to failure in the electrical power system. Thus other failure causes are not reflected in the model.

There was scarcity of suitable data for the RACC electrical system components. Lack of data was overcome by including expert judgment. The gathering of information was conducted by interviewing experts within the company. Therefore reliability data is mainly based on the opinion of these experts. This limits the results as reliability results are only as accurate as the data available for the components of the system. Even if the

absolute values are not very accurate, reliability analysis can be useful for comparing alternative design options and for performing sensitivity analysis (Bailey, Frank-Schultz, Lindeque, & Temple III, 2008).

#### **6.4. Feasibility of using reliability models for ATM systems**

The approach and reliability methods applied in this research project, i.e. Reliability Block Diagrams including the BlockSim software, works very well to analyze and determine the reliability of ATM systems. It is based on mature and recognized modeling techniques that provide a convenient description of how various subsystems and components interact to deliver the designed functionality of the system. The construction of a reliability model leads to a better understanding of the system design, including aspects such as component interdependencies, interconnection of equipment/subsystems and reliability weaknesses (Bailey, Frank-Schultz, Lindeque, & Temple III, 2008).

The two techniques employed in this work, i.e. the RBD method and the FMECA are complementary and work well together. FMECA provides a good basis for applying the RBD model technique. The RBD is supported by the BlockSim software system that was applied to perform the model reliability calculations. The BlockSim provides a comprehensive platform for reliability calculations and is well suited for handling large and complex systems such as the RACC ATM system. One of many impressive features of the system is the ability to provide the analytical reliability equation of the system which the software uses to calculate the exact reliability metrics of the system (an example was shown in section 6-1). Other impressive features of the system include the Reliability Allocation and Reliability Importance that have been elaborated on in this research project. Also, many maintenance factors such as number of spare parts and the need for inspections can be provided. However there is one shortcoming. When modeling common cause failures, such as electrical power outages, mirrored blocks must be used. These are normally used to model the same units multiple times in a model. The software does not allow for the mirrored components to be analyzed in the same way as distinct components (such as FDPS, RDPS and so on). For this reason the Reliability Allocation features cannot be used to analyze the ATM components. This task was performed by instead using a trial and error procedure, which provides equivalent results.

One of the most significant benefits of the aforementioned techniques is that they work well for highly complex systems such as an ATM system that would be very difficult to handle in any other way. Even when there is lack of reliability data an RBD analysis can still be useful for comparing alternative design options and for performing sensitivity analysis even if the absolute values are not very accurate (Bailey, Frank-Schultz, Lindeque, & Temple III, 2008). Thus, applying the RBD approach increases understanding of system functionality and how it is dependent on individual components and subsystems. These results in an overview of system functionality which is an important part of evaluating what elements should be brought into focus when attempting to further increase the reliability of the system.

It is concluded that the RBD model and the BlockSim software are very attractive for further modeling of the Reykjavik ATM system. This is discussed further in the following chapter.

## 7. Conclusions and Recommendation

---

This chapter provides a summary of the research project, conclusions and recommendations.

### 7.1. Summary

Air traffic management (ATM) systems are critical to flight safety. Any downtime is typically very costly in terms of economic penalties and if serious they can negatively impact flight safety. In extreme cases ATM system failure can result in loss of life. Even the most reliable systems can fail, as no system is perfect. Probability of a system failure may be very low but it is not zero (United States Army, 2003). The development of a model to verify that the reliability of a complex safety-critical system is often a stated requirement as this is of significant value from safety assurance point of view as well as for economic reasons.

There are several possible failure causes in the ATM system, e.g. technical failures which include computer equipment failures (software and hardware) and electrical power system failures. Other failure causes include human failures.

The main focus of this research project was on technical failures and in particular failures of the electrical power system used by the Reykjavik Area Control Center (RACC) ATM system. The electrical power system is a logical starting point as presence of electrical power is absolutely vital to the ATM system as is the case of any safety critical system. Non-availability of electrical power can lead to total system break-down which is unacceptable in systems of this type. Thus it is clearly very important to ensure that all necessary precautions have been made to prevent failures of the electrical power system in the RACC.

The aim was to investigate, select and adapt a recognized general reliability method and apply this method to computing the reliability of the ATM system.

Using proven methods, i.e. Reliability Block Diagram (RBD) and Failure Mode, Effects, and Criticality Analysis (FMECA), for modeling system reliability a quantitative model was developed to determine the effect of electrical power failure on the reliability of the overall ATM system. A software system, BlockSim, was used for calculation. The software has not been used in Iceland before. It is a vital tool as calculating reliability of complex systems like the RACC system by hand would be a difficult or at least very time-consuming task.

This approach of evaluating the reliability of the Icelandic ATM system has not been used in the past. Furthermore this is the first time that an attempt has been made to calculate the reliability of the system as a whole on the basis of a reliability model.

The quantitative model generates calculations of reliability and availability of the system based on assumptions regarding system functionality expressed by the choice of a few Failure Modes (discussed in chapters 5.2 and 6). Availability is no less important

than reliability. Reliability does not take maintenance into account but availability does. Therefore it can be argued that availability is a more realistic measurement of system operability. Reliability is expressed in terms of the probability that the system does not fail in a time interval whereas availability is the probability that the system is functioning at a given point in time. Average availability gives the percentage of time that a system is available to perform its required functions (Xie, Poh, & Dai, 2004).

## **7.2. Conclusions**

The model returns statistical values for reliability and availability. Failure Mode 2 provides results of most interest as it represents the minimum equipment that must be operational without affecting operational staff or ATC Center capacity. This is intended to be close to the actual operational functionality of the system. It was found that the reliability of the ATM system, taking into account potential failures of the electrical power system, is 92.89% for normal operation (Failure Mode 2). This does not consider the effect of maintenance. This means that there is 7.11% probability of failure of the system within a period of one year. By adding maintenance to the model would result in availability of 99.99%. Availability suggests that the system has decreased functionality for 15.5 minutes pr. year in the worst case, 23 seconds/year when maintenance takes 24 hours and 0.3 seconds/year when maintenance takes only one hour.

If the reliability of the system is to be improved the efforts should be focused on first improving the reliability of the component or components that have the most significant effect on overall system reliability. By applying Reliability Importance, Reliability Allocation and by using a trial and error approach it was found that the fuse boards affect the reliability of the ATM system the most. Thus to improve system reliability it would be most beneficial to add a fuse board to the electrical power system. The reliability of the ATM system would however depend on which equipment would be connected to the new fuse board component. Therefore the next best option was considered; i.e. adding a third UPS system. If a third UPS system would be added to the electrical power system, the reliability of the ATM/CNS systems Failure Mode 2 would become 94.41%. This means that the system reliability would increase approximately 1.63% which adds half a year to Mean Time To Failure (MTTF).

What-if analysis revealed that when Q33<sup>57</sup> fails the system loses more paths through the ATM system than in the case of failure of any of the other fuse boards. Thus failure of Q33 has the most influence on system functionality. Q30 failing has the least influence on the system. The system also loses the most in terms of redundancy if Q33 fails (Figure 6-10), then Q32 (Figure 6-9), then Q30 (Figure 6-7), and finally if Q31 fails (Figure 6-8) in that order of importance. Thus when changes are to be made in the ATM system configuration by adding components for added redundancy it is recommended to use Q30 and Q31 (pink and orange). However each decision must consider how prior existing equipment in the system is connected.

---

<sup>57</sup> Q30-Q33 represent fuse boards. Each equipment is connected to at least one fuse board which provides it with electrical power.

The reliability model was also used to try out different changes in configuration of the ATM system to identify equipment or subsystems that need to be improved in terms of reliability. Based on this, recommendations regarding improvements of the RACC ATM system can be made by considering:

- Connecting one of the dual Radar Data Processing Systems (RDPS) to Q30 and Q33.
- Connecting some radar Black Boxes to Q31 and Q32.
- Adding a third VCS that is connected to both UPS systems if both Voice Communication System (VCS) A and B are needed for satisfactory system operation.
- Adding an AFTN terminal and a path for a submarine communication cable connection that are connected to Q30 as the communications and data paths are the weakest link in the FDPS submodel function.

Improving the RDPS submodel reliability has the most effect on the reliability of the ATM system so it is recommended that it should be given priority. The next actions would be to change the VCS submodel and then Flight Data Processing System (FDPS) submodel which is the most reliable submodel. Making the changes above to the ATM system would result in reliability increase of 3.28%, 3.78% and 3.53% for FDPS, RDPS and VCS respectively. If the RDPS submodel is improved the MTTF would increase from 5.2 years to 9.8 years. If the VCS submodel is improved the MTTF would increase from 5.2 years to 8.6 years. And if the FDPS submodel is improved the MTTF would increase from 6.4 years to 8.6 years.

### **7.3. Further research and development work**

This research project provides a feasibility study and initial analysis of the reliability of the RACC ATM system which is the most complex command and control system operated in Iceland. This research has focused on an important part of the system, i.e. the electrical power system. This is an important part of the ATM system. However there are several other possible failure causes that are also important. For this reason much more research work is needed for modeling and evaluating this system in order to incorporate all of the subsystems and components failures into the model. The inclusion of models for representing software reliability is an area that is very challenging.

The quantitative model that has been developed in this research project accounts for electrical power failures. Thus it is assumed that components or subsystems do not fail except due to the lack of electrical power. As this is only one possible cause of technical failure it is necessary to extend the model to account for other causes of technical failures as well as human failures and failures due to degradation of components or subsystems. This would result in a model that provides an overall reliability model of the ATM system. Although the focus in this research is on the electrical power system, the whole ATM system was modeled in such a manner that only statistical failure data (along with minor adjustments) for the remainder of the subsystems and equipment will be needed to extend the model in this manner. Hence, this research project provides

valuable information about the RACC ATM system behavior and provides a model that can be used as basis for further research.

The reliability model can easily be extended with additional modeling work to account for other failure modes and types. This was explained and shown in chapter 5.3. When the model is extended systems outside the ATC Center could also be modeled, such as the communications networks, radar stations and even aircraft systems. These were not included in this research project as they do not depend in any way on electrical power from the ATC Center. The estimation of overall reliability is important to evaluate the need for special measures in order to increase reliability, e.g. to add an extra redundant component of an ATM system in an ATC Center or to establish a back-up system that is remotely located.

Systems such as the ATM system are always being up-graded and changed. Analyzing reliability should consequently be an on-going activity that starts with the initial design and continues through the evaluation of alternate design options, redesigns, and corrective actions (United States Army, 2003). The model developed in this research project can be used as a basis for this kind of analysis.

Modeling is never totally accurate as many simplifying assumptions are made in these models and statistical data on reliability are often limited. Reliability data should be continuously collected and readily available when needed for analysis and model development. Thus a standardized systematic data gathering program should be implemented at the RACC. The reliability model can be improved by getting more accurate MTTF and Mean Time To Repair (MTTR) values for the electrical components as well as values relating to other failure types. This means that it would be recommended to document failure i.e. when it occurs, when repair action start and when the component has been repaired for all components that will be modeled. These are the most important information for reliability modeling, there are however many features within BlockSim that may be used to reflect reality better e.g. information regarding preventive maintenance and spare parts availability can be modeled. For further studies would be interesting to obtain cost information for each of these components and carry out a cost-benefit analysis, i.e. to compare the relative reliability increase to component and implementation costs.

As the Voice Communications System (VCS) is highly complex the VCS functionality was simplified more than the other subsystems for the purpose of this analysis. Thus this could be an interesting topic for another study.

To sum up how the model could be extended:

- Other failure modes and failure types could be included.
- More accurate reliability data (including MTTF and MTTR values) should be collected to compute the most suitable probability distribution for the values.
- Cost of improving the reliability of components could be considered.
- Remotely located systems and equipment could be added.

- More detailed models for the VCS system should be developed.

In general it is recommended that further research in the area of reliability should be carried out. Expanding the model would provide an even more realistic overview of the system reliability in order to determine the robustness of the system, permitting identification of equipment or subsystems that need to be improved and in order to evaluate the impact of system modifications on reliability.

The research project has successfully calculated reliability of the ATM system. It is concluded that BlockSim is suitable and has proven to be a useful tool for this purpose.



## 8. References

---

- Apthorpe, R. (2001). A Probabilistic Approach to Estimating Computer System Reliability. *2001 LISA XV* (pp. 31-46). San Diego: The USENIX Association.
- Australian Government & Civil Aviation Safety Authority. (2012, March). *ADS-B Automatic Dependent Surveillance - Broadcast*. Retrieved June 10, 2012, from Civil Aviation Safety Authority:  
[http://www.casa.gov.au/wcmswr/\\_assets/main/pilots/download/ads-b.pdf](http://www.casa.gov.au/wcmswr/_assets/main/pilots/download/ads-b.pdf)
- Bahr, N. J. (1997). *System Safety Engineering and Risk Assessment: A Practical Approach*. London: Taylor and Francis.
- Bailey, D., Frank-Schultz, E., Lindeque, P., & Temple III, J. L. (2008). Three reliability engineering techniques and their application to evaluating the availability of IT systems: An introduction. *IBM Systems Journal* , 577-589.
- Bakker, G. J., & Blom, H. A. (1993). Air traffic collision risk modeling. *The 32nd IEEE Conference on Decision and Control*. San Antonio.
- Bakker, G. J., Kramer, H. J., & Blom, H. A. (2000). Geometric and probabilistic approaches towards conflict prediction. *Third USA/Europe Air Traffic Management R&D Seminar*. Napoli.
- Blake, J. T., Reibman, A. L., & Trivedi, K. S. (1988). *Sensitivity Analysis of Reliability and Performability Measures for Multiprocessor Systems*. Durham: Duke University.
- Blanche, K. M., & Shrivastava, A. B. (1994). Defining failure of manufacturing machinery and equipment. *Proceedings from the Annual Reliability and Maintainability Symposium.*, (pp. 69-75).
- Blom, H. A., Bakker, G. J., Blanker, P. J., Daams, J., Everdij, M. H., & Klompstra, M. B. (1998). Accident risk assessment for advanced ATM. *The Second USA/Europe Air Traffic Management R&D Seminar*. Orlando.
- Blom, H., Bakker, G., Blanker, P., Daams, J., Everdij, M., & Klompstra, M. (2001). *Accident Risk Assessment for Advanced Air Traffic Management*. Amsterdam: National Aerospace Laboratory NLR.
- Blom, H. A., & Bakker, G. J. (2002). Conflict probability and in-crossing probability in air traffic management. *The 41st IEEE Conference on Decision and Control*. Las Vegas.
- Blom, H. A., Bakker, G. J., Everdij, M. H., & van der Park, M. (2003). Collision risk modelling of air traffic. *The European Control Conference*. Cambridge.
- Boeing Commercial Airplanes. (2006). *Statistical Summary of Commercial Jet Airplane Accidents: Worldwide Operations 1959–2005*. Seattle: Boeing Commercial.

Chandrupatla, T. R. (2009). *Quality and Reliability in Engineering*. New Jersey: Rowan University.

Christensen, R., & Fogh, N. (2008, June 04). *Inertial Navigation System*. Retrieved February 15, 2012, from Aalborg Universitet:  
[http://www.control.aau.dk/uav/reports/08gr1030a/08gr1030a\\_student\\_report.pdf](http://www.control.aau.dk/uav/reports/08gr1030a/08gr1030a_student_report.pdf)

EUROCONTROL. (2006, July 17). *EUROCONTROL - Objectives*. Retrieved February 14, 2012, from EUROCONTROL - Central Flow Management Unit (CFMU):  
[http://www.cfm.eurocontrol.int/cfm/public/standard\\_page/about\\_objectives.html](http://www.cfm.eurocontrol.int/cfm/public/standard_page/about_objectives.html)

EUROCONTROL. (2011, October 01). *Principles for Establishing the Cost - Base for En Route Charges and the Calculation of the Unit Rates*. Retrieved February 15, 2012, from EUROCONTROL:  
<http://www.eurocontrol.int/sites/default/files/content/documents/route-charges/reference-documents/201110-principles-for-establishing-cost-base-for-route-charges-and-unit-rates.pdf>

EUROCONTROL. (2012a). *What is air traffic management?* Retrieved August 17, 2012, from EUROCONTROL: <http://www.eurocontrol.int/articles/what-air-traffic-management>

EUROCONRTOL. (2012b). *EUROCONTROL Specification for ATM Surveillance System Performance (Volume 1)*. Brussels: Eurocontrol.

EUROCONTROL. (2012c). *EUROCONTROL Specification for ATM Surveillance System Performance (Volume 2)*. Brussels: Eurocontrol.

European and North Atlantic Office of ICAO. (2005, September). *North Atlantic MNPS Airspace Operations Manual*. Retrieved February 15, 2012, from Global Operators Flight Information Resource:  
[http://www.gofir.com/general/north\\_atlantic\\_mnps\\_manual\\_2005/MNPSA\\_2005.pdf](http://www.gofir.com/general/north_atlantic_mnps_manual_2005/MNPSA_2005.pdf)

Everdij, M. H., Blom, H. A., & Kirwan, B. (2006). *Development of a Structured Database of Safety Methods*. Brussels: Eurocontrol.

FAA & EUROCONTROL. (1998). *Concept Paper for Separation Safety Modelling*. Washington, DC: Federal Aviation Administration, European Organization for Safety of Air Navigation.

GAIN Working Group B. (2003). *Guide to Methods and Tools For Safety Analysis in Air Traffic Management*. Washington, DC: Abacus Technology Corporation.

Gnedenko, B. V., & Khichin, A. Y. (1962). *An Elementary Introduction to the Theory of Probability*. New York: Dover Publication.

Gray, J., & Reuter, A. (1993). *Transaction Processing: Concepts and Techniques*. San Francisco: Morgan Kaufmann Publishers.

Hafsteinsson, Á. P. & Sigurþórsson, S. (2012, July 02). Operations Manager & Project Manager - Electrical Services. (U. Þórleifsdóttir, Interviewer)

Haraldsdottir, A., Schoemig, E. G., Schwab, R. W., Singleton, M. K., Sipe, A. H., & van Tulder, P. A. (2003, June). *Boeing Capacity - Increasing ATM Concept for 2020*. Retrieved February 14, 2012, from ATM Seminar:  
[http://www.atmseminar.org/seminarContent/seminar5/papers/p\\_115\\_AGC.pdf](http://www.atmseminar.org/seminarContent/seminar5/papers/p_115_AGC.pdf)

Hung, O. K., & Gough, W. A. (1996). Elements of a power systems risk analysis and reliability study. *Petroleum and Chemical Industry Conference, 1996, Record of Conference Papers. The Institute of Electrical and Electronics Engineers Incorporated Industry Applications Society 43rd Annual*, (pp. 163 - 168). Philadelphia.

Icelandic Civil Aviation Administration. (2011, December 16). *Flugmálahandbók - Ísland*. Retrieved February 14, 2012, from Flugmálastjórn Íslands:  
<http://www.caa.is/media/PDF/ENR.pdf>

IEC 50(191). (1990). *International Electrotechnical Vocabulary (IEV) - Chapter 191 - Dependability and Quality of Service*. Geneva: International Electrotechnical Commission.

IEEE Std. 352. (1982). IEEE Guide for General Principle of Reliability Analysis of Nuclear Power Generating Station Protection Systems. New York: IEEE.

International Civil Aviation Organization. (2007). *Air Traffic Management*. Retrieved February 14, 2012, from ICAO-dokumenter fra Statens Luftfartsvæsen:  
<http://dcaa.trafikstyrelsen.dk:8000/icaodocs/Doc%204444%20-%20Air%20Traffic%20Management/ATM%20%2015%20ed.pdf>

Irvine, R. (2002). A geometrical approach to conflict probability estimation. *Air Traffic Control Quarterly* 10 , 85 - 113.

Isavia. (2011). *VL420 03-1 Rýmingar- og viðbragðsáætlun*. Reykjavík.

Isavia. (2012a). *Reykjavik Control Area*. Retrieved February 14, 2012, from Isavia:  
<http://www.isavia.is/english/air-navigation/reykjavik-area-control-centre/reykjavik-control-area/>

Isavia. (2012b). *North Atlantic Organized Track System (NAT OTS)*. Retrieved June 19, 2012, from Isavia: from [http://www.isavia.is/english/air-navigation/reykjavik-area-control-centre/north-atlantic-organized-track-system-\(nat-ots\)/](http://www.isavia.is/english/air-navigation/reykjavik-area-control-centre/north-atlantic-organized-track-system-(nat-ots)/)

ITEM Software, Inc. (2007). *Reliability Block Diagram (RBD)*. Retrieved August 15, 2012, from Reliability Engineering Basics: <http://www.reliabilityeducation.com/rbd.pdf>

ITEM Software, Inc. (2012). *Glossary of Common Terms*. Retrieved October 13, 2012, from Reliability Engineering education resources for professionals:  
<http://www.reliabilityeducation.com/glossary.html>

- IVAO. (2012). *North Atlantic Airspace*. Retrieved February 14, 2012, from IVAO Gander / Shanwick Oceanic: <http://occ.iviao.aero/index.php?site=airspace>
- Janic, M. (2000). An assessment of risk and safety in civil aviation. *Journal of Air Transport Management* , 43-50.
- Kececioglu, D. (2002). *Reliability Engineering Handbook - Volume 2*. Lancaster: DEStech Publications, Inc.
- Kristinsson, A. B. (2012, July 02). Projects Manager. (U. Þórleifsdóttir, Interviewer)
- Kumamoto, H., & Henley, E. (1996). *Probabilistic Risk Assessment and Management for Engineers and Scientists*. New York: Institute of Electrical and Electronics Engineers Press.
- Kusy, K. (2012, May 11). Technical Sales Manager, at ReliaSoft. (U. Þórleifsdóttir, Interviewer)
- Leemis, L. M. (1995). *Reliability - Probabilistic Models and Statistical Methods*. New Jersey: Prentice Hall, Inc.
- Leveson, N. (1992). High-Pressure Stream Engines and Computer Software. *International conference on Software Engineering*. Melbourne.
- Luxhoj, J., & Coit, D. (2006). Modeling low probability/high consequence events: an aviation safety risk model. *2006 Reliability and Maintainability Symposium (RAMS)*. Newport Beach.
- Machol, R. E. (1975). An aircraft collision model. *Management Science* 21 , 1089 - 1101.
- Machol, R. E. (1995). Thirty years of modelling midair collisions. *Interfaces* 25 , 151 - 172.
- MIL-STD-1629A. (1980). *Procedures for Performing a Failure Mode, Effects and Criticality Analysis*. Washington, DC: U.S. Department of Defence.
- MIL-STD-882D. (2000). *Standard Practice for System Safety*. Washington, DC: U.S. Department of Defence.
- Míla ehf. (2012). *Our Organization*. Retrieved February 16, 2012, from Míla: <http://mila.is/english/about-us/our-organization/>
- NASA. (1999, March 02). *DHB-S-001, NASA DRYDEN SYSTEM SAFETY*. Retrieved November 15, 2012, from EverySpec: [http://www.everyspec.com/NASA/NASA-General/DHB-S-001\\_11410/](http://www.everyspec.com/NASA/NASA-General/DHB-S-001_11410/)
- NASA. (2002). *Fault Tree Handbook with Aerospace Applications*. Washington, DC: NASA Office of Safety and Mission Assurance.

National Transportation Safety Board. (1996). *AIR TRAFFIC CONTROL EQUIPMENT OUTAGES*. Washington: National Transportation Safety Board.

Netjasov, F., & Janic, M. (2008). A review of research on risk and safety modelling in civil aviation. *Journal of Air Transport Management* , 213-220.

NLR. (2010, December 7). *Documents*. Retrieved July 13, 2012, from NLR - National Aerospace Laboratory of the Netherlands: <http://www.nlr.nl/downloads/safety-methods-database.pdf>

Nolan, M. S. (2011). *Fundamentals of air traffic control*. New York: Delmar Cengage Learning.

Paielli, R., & Erzberger, H. (1997). Conflict probability estimation for free flight. *Journal of Guidance, Control and Dynamics* 20 , 588 - 596.

Paielli, R., & Erzberger, H. (1999). Conflict probability estimation generalized to nonlevel flight. *Air Traffic Control Quarterly* 7 , 195 - 222.

Rausand, M., & Høyland, A. (2004). *System Reliability Theory. Models, Statistical Methods and Application*. New Jersey: John Wiley & Sons, Inc.

Reich, P. (1966). Analysis of long range air traffic systems: separation standards - I, II and III. *Journal of the Institute of Navigation* 19 , 88 - 96, 169 - 176; 31 - 338.

Reliasoft. (2007). *System Analysis Reference - Reliability, Availability & Optimization*. Tucson: Reliasoft Publishing.

Reliasoft. (2010). *Blocksim 7 Training Guide*. Tucson: Reliasoft Publishing.

Roelen, A. L., Wever, R., Cooke, R. M., Lapuhaa, R., Hale, A. R., & Goossens, L. H. (2003a). Aviation causal model using bayesian belief nets to quantify management influence. *ESREL 2003—European Safety and Reliability Conference*. Maastricht.

Roelen, A. L., Wever, R., Hale, A. R., Goossens, L. H., Cooke, R. M., Lapuhaa, R., et al. (2003b). Causal modelling for integrated safety at airports. *ESREL 2003—European Safety and Reliability Conference*. Maastricht.

Rouvroye, J., & Bliet, E. v. (2002). Comparing safety analysis techniques. *Reliability Engineering and System Safety* , 289-294.

Saltelli, A., Ratto, M., Andres, T., Campolongo, F., Cariboni, J., Gatelli, D., et al. (2008). *Global Sensitivity Analysis: The Primer*. Chichester: John Wiley & Sons Ltd.

Sarakakis, G., Gerokostopoulos, A., & Mettas, A. (2011). *Special Topics for Consideration on a Design for Reliability Process*. Tucson: Reliasoft Publishing.

Shortle, J. F., Xie, Y., Chen, C. H., & Donohue, G. L. (2004). Simulating collision probabilities of landing airplanes at non-towered airports. *Simulation* 80 , 21 - 31.

Spouge, J. (2004). *A Demonstration Causal Model for Controlled Flight into Terrain*. London: Det Norske Veritas.

Subotic, B. (2007). *Framework for the Analysis of Controller Recovery from Equipment Failures in Air Traffic Control*. London: Department of Civil and Environmental Engineering, Imperial College London.

Taylor, M. (2009). *What is sensitivity analysis?* London: Hayward Medical Communications.

Testability.com. (2008, June 16). *Reliability Terms*. Retrieved October 13, 2012, from Reliability Engineering Definitions:  
<http://www.testability.com/Reference/Glossaries.aspx?Glossary=Reliability>

The European Parliament and the Council of The European Union. (2004, March 10). *Regulation (EC) No 549/2004 of the European Parliament and of the Council*. Retrieved February 14, 2012, from SKYbrary Aviation Safety:  
<http://www.skybrary.aero/bookshelf/books/460.pdf>

Turner IV, W. P., Seader, J. H., Renaud, V., & Brill, K. G. (2008). *Tier Classifications Define Site Infrastructure Performance*. Santa Fe: Uptime Institute.

United States Army. (2003). *Reliability Primer for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities*. Washington, DC: Department of the Army.

United States Army. (2007). *Reliability/Availability of Electrical & Mechanical Systems for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities*. Washington, DC: Department of the Army.

United States General Accountability Office. (1998, August 14). *Information Concerning Equipment Outages at Two Kansas City Area Facilities*. Retrieved August 03, 2012, from U.S. General Accountability Office:  
<http://www.gao.gov/assets/90/88156.pdf>

Vishay. (2008, August 27). *Reliability and Statistics Glossary*. Retrieved October 13, 2012, from Vishay - manufacturer of discrete semiconductors and passive components:  
<http://www.vishay.com/docs/80088/reliabil.pdf>

Vismari, L. F., & Junior, J. B. (2011). A safety assessment methodology applied to CNS/ATM-based air traffic control system. *Reliability Engineering & System Safety*, 727-738.

Xie, M., Poh, K.-L., & Dai, Y.-S. (2004). *Computing System Reliability: Models and Analysis*. New York: Kluwer Academic/ Plenum Publishers.

## 9. Appendixes

---

### A. Abbreviations

This is a list of abbreviations used in this research project,

<b>A/C</b>	-	Air craft
<b>ACC</b>	-	Area Control Center
<b>ADS-B</b>	-	Automatic Dependent Surveillance Broadcast
<b>ADS-C</b>	-	Automatic Dependent Surveillance Contract
<b>AFTN</b>	-	Aeronautical fixed communication network
<b>ANSP</b>	-	Air navigation service provider
<b>ATC</b>	-	Air Traffic Control
<b>ATM</b>	-	Air Traffic Management
<b>ATS</b>	-	Air Traffic Service
<b>CDF</b>	-	Cumulative Distribution Function
<b>CFMU</b>	-	Central flow management unit
<b>CNS</b>	-	Communications, Navigation and Surveillance
<b>COM</b>	-	Communication
<b>CPDLC</b>	-	Controller Pilot Data Link Communication
<b>CPL</b>	-	Current plan
<b>CRC</b>	-	Control and Reporting Center
<b>CWS</b>	-	Controller Work Station
<b>DLCS</b>	-	Data link Communication System
<b>DLSP</b>	-	Data Link Service Provider
<b>FANS</b>	-	Future Air Navigation System
<b>FDE</b>	-	Flight Data Entry
<b>FDPS</b>	-	Flight Data Processing System
<b>FIS</b>	-	Flight information service
<b>FMECA</b>	-	Failure Mode, Effects and Criticality Analysis
<b>FMS</b>	-	Flight Management system
<b>FPL</b>	-	Flight Plan
<b>GNSS</b>	-	Global Navigation Satellite System
<b>HF</b>	-	High Frequency
<b>ICE</b>	-	Integrated Controller Environment
<b>INS</b>	-	Inertial Navigation System
<b>IOT</b>	-	Input/Output Terminal
<b>iPOS</b>	-	Operator Position
<b>IRS</b>	-	Inertial Navigation System
<b>ISDS</b>	-	Integrated Situation Display System
<b>NAT</b>	-	North Atlantic
<b>OLDI</b>	-	On-Line Data Interchange
<b>PDF</b>	-	Probability Density Function
<b>POS</b>	-	Position

<b>PRM</b>	-	Preferred route message
<b>RACC</b>	-	Reykjavík Area Control Center
<b>RBD</b>	-	Reality Block Diagram
<b>RDPS</b>	-	Radar Data Processing System
<b>ROFDS</b>	-	Radio Operator flight Data System
<b>SAT</b>	-	Satellite
<b>SSR</b>	-	Secondary Surveillance Radar
<b>STCA</b>	-	Short Term Conflict Alert
<b>TAMS</b>	-	Tern ATS message system
<b>VDL</b>	-	VHF Data Link
<b>VHF</b>	-	Very High Frequency



## B. Air Traffic Management system

In this chapter an overview of the Air Traffic Management (ATM) systems will be provided. First an information flow between four different operational functions of the ATM system is presented. Then the technical side of the system will be described where the main building blocks are equipment and software used in the system. The overview of the system is focused on normal operational modes and does not consider information flow under hazardous and unforeseen circumstances.

This chapter and next chapter were prepared on the basis of information from Professor Þorgeir Pálsson and the following specialists at Isavia: Arnar Þórarinnsson, Arnór Bergur Kristinnsson, Guðmundur Karl Einarsson, Guðmundur Kristjánsson, Hjalti Pálsson, Jón Gunnlaugsson, Kristján Torfason, Magnús Ásbjörnsson, Steingrímur Hálfðánarson and Steinunn Arna Arnardóttir.

### B.1. Air Traffic Management

The main objective of Air Traffic Management is to ensure the safety of an aircraft from gate to gate. This is done by assuring safe separation between the aircraft and other objects, including other aircraft, on the ground and in the air.

ATM is defined by the International Civil Aviation Organization<sup>58</sup> (ICAO) as the aggregation of the airborne functions and ground-based functions required to ensure the safe and efficient movement of aircraft during all phases of operations. Included in this is: airspace management, air traffic flow management and air traffic services, where Air Traffic Service (ATS) is a generic term meaning variously, flight information service, alerting service, air traffic advisory service and air traffic control service (International Civil Aviation Organization, 2007) .

Figure B-1 shows an overview of the main parts of the ATM system, how each part of the system interacts and the flow of information within the system. Of all the Air Traffic Services the major part of the operation lies in the Air Traffic Control (ATC) function. For this reason the focus of this research will be on that part. In Figure B-1 the ATC is divided into **ATC Planning** and **Separation Service**, where the **ATC Planning** is the pre-tactical planning of the air traffic by looking at each flight before they enter into the Reykjavik control area and the **Separation Service** is the tactical operation when the aircraft have entered the controlled airspace and are monitored and controlled in order to ensure safe separation between other aircraft and objects. The gray boxes represent main ATM functions within Isavia and references in the text to those functions are indicated with bold format. The arrows represent information flow and references in the text to that information are indicated with *italic* format. The main responsibilities which currently are in the hands of the supervisor<sup>59</sup> and the air traffic controllers are defined by dash-lined boxes but this definition is not accurate, the supervisor is for example only partly responsible for the **Airspace Management**. The external parties involved,

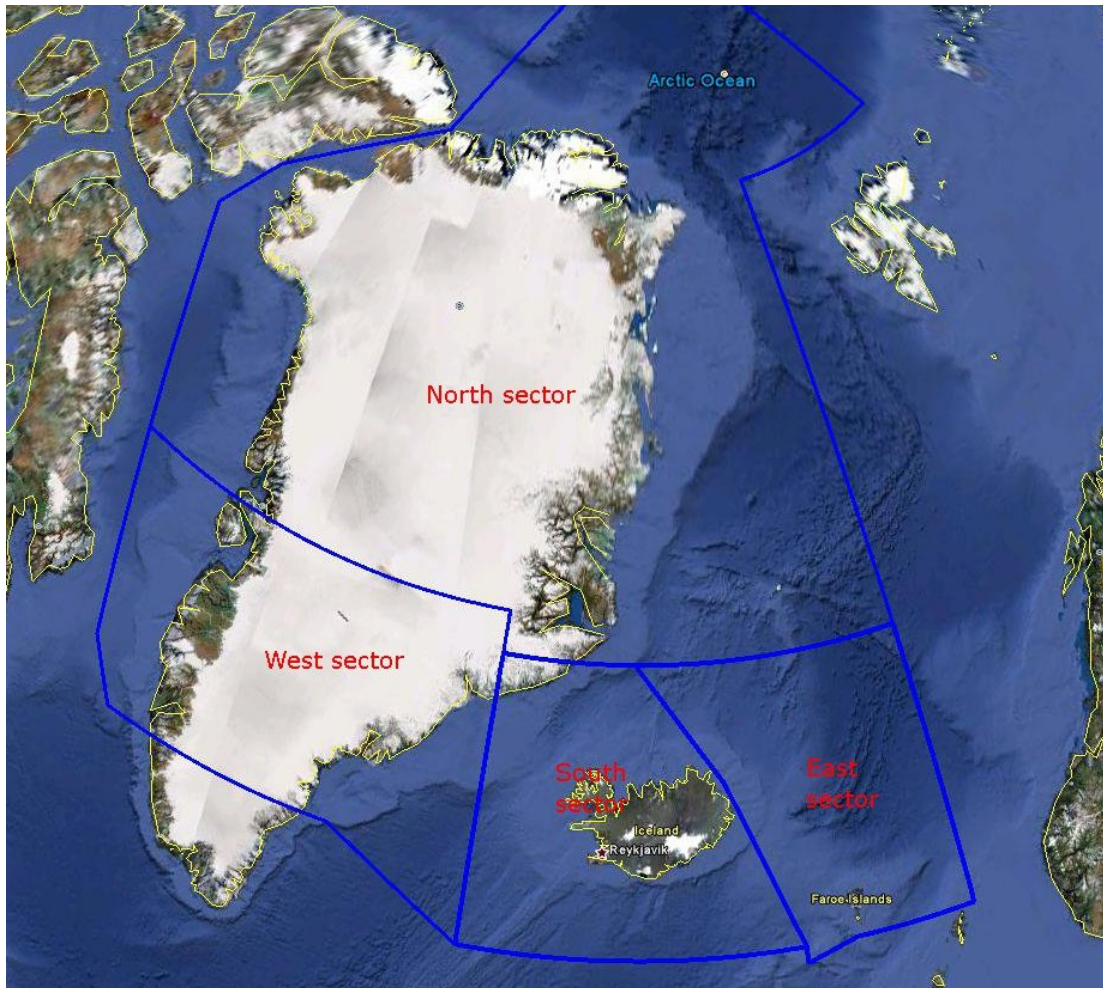
---

<sup>58</sup> ICAO is an agency of the United Nations established to promote the safe and orderly development of international civil aviation throughout the world.

<sup>59</sup> At Isavia there is always one supervisor on shift, his responsibilities are described later in the chapter.



years. When traffic load increases, further division of the sectors may be necessary. This division is horizontal, i.e. the sectors are further divided by altitude in such a way that one or two air traffic controllers control certain altitudes within that sector. The decision to divide one of the four sectors further is made by the **Capacity Planning** on the basis of daily traffic.



**Figure B-2. Division of Reykjavik control area into sectors (Isavia, 2012a).**

Although Iceland is a member of NATO it is one of few countries without armed forces. The airspace controlled by Iceland is therefore generally open to international air traffic since no airspace is reserved for military use. However, as a member of NATO, Iceland hosts NATO military exercises. On such occasions, which are about 4 times per year, blocks of airspace are set aside for the military units and are meanwhile closed for other air traffic. There are predefined blocks of airspace planned for this purpose, selected to cause as little disruption of other air traffic as possible and the time of reservation for the military units is limited to the actual use. This is what is referred to as “time-sharing” in the definition of **Airspace Management** here above; allocation of airspace to the military shall have as little effect on the civil air traffic as possible. These defined blocks of military airspace are therefore only closed for a limited period of time.

In the Reykjavík Control Area there are no fixed routes issued. Large portion of the air traffic over the North Atlantic Ocean follows tracks which are defined every 12 hours. This track system is called North Atlantic Organized Track System (Isavia, 2012b; IVAO, 2012).

Over the North Atlantic Ocean lies jet stream directing strong wind from west to east. The jet stream affects the air traffic and the airlines plan their flight routes with the aim to maximize tail winds and minimize head winds. Depending on the location of the jet stream the position of the NAT tracks varies from day to day and the track do not always enter the Reykjavik control area. In 2010, the NAT tracks for traffic heading west entered the Reykjavik control area 111 days while the NAT tracks for traffic heading east entered the Reykjavik control area only 6 days (Isavia, 2012b).

Control centers in the North Atlantic airspace receive, on the day before the flight, Preferred Route Messages (PMR) from the larger airlines (such as British Airlines and Delta) indicating which routes they would like to fly having taken into account the weather forecast. These *PRM* messages are then used to prepare the North Atlantic (NAT) tracks. Isavia receives suggestions for *NAT tracks* prepared by either Gander or Shanwick control units (European and North Atlantic Office of ICAO, 2005). The suggested tracks are evaluated and in most cases accepted unless there are certain conditions where Isavia would like to add tracks further north due to high traffic load. On rare occasions the tracks are moved further south in order to limit the traffic in the Reykjavík control area. After the tracks have been accepted by the control units involved, the *NAT tracks* are published. Aircraft that fly within the airspace where the tracks have been defined have to follow one of these tracks but in other areas within the Reykjavík control area there are random routes<sup>60</sup>. By using tracks the traffic control in that area becomes more manageable allowing a larger number of aircrafts to be controlled by each air traffic controller. In areas where the traffic is controlled by using tracks the efficiency will increase and larger number of aircraft can fly in the area. Although the tracks solve the problem of excess demand they limit the possibilities of the airlines to choose their preferred route which may be different from the track routes.

As can be seen in Figure B-1 **Airspace Management** provides resources for the **Capacity Planning**, i.e. the information of available airspace and NAT tracks. **Airspace Management** receives *Load Estimates* (estimated traffic load) from **Capacity Planning** in order to evaluate the NAT tracks and for the allocation of airspace to military use. If the **Capacity Planning** detects capacity problems while there are some limitations of available airspace they may request more airspace, such as opening of military airspace sooner than planned. Too much traffic load can in a similar way induce a request from **ATC planning** for more airspace. As mentioned before the airspace controlled by Iceland is only closed for military purposes on rare occasions and therefore capacity and demand imbalances are seldom solved in this manner.

---

<sup>60</sup> Random routes means that the route flown is based on a request for a flight route from the airlines on a per flight basis; they are not predefined or published as fixed routes.

The air traffic controller informs **Airspace Management** if the traffic load becomes too high, **Airspace Management** can then provide more resources. When a controller informs the supervisor that the traffic load is too high, the supervisor can provide more resources such as dividing the sector and/or providing assistance for the controller to manage the traffic.

At Isavia the responsibility of **Airspace Management** is currently in the hands of the supervisor with support from the ATC Procedure Manager. The supervisor is also responsible for the **Capacity Planning**.

### **B.3. Flow Management**

Since capacity of the resources is limited, the flow of air traffic must be controlled to ensure safety. The resources of concern to Flow Management include airspace sector capacities, and airport arrival/ departure rates (Subotic, 2007). Flow management has overview over multi-sector airspace, monitoring capacity and demand imbalances up to a day before operation.

Eurocontrol<sup>61</sup> defines Flow Management as follows:

*“Flow management is a function established with the objective of contributing to a safe, orderly and expeditious flow of air traffic by ensuring that ATC capacity is utilized to the maximum extent possible, and that the traffic volume is compatible with the capacities declared by the appropriate air traffic service providers” (EUROCONTROL, 2011).*

In Europe the Air Traffic Flow Management is performed by the Central Flow Management Unit (**CFMU**) which is operated by Eurocontrol (EUROCONTROL, 2006). Isavia is not a member of the **CFMU** but there is close cooperation between the two.

Isavia does not perform all aspects of Flow Management as performed by **CFMU**, e.g. Isavia does not allocate slot time. However, the focus within Isavia is on one main aspect of Flow Management; the **Capacity Planning**.

In Isavia there are primarily two levels of **Capacity Planning**; pre-tactical and tactical levels. The pre-tactical level includes route and personnel allocation, producing a traffic forecast and a daily capacity plan. Traffic forecast is based on Preferred Route Messages and on statistical traffic data. The tactical level involves capacity monitoring and updating the daily plan according to the actual traffic and capacity at the day of operation.

---

<sup>61</sup> Eurocontrol, also known as the European Organization for the Safety of Air Navigation, is an intergovernmental organization made up of 39 member states and the European community

### B.3.1. Capacity Planning

The **CFMU** receives flight plans from **Airlines & Adjacent Control Centers**<sup>62</sup> which represent the demand for the resources available. **CFMU** accepts the flight plans or suggests amendments to them. Then the **CFMU** forwards the flight plan to Isavia's **Capacity Planning** anywhere from 30 minutes up to a few hours before the operation. In addition to the flight plan **CFMU** forwards pending *Traffic Counts* i.e. number of aircrafts per sector per time unit. The *Traffic Counts* are based on flight plans and are presented in a histogram showing number of aircrafts expected to enter each sector on hourly basis.

The **Capacity Planning** unit detects any capacity and ATC demand imbalances and reacts accordingly. **Capacity Planning** receives information about aircraft in each sector (*A/C state*) from the surveillance systems to monitor the air traffic.

**Capacity Planning**'s main operation is monitoring and forecasting traffic capacity and responding to capacity issues that come up. **Capacity Planning** actions are restrained by the availability of resources. Thus there are specified limits to the number of aircraft passing through a sector within a certain time span without more resources. If the traffic load is too high and capacity cannot be increased, **Capacity Planning** can decrease the load by requesting limitations on incoming traffic. Then the **CFMU** will temporarily limit the traffic into the Reykjavík control area. It is however only under exceptional conditions, that capacity limits are requested in the Reykjavík control area. In 2011 there were no such limitations and there were only few limitations in 2010 due to the eruption in Eyjafjallajökull which caused unprecedented increase in traffic load in the area.

Airspace allocation, qualified personnel and systems infrastructure are needed to be able to provide Air Traffic Services. Short term shortages of these elements call for actions by the **Capacity Planning** that make the best use of the available resources.

**Capacity Planning** determines *Sector Capacity* and sets the *capacity limits*. Under normal circumstances the *Sector Capacity* in the Reykjavík control area is around 35 aircrafts per hour per sector. However, it depends on the application of fixed tracks and general traffic patterns. **Capacity Planning** provides reports on *Sector Capacity* to **ATC Planning**. *Sector Capacity* problems occur for example when air traffic controllers' ability to handle the traffic load is diminished. Under normal conditions the controller is in working position for a maximum 90 minutes, followed by a 30 minutes break. A minimum of six air traffic controllers are therefore required to man four sectors and when sectors are divided one or two additional controllers are required in each new sector. In some cases instead of opening a new sector, the sectors with much traffic load are manned with two controllers that cooperate closely to control traffic within that sector. Thus personnel are closely connected to *Sectorisation* and traffic demand. The **Capacity Planning** prepares demand forecasts on the basis of the

---

<sup>62</sup> Adjacent Control Centers to Reykjavík control area are Stavanger, Scottish, Shanwick and Gander.

preferred route messages and these forecasts are used to plan the number of AIR TRAFFIC CONTROLLERS working each day. Furthermore, on weekdays there are several controllers on other duties which can be reached if required.

In case of excess demand capacity may be increased by limiting the service provided, e.g. by declining requests for changes in flight levels and other route changes.

**Capacity Planning** decides in cooperation with air traffic controllers if two sectors should be merged into one due to reduced load or vice-versa if a sector needs to be split during increasing load.

In case of equipment malfunction, **Capacity Planning** checks if it is sufficient to add personnel or decrease service in order to increase capacity. If not **Capacity Planning** may ask the CFMU to put up *Flow Constraints*.

To sum up **Capacity Planning** aligns information from the CFMU, Airlines & Adjacent Control Centers with the available resources. **Capacity Planning** produces a traffic flow forecast for the next day, provides *Load Estimates* based on the traffic forecasts and determines *Sector Capacity*. **Capacity Planning** monitors the flow a few hours before operation, arrival and departure rates and compares actual traffic flow to forecasted traffic flow. In case of capacity problems **Capacity Planning** proposes resolutions such as allocating personnel<sup>63</sup>, defining routes and dividing sectors (*Sectorisation*).

#### **B.4. Air Traffic Control**

The main objectives of the Air Traffic Control are the separation of the aircraft from each other and from objects on the ground. Maintaining an orderly flow of air traffic, notifying search and rescue if needed and providing advice and information allowing safe and efficient conduct of flights are also important parts of ATC (Icelandic Civil Aviation Administration, 2011).

Air Traffic Control is performed by a system where air traffic controllers play key role in decision making.

In Figure B-1, Air Traffic Control is divided into **ATC Planning** and **Separation Service**. At Isavia the tasks of both the ATC Planning and the Separation Service are usually in the hands of one air traffic controller, although these tasks are commonly performed by two air traffic controllers with a different kind of training.

#### **B.5. ATC Planning**

**ATC planning** is in many ways similar to **Capacity Planning**. The main difference between the two is that **Capacity Planning** focuses on total traffic flow whereas **ATC planning** focuses on individual aircraft.

---

<sup>63</sup> Necessity for Personnel is assessed based on tracks, CFMUs Traffic Counts, traffic forecast and need for sectorization.

A *New Flight plan* is received from **Airlines & Adjacent Control Centers** or from **CFMU**. Then about 15-60 minutes before the aircraft arrives into the sector a clearance<sup>64</sup>, estimate<sup>65</sup> or current plan<sup>66</sup> (CLR/EST/CPL) is received.

The flight plans enters the Flight Data Processing System (FDPS)<sup>67</sup> at Isavia and are examined for errors, which the data specialist corrects before they are reviewed by the air traffic controller.

If an air traffic controller agrees with the flight plan he forwards the *Proposed Routes, Altitude and Speed* to the **Separation Service**. **Separation Service** will then make sure that the aircraft follows that plan. If the controller does not agree with the plan, clearance changes are made.

When an aircraft arrives in an oceanic sector (like the one controlled by Isavia) the air traffic controller provides oceanic clearance to ensure a specific route, flight levels and speed throughout the airspace.

In addition to sending *New Flight plan*, airlines sometimes have *User Constraints* such as restrictions due to types of aircraft or the equipment onboard i.e. it can only fly up to a certain speed and cannot go higher than a certain altitude etc. This can impact **ATC planning** especially if the constraints would result in changes that are inconvenient or not possible due to traffic load. Blue Spruce Routes<sup>68</sup> have been defined for aircraft with limited navigation capabilities.

If the air traffic controller deems there is too much traffic load he informs the **Capacity Planning** which can take the necessary steps to increase the capacity or, on rare occasions, decrease the load by requesting limitations on incoming traffic for a specific period of time.

To sum up **ATC planning** focuses on individual aircraft, issues clearances, suggests alternative routes and/or levels and alerts Airspace Management and/or Capacity Planning if the traffic load is becoming unmanageable.

## **B.6. Separation Service**

**Separation service** is provided on a tactical level, when the aircraft enters the Reykjavík control area. The air traffic controller manning the controller workstation

---

<sup>64</sup> A clearance is an abbreviation of Air Traffic Control Clearance. The clearance authorizes a pilot to proceed according to a specific request. To indicate the type of request the clearance may be prefixed by the words "taxi", "take-off", "departure", "en route", "approach" or "landing". Oceanic clearance is issued for every aircraft entering an oceanic airspace in the North Atlantic (NAT) Region. The oceanic clearance includes a specific route, flight levels and speed from the arrival of the aircraft into a controlled oceanic airspace and until it exits the airspace.

<sup>65</sup> Estimated flight plan.

<sup>66</sup> Actual flight plan.

<sup>67</sup> Definition and discussion of FDPS can be seen in Appendix C.

<sup>68</sup> Routes where the aircraft is at all times within VHF range of a land station (Icelandic Civil Aviation Administration, 2011).



monitors the aircraft within his sector to ensure that separation between aircraft are in accordance with the prescribed separation minima and that the actual route of the aircraft is in accordance with the cleared route.

Separation criteria are the rules which specify the separation minima between aircraft within the airspace. The North Atlantic System Planning Group (NAT SPG) defines the separation criteria for the Reykjavík control area and how it changes in each area if equipment such as individual radars becomes unavailable. These separation criteria are listed in operation manuals.

The air traffic controller communicates with the pilot and provides instructions, clearances and advice regarding flight conditions (Subotic, 2007; Icelandic Civil Aviation Administration, 2011). The advisory service is called Flight Information Service (*FIS*) and contains weather information, including Significant Meteorological Information (*SIGMET*), traffic information and information issued in Notices To Airman (*NOTAM*). *NOTAMs* include a variety of messages concerning aeronautical facilities, such as changes in services, non-standard conditions or hazard (International Civil Aviation Organization, 2007). The messages are in standard format.

The state<sup>69</sup> of the aircraft is detected by the radar surveillance system (or by *ADS-B* when the *ADS-B* service will be available). In the area where there is radar coverage the air traffic controller can monitor aircraft with high accuracy. Therefore there are specific rules that apply to the minimum separation between aircraft while they are located in a radar area and under radar control. In areas where there is no radar coverage, pilots report their position with regular intervals through voice or data link communication. In such cases the air traffic controller uses so-called procedural separation rules. The separation minima for procedural separation is much greater than in radar separation since the former is based on less accurate position and the response time for the air traffic controller and the pilot is longer as they are not necessarily in direct voice contact with each other.

The main separation rules<sup>70</sup> which apply in the Reykjavik control area while the aircraft is in cruising are (Icelandic Civil Aviation Administration, 2011):

1. Procedural separation:
  - a) The vertical separation minimum is 1000 feet in flight levels up to 410 inclusive and 2000 feet above that. Between flight levels 290 and 410 there is a Reduced Vertical Separation Minimum (*RVSM*) airspace<sup>71</sup>.
  - b) The minimum lateral separation outside radar coverage is from 50 NM (93 km) but can be up to 120 NM (223 km) under certain conditions. Between

---

<sup>69</sup> The state of the aircrafts includes it's position, velocity (e.g. ground speed and course) and altitude.

<sup>70</sup> The separations rules within the domestic area are not included.

<sup>71</sup> *RVSM* airspace is an airspace where it is allowed to use 1000 feet vertical separation instead of 2000 feet separation if the aircraft is equipped for *RVSM*.

flight levels 290 and 410 there is a Minimum Navigation Performance Specification (MNPS) airspace<sup>72</sup>.

- c) The longitudinal separation is from 10 to 30 minutes, depending on the type of aircraft and separation technique used. The longitudinal separation between two aircrafts can be reduced where the aircraft's speed of the second aircraft is lower. Depending on the difference in speed the longitudinal separation minima can be reduced down to 5 minutes.

2. Radar separation:

- a) The minimum horizontal separation within radar coverage is from 5 NM (9,3 km) to 10 NM (18,5 km) depending on flight levels. The minimum horizontal separation is reduced to 3NM (5,6 km)<sup>73</sup> when the distance from Keflavik airport is 30 NM (55,6 km) or less.

The pilot may request changes to the cleared profile, such as altitude, route or speed changes. When the air traffic controller receives such requests he considers other traffic and obtains acceptance of changes at the sector boundaries. Having taken this into account the controller will either reject the request or issue a clearance including the new profile, flight level or speed.

When the aircraft reaches the boundary between two sectors the FDPS performs hand-off<sup>74</sup> by automatically changing the controlling sector of the aircraft.

To sum up, within the **Separation Service** the air traffic controller monitors all aircraft in its airspace with respect to separation minima based on surveillance data and/or position reports. The controller also receives requests for changes in flight profiles from aircraft and approves or rejects these requests if necessary. **Separation Services** also provides general Flight Information Services.

---

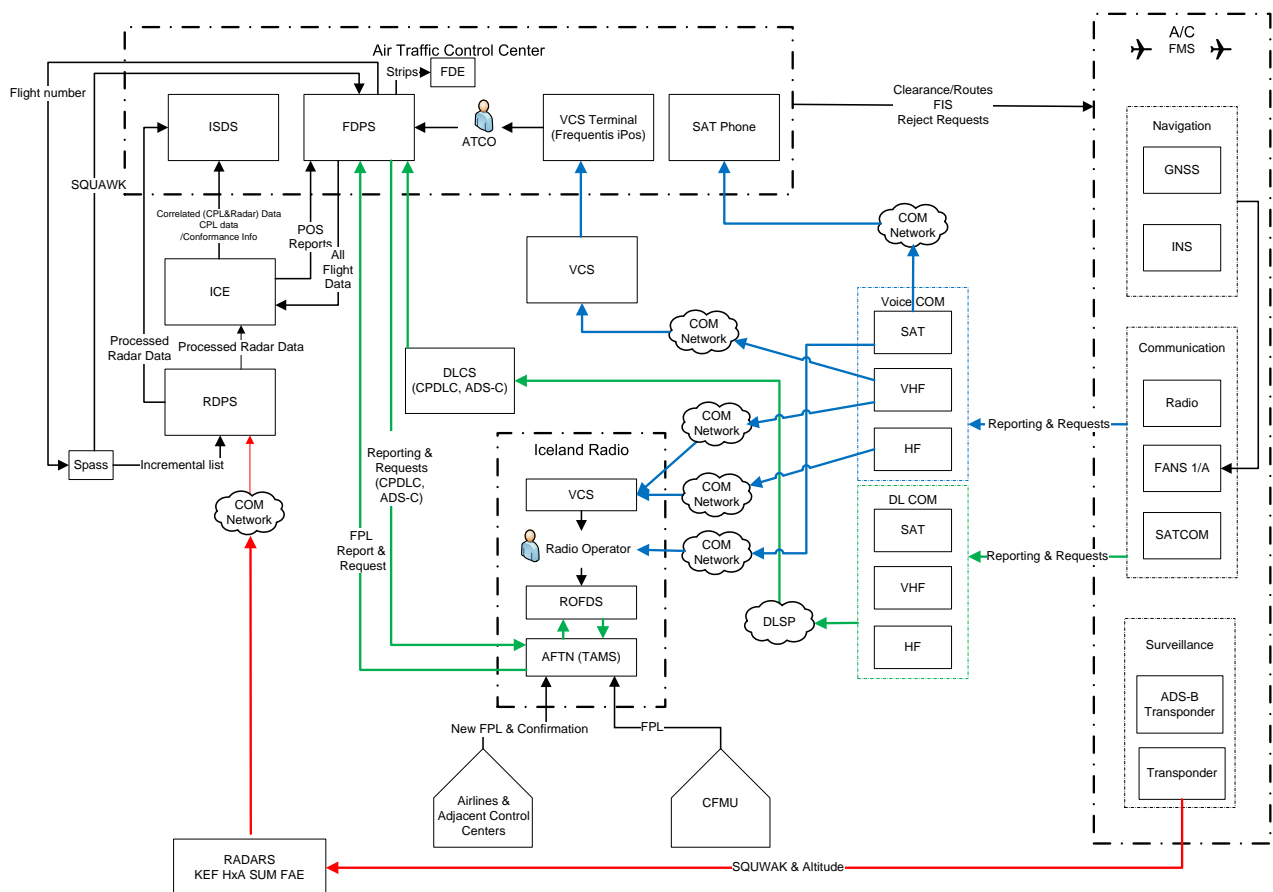
<sup>72</sup> MNPS airspace is an airspace where there are only allowed aircraft which meet certain lateral navigation performance capabilities.

<sup>73</sup> A further condition for the reduction of the separation minima to 3 NM is that primary surveillance radar is in range.

<sup>74</sup> Hand-off is the act of passing control of an aircraft from one air traffic controller to another in an adjacent sector.

### C. The Air Traffic Control system at Isavia

In this chapter the focus is on the equipment and systems used for the Air Traffic Control. ATC is generally divided into en-route Air Traffic Control, Approach Control and Aerodrome Control. Approach Control and Aerodrome control are mainly operated in towers at each airport. Approach control focuses on flights arriving/departing from airport Terminal Areas that typically can extend to 60 NM from the airport. Aerodrome control directs air traffic in the vicinity of the airport and on the ground. Thus, Approach and Aerodrome controllers work closely together (Subotic, 2007). En-route ATC on the other hand concentrates on the traffic control while the aircraft is in the air and is operated by en-route Area Control Centers (ACCs). Since the research project is concentrated on en-route air traffic control the focus of this chapter will be on the Reykjavik en-route ACC. En-route control is divided into Air Traffic Management, Communication, Navigation and Surveillance i.e. ATM/CNS. Figure C-1 shows systems and equipment used in Reykjavik ACC.



**Figure C-1: Information systems and equipment used in Reykjavik ACC.**

In Figure C-1 the arrows represent the input/output from each system/equipment. The aircraft (A/C) is displayed on the right hand side whereas the systems/equipment used by air traffic controllers at the Air Traffic Control Center are displayed in a dashed box at the top left corner. In order to simplify the figure the voice and data (the arrow containing: Clearance/Routes, FIS, Reject Requests) from the Air Traffic Control Center to the aircraft is shown as a single arrow from the Air Traffic Control Center to

the aircraft, although the actual route is in most cases through the same channels as the information flow from the aircraft to the Air Traffic Control Center.

## C.1. Surveillance

Surveillance systems are used to monitor flights and compare them to confirmed flight plans. The Surveillance system at Reykjavik Area Control Center consists of radars, communication network, Radar Data Processing System and a Squawk Allocation System (SPASS<sup>75</sup>).

### C.1.1. Radars

The ATC Center is connected via a communications network to eight radars; in Keflavik (two radars –KFM and H-1), Bolafjall, Gunnólfsvíkurfjall, Stokksnes, two in Faroe Islands and one in Sumburgh in the Shetland Islands (Scotland). In the area where there is radar coverage, radars provide near continuous surveillance of aircraft with identity (squawk) and altitude, the radar data arrives at 10 second intervals. Figure C-2 shows the radar stations as well as the overall radar coverage area. At each radar site there are both primary and secondary radars except in the Faroe- and Shetland Islands, which provide secondary data only.

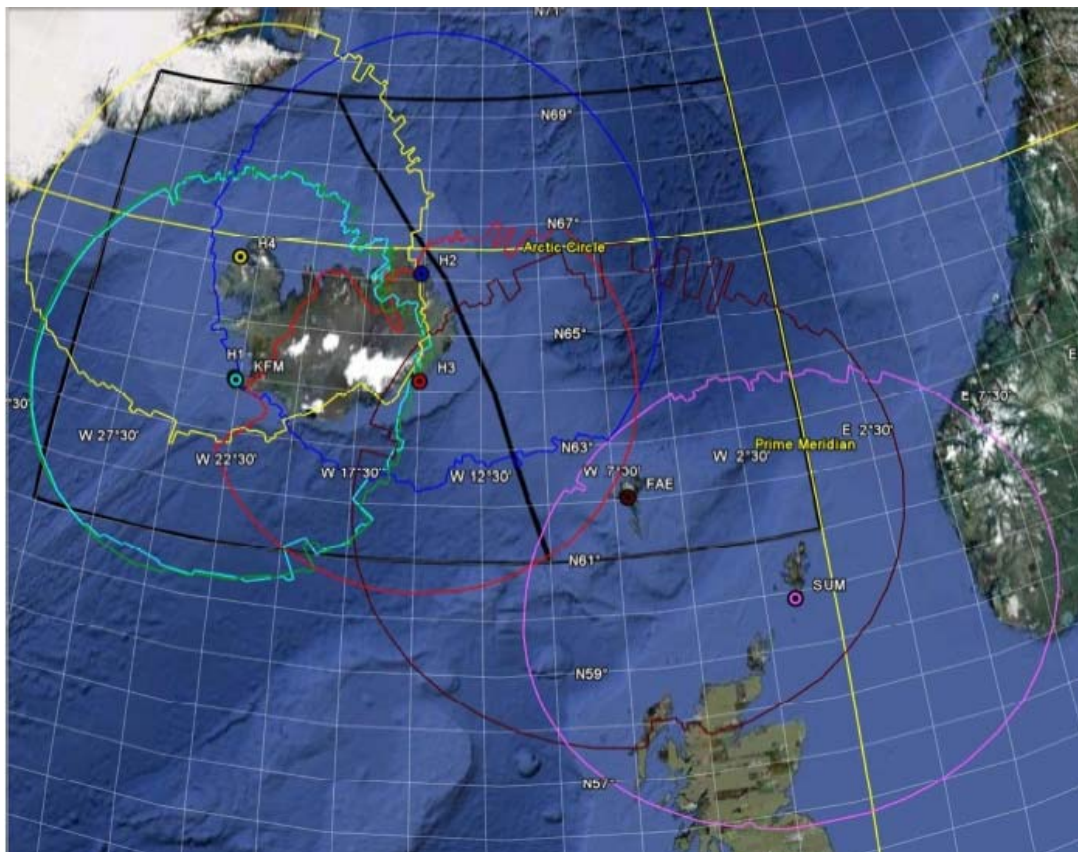


Figure C-2. Radar stations and radar coverage in the Reykjavík control area at 40 thousand feet.

<sup>75</sup> SPASS stands for Strip Printing and Squawk Allocation System, however the strip printing is no longer a part of the system.

#### ***C.1.1.1. Primary radar***

Primary radar provides precise knowledge of the position of aircraft but does not identify them. The radar provides independent surveillance of aircraft and can report the position of anything that reflects transmitted electromagnetic signals including, aircraft, birds, weather etc. Even though its information is more limited than in Secondary Surveillance Radar primary radar is used at Isavia mainly for backup purposes. Primary radar is not used directly during air traffic control at Isavia, however it does provide augmentation of the secondary radar measurements of position (Nolan, 2011).

#### ***C.1.1.2. Secondary Surveillance Radar (SSR)***

SSR is more sophisticated than primary radar as it provides additional information such as identity and altitude in addition to the position of the aircraft. Unlike primary radar systems, SSR is dependent on aircraft being equipped with a radar transponder (Nolan, 2011). The transponder replies to the signal from the SSR by transmitting a transponder code which is a four digit octal code called squawk.

#### **C.1.2. Transponder (Transmitter- responder)**

A transponder is an electronic device located in aircraft, used to receive secondary radar signals and automatically respond to them. The transponder code is assigned by air traffic control center to uniquely identify an aircraft. This allows easy identification of the aircraft on radar and on other aircraft's collision avoidance systems.

#### **C.1.3. Squawk Allocation System (SPASS)**

SPASS (also known as ADT) assigns a squawk code to a call sign upon a request from the Flight Data Processing System (FDPS) i.e. FDPS says "I have ICE520, what squawk code should I assign to it?" to which SPASS replies "ICE520 has been assigned squawk code 3321". SPASS also informs RDPS what call sign (e.g. ICE520) matches a squawk code (e.g.3321).

When the RDPS requests data from the SPASS, the SPASS provides an “incremental” list. The incremental list holds all squawk codes that were assigned from the last request and when the codes will expire.

#### **C.1.4. Automatic Dependent Surveillance Broadcast (ADS-B)**

ADS-B is a surveillance technique that broadcasts identification, position, altitude, velocity and other data automatically from the aircraft at a high rate (once pr. second). As the signal is broadcasted the originating source has no knowledge of who receives it. To operate the ADS-B needs ground-based receiving stations, a transponder within the aircraft as well as the on-board systems providing the data to be transmitted. ADS-B is expected to be operational at the Reykjavik ACC in the near future. ADS-B expands and augments the more traditional SSR networks and may eventually replace the radars used today. ADS-B which is sometimes referred to as pseudo-radar provides more accurate and comprehensive information than conventional radar (Australian Government & Civil Aviation Safety Authority, 2012) .

### **C.1.5. COM Network - Communication network**

The Reykjavik ACC communications network in Iceland is provided by the telecommunication company Míla<sup>76</sup>. The building blocks of the network are a copper system, optical fiber network and microwave system (Míla ehf., 2012).

Radar signals arrive into a central unit called Control and Reporting Center (CRC; NATO facility) at Keflavík and from there they are transmitted through optical fiber/microwave to the Radar Data Processing System at Isavia's ACC in Reykjavik.

### **C.1.6. Radar Data Processing System (RDPS)**

The RDPS system provides simultaneous data processing from radar data while performing real-time monitoring and data extrapolation.

RDPS merges the radar data from eight secondary surveillance radars, processes the data by using extrapolation and filtration to generate a single "system track". This provides velocity, direction and identification call-sign of every individual aircraft flying through the area on a 2D ATC situation display which is updated every 3 seconds. This display provides core information on the traffic to the radar air traffic controller. The system also provides a range of supporting functions i.e. distance measures, separation measures, velocity measures, time plans etc. RDPS also includes a Short Term Conflict Alert (STCA) which alerts the air traffic controllers in case of impending or actual separation minimum violations.

### **C.1.7. Flight Data**

In this chapter the main focus is on how equipment and systems contain and process flight data<sup>77</sup>. The systems that handle flight related data at Isavia are Flight Data Processing System (FDPS), Integrated Controller Environment (ICE), Integrated Situation Display System (ISDS) and Flight Data Entry (FDE).

### **C.1.8. Flight Data Processing System (FDPS)**

The FDPS is one of the most important systems used by air traffic controller at Isavia and is in continuous development. FDPS is a complicated system that consists of many processes working together and receives all flight information other than radar data.

FDPS is a message driven system which automatically processes all the information related to the flight and aircrafts relative position (*A/C state*) into electronic progress strips<sup>78</sup>. These strips are vital for operation and should always contain the newest known information. FDPS uses a weather model to calculate the progress of the flight. The system alerts air traffic controller if some changes could result in minimum separation violation.

---

<sup>76</sup> In figure 3 COM Network represents Míla except for in satellite communication which is transmitted through Radiomiðlun.

<sup>77</sup> All data used to track a flight in ATC, generally contains all information related to position of the aircraft e.g. aircraft identification (e.g. a flight number), aircraft type (e.g. B744 for a Boeing 747-400), flight level (assigned altitude), departure, destination and time.

<sup>78</sup> A strip contains updated information from the flight plan displayed in a specific format.

The system automatically distributes information between air traffic controllers within the ATC Center and also outside of the ATC Center, such as Reykjavik and Keflavik tower, CRC and adjacent ANSPs. Other functions include creating basis for clearance, receiving and processing all flight plans and updating *A/C state* according to position (POS) reports etc.

FDE continuously receives flight data strips from the FDPS for storage and is therefore a backup for the most important information provided by the system. The strips can be printed out as last resort backup if the FDPS backup fails.

#### **C.1.9. Integrated Controller Environment (ICE)**

Main function of the ICE system is to provide a stand-by database backup of FDPS data. If there is a problem with the primary FDPS system then the backup FDPS system can be started with data from the ICE system. The data is also used to send current flight plan (CPL) information to Integrated Situation Display System.

ICE also communicates with the RDPS to supply the FDPS system with more accurate POS reports<sup>79</sup> and does a correlation between CPL and radar data. The result is sent to ISDS. ICE data is also used to perform conformance monitoring i.e. to compare actual position of the aircraft with the cleared routes and reports discrepancy to ISDS.

#### **C.1.10. Integrated Situation Display System (ISDS)**

ISDS is a display system that provides a visual representation of flight profiles, flight estimates, crossing times etc. ISDS integrates two fundamental systems in the Reykjavik Oceanic Area Control; the RDPS and FDPS. ISDS combines information from the different systems into one situation display for the air traffic controller which enhances the controller's situation awareness. The ISDS displays useful information showing both radar and CPL tracks in convenient and timely manner. The system uses Processed Radar Data from RDPS. ISDS also uses Correlated CPL and Radar Data from ICE as well as conformance information.

The system provides lateral- and vertical conformance monitoring against the cleared oceanic flight profile. Air traffic controllers use the information displayed on the screen and data from FDPS to maintain separation and control traffic.

### **C.2. Communication**

There are three ways for communication between the pilot and air traffic controller:

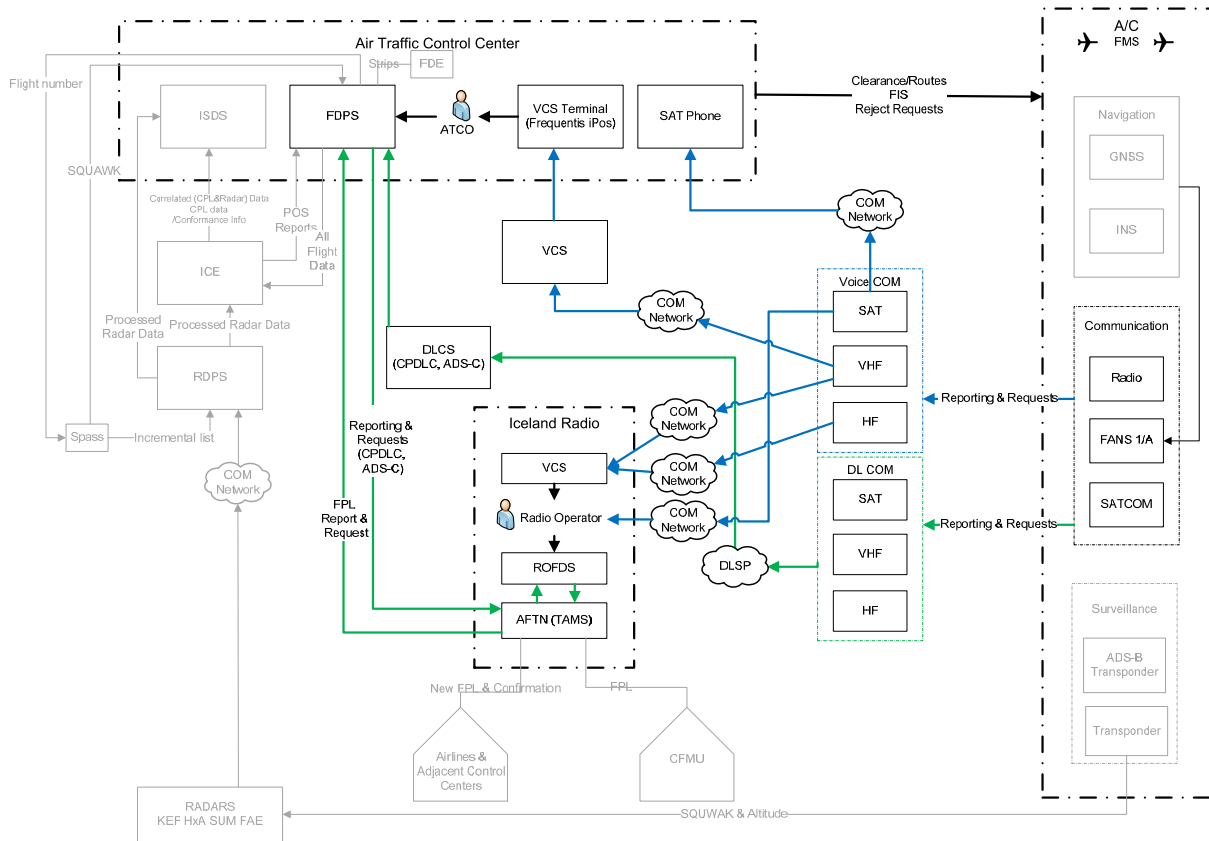
1. Direct voice communication between pilot and air traffic controller through VHF radio or satellite phone.
2. Data communication through data link between pilot and air traffic controller, such as CPDLC.

---

<sup>79</sup> POS report is a position report usually communicated through Iceland Radio. These reports are needed in certain places when there is no radar coverage. Position reports replace radar or ADS.

3. Communication through a radio operator at Iceland Radio<sup>80</sup> using VHF radio, HF radio or satellite phone.

Figure C-3 shows the communication part of the system, voice communication is shown in green and data communication is shown in blue.



**Figure C-3: The communication between the ATCC and the Aircraft. The path of the voice communication is shown in blue color and the path of data communication is shown in green.**

Figure C-3 shows the equipment and systems used in the communication between the air traffic controller and the pilot. It also shows what kind of information is communicated. Although the information flow from the controller to the pilot is shown in one arrow directly between the control center and the aircraft the actual way of communication is through the channels shown for the communication from the communication system of the aircraft to the control center. This is done to simplify the drawing.

The direct voice communication path between the pilot and the air traffic controller is shown in blue in Figure C-3 i.e. from the communication equipment in the aircraft, through VHF radio and communication network to a Voice Communication System (VCS) in the control center. A terminal for VCS is located at the air traffic controllers

<sup>80</sup> Iceland Radio, which is a part of the Air Navigation Division at Isavia, is a communication center located in Gufunes that provides aeronautical telecommunication service.



workstation. The controller can also communicate with the pilot directly through satellite phone.

The data communication path is shown in green in Figure C-3 i.e. from the communication equipment in the aircraft, through data link communication provided by Data Link Service Providers (DLSP) to the Data Link Communication System in the control center. The information communicated this way appears in FDPS where the air traffic controller can see it on the screen.

The communication path through Iceland Radio is shown in Figure C-3. It begins in communication equipment in the aircraft, through satellite phone, VHF or HF radio and communication network to VCS or a radio operator in Iceland Radio. There the radio operator converts voice communication to data which are then transferred to FDPS where the air traffic controller receives the data.

### **C.2.1. High Frequency Radio (HF Radio)**

Used for voice communication between the pilot and a radio operator. HF is also used by Data Link Service Providers<sup>81</sup> (DLSP) as a data link, HF DL. Iceland Radio runs seven HF ground stations. HF radio signals cover larger area than VHF and can therefore be used when other communication technology is out of range, for example in the polar area. It is however subject to noise and disturbances from other equipment.

### **C.2.2. Very High Frequency Radio (VHF Radio)**

Used for voice communication between the pilot and a radio operator or air traffic controller. VHF is also used by DLSPs as a data link, it is for example used by ARINC<sup>82</sup> in CPDLC. Isavia runs twelve VHF stations in Iceland and two in the Faroe Islands. Iceland Radio runs six stations in Iceland, two in Greenland and two in the Faroe Islands. As there is VHF radio coverage within the radar areas the air traffic controllers at the Reykjavík ACC can communicate through VHF radio while the aircraft is in radar coverage.

### **C.2.3. Satellite Communication (SATCOM)**

Voice or data communication through satellites. The satellite communication is today mainly a data link communication through Data Link Service Providers as intermediates. The Reykjavík ACC and Iceland radio are also equipped with satellite phones for voice communication with the pilot.

### **C.2.4. Controller Pilot Data Link Communication (CPDLC)**

CPDLC is a means for communication between air traffic controller and pilot through a data link. The data links are mainly through either VHF or satellite. DLSP, such as SITA<sup>83</sup> and ARINC are intermediates for this service.

---

<sup>81</sup> DLSP are Companies that provide air-ground communication service via data link.

<sup>82</sup> ARINC is a Data Link Service Provider.

<sup>83</sup> SITA is a Data Link Service Provider.

The CPDLC application provides air-ground data communication of messages such as *Clearances/Routes*, requests, *FIS*, and reports in a format which corresponds to phraseologies used in the radiotelephony environment. There is also an option to send messages in a free format (International Civil Aviation Organization, 2007).

#### **C.2.5. Automatic Dependent Surveillance - Contract (ADS-C)**

This is surveillance equipment which automatically transmits information from other systems in the aircraft, such as identification, position and speed to the air traffic controller through data link. In ADS-C the data is only sent between the ground system and the aircraft as opposed to ADS-B (Automatic Dependent Surveillance – Broadcast) where the data is broadcasted constantly to all possible recipients (International Civil Aviation Organization, 2007).

#### **C.2.6. Future Air Navigation System (FANS 1/A)**

FANS-1/A is a system (hardware, software and communication networks) for data communication between air traffic controller and pilot, located in the aircraft as a part of the Flight Management System (FMS). The communication may be in the form of clearances, requests and position reporting. Both ADS-C messages and CPDLC communication are services provided through the FANS-1/A system. FANS-1/A is mainly used in oceanic airspace.

#### **C.2.7. Voice Communication System (VCS)**

VCS is a telecommunication control system. VCS from Frequentis<sup>84</sup> is located in the Air Traffic Control Center. This system is used by air traffic controllers for most of their air-to-ground and ground-to-ground voice communication. With this system, radio contact is made with the aircrafts through ground stations located around Iceland and in the Faroe Islands. Telephone communications with adjacent control units, towers, etc. go through this system as well. Each air traffic controller's workstation is equipped with a VCS terminal, called iPOS.

#### **C.2.8. Aeronautical Fixed Telecommunication Network (AFTN)**

AFTN is a ground-to-ground communication system for transmitting flight data messages. The system is a part of a worldwide network for transmitting messages between ANSPs, the CFMU, airlines, etc. The format of the messages is according to standards prepared by ICAO. The system that manages the messages at Iceland Radio was created by Tern Systems and is called TAMS.

#### **C.2.9. Radio Operator Flight Data System (ROFDS)**

A system that handles and keeps track of messages between aircraft and the radio operator. The radio operator at Iceland Radio communicates with the pilots through satellite phone, VHF or HF radio and enters the communication into ROFDS which creates AFTN messages that are transmitted to TAMS and then from TAMS to FDPS.

---

<sup>84</sup> Frequentis AG is an international supplier of communication and information systems.

### **C.3. Navigation**

Navigation systems are located in the aircraft enabling the pilot to ascertain the position of the aircraft. Navigation equipment feeds information to FMS. Common navigation equipment include Automatic Direction Finder (ADF), measuring equipment, altitude sensors, speed sensors, Global Navigation Satellite System (GNSS), Inertial Navigation System (INS) and so on. GNSS and INS are frequently used for navigation onboard aircraft and will be discussed in further detail here below.

#### **C.3.1. Global Navigation Satellite System (GNSS)**

GNSS is a system that uses satellites for three dimensional positioning. GNSS operations are based on triangulation from a group of satellites reference points in space that provide mainly three dimensional positioning, velocity and time (Nolan, 2011).

European Geostationary Navigation Overlay Service (EGNOS) is a space based augmentation system (SBAS) that increases the accuracy and integrity of GNSS signals for safety-of-life navigation reliability for aviation. Isavia participates in the EGNOS program by deploying and servicing EGNOS ranging and integrity monitoring stations (RIMS) in Iceland in cooperation with the European GNSS Agency (GSA). Position of aircraft relative to the satellite can affect GNSS signals making them inaccurate or blocked. Other signals, area surroundings e.g. mountains and so on, can also influence the GNSS signals (Kristinsson, 2012).

#### **C.3.2. Inertial Navigation System (INS)**

This navigation system can be independent of ground-based radio navigation stations and GNSS for a limited period of time and thus INS can be suitable for navigation when GNSS is not a viable solution (Christensen & Fogh, 2008).

INS can measure the slightest change in an aircraft's speed or direction of flight. Using this information, the INS can calculate the altitude, velocity, position, course to be flown and the estimated time of arrival (Nolan, 2011). When used correctly, the INS is highly accurate; however, the accuracy of the INS deteriorates with distance flown due to measurement inaccuracies (Christensen & Fogh, 2008).

## **D. Short overview of Reliability methods for human error and collision risk**

The following presents examples of methods frequently used for human error risk and collision risk and provides an overview of the safety research methods previously conducted and related literature concerning the different risk perspectives. As this is primarily a short overview for theoretical purposes the following description of the research methods is extracted (with small adaption) from (GAIN Working Group B, 2003; Netjasov & Janic, 2008; NLR, 2010).

### **D.1. Human error risk.** - The risk of accidents due to human error (by aircraft crew and/or controllers).

One of the most frequent causes of accidents relating to aviation is “Human error” (Boeing Commercial Airplanes, 2006). Human error can include various things. It is defined as an incorrect execution by a human operator of a particular task, which then triggers a series of subsequent reactions in the execution of other tasks, resulting in an undesirable event or possibly an aircraft accident (Netjasov & Janic, 2008). The methods that have been developed in order to reduce the probability of Human errors include the following:

#### **The Hazard and Operability (HAZOP)**

The method aims to discover potential hazards, operability problems, and possible deviations from the intended operational conditions, including estimating the probability and consequence of such an event. In practice, the name HAZOP is sometimes used for any brainstorming with experts to fill a table with hazards and their effects. The method was first developed in the chemical industry in the 1960s. Later the UK National Air Traffic Service (NATS) applied the method to aspects of planning to assess hazards in operation of the national ATC/ATM system. This was done in order to identify hazards due to human failures that could lead to accidents. HAZOP can provide a basis for other reliability analysis (Netjasov & Janic, 2008; NLR, 2010).

#### **Human Error Assessment and Reduction Technique (HEART)**

Human Error Assessment and Reduction Techniques (HEART) identifies and quantifies human errors in operator tasks on a combination of numerical factors provided by expert opinion. It was developed in 1985 for considering particular ergonomic and other task and environmental factors that can negatively affect performance. The impact of a particular factor on an operator’s action while performing particular tasks is estimated and the human error probability is then calculated as a function of the product of those factors identified for a particular task. The method has been applied by the UK NATS, in combination with other methods, for identification of potential human errors in ATC/ATM. The HEART has been tailored to application in ATC safety assessment and is then referred to as CARA (Controller Action Reliability Assessment) (GAIN Working Group B, 2003; Netjasov & Janic, 2008).

### **Technique for the Retrospective Analysis of Cognitive Errors (TRACER-Lite)**

The Technique for the Retrospective Analysis of Cognitive Errors (TRACER-Lite) was developed in 1999 by UK NATS. The aim is to predict human errors that can occur in ATM systems, and to derive error reduction measures for ATM. The method is retrospective and is used for classifying types of errors contributing to air traffic incidents that have happened. The design process is improved by trying to identify beforehand what errors could occur, thus helping to focus design efforts. TRACER-Lite was designed to be a support tool for ATM system designers and other operational personnel by identifying and classifying the “mental” or “human” aspects of the error, the recovery opportunities, and the general context of the error. This includes the factors that aggravated the situation that occurred due to human error, or made the situation more exposed to error (Netjasov & Janic, 2008; NLR, 2010).

TRACER-Lite has been applied in the analysis of errors causing AIRPROX<sup>85</sup> incidents in UK national airspace during the period 1996 - 1999. In recent years, Eurocontrol has applied the method to two of their projects, they are: Time-Based Separation During Approach and Airborne Separation Assurance System (ASAS) concept.

### **Human Error in ATM (HERA)**

The Human Error in ATM (HERA) approach was developed at Eurocontrol in the beginning of the 2000s. It is a retrospective method and provides insight into air traffic controllers' cognitive processes as air traffic incidents are dealt with. It consists on the one hand of a retrospective element for incident analysis, and on the other hand a prospective part that uses the information collected on the assessment of probability of human errors in cases of compromised safety. It identifies the ATC behavior, the equipment used and the ATC function being performed by placing the air traffic incident in its ATM context. The method gains a better understanding of the constraints and circumstances under which air traffic controllers have to operate. The method is somewhat limited and does for instance not provide insight into the operators' errors at other levels of ATC/ATM such as maintenance, management and regulation. The method has been a part of the Eurocontrol staff educational and training system as it has been applied to ATC/ATM safety management (GAIN Working Group B, 2003; Netjasov & Janic, 2008).

### **Human Factor Analysis and Classification System (HFACS)**

The Human Factor Analysis and Classification System (HFACS) was developed in the US in the early 2000s. It categorizes latent and immediate causal factors associated with aviation accidents. Being based on analysis provided by aviation accident reports the method's main purpose is to serve as a tool for accident trend assessment and to provide a framework for accident investigations. HFACS examines cases of human error as part of a complex productive system that includes management and organizational vulnerabilities by distinguishing between the "active failures" of unsafe acts, and "latent

---

<sup>85</sup> “A situation in which, in the opinion of a pilot or air traffic services personnel, the distance between aircraft as well as their relative positions and speed have been such that the safety of the aircraft involved may have been compromised” (International Civil Aviation Organization, 2007) .

failures" of preconditions for unsafe acts, unsafe supervision, and organizational influences. The method was originally developed for the US Navy in the investigation of military aviation incidents.

FAA Civil Aerospace Medical Institute applied the method to air traffic operational error reports (GAIN Working Group B, 2003) and in NASA's Aviation System Risk Model (ASRM 86) in order to facilitate consistency in the use of disparate causal factors (Luxhoj & Coit, 2006). This method is currently being used by the FAA to investigate civil aviation incidents (Netjasov & Janic, 2008; NLR, 2010).

#### **Analytic Blunder Risk Model (ABRM)**

While some other tools predict the probability of an error occurring, ABRM computes the probability that a particular error will result in a collision. ABRM was developed by FAA in the 1980s. Given a particular blunder (controller error, pilot error, equipment malfunction) between one aircraft involved in the error (the "blunderer") and another aircraft (the "evader"), ABRM can evaluate the probability of a collision. ABRM assumes no intervention and timely intervention by pilots and controllers and computes the probability of collision for both situations. It uses empirical probability distributions for reaction times and a closed form probability equation to compute the probability that a collision will occur. This allows it to consider combinations of events with small probabilities efficiently and accurately (NLR, 2010).

#### **Reduced Aircraft Separation Risk Analysis Model (RASRAM)**

The Rannoch Corporation is the developer of this model and it is used for quantitative assessment of the increase in risk of aircraft operations that mainly concern reduced separation requirements, and/or reduced risk due to new surveillance or navigational technology. A large database of aircraft data, incorporating aircraft and air traffic controller data, is the foundation of the methodology. It works directly with the functional form of probability distributions, instead of relying on Monte Carlo simulation techniques. The probability of a collision of aircraft is found by first computing the probability of a Near Mid-Air Collision (NMAC) and then the probability distributions of lateral miss distance and simultaneous runway occupancy (GAIN Working Group B, 2003).

**D.2. Collision risk.** - The risk of aircraft collision due to deterioration of separation rules.

ATC is concerned with preventing conflicts that might escalate to a collision of an aircraft with another aircraft during the en route phase<sup>87</sup>, or with fixed obstacles during landing or take-off. In general, separating aircraft using space and time separation standards (minima) has prevented conflicts and collisions. *"It could be observed that*

---

<sup>86</sup> ASRM has been used to provide a systematic, structured approach for understanding the aircraft accident causality as well as performing the assessments of new aviation safety products developed through NASA's Aviation Safety and Security Programme.

<sup>87</sup> En route phase concentrates on the traffic control while the aircraft is in the air (EUROCONTROL, 2011).

*the absence of minima separation leads aircraft to a state of high collision probability”* (Vismari & Junior, 2011). Due to reduction of this separation (bringing aircraft closer together) in order to increase airspace capacity, assessment of the risk of conflicts and collisions under such conditions has been a popular research subject (Netjasov & Janic, 2008). The methods that have been developed include the following:

### **Reich-Marks model**

Reich and Marks started development of the first Collision Risk Assessment model in 1963 and it was further developed by the UK’s Royal Aircraft Establishment in the early 1960s (Reich, 1966). *“The model was developed to estimate the collision risk for flights over the North Atlantic and to specify appropriate separation rules for the flight trajectories”* (Shortle, Xie, Chen, & Donohue, 2004). Aircraft are represented as three-dimensional boxes reflecting the ATC minima separation rules. The model assumes random deviations of aircraft position and speed. These are used to compute the probability of aircraft state and the conditional probability of collision of two boxes given the states of the two aircraft. (Machol, 1975; FAA & EUROCONTROL, 1998).

### **Machol-Reich model**

The North Atlantic System Planning Group (NAT SPG) established by the International Civil Aviation Organization (ICAO) refined the Reich-Marks model in the nineteen sixties. The model was modified using actual data enabling more accurate prediction of vertical, horizontal and longitudinal collision risks. ICAO adopted this solution and added a fourth type of separation, the diagonal–lateral separation. This separation nearly doubled the capacity of North Atlantic airspace by reducing the actual separation of aircraft. NAT SPG took accidents data from all ICAO member states into consideration and used this method to adopt a threshold for risk of collision due to loss of planned separation (Machol, 1975; 1995).

### **Intersection and Geometric conflict model**

The intersection models are based on assumptions that aircraft follow predetermined crossing trajectories at constant speeds. The probability of a collision at an intersection is computed using the traffic load, aircraft speeds and the airplane geometry (Siddiquee (1973), Geisinger (1985) and Barnett (2000)).

*“The geometric conflict models are similar to intersection models. They were developed in the 1990s and take the speed of any two aircraft as constant, but their initial three dimensional positions are random. Based on extrapolating their positions in time, it is possible to geometrically describe the set of initial locations that eventually lead to a conflict. This occurs when two aircraft are closer than the prescribed separation rules”* (Netjasov & Janic, 2008).

The probability density of the initial aircraft positions can then be integrated over the conflicting region. By doing so the conflict probability can be estimated (Paielli & Erzberger, 1997; 1999; Irvine, 2002).

**Generalized Reich model**

Following redesign of a system or technology “The generalized Reich model” provides designers of advanced ATC/ATM systems with a feed-back in terms of flight safety. Such a generalized collision model was developed during the 1990s and has been used as a part of the TOPAZ methodology. It uses Monte Carlo simulations of the Petri Net models to assess safety by identifying hazards relevant to a given air traffic scenario and quantifies risk and safety. A simulation model related only to the airspace in which collisions are likely to occur can be created if critical hazards have been identified. The generalized Reich model can be used to further improve the efficiency of simulations (Bakker & Blom, 1993; Blom & Bakker, 2002; Bakker, Kramer, & Blom, 2000; Blom H. A., Bakker, Blanker, Daams, Everdij, & Klompstra, 1998; Blom H. A., Bakker, Everdij, & van der Park, 2003; Shortle, Xie, Chen, & Donohue, 2004).

The Federal Aviation Administration (FAA) has applied the Reich model widely in various forms in order to increase the number of tracks and reduce the lateral and vertical separation minima.



## **E. Additional information on the Electrical Power system at Isavia**

The purpose of this appendix is to provide a more detailed description of the electrical power system components. All important information regarding the electrical system, which is needed for modeling, is summarized in Table E-1 at the end of this appendix.

### **Mean time to failure (MTTF) of electrical equipment**

In order to compute the reliability of a system, the reliability distribution and its parameters for each component must be known or assessed. Thus, MTTF values for all components are needed to analyze the reliability of the system. MTTF represents the mean time the equipment is expected to operate before failing.

Failure within the electrical system is in most cases due to failure of a component due to a very powerful electrical pulse from grid, human error, water damage etc. In this study there is only one MTTF value for each equipment and it is not speculated for what reason it occurs.

The MTTF values are based on specialists judgments and considers the usage of each individual component within Isavias' system. The MTTF values will now be presented.

### **The Grid**

As previously mentioned, Orkuveita Reykjavíkur (the public utility company), provides Isavia with electrical power through an electrical power grid connected to Isavia through 3 service lines. Failure mainly occurs if mistakes are made during construction operations somewhere in the Reykjavík area resulting in cutting a cable that happens to be crucial for providing Isavia with electricity. This kind of failure is therefore mostly due to construction activities although electrical fluctuations for example can also lead to failure. A failure has been known to happen once or twice a year. In conclusion MTTF is considered to be 1 year.

### **Master switch / Switch boards (Circuit breaker)**

The switches are all new equipment; the equipment was renewed because of a failure that occurred in one of the backup switch boards in 2010. They tolerate up to 800A and 690 V. When all equipment is operating it only amounts to approximately 550A.

The switches for the grid and for the backup generators are all of the same type. One of the maintenance functions for the switches involves manually removing specific parts from a working switch to use as spares for a switch that has failed. This maintenance action takes about 10 minutes (this is done manually and thus ignored in the modeling).

The switch boards are hot stand-by components because they are kept locked, ready to take over at any second. For this reason the components have the same failure distribution in stand-by and active mode and thus MTTF values for the master and back-up switches are the same. The MTTF of switch boards depends on how often the breaker is coupled.

In conclusion MTTF of the master switch and switch boards for the power generators is considered to be 25 years.

### **Automatic transfer switch**

The automatic transfer system monitors the electricity coming in from the grid and senses if action is needed. If action is necessary it automatically alerts specialists via SMS that the Diesel power generators have been activated.

The automatic transfer system is used in at least 10 places in Iceland, other than Isavia. Failure in those places has only occurred once over the last 10 years. These systems are monitored and maintained on an annual basis.

In conclusion MTTF is considered to be 25 years.

### **Diesel powered generators**

Diesel powered generators provide back-up power for the system. They have operated approximately 213 hours of systems operation. When electricity has been stable for 10 minutes the load is shifted back to its' normal path. When running on the back-up generators the maximum capacity of the system is 550A and therefore it bypasses the humidity system but runs the cooling system.

There is an interlock device preventing both generators from taking over the electricity at once and thus coordinates the function of the two diesel powered generators. This device is a part of the generators and thus can be one failure mode for the generators. The MTTF of this device is built into the MTTF of the generators. Diesel power generators can fail due to various reasons, e.g. run out of oil, filters needing to be changed and so forth.

The generators are started biweekly (every other Tuesday) to test whether they work and to maintain motor oil. This test has no influence on the system. The generators are maintained and tested annually.

In conclusion MTTF is considered to be 30 years.

### **Distribution boards (East/West)**

This unit is very important to the electrical power system; if e.g. the east distribution board fails it means that the fuse boards Q31 and Q33 do not get any electrical power.

These components are believed to be highly reliable since they are mechanical in nature. Failure could occur for example due to human failure or due to a electrical wire burning over.

In conclusion MTTF is considered to be extremely high or 50 years.

## Uninterrupted Power Supply (UPS)

There are 4 UPS in the system, 2 at the east part of the air traffic control center and 2 at the west. They all run at the same time and therefore share the load. UPS 1 and 2 automatically share the load even though only one is needed for the system to operate. In the event that UPS 1 fails, then UPS 2 takes on an increased load to keep the system operating. Thus UPS 1 is a back-up for UPS 2 and vice versa.

Key equipment in the air traffic control center is **connected** to both UPS branches which are **connected** to the distribution boards.

Even though the UPS are considered as a back-up system they are vital for the electrical system to function and therefore electricity has to be able to pass through them. If it is not an option to have the power pass through the UPS it can be directed through another path (this is done manually and thus ignored in the modeling).

UPS can generate backup power for the system with assistance of batteries. There are four sets of batteries, one set for each UPS. The batteries do not fail but only operate for a limited time period. According to specification they run for one hour but tests show that they are able to run for 2 hours. Tests are performed at least once a year where batteries are replaced if necessary (Isavia replaced all batteries in 2008).

The UPS system at Isavia is a highly reliable 2N system which means that the system is comprised of two independent systems in order to provide two sources of power to each equipment. According to associated Tier standards<sup>88</sup> the UPS system at Isavia has end user down-time 0.8 hours per year. Resulting in a reliability of 99.99% (Turner IV, Seader, Renaud, & Brill, 2008).

In conclusion MTTF is considered to be 15 years<sup>89</sup>.

## Fuse Boards

There are 2 power supplies for 4 fuse boards, which distribute power to 16 smaller independent units or fuse boxes. Failure of individual fuses has no effects on the system as a whole only to the equipment attached to that specific fuse. Important equipment is connected to more than one fuse board. Nagios monitor system alarms the supervisor<sup>90</sup> if a failure occurs in the fuse boards.

A failure has occurred once in these 16 units or boxes in the last 20 years. At that time all were replaced.

---

<sup>88</sup> Tier standards are a standardized methodology used to determine availability, developed by the Uptime Institute.

<sup>89</sup> The second value needed for loadsharing was based on values (at unit level) provided by vendor. For a 120 KW UPS, of MTBF 533,333hrs, these values are for a 120 KW UPS but at Isavia the UPSs are 40 KW of that same type. The values can however be used as a benchmark for estimating the MTTF of the 40 KW UPS.

<sup>90</sup> Information on the supervisors' responsibilities can be seen in appendix B.

In conclusion MTTF is considered to be 20 years.

Fuse board input terminals have a separate MTTF value of 15 years.

### **Main cables/wires and connectors**

All components of the electrical system are connected with cables or wires. The cables/wires are independent, i.e. if one fails it has no effects on the other cables/wires. Failure can occur because of a corrosion of contacts, bent connector pins and electrical erosion but most likely due to a human mistake during construction or layout changes.

There is an interconnecting link between distribution boards East and West (as can be seen in 5-1 in chapter 5). This is a back-up link which can be used when distribution board east/west fail or if one main cable fails. This link connects the boards so the other distribution board can take over if needed. This link needs to be activated manually and for that reason it is not modeled in the reliability model.

Cables can last for several hundred years without failing, on the condition that they are properly placed in the ground and protective equipment works properly (Personal communication, Valur Harðarson 2011). The protective device meets IEC standard and protects from: Overloading, overheating etc.

MTTF is based on the assumption that cables are correctly placed in the ground and protective equipment are working properly. According to Gray and Reuter: *"Connectors and cables are commonly rated at 1,000 years MTTF"* (Gray & Reuter, 1993) and thus MTTF is considered to be 1,000 years for this system as well.

**Table E-1: Presents the components of the electrical system, their function, detection of failure or tests, effects of failure, MTTF values and risk reducing measures.**

Description of component		Function	Detection of failure/TEST	Effect of failure	MTTF	Risk reducing measures
Item	Model			On the system function		
Electrical grid		Orkuveita Reykjavíkur is a public utility company that provides Isavia with electricity.	The automatic transfer system monitors the electricity coming in from the grid and senses if action is needed. If action is necessary it automatically alerts specialists via SMS that the Diesel power generators have been activated.	The system can operate on electricity from 2 diesel power generators or for a limited time from UPS.	1 year	3 service lines.
Transforming station/ transformer substation		Master switch, switch boards and diesel power generators are located at the transforming station.				
Master switch/switch board	Schneider electric, Masterpact NW08 H1	Circuit breaker (H1: high performance with total discrimination).	See Electrical grid.	Automatic transfer system switches to backup power generators.	25 years	The switches are the same type and can be used as spare parts for each other.
Automatic transfer switch	Deep sea Electronics Model 530	Automatically activates Diesel Power generators when needed and transfers activity back when possible .	Annual maintenance.	The system can operate on electricity from UPS.	25 years	None.
Switch board for diesel powered generators	Schneider electric, Masterpact NW08 H1	Circuit breaker (H1: high performance with total discrimination).	See Electrical grid.	System switches to backup power from UPS.	25 years	The switches are the same type and can be used as spare parts for each other.
Diesel - powered generators	Caterpillar 340 6B	A back-up power generator.	Started biweekly to test whether it works and to maintain motor oil. This has no influence on the system. + Annual maintenance.	The system can operate on electricity from UPS.	25 years	Annual maintenance performed by Hekla.
<b>ATC center</b>						
Distribution board (East/West)	T1.1/ T1.2	Distribute electricity to equipment and the ATC center (e.g. to offices).	Annual maintenance.	Complete failure of the system (if both fail).	100 years	There are 2 distribution boards, important equipment is connected to both.
Uninterrupted Power Supply (UPS)	APC Silcon DP360E from Schneider Electric	Provides emergency power and guarantees a pure sinus wave to the equipment.	Annual maintenance.	Only need one of the two on each side to operate.	60 years	Redundancy. 2 units in east side of the building and two in the West. Both run at the same time and share the load. UPS works as a backup for 1 hour according to specifications.
Batteries		There are four sets of batteries, one set for each UPS.	Tested once annually and replaced if necessary.	Do not fail.	Do not fail, assumed to work for 1 hour.	There are 4 independent set of batteries, one for each UPS.
Fuse board	Siemens 16B amp fuses	There are 2 power supplies for 4 fuse boards, which distribute power to 16 smaller independent units or fuse boxes.	Nagios monitor system alarms the supervisor if a failure occurs.	The equipment connected to the unit fails.	20 years	The fuse boards are independent of each other. Important equipment is connected to more than one fuse board.
Fuse board input terminal		There are 2 fuse board intakes that receive electricity, one for Q30 and Q32 and one for Q31 and Q33.	See Fuse board.	The equipment connected to the unit fails.	15 years	None.
Cables/wires and connectors		Connect electricity to relevant units.		Independent and thus only effects that specific path i.e. if one fails it has no effects on the other cables/wires.	1,000 years	Interconnection. A back-up link useful when distribution board East/West or a main cable fails.

## F. Concepts and definitions

The main subject of this research project is reliability calculations. Definitions of reliability and some associated key concepts are given below. Additional terms relating to BlockSim and abbreviations used in the research project are given in the appendix G and A.

**Accelerated life tests:** A test where conditions (stress, strain etc.) are changed to force the item to fail more quickly than under normal circumstances i.e. accelerates failure for the purpose of quantifying the life characteristics of the unit at normal conditions (Reliasoft, 2007).

**Active Redundancy:** A type of redundancy where all components are simultaneously active and participating within the system during normal operation (Kececioglu, 2002; Rausand & Høyland, 2004).

**Analytical approach:** The use of an *appropriate* process to break a system down to produce an exact mathematical expression that describes the reliability of the system i.e. it generates the Cumulative Distribution Function (*CDF*) for the system (Reliasoft, 2007).

**Availability  $A(t)$ :** Availability of a system is defined as the probability (*Pr*) that the system is available to perform its required function at time *t* (Xie, Poh, & Dai, 2004). Mathematically:

$$A(t) = Pr(\text{System is functioning/available at time instant } t)$$

The availability function is a complex function of time but has a simple “steady-state” or average availability that is given by (Xie, Poh, & Dai, 2004):

$$A_{av} = \lim_{t \rightarrow \infty} A(t) = \frac{\text{System uptime}}{\text{System uptime} + \text{System downtime}} = \frac{MTTF}{MTTF + MTTR}$$

This gives the percentage of time that a system is available to perform its required functions (United States Army, 2003).

Availability accounts for both failures and repairs of the system. When the system is non-repairable, availability is equal to reliability (Reliasoft, 2007).

**Bathtub Curve:** A plot of the failure rate of an item vs. time (or number of cycles) shaped like a bathtub. The failure rate initially decreases, then stays nearly constant but then it increases (Vishay, 2008; Chandrupatla, 2009).

**Binomial distribution:** A probability distribution of with parameters *n* and *R*, then the probability of getting exactly *i* successes in *n* trials is given by (Xie, Poh, & Dai, 2004; Reliasoft, 2007):

$$R_s = \sum_{i=k}^n \binom{n}{i} R^i (1-R)^{n-i} = \sum_{i=k}^n \frac{n!}{i!(n-i)!} R^i (1-R)^{n-i}$$

$$R(t) = 1 - F(t) = \Pr(T > t) \quad \text{for } t > 0$$

**Cold stand-by mode:** See appendix G.

**Common Cause Failure:** “Multiple component faults that occur at the same time or that occur in a relatively small window and that are due to a common cause” (NASA, 2002).

**Conditional Probability  $Pr(A/B)$ :** The probability of an event ( $A$ ), given that another event ( $B$ ) is known to have occurred i.e. the probability of  $A$  given  $B$  (Testability.com, 2008).

**Configuration:** The arrangement or construct of components (Reliasoft, 2007).

**Container:** See appendix G.

**Corrective Action/maintenance:** An action, taken as a result of a failure, to restore a failed component. A documented design, process, procedure, or materials change implemented to correct the cause of failure (Testability.com, 2008; ITEM Software, Inc., 2012).

**Criticality:** A unitless measure used to rank the failure modes to find which ones have most potential impact on the system. Typically, combines both the consequences (i.e., severity) of a particular failure mode and its frequency of occurrence (Testability.com, 2008; ITEM Software, Inc., 2012).

**Cumulative Distribution Function (CDF):** The probability that the random variable takes on a value less than or equal to a value  $x$ , e.g. for every real number  $x$  the CDF is given by:  $F(x) = CDF(x) = \Pr(x \leq X)$  (Vishay, 2008).

**Distribution (Life/failure/reliability/probability/statistical):** A mathematical function that describes the probability of failure (or the probability of success – reliability) of the component over time. Also known as a Probability Density Function (**PDF**). “This function can be utilized to determine the probability that a failure takes place in a given time interval” (Testability.com, 2008).

**Exponential Distribution:** The most known and used probability distribution in reliability engineering. Used for time dependent data where the rates at which events occur does not vary. This means that exponential distribution implies a constant failure rate and does not take into account the infant-mortality and wear-out failures (Apthorpe, 2001; United States Army, 2003; ITEM Software, Inc., 2012).

**Failure causes:** The circumstances that have led to failure. “The basic reason(s) for a failure” (Testability.com, 2008).

**Failure Effect:** The consequences a failure has on the operation, function or status of a component/system (Testability.com, 2008).

**Failure mode:** A description of a fault. This is a no fulfillment of a functional requirement. A failure mode generally describes the way the failure occurs and is the manifestation of failure as seen from the outside (Rausand & Høyland, 2004; Vishay, 2008).

**Failure Modes, Effects and Criticality Analysis (FMECA):** An inductive, bottom-up method to analyze system design for safety and performance. It determines the effects of component and functional failure modes on the system and includes criticality ranking calculations for each failure mode and effect (Testability.com, 2008; ITEM Software, Inc., 2012).

**Failure rate/hazard rate:** A function that describes the number of failures experienced or expected per time unit or cycles. It can be computed as the inverse of MTBF (Rausand & Høyland, 2004; Testability.com, 2008).

**Failure/Hazard:** The occurrence of an undesirable event resulting in termination of a required function of a component or performance below specified levels.  $F(t) = Pr(\text{failure})$ . Failure is the manifestation of a fault (Rausand & Høyland, 2004; Testability.com, 2008; Vishay, 2008)..

**Fault:** “...the state of an item characterized by inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources” (IEC 50(191), 1990). In other words, fault is a state resulting from a failure.

**Hot stand-by mode:** See appendix G.

**“Infant-mortality” or “burn-in” stage:** A stage immediately after an item enters service. At this stage premature catastrophic failures occur at a much greater rate than during the steady-life stage (Apthorpe, 2001; Rausand & Høyland, 2004; Vishay, 2008).

**“K-out-of-n”:** See appendix G.

**Load sharing:** See appendix G.

**Mean Time Between Failure (MTBF):** The expected operating time between failures, calculated by dividing uptime (functioning lifetime) by the total number of failures. MTBF is a measure of reliability for repairable systems. MTBF is the inverse of the failure rate (Testability.com, 2008; ITEM Software, Inc., 2012).

**Mean Time to Failure (MTTF):** The expected lifetime before a failure occurs (Xie, Poh, & Dai, 2004). MTTF is a measure of reliability for non-repairable systems. MTTF is the inverse of the failure rate (Xie, Poh, & Dai, 2004; ITEM Software, Inc., 2012).



**Mean Time To Repair (MTTR):** The mean time it takes to repair the component in the event of failure. The total corrective maintenance repairs time divided by the total number of those repairs (Xie, Poh, & Dai, 2004; Vishay, 2008).

**Node:** See appendix G.

**Outage:** A system failure i.e. the entire system becomes unavailable. Also referred to as a complete failure (United States General Accountability Office, 1998).

**Parallel:** See appendix G.

**Power outage:** A system failure resulting when the supply of electrical power fails.

**Qualitative:** A modeling approach that considers the components which make up a system and how they interact with each other logically. Qualitative techniques provide a rank ordering description of the factors that might cause accidents (Spouge, 2004; ITEM Software, Inc., 2012).

**Quantitative:** A modeling approach which is based upon a qualitative foundation, but includes probability distributions, to determine statistical results. Quantitative techniques estimate the risk of accident by estimating the probability of occurrence of each failure cause (Spouge, 2004; ITEM Software, Inc., 2012).

**RBD:** See appendix G.

**Redundancy:** The existence of more than one component (a backup component) that can perform a required function, in the event that the primary component fails. Redundancy allows the system to operate despite the event of component failure and thus preventing or mitigating the occurrence of equipment failures (Subotic, 2007; Testability.com, 2008).

**Reliability  $R(t)$ :** Reliability is defined as the probability that a system (or a component) can perform its intended function under stated working condition for a specified time period (Xie, Poh, & Dai, 2004; Chandrupatla, 2009). In other words, reliability is a design characteristic that indicates a system's ability to function without failure in a specific time interval.

$$R(t) = \text{Pr}(\text{component does not fail in a time interval } (0, t])$$

Assuming the system was operating at time zero, Reliability is the probability that it continues to operate until time  $t$  (ITEM Software, Inc., 2007). “ $R(t)$  is the probability that the item does not fail in the time interval  $(0, t]$ , or in other words the probability that the item survives the time interval  $(0, t]$  and is still functioning at time  $t$ ” (Rausand & Høyland, 2004).

**Risk:** Something that creates or suggests a failure/hazard or the possibility of failure preventing normal system operation.

**Safety:** *“Freedom from those conditions that can cause death, injury, occupational illness, or damage to or loss of equipment property”* (MIL-STD-882D, 2000). Since most activities are never totally free from risk, safety is often defined as acceptable level of risk (Rausand & Høyland, 2004).

**Sensitivity Analysis:** Analysis to determine how sensitive a system is to changes in reliability of the components (ITEM Software, Inc., 2012).

**Series:** See appendix G.

**Severity:** “Severity considers the worst potential consequence of a failure, determined by the degree of injury, property damage or system damage that could ultimately occur” (MIL-STD-1629A, 1980).

**Single Point Of Failure (SPOF)/Single Point Failure (SPF):** *“The failure of an item which would result in failure of the system and is not compensated for by redundancy or alternative operational procedure”* (MIL-STD-1629A, 1980).

**Stand-by Redundancy:** A type of redundancy where some components are off/ waiting for the active component to fail (Kececioglu, 2002).

**“Steady-life” stage:** A nearly constant failure rate life stage after the “infant-mortality” stage (Apthorpe, 2001; ITEM Software, Inc., 2012)

**Survivor function:** The survivor function is sometimes referred to as reliability or success function (Rausand & Høyland, 2004).

**System:** See appendix G.

**Unavailability:**  $1 - \text{Availability}(t)$ . *“The probability a system has failed at a specific point in its lifetime”* (ITEM Software, Inc., 2012).

**Unreliability:**  $1 - \text{Reliability}(t)$ . The probability a system fails in a specific time period. (Rausand & Høyland, 2004; ITEM Software, Inc., 2012).

**Warm stand-by mode:** See appendix G.

**“Wear-out” stage:** A stage after the “steady-life” stage where the failure rate increases as components degrade due to wear (Apthorpe, 2001).

**“What-if” analysis:** “What-if” scenarios are constructed by switching components off and results compared to determine the weak points of the system (ITEM Software, Inc., 2012).

## G. The BlockSim terminology

BlockSim 7 is a software that provides a comprehensive platform for system reliability, availability and maintainability. It uses a reliability block diagram (RBD) approach, a fault tree diagram (FTD) approach or a combination of both. BlockSim 7 allows analyzes of any process or product to obtain exact system reliability results (including system reliabilities, mean times, failure rates, etc.). The results are used to calculate the optimum scenario to meet system reliability goals and to obtain maintainability, availability and throughput results through discrete event simulation and so on.

Reliability probability distribution of a system can be quantified based on component data and system configuration. BlockSim provides an extensive array of RBD configurations including additional RBD constructs that are not standard in the traditional RBD methodology.

It is very important that all main terminology, concepts and functions used during the modeling are defined in an unambiguous way, especially the constructs that are not standard in the traditional RBD methodology. Definitions of a RBD, a system, blocks, reliability distribution, series systems, parallel systems, nodes, complex configuration, containers, load sharing configuration, stand-by configuration sub diagrams, multi blocks and mirrored blocks are given below. These will be summarized from ReliaSoft's System Analysis Reference (Reliasoft, 2007). Further features of the concepts provided by the software and how they are used are presented in appendix H.

### Reliability Block Diagram (RBD)

A reliability block diagram represents graphically how components of a system are connected reliability-wise. Blocks (components of the system) which are connected with direction lines, that represent the reliability configuration of a system, make up the RBDs. This however may differ from how the components are actually connected. An example of RBD and other BlockSim terms is illustrated in Figure G-1.

A few factors have direct effect on a systems' reliability namely quantity of components, component properties and their design configuration.

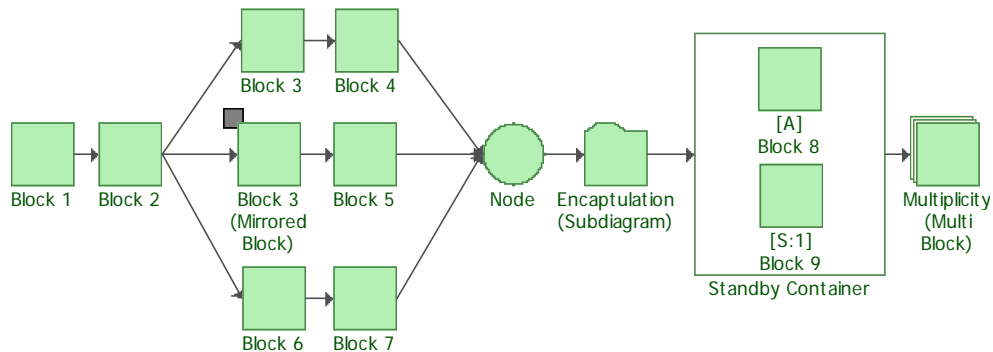


Figure G-1: A graphical representation of important BlockSim terms.

Load sharing container looks the same as a load sharing container except there is no [A] and [S:1] in front of the blocks name. These labels represent which units are active and which are stand-by.

## **A System**

A system consists of a collection of components and/or subsystems that are arranged in a specific design in order to achieve desired functionality. System definition depends on the level of detail in question. Ideally, system definition granularity should be to the lowest actionable level.

## **A Block**

In a RBD, blocks represent the component, subsystem or assembly of interest<sup>91</sup>. A block can represent a failure mode or a function of the component. The Block includes information as to how this component fails, i.e. the reliability model or the failure distribution of the block. Once the blocks reliability characteristics/properties are determined, they can be connected in a reliability-wise manner to create a RBD.

## **Failure Distribution/Reliability Distribution (Life data)**

Component reliability is quantified using a mathematical model that describes the probability of failure (or the probability of success – reliability) of the component at different ages. This is referred to as a failure or reliability distribution of the component. Each component can be described by a different model.

In general, life data is gathered by standard life testing, accelerated life testing, field data, engineering knowledge, vendor information or similarity to prior design.

## **RBD Component Configurations**

Configuration of the system is the manner in which components are connected. There are two types of configurations, series and parallel. Series and parallel configurations can be used simultaneously combined in one diagram<sup>92</sup>.

*A series structure* is a configuration such that, if one component fails, the entire system fails. It is as weak as its weakest link. The total system reliability is less than the reliability of the least reliable component.

*A parallel structure* is a configuration such that, as long as not all components fail, the entire system works. The total system reliability is higher than the reliability of any single component.

*K-out-of-n structure* is a configuration such that, as long as less than k out of a total of n components fail the entire system works.

---

<sup>91</sup> Use component or block from now on.

<sup>92</sup> Components are assumed to be independent.

A *node* is used to signify k-out-of-n redundancy in parallel configuration. The basic property of the node is to define how many paths leading into a node must be operational in order for the node to function. A node can have properties such as a failure distribution.

*Complex configurations* cannot be expressed as a simple combination of series and/or parallel. Complex combinations are needed when additional redundancy constraints are present and when performing failure mode analysis, network analysis, ancillary analysis etc. Complex configurations require the use of methods such as: Bayes' theorem, Boolean truth table, probability maps, logic diagrams, the decomposition, the event space or the path-tracing method<sup>93</sup>.

### **More complex redundancy schemes**

BlockSim provides additional RBD constructs that are not standard in the traditional RBD methodology. These constructs will be defined below and include Load sharing containers, Stand-by containers, Encapsulation, Multiplicity and Mirroring.

#### *The Container concept*

Container blocks allow identification of dependant blocks (contained blocks) that operate in a stand-by or load sharing configuration. The container block has properties<sup>94</sup> that describe the way the container behaves and the configuration of the blocks within the container, e.g. can be used to define the number of required units, k-out-of-n.

In a *load sharing configuration*, there is a dependency upon the redundant components<sup>95</sup>. In the event a component fails, the other components compensate for the failure by taking on an increased load to keep the system operating.

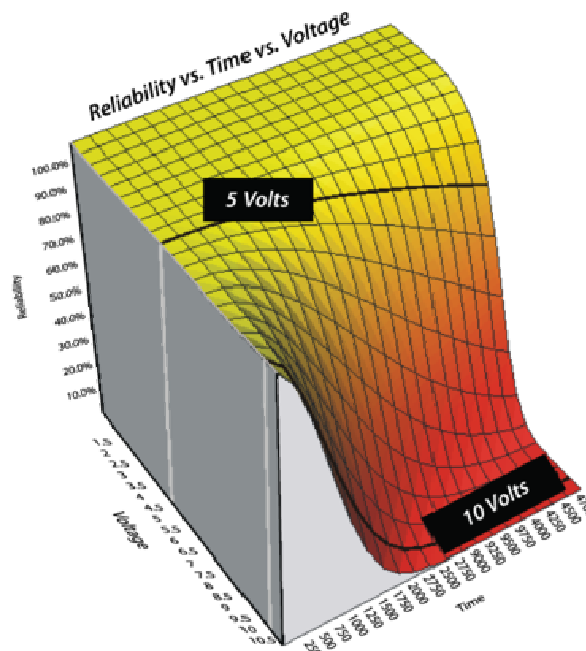
When dealing with load sharing components, a single failure distribution is not sufficient to describe the failure distribution of the block. The failure distribution of the block will change depending on the load carried. Thus an additional function is needed to describe the effect of the load on life, i.e. stress. An example of *PDF* and life-stress relationship describing the probability of failure at different loads can be seen in Figure G-2.

---

<sup>93</sup> Applying these methods by hand is difficult and time consuming, thus BlockSim software will be utilized for the analysis.

<sup>94</sup> Contained block properties can be seen in appendix H.

<sup>95</sup> independence was assumed for simple parallel configurations



**Figure G-2: Example of PDF and life-stress relationship.**

*“BlockSim provides life-stress models (derived from the ALTA software) to quantify the effect of the increased load on the operating components when other load sharing components fail” (Reliasoft, 2007).*

In a *stand-by configuration*, one or more stand-by components are available to take over if the active component fails. Units in stand-by redundancy are considered inactive until needed and become active when the primary unit fails. Units may age and fail while inactive and thus have both active failure distribution and stand-by (quiescent) failure distribution.

A stand-by container allows clear identification of the component’s active and stand-by distributions as well as the probability of switching between active and stand-by components when needed. For the switching mechanism, the container can be defined with delays and its own probabilities of successful activation of stand-by units when needed. Failure of the container means failure in activating the needed components but does not cause the system to fail<sup>96</sup>. If the active component fails and the switch has also failed, then the system cannot be switched to the stand-by component and therefore it fails.

There are 3 types of stand-by modes:

- **Cold Stand-by** component cannot fail while in stand-by mode (i.e. no quiescent distribution).

<sup>96</sup> For this reason the methodology is not the same as treating the switching device as a series component with the stand-by component

- **Warm Stand-by** components has a lower failure rate when in stand-by than when in active mode (i.e. has both quiescent and active failure mode).
- **Hot Stand-by** component has the same failure distribution in stand-by mode as when in active mode (i.e. simple parallel case).

### **Encapsulation**

A block that encapsulates another RBD inherits the properties from the encapsulated RBD. This block serves as a sub diagram to the current diagram. This allows using a single distribution approximation for the reliability equation of the encapsulated component, instead of the complete solution. This links diagrams by using existing RBDs as components in other diagrams.

### **Multiplicity**

Multi blocks is a single block that represents more than one component with the same properties configured in series, parallel or k-out-of-n.

### **Mirrored Blocks**

Mirrored blocks are used to represent the exact same component in more than one location within the RBD allowing additional flexibility when modeling. This can be useful for simulating more complex systems, bi-directional paths and common cause failures.

## H. Features of BlockSim

This appendix is intended to introduce features available in BlockSim 7 in order to provide a description of how the reliability model of the RACC ATM system was made in BlockSim and some of the knowledge needed to be able to extend the model in BlockSim. Thus this appendix is a tutorial for the software that is fairly technical. For this reason it is recommended to have access to the software while reading this appendix. This appendix holds a summary of some of the features presented in the training guide (Reliasoft, 2010) and some other useful features learned while using the software. For further knowledge on BlockSim go to <http://www.reliasoft.tv/blocksims/index.htm>, contact author or the ReliaSoft Corporation (Support@ReliaSoft.com).


BlockSim is “an intelligent, flexible and completely integrated” software tool that provides a comprehensive, easy-to-use package platform for system reliability, availability and maintainability. BlockSim generates a reliability probability distribution of a system based on data and system configuration such as series, parallel and “k-out-of-n” configurations, as well as complex combinations of those configuration types. Standby and load sharing redundancy configurations can also be created. When each block’s maintenance characteristics are defined, maintainability/availability, simulations can also be performed. BlockSim analysis and optimization is performed using a Reliability Block Diagram (RBD) approach (Reliasoft, 2010).

### Basic features

#### Creating a Template Block

**Templates** store pre-defined reusable blocks. Characteristics of a component then only have to be defined once but the block can be used often in many diagrams.

A new Template Block is created by clicking the Template Panel or double-clicking the Template name.

- Select **Add Block** from the **Template** menu or click the **Add New Block** icon  in the Diagram Tools toolbar<sup>97</sup>.



A block will appear in the Template.

When block properties have been defined the block can be dragged from the Template Panel into the Diagram. Then a copy of the block is placed in the Diagram Sheet and the Template block remains in the Template Panel. The new block in the Diagram Sheet is independent of the block in the Template i.e. changing the properties of a block within

---

<sup>97</sup> Blocks can also be added directly to the Diagram Sheet in the same way, by clicking the diagram and then clicking the **Add New Block** icon.



the Template Panel will not, change the properties of blocks already positioned in the Diagram Sheet.

### Defining/Editing Block properties

Characteristics of blocks can be defined with the failure, maintenance, reliability optimization, and other characteristics.

- Double-click the block to get **Block Properties**.

The Block Properties window will appear, as shown in Figure H-1:

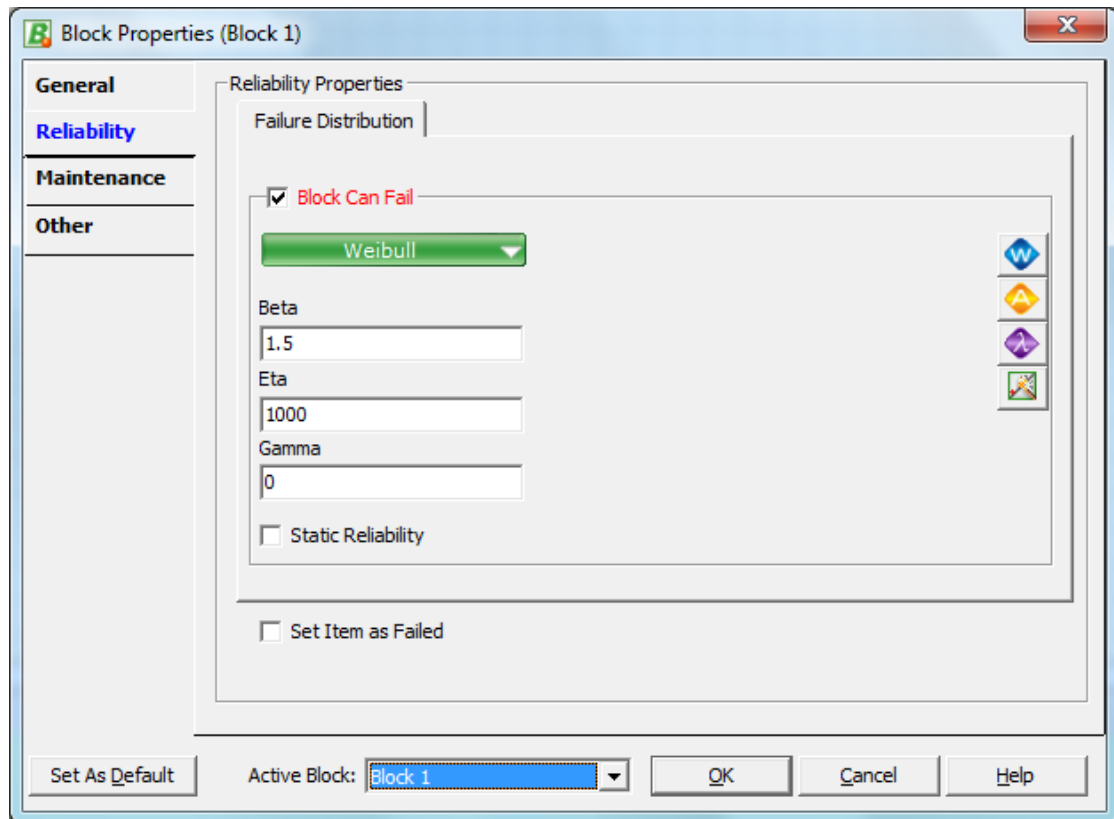


Figure H-1: Block Properties window.

#### Define block name:

- General tab (Item page) → define the block name → OK.

#### Define the failure distribution<sup>98</sup> of a component:

- Reliability tab (Failure Distribution page) → select the **Block Can Fail** option → Select the failure distribution from drop-down menu bar<sup>99</sup> → provide parameters for the distribution<sup>100</sup> → OK.
  - This is used when specifying the properties of all electrical components.

<sup>98</sup> Failure distribution is also referred to as life data distribution /reliability distribution/ reliability characteristics.

<sup>99</sup> Life distributions include Weibull, mixed Weibull, normal, lognormal, exponential, generalized gamma, gamma, logistic, loglogistic and Gumbel distributions.

<sup>100</sup> BlockSim requires uniformity of units among required inputs as it is not possible to specify different units for different components. The units for the results are the same as the units for the data inputs.

**Define reliability at a fixed point in time:**

- Reliability tab (Failure Distribution page) → select the **Block Can Fail** option → Select the Static Reliability option → an input box will appear for the reliability of the component at a fixed point in time → OK.

**Define components that do not fail** (the reliability of the block at all times is considered to be 100%):

- Reliability tab (Failure Distribution page) → de-select the **Block Can Fail** option → OK.
  - This is used when specifying the properties of 'Start' and 'End' blocks of the ATM reliability model.


**Defining/Editing Block properties of many components at once:**

- Go to Project Tab → Item Properties Table – here all fields can be modified like in Excel.

**Arranging and Connecting the Blocks**

The blocks can be moved into the desired position, by dragging it, and then connected by adding relationship lines to represent the relationships between the components of the system.

**Add relationship lines:**

- Select **Join Blocks** from the **Diagram** menu or click the **Join Blocks** icon  → Hold down the left mouse button and drag a line from the first block to the second block and then release the button. A relationship line will now connect the two blocks.

**Stop adding relationship lines:**

- Right-click or double-click the Diagram Sheet or click the **Join Blocks** icon again to stop adding relationships and return to BlockSim's normal mode.

**Making the Reliability Model**

Start with making the model of the electrical system (see Figure H-2). Specific components within the system will be demonstrated next starting with the stand-by container used to model the automatic switching system.

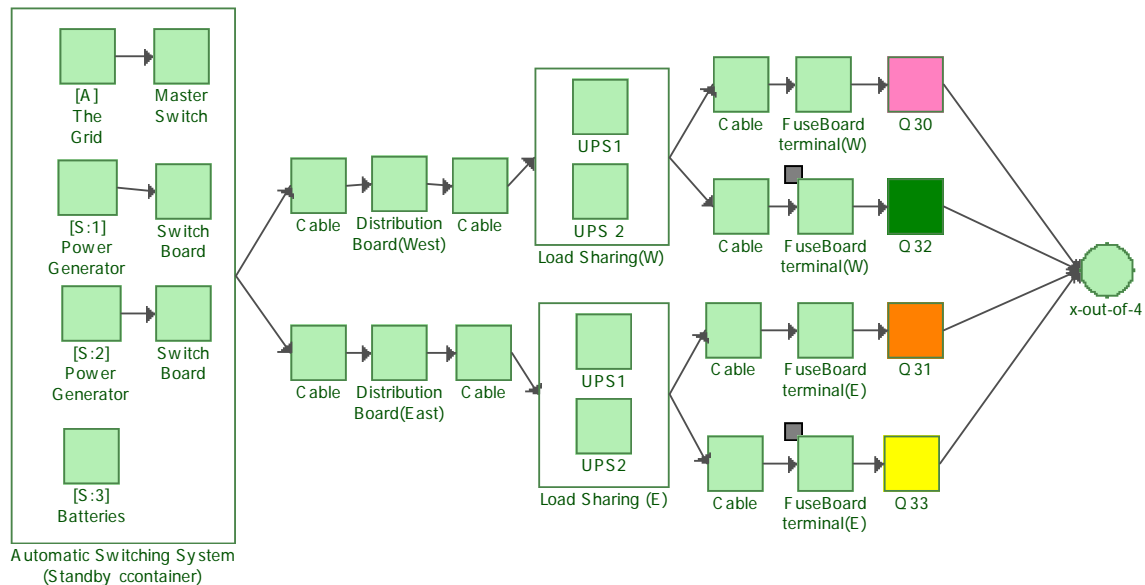


Figure H-2: RBD of the electrical power system.

### Standby container (Automatic Switching system)

- Choose Diagram → Add Standby Container or click the Add Standby container icon. 

**Defining Container properties** → Double-click the Container to open the Container Properties window.

### To define number of required active units:

- General tab (Item page): Specify the Number of Paths Required to indicate how many are required in order for the system to succeed and specify if a container is a standby or a load sharing container.

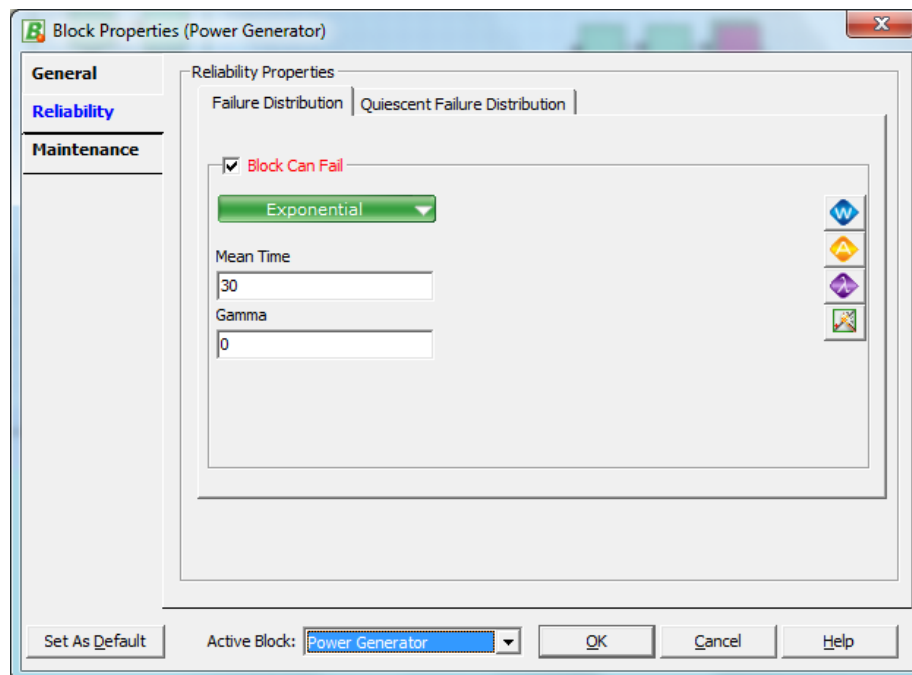
### To define the failure distribution of the switch while operating:

- Reliability tab (Failure Distribution page): Select the **Block Can Fail** option → Select the failure distribution from drop-down menu bar → provide parameters for the distribution → OK.
- Reliability tab (Switch Action Reliability page). The following can be defined:
  - Probability of switching per request (static probability).
  - Probability that the switching action will be re-attempted if it failed.
  - Number of times the re-attempt is performed.
  - Delay time between requests.

**Defining contained block properties is the same as other blocks except for the following key features:**

- General tab (Item page): Specify if the component is active or standby at the beginning. The grid is the active component in the electrical system and is reactivated after repairs.

Units may age and fail while inactive and thus components can have two failure distributions active failure distribution (while operating) and quiescent failure distribution (while in standby). These are selected on the Reliability tab – failure distribution page and quiescent failure distribution page as shown in Figure H-3.



**Figure H-3: The Reliability tab where failure distributions are identified.**

#### **Load Sharing container (UPS system)**


- Choose Diagram → Add Load Sharing Container or click the Add Load Sharing Container icon. 

**Defining Container properties** → Double-click the Container to open the Container Properties window.

- General tab (Item page): Specify the same as in the standby container and the load value.


**Defining contained block properties is the same as other blocks except for the following key features:**

Define failure distribution that changes depending on the load carried:

- Reliability tab (Failure Distribution page): Select the **Block Can Fail** option → Select the life-stress relationship and the failure distribution from drop-down menu bar → provide parameters for the distribution → OK.
- The parameters can be calculated using the Parameter Experimenter. 
- Reliability tab (Failure Distribution page): Define the load for each item by using the weight proportionality factor.
- Various life-stress relationships exist and the most appropriate one can be found using accelerated life tests. As this is not an option in this research it was decided to use the inverse power law relationship which applies to most mechanical and non-thermal stressing of components (Reliasoft, 2007; Kusy, 2012).


### **Mirror blocks (Fuse board intake E/W)**

Mirror blocks can be used to represent a single item with more than one block placed in multiple locations within the diagram. When simulation is performed on a Diagram Sheet with mirror blocks, every event associated with the “source” block will be exactly the same for every event associated with the “Mirror” Blocks. Mirrored blocks are used to model common cause failures or to represent exactly same component which in this case results in common cause failures in the ATM system.

- Click the source block that is supposed to be mirrored → choose **Block** → **Mirror Block** or click its icon.  → Click the target block, a grey box will appear at the top left corner of the “target” block, as can be seen in the model Figure H-2 (Fuse Board terminals), to indicate that the block is a mirror block.

### **A Node block (so-called x-out-of-4)**

A Node block is a type of block that can be defined to indicate the number of paths that must successfully pass through the block in order for the system to succeed (“k-out-of-n”).

- Choose Diagram → Add Node to Diagram or click the Add New Node icon. 

**Defining properties** → Double-click the Node block to open the Node Properties window.

- General tab (Item page): Specify the Number of Paths Required to indicate how many are required in order for the system to succeed.
- Reliability tab (Failure distribution page): Specify if the block can fail (can only fail when the node represents a component of the system, otherwise when it's only being used as a counter of paths it is specified as block cannot fail). →OK.

The next step when modeling the reliability of the ATM system was to use different versions of this electrical power system reliability model as component reliability

characteristics for the components of the ATM system. This was performed by using subdiagrams.

### Subdiagram (A block that represents other diagrams)

BlockSim provides the ability to link diagrams by using existing RBDs as components in other diagrams.

A subdiagram is defined by opening the **Block Properties**.


- General tab (Subdiagram page): Select the Block As Diagram<sup>101</sup> option and select diagram in the current project from the drop-down list.

The appearance of the block has now been modified to the shape of a folder. This is the way that BlockSim identifies subdiagram blocks (blocks that represent other diagrams).

### Analyzing the reliability model

When the assumptions made in section 5.2 have been reflected in the ATM model (by specifying the node value i.e. how many paths are needed through the system) the model is analyzed.

**To analyze the system:**

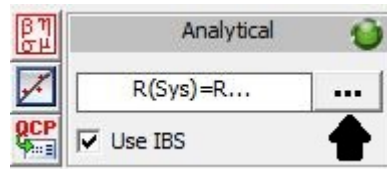
- Choose **Tools** → **Analyze** or by click the **Analyze** icon. 

**View reliability equation:**

The exact analytical equation used for the analysis can be viewed:

- Select **Show Algebraic Solution** from the **Tools** menu or by click the **Show**

**Algebraic Solution** icon




on the Diagram Sheet Control Panel.

### Calculating System Reliability

BlockSim generates reliability results based on the exact system reliability function.

**To calculate the reliability of the system at a specified time:**

- Choose **Tools** → **Analytical Quick Calculation Pad (QCP)**<sup>102</sup> or click the **Analytical QCP** icon  → General page → select **Std. Probability Calculations** under System Calculations → Type a Mission End Time

---

<sup>101</sup> “Block As Diagram” option creates a block that represents the reliability characteristics of an existing BlockSim diagram. This block serves as a subdiagram to the current diagram. This subdiagram block can then be placed into any diagram as a component.

<sup>102</sup> Simulation QCP works in a similar way to analytical QCP, allowing calculations based on simulation results. These calculation results include availability, unavailability, reliability, probability of failure, mean availability, mean unavailability, availability time, reliability time and MTTF.

(Required Input from User) → click **Calculate** and the estimated system reliability at the given time will appear under Results.

### Extending the model

To extend the model, two useful features in BlockSim can be used. These are adding maintenance and using ReliaSoft's Weibull++ life data analysis software and/or ReliaSoft's ALTA accelerated life testing analysis software to compute the appropriate distribution and parameters for components.

### Determine an appropriate failure distribution based on data


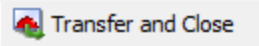
In the future when failure data will be available within Isavia BlockSim can be used to derive the reliability distribution for the component based on that data. This is done by using ReliaSoft's Weibull++ life data analysis software or ReliaSoft's ALTA accelerated life testing analysis software (software that is linked to BlockSim). Simply copy the data into the system and it generates parameters for the distributions and ranks them with regards to which one fits best to the data.

**Block Properties** → Reliability tab (Failure Distribution page) → Click the **Compute parameters using Weibull++ button**. 

- This will open ReliaSoft's life data analysis software (Weibull++) → Create a New Data Folio → Select the appropriate Data Entry Spreadsheet for the component's life data → OK.
  - A Data Entry Spreadsheet will be created based on the selections.
- Enter the failure data for the component into the Data Entry Spreadsheet.

Various estimation methods can be used to estimate the parameters. Which method is used is specified by clicking the Analysis tab on the Data Folio Control Panel. Return to the Main page of the Control Panel by clicking the Main tab.

The Distribution Wizard utility in Weibull++ conducts a variety of goodness-of-fit tests designed to suggest the best distribution for the data.

- Choose Data → *Distribution Wizard* or click the Distribution Wizard icon. 
- The Distribution Wizard will appear. Click Analyze so that the Distribution Wizard can go through the process of suggesting a distribution. After the Distribution Wizard has finished conducting the tests, a distribution will be suggested (indicated by 1 in the Ranking column next to the distribution).
- Click *Implement* which calculates the parameters using the selected distribution.
- Click the *Transfer and Close* button  to transfer the calculated data to BlockSim and close Weibull++.

Now the parameter values that were calculated using Weibull++ have been inserted as the parameter values of the failure distribution of the Block.

## Maintenance

BlockSim allows definition of the following maintenance policies types:

- *“**Corrective Maintenance Policies**, which describe the conditions that determine when corrective maintenance will be performed on an item.*
- ***Preventive Maintenance Policies**, which describe the conditions that determine when preventive maintenance will be performed on an item.*
- ***Inspection Policies**, which describe the conditions that determine when an inspection will be performed on an item.*
- ***Crew Policies**, which describe the conditions that determine when a crew will be available to perform specific actions and specifies the logistical time and costs associated with engaging the crew.*
- ***Spare Parts Pools**, which describe the conditions that determine whether a spare part will be available when needed and specifies the logistical time and costs associated with obtaining the spare part.*
- ***Feasibility Policies**, which allows definition a cost function for the difficulty or cost of increasing the reliability of a block” (Reliasoft, 2010).*

Thus the model may be extended by adding maintenance information. BlockSim offers multiple features regarding maintenance policies. For further details refer to the training guide of BlockSim (Reliasoft, 2010).

The model did not truly reflect operations when it was non-repairable as it is repaired. Therefore it was decided to add fixed corrective maintenance times to all components so the system will be repaired and reflect operations more realistically. This was performed by doing the following:

In the **Block Properties** → click **Maintenance tab**.

Select **Can Maintain correctively** → choose Fixed Duration



## I. FMECA example

This is an example of a FMECA worksheet and also the worksheet used for the FMECA conducted on the RACC ATM system.

[illegible]

## J. FMECA results

Description of component		Description of failure	Effect of failure on the system function	Criticality/Severity			
Item	Function	Failure mode of the system		Capacity	Workload	Risk reducing measures	Comments
All Radars:	Determine location and SQUWAK of A/C, provide feed into RDPS system	Partial failure	When a radar fails the level of service drops and A/Cs are more likely to be assigned to communicate with Iceland Radio, thus increasing the workload at Iceland Radio and decreasing workload at Isavia. Overall the workload stays the same or increases. Staff has procedural training on how to operate when radar is not available. Thus Staff is equipped to handle these situations although this may result in more workload and sometimes capacity restrictions due to increase in higher separation minimum.	3	2	Other radars cover parts of the region	Most radars have been unavailable at some point due to e.g. maintainance without causing any critical circumstances.
H1 (suðvestur)	See function of all radars	Partial failure		1	0	Back-up: KEF (less coverage but does not affect overall functionality) , H2, H3 and H4	
H1, KEF	See function of all radars	Partial failure	It is not possible to further divide up this sector based on altitudes because the A/Cs are landing in this sector. This is why the number of staff is not increased. If these fail all A/Cs are distributed on longitudes and latitudes according to procedures, thus increasing capacity restrictions.	2	1		
H2 (Gunnhólfsvíkur-fjall)	See function of all radars	Partial failure	Small low density area not covered. This results in less visualization of A/Cs coming from Egilsstaðir since the A/Cs arrive late and depart early from the radar screen. Same applies to A/C leaving Akureyri travelling to Vopnafjörður.	1	0	Back-up: H1,H3 and H4	
H3 (Höfn)	See function of all radars	Partial failure	Failure has more influence on the oceanic area.	1	0	Back-up: H1, H2,H4, and FAE cover some of the area	This is used in domestic flight when A/Cs fly low e.g. to Hornafjörður
H4 (Bolaþjall)	See function of all radars	Partial failure	Similar to H2, same problems present themselves in Ísafjörður and Bíldudalur as discussed in Egilsstaðir (radar H2).	1	0	Back-up: H1 and H2	
H1H2	See function of all radars	Partial failure		1	0	KEF backs up most of H-1	
H2KEF	See function of all radars	Partial failure	Same as if only H-2 fails	1	0		
H1H2KEF	See function of all radars	Partial failure		2	1		
H1H3	See function of all radars	Partial failure		1	0	KEF	
H1H3KEF	See function of all radars	Partial failure		2	2		
H1H4	See function of all radars	Partial failure		1	0	KEF	
H1H4KEF	See function of all radars	Partial failure	Same as if H1H2KEF fails	2	1		
H2H3	See function of all radars	Partial failure	Similar to H-3 failing	1	1		
H2H4	See function of all radars	Partial failure		1	1		
H3H4	See function of all radars	Partial failure		1	1		
H1H2H3	See function of all radars	Partial failure	Similar to only H2H3 failing if KEF is operational	1	1	KEF	
H1H2H4	See function of all radars	Partial failure		1	1		
H1H3H4	See function of all radars	Partial failure		1	1		
H1H2H3KEF	See function of all radars	Partial failure	Same as if H-2 were operational	2	2		

H1H2H4KEF	See function of all radars	Partial failure		2	2		
H1H3H4KEF	See function of all radars	Partial failure		2	2		
H2H3H4	See function of all radars	Partial failure	Most of the flow is going inbound/outbound to Keflavik and Reykjavik (H-1). The failure would result in big blanks in the oceanic area.	1	1	FAE provides a backup for some of H-3 area	
H1H2H3H4	See function of all radars	Partial failure	The failure would result in big blanks in the oceanic and domestic area. Only have KEF suited for approach.	2	2		
H1H2H3H4KEF	See function of all radars	Severe partial failure		3	2 (isavia only) 3 (with Iceland Radio)		Need to use procedural separation and thus more staff is needed.
KEF	See function of all radars	Partial failure		0	0	Back-up: H1 (does not affect coverage but updates are slower in H1)	TPX has been down for some time now and does not affect ATC.
FAE	See function of all radars	Partial failure	This mainly affects traffic arriving and departing The Faroe Islands because the ATCO sees the traffic later than usual.	0	0,5	Back-up: SUM, H2 and H3	
SUM	See function of all radars	Partial failure		0	0,5	Back-up: FAE	Covers 240 nautical miles
FAE&SUM	See function of all radars	partial failure	Failure causes a non radar procedural control in East sector because A/Cs appear later on the screen. This could result in the need to divide a sector.	1	1	H-3 and H-2 provide a backup for some of the area	
RDPS	Simultaneous data processing from radar while performing real-time monitoring and data extrapolation	Severe partial failure	See affects of failure on the system function of all radars	3	2	Redundancy i.e. There are 2 redundant and therefore independent radar systems that are booth running but only one (master) is actively sending to ISDS	Have all flight data (FDPS)
STCA	Alerts ATCOs in case of separation minimum violation	Partial failure	Increases RISK	0	0		
FDPS	Receives all flight information other than radar data and automatically processes all the information related to the A/Cs relative position into electronic progress strips	Severe partial failure	Results in flow constraints - need to request no more flow. Can only see A/C on radar but don't see any in the north and west sector. Aircraft already in airspace are not in danger.	3	3	There are 2 redundant and therefore independent FDPS and each one has built in redundancy. Hence there are 2 masters and 2 backups for the system where only one master is running at any given time but both the backup and the other master is ready to take over in the event of failure. ICE provides a backup database and FDE provides the option of stripprinting (FDE is last resort back-up).	

FDE	A back-up system for FDPS, stores electronic data strips	Partial failure	Increases RISK	0	0		Not all staff knows how to use non-electronic strips.
SPASS	Provides the FDPS with the squawk code and RDPS with incremental list	Partial failure	A failure in Spass regarding squawk has no serious consequences because the information exists in a different slightly inferior format in FDPS. A/C only have transponder code instead of call signals which creates more workload because ATCOs need to compare the squawk to strips to know who is who.	0	0,5=some extra load on current staff		The system still provides only one target of correlated CPL and radar data
ICE	Standby database backup of FDPS data, does a correlation between CPL and radar data and provides more accurate POS reports	Partial failure	Have no CPL tracks on the screen - ATCO needs to draw routes	0	1		
ICE	POS report	Partial failure (partial failure of the Item)		0	0	Redundancy	
ICE	ISDS data: Correlated (CPL& Radar) Data, CPL data, Conformance info	Partial failure (partial failure of the Item)	Increases RISK, it is less likely that ATCO notices if A/C is not following the clearance specifications. Thus, less conflict resolution.	0	0		
ICE	Database (A back-up system)	Partial failure (partial failure of the Item)	Increases RISK	0	0		
ISDS	Provides a visual representation of flight profiles, flight estimates, crossing times, both radar and CPL tracks etc.	Severe partial failure	Same as RDPS failing, loose situational awareness and estimated targets gathered from CPL reports	3	2		
VCS	VCS is a telecommunication system including phones, VHF radios and SAT phones	Severe partial failure	Restricted communication with Iceland Radio. Workload increases because ATCO can not use speed dial but rather has to look up all phone numbers. Bourdieu and Embleton are examples of control units that need communication through VCS	3	2	Back-up: back-up radio, emergency phones, commercial phones, SAT phones, automatic correlation	
Radio stations: E-2, E-3, E-4, E-5, E-7, E-9, H-3, H-4	Reives and transmits electronic signals	Partial failure		2	2		The most important radio stations are E-7, H-3 and H-4
E-2	Reives and transmits electronic signals	Partial failure	If one of the less important radio stations fails it has no consequence	0	0	Back-up: E-9, E-3	
E-7 (Bláfjöll)	Reives and transmits electronic signals	Partial failure		0	1	H-3 and E-9. The stations provide coverage for domestic flight	This is a very important link in the radio system. Has influence on the oceanic area.
H-3 (Stokksnes)	Reives and transmits electronic signals	Partial failure		0	1	Back-up: E-3, E-2, E-7 and E-9	
E-7, H-3	Reives and transmits electronic signals	Partial failure		1	1	Back-up: E-3, E-2 and E-9	

VHF	Used for voice- and data link communication	Partial failure	A/C communicate with Iceland Radio	2	2	Another way to communicate is via phone	
Back-up radios	A back-up for VCS	Partial failure	Increases RISK	0	0		This is a last resort device that can not be used to control traffic because of low range but can be used to give the heads up that the VCS system has failed.
Emergency phones	A back-up for VCS	Partial failure	Increases RISK	0	0		
Commercial phones	A back-up for VCS	Partial failure	Increases RISK	0	0		
SAT Phone	Communication through satellites	Partial failure		0	0		SAT Phones are not used allot
DLCS	Processes CPDLC, ADS-B and automatic POS reports	Partial failure	ATCO consequently needs to request POS reports from A/Cs	0	1	Back-up: VHF voice communication and Iceland Radio (HF/VHF)	
CWSs	1/2 of the ATC centres CWS	partial failure	The CWS contains the computer and communication systems used by ATCOs i.e. this needs to be operating for all systems used by ATCO.	0,5	1	The CWSs are connected to different fuse boards. Each CWS has only one powersupply, this means that if one fails the ATCO can move to another computer (have more than enough of CWS that are not in use)	Normal operation requires 6-7 CWS. Approximately 3 for south sector, 1 for East sector and 2 for West sector.
AFTN	A ground-to-ground communication system for transmitting flight data messages. The external data goes through AFTN e.g. : FLP, automatic coordination, ACT reports ( Scottish, Stavanger ), CPL to Gander, CLR to Shanwick, weather information, TRACK reports	Severe partial failure	Don't get any external reports or flight plans, all communication go through Iceland Radio, sector coordination must be done through voice communication.	2,5	2		
COM network (Mila)	A communication network that transmits signals	Severe partial failure	Loose radar and radio stations except for E-7 (Isavia has a separate private link to E-7)	3	2		
Dan ice and Far ice	Automatic coordination, Data links	Partial failure	Results in more work load. If these data links fail the ATC centre does not get any data from the devices connected to it e.g. FAE and SUM radar. Would not get any data into AFTN so equally critical	0	0,5	Back-up: phones	

Dan ice	Automatic coordination, Data links	Partial failure		0	0	Back-up: far ice backup except for voice communication to Edmundton, voice back-up: SAT phone and commercial phones	
Far ice	Automatic coordination, Data links	Partial failure		0	0,5	Back-up: dan ice except for SUM	SUM is singular on far ice
FDPS, VCS	See function of FDPS and VCS above	Complete failure	complete failure of the system occurs if at least these systems fail at the same time.	3+	3+		
FDPS, VHF	See function of FDPS and VHF above	Complete failure	complete failure of the system occurs if at least these systems fail at the same time.	3+	3+		
AFTN, VCS	See function of AFTN and VCS above	Severe partial failure	This would result in a serious downgrade of the whole system. FDPS data is still available. Would have the possibility of mobile communication with Iceland Radio and SAT phone communication with aircraft.	3	2		
AFTN, VHF	See function of AFTN and VHF above	Severe partial failure	This would result in a serious downgrade of the whole system. FDPS data is still available. Would have the possibility of mobile communication with Iceland Radio and SAT phone communication with aircraft.	2,5	2		
FDPS, Com network (Mila)	See function of FDPS and COM network above	Complete failure	complete failure of the system occurs if at least these systems fail at the same time.	3+	3+		
AFTN, Com network (Mila)	See function of AFTN and COM network above	Severe partial failure	This would result in a serious downgrade of the whole system. FDPS data is still available. Would have the possibility of mobile communication with Iceland Radio and SAT phone communication with aircraft.	3	2		
ISDS, VCS	See function of ISDS and VCS above	Severe partial failure	This would result in a serious downgrade of the whole system. FDPS data is still available. Would have the possibility of mobile communication with Iceland Radio and SAT phone communication with aircraft.	3	2		
GPS clocks	GPS data stamping and synchronisation	Partial failure	If both clocks would fail at the same time it would not effect the system for about 48 hours depending on how fast the equipment clocks would be drifting away from the GPS clocks.	0	0	Redundantcy	

### **Criticality/Severity ranking:**

Capacity		Workload	
Criticality ranking	Ranking signifies:	Criticality ranking	Ranking signifies:
0	No affects on capacity	0	No affects to workload
1	Not severe but has some affect on capacity	1	considerable pressure on the staff on a shift
2	Intermediary severe	2	increase in staff needed e.g. staff on a break come to help
3	very severe and has considerable affects on capacity	3	significant increase in staff needed

### **Failure definition:**

Failure mode	
Complete failure	Failure that causes complete lack of a required function of the system
Severe Partial failure	Failures that lead to a lack of some function but do not cause a complete lack of a required function, but causes severe consequences.
Partial failure	Failures that lead to a lack of some function but do not cause a complete lack of a required function

## K. Stand-by construct with three components

The general equation for stand-by container with two units was presented in chapter 4. This appendix is intended to show how complexity of calculations rises as one extra unit is added to the stand-by construct.

The system's reliability for the exponential case is given by:

$$\begin{aligned}
R(T) &= e^{-(\lambda_1 + \lambda_{SE} + \lambda_{SWO})T} + \int_{T_1=0}^T \lambda_1 e^{-\lambda_1 T_1} e^{-\lambda_{SE} T} e^{-\lambda_{SWO}(T-T_1)} e^{-\lambda_{SWQ} T_1} e^{-\lambda_{SWE} \cdot 1} e^{-\lambda_{2Q} T_1} e^{-\lambda_2 (T-T_2)} dT_1 \\
&+ \int_{T_2=0}^T \int_{T_1=0}^{T_2} \lambda_1 e^{-\lambda_1 T_1} e^{-\lambda_{SE} T_2} e^{-\lambda_{SWO}(T-T_2)} e^{-\lambda_{SWQ} T_1} e^{-\lambda_{SWE} \cdot 1} e^{-\lambda_{2Q} T_1} \lambda_2 e^{-\lambda_2 (T_2-T_1)} e^{-\lambda_{SWQ}(T_2-T_1)} e^{-\lambda_{SWE} \cdot 1} e^{-\lambda_{3Q} T_2} e^{-\lambda_3 (T-T_2)} dT_1 dT_2 \\
&+ \int_{T_1=0}^{T_2} \lambda_1 e^{-\lambda_1 T_1} e^{-\lambda_{SE} T_1} e^{-\lambda_{SWO}(T-T_1)} e^{-\lambda_{SWQ} T_1} e^{-\lambda_{SWE} \cdot 1} \left(1 - e^{-\lambda_{2Q} T_1}\right) e^{-\lambda_{SWE} \cdot 1} e^{-\lambda_{3Q} T_1} e^{-\lambda_3 (T-T_1)} dT_1 \\
&= e^{-(\lambda_1 + \lambda_{SE} + \lambda_{SWO})T} + \lambda_1 e^{-[\lambda_{SWE} + (\lambda_{SE} + \lambda_{SWO} + \lambda_2)T]} \int_{T_1=0}^T e^{-(\lambda_1 - \lambda_{SWO} + \lambda_{SWQ} + \lambda_{2Q} - \lambda_2)T_1} dT_1 \\
&+ \lambda_1 \lambda_2 e^{-[2\lambda_{SWE} + (\lambda_{SWO} + \lambda_3)T]} \int_{T_1=0}^{T_2} e^{-(\lambda_{SE} - \lambda_{SWO} + \lambda_2 + \lambda_{SWQ} + \lambda_{3Q} - \lambda_3)T_2} \left\{ \int_{T_1=0}^{T_2} e^{-(\lambda_1 + \lambda_{2Q} - \lambda_2)T_1} dT_1 \right\} dT_2 \\
&+ \lambda_1 e^{-[2\lambda_{SWE} + (\lambda_{SWO} + \lambda_3)T]} \int_{T_1=0}^T e^{-(\lambda_1 + \lambda_{SE} - \lambda_{SWO} + \lambda_{SWQ} + \lambda_{3Q} - \lambda_3)T_1} \left(1 - e^{-\lambda_{2Q} T_1}\right) dT_1 \\
&= e^{-AT} + \frac{\lambda_1 e^{-(\lambda_{SWE} + BT)}}{C} (1 - e^{-CT}) + \lambda_1 \lambda_2 e^{-(2\lambda_{SWE} + GT)} \left\{ \frac{1}{DE} (1 - e^{-DT}) - \frac{1}{E(D+E)} [1 - e^{-(D+E)T}] \right\} \\
&+ \lambda_1 e^{-(2\lambda_{SWE} + GT)} \left\{ \frac{1}{F} (1 - e^{-FT}) - \frac{1}{F + \lambda_{2Q}} [1 - e^{(F + \lambda_{2Q})T}] \right\}
\end{aligned}$$

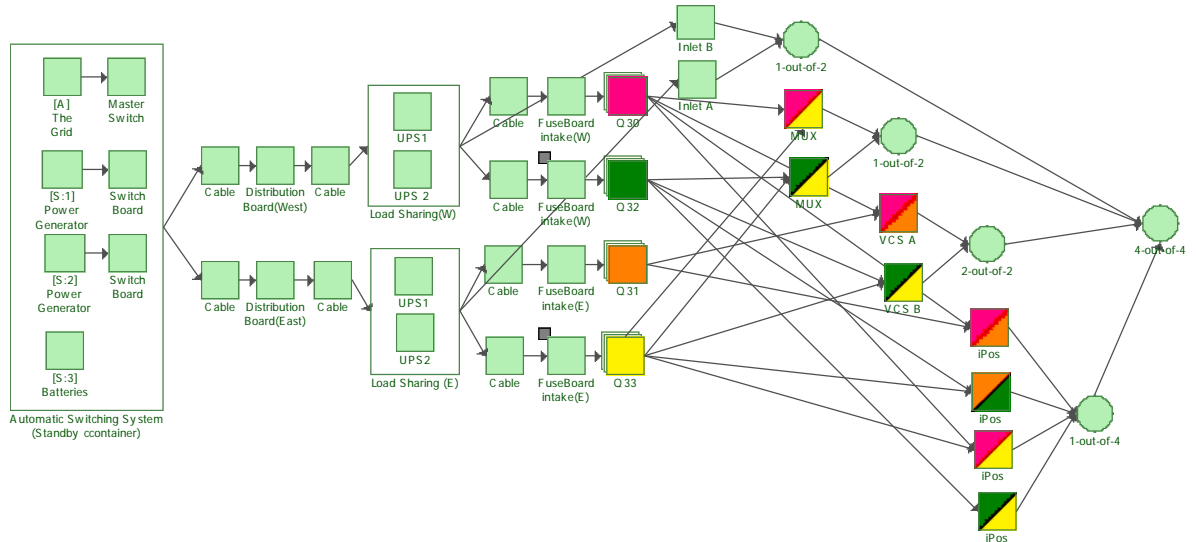
where

$$\begin{aligned}
A &= \lambda_1 + \lambda_{SE} + \lambda_{SWO}, \\
B &= \lambda_{SE} + \lambda_{SWO} + \lambda_2, \\
C &= \lambda_1 - \lambda_{SWO} + \lambda_{SWQ} + \lambda_{2Q} - \lambda_2, \\
D &= \lambda_{SE} + \lambda_2 + \lambda_{SWQ} - \lambda_3 - \lambda_{SWO}, \\
E &= \lambda_1 + \lambda_{2Q} - \lambda_2, \\
F &= \lambda_1 + \lambda_{SE} - \lambda_{SWO} + \lambda_{SWQ} + \lambda_{3Q} - \lambda_3, \\
G &= \lambda_{SWO} + \lambda_3.
\end{aligned}$$

This includes the assumption that there is only one sensing (SE) unit in the system and its function stops as soon as the standby component three is brought into service. As can be seen above the equation has double integrals. If there were n number of components the equation would have n-1 integrals. The same would apply for load-sharing constructs.

## L. First approach

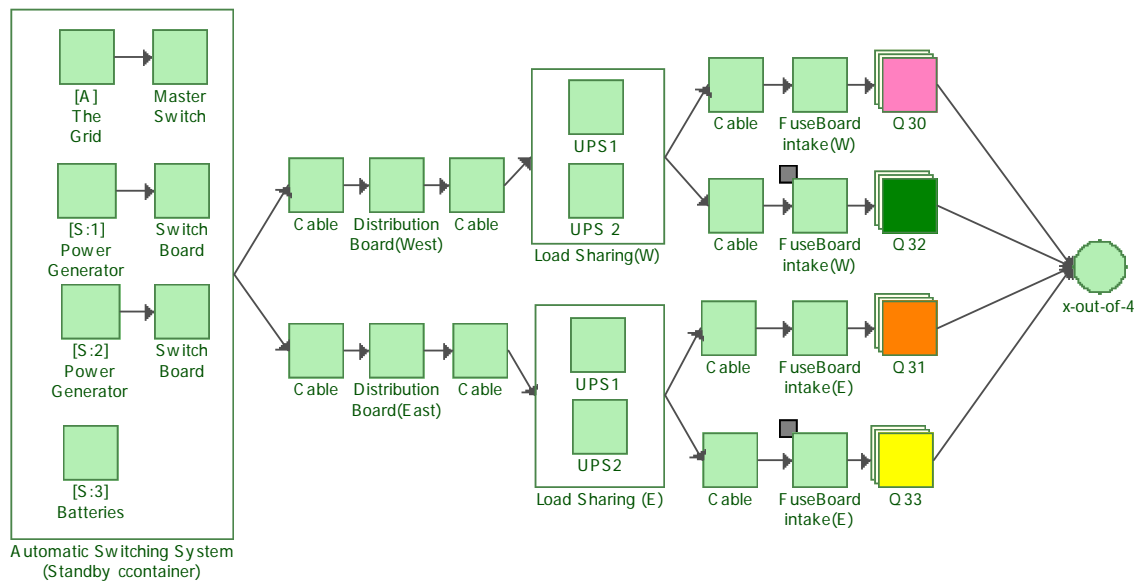
The first approach only included how the ATM equipment is connected to electricity but not how subsystems and equipment is connected to provide the functionality of the system. The figure below shows how the VCS submodel was modeled with this approach.



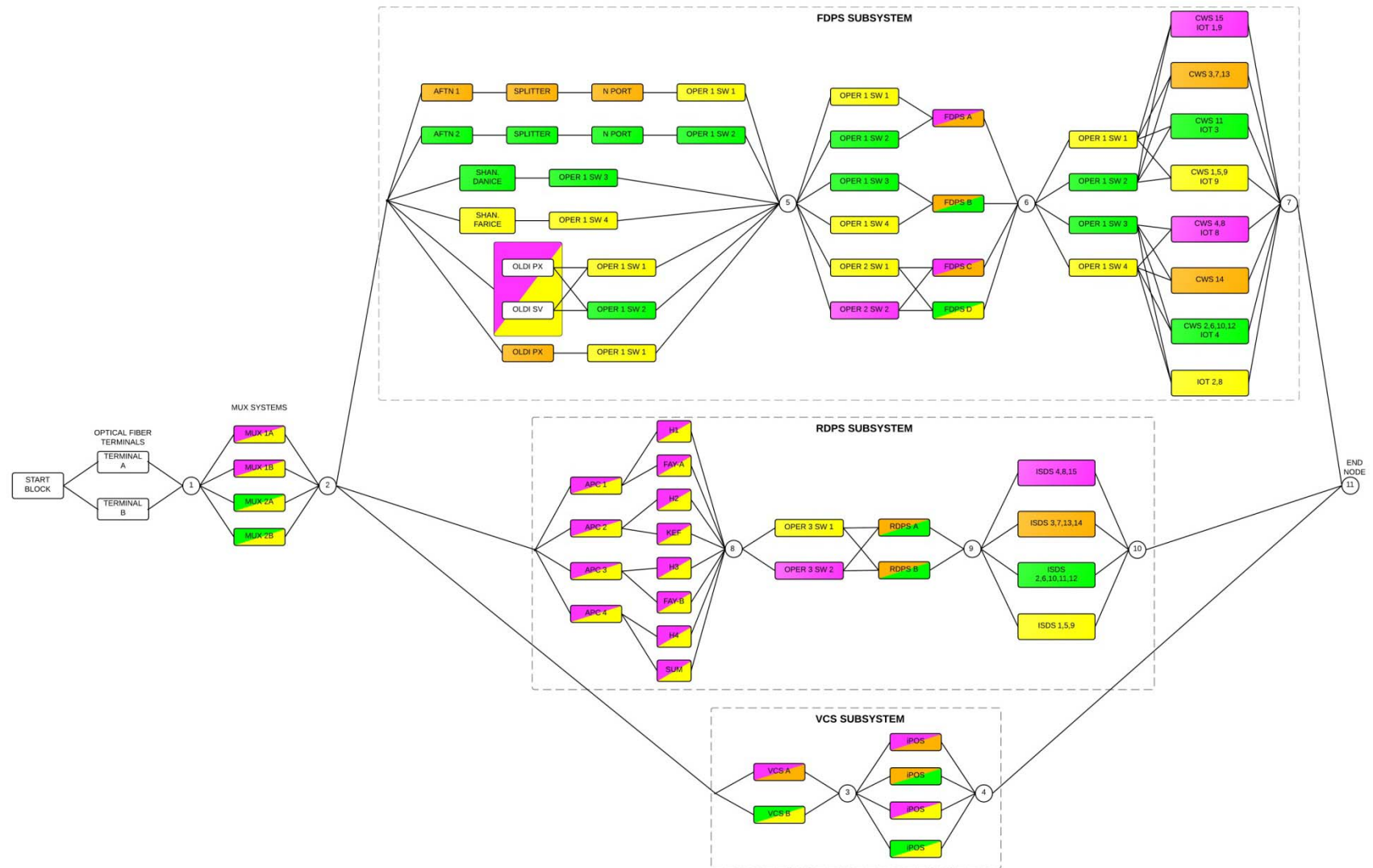


## M. Reliability models

### The Reliability model of the Electrical Power System



## The Reliability model of the ATM System



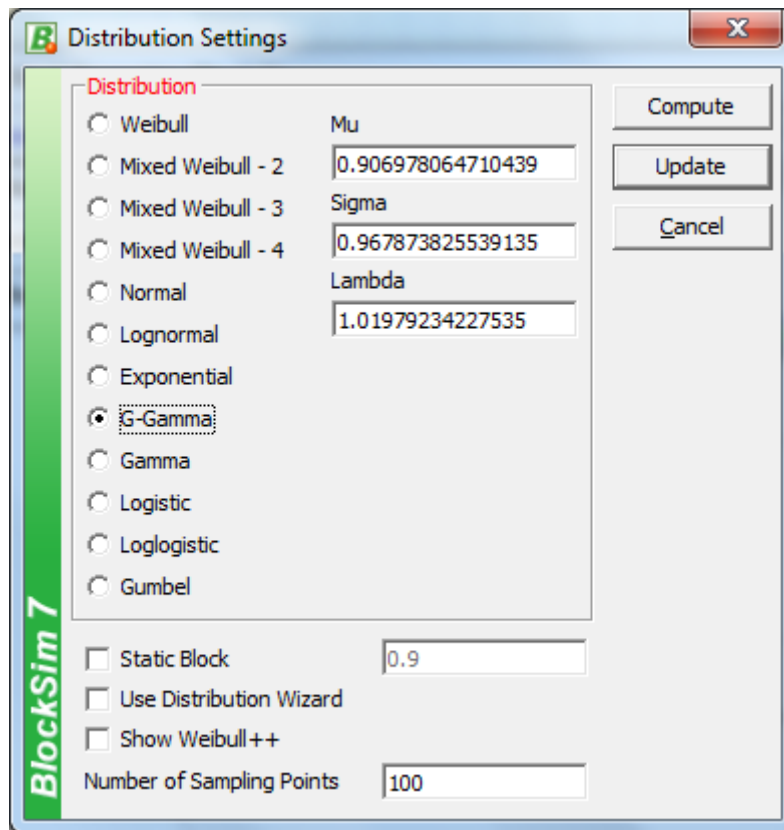
## N. Reliability models

This appendix provides the reliability equation and distribution of the electrical power system for each failure mode.

**The reliability equation for Failure Mode 1 is:**

$$R_s = (R_{\text{Automatic Switching System (Standby ccontainer)}} \cdot R_{\text{x-out-of-4}} (R_{Q32} \cdot R_{\text{FuseBoard terminal(E)}} \cdot R_{Q33} \cdot R_{\text{Cable}} \cdot R_{\text{Cable}} \cdot R_{\text{Cable}} \cdot R_{\text{Cable}} \cdot R_{\text{Cable}} \cdot R_{\text{Cable}} \cdot R_{\text{Load Sharing(W)}} \cdot R_{Q31} \cdot R_{\text{Load Sharing (E)}} \cdot R_{\text{Cable}} \cdot R_{\text{Distribution Board(West)}} \cdot R_{\text{Distribution Board(East)}} \cdot R_{\text{Cable}} \cdot R_{\text{FuseBoard terminal(W)}} \cdot R_{Q30}))$$

**Reliability distribution for Failure Mode 1 is:**



N-1: Shows the distribution that BlockSim recommends for Failure Mode 1.

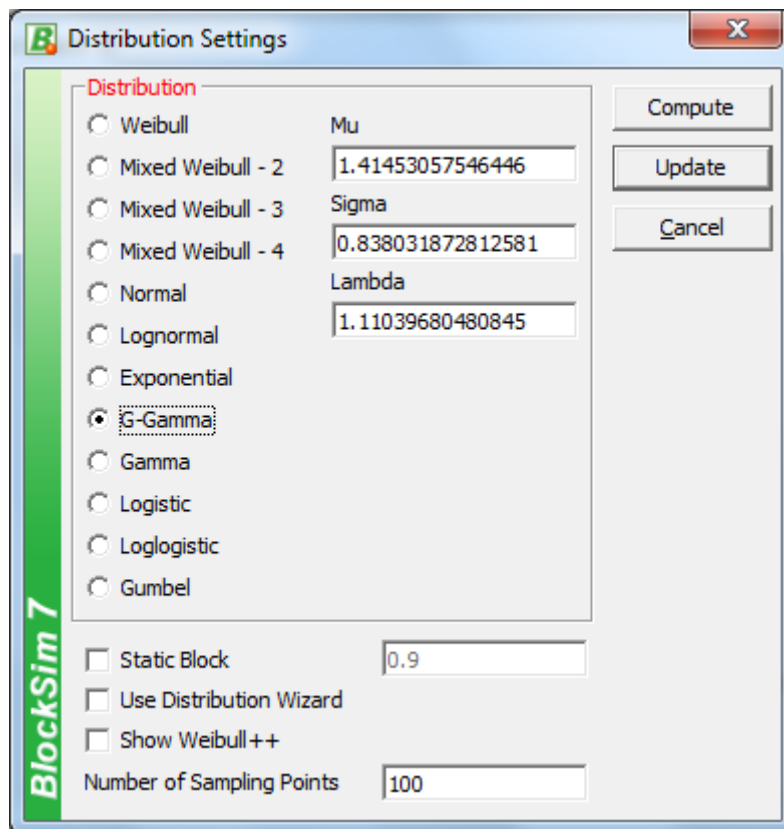
**G-Gamma** is short for generalized gamma distribution. Mu is a scale parameter but sigma and lambda are shape parameters. For information on the G-Gamma distribution, refer to [http://reliawiki.com/index.php/The\\_Generalized\\_Gamma\\_Distribution](http://reliawiki.com/index.php/The_Generalized_Gamma_Distribution).

**The reliability equation for Failure Mode 2 is:**

$$R_s = (R_{\text{Automatic Switching System (Standby ccontainer)}} \cdot R_{\text{x-out-of-4}} (-3R_{Q32} \cdot R_{\text{FuseBoard terminal(E)}} \cdot R_{Q33} \cdot R_{\text{Cable}} \cdot R_{\text{Cable}} \cdot R_{\text{Cable}} \cdot R_{\text{Cable}} \cdot R_{\text{Cable}} \cdot R_{\text{Cable}} \cdot R_{\text{Load Sharing(W)}} \cdot R_{Q31} \cdot R_{\text{Load Sharing (E)}} \cdot R_{\text{Cable}} \cdot R_{\text{Distribution Board(West)}} \cdot R_{\text{Distribution Board(East)}} \cdot R_{\text{Cable}} \cdot R_{\text{FuseBoard terminal(W)}} \cdot R_{Q30} + R_{Q32} \cdot R_{\text{FuseBoard terminal(E)}} \cdot R_{Q33} \cdot R_{\text{Cable}} \cdot R_{\text{Cable}} \cdot R_{\text{Cable}} \cdot R_{\text{Cable}} \cdot R_{\text{Cable}} \cdot R_{\text{Load Sharing(W)}} \cdot R_{Q31} \cdot R_{\text{Load Sharing (E)}} \cdot R_{\text{Cable}} \cdot R_{\text{Distribution Board(West)}} \cdot R_{\text{Distribution Board(East)}} \cdot R_{\text{Cable}} \cdot R_{\text{FuseBoard terminal(W)}} \cdot R_{Q30}))$$

Board(East).RCable.RFuseBoard terminal(W).+RQ32.RFuseBoard  
terminal(E).RQ33.RCable.RCable.RCable.RCable.RCable.RLoad Sharing(W).RLoad Sharing  
(E).RCable.RDistribution Board(West).RDistribution Board(East).RCable.RFuseBoard  
terminal(W).RQ30.+RQ32.RFuseBoard terminal(E).RCable.RCable.RCable.RCable.RCable.RLoad  
Sharing(W).RQ31.RLoad Sharing (E).RCable.RDistribution Board(West).RDistribution  
Board(East).RCable.RFuseBoard terminal(W).RQ30.+RFuseBoard  
terminal(E).RQ33.RCable.RCable.RCable.RCable.RCable.RLoad Sharing(W).RQ31.RLoad Sharing  
(E).RCable.RDistribution Board(West).RDistribution Board(East).RCable.RFuseBoard terminal(W).RQ30))

**Reliability distribution for Failure Mode 2 is:**



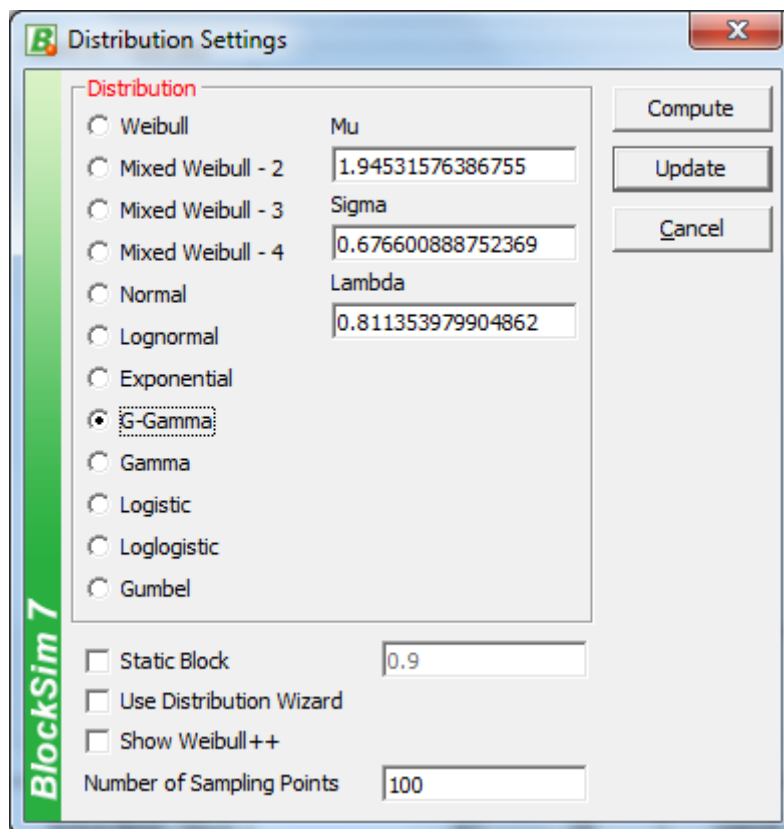
N-2: Shows the distribution that BlockSim recommends for Failure Mode 2.

**The reliability equation for Failure Mode 3 is:**

$R_s = (R_{\text{Automatic Switching System (Standby ccontainer)}} \cdot R_{x\text{-out-of-4}} (3R_{Q32} \cdot R_{\text{FuseBoard terminal(E).RQ33.RCable.RCable.RCable.RCable.RCable.RCable.RCable.RLoad Sharing(W).RQ31.RLoad Sharing (E).RCable.RDistribution Board(West).RDistribution Board(East).RCable.RFuseBoard terminal(W).RQ30 - 2R_{Q32} \cdot R_{\text{FuseBoard terminal(E).RQ33.RCable.RCable.RCable.RCable.RCable.RCable.RLoad Sharing(W).RQ31.RLoad Sharing (E).RCable.RDistribution Board(West).RDistribution Board(East).RCable.RFuseBoard terminal(W) - 2R_{Q32} \cdot R_{\text{FuseBoard terminal(E).RQ33.RCable.RCable.RCable.RCable.RCable.RCable.RLoad Sharing(W).RLoad Sharing (E).RCable.RDistribution Board(West).RDistribution Board(East).RCable.RFuseBoard terminal(W).RQ30 - 2R_{Q32} \cdot R_{\text{FuseBoard terminal(E).RCable.RCable.RCable.RCable.RCable.RLoad Sharing(W).RQ31.RLoad Sharing (E).RCable.RDistribution Board(West).RDistribution Board(East).RCable.RFuseBoard terminal(W).RQ30 -$

2RFuseBoard terminal(E).RQ33.RCable.RCable.RCable.RCable.RCable.RLoad Sharing(W).RQ31.RLoad Sharing  
(E).RCable.RDistribution Board(West).RDistribution Board(East).RCable.RFuseBoard  
terminal(W).RQ30 + RQ32.RFuseBoard terminal(E).RQ33.RCable.RCable.RCable.RCable.RLoad Sharing(W).RLoad  
Sharing (E).RCable.RDistribution Board(West).RDistribution Board(East).RCable.RFuseBoard  
terminal(W) + RQ32.RFuseBoard terminal(E).RCable.RCable.RCable.RCable.RLoad Sharing(W).RQ31.RLoad  
Sharing (E).RCable.RDistribution Board(West).RDistribution Board(East).RCable.RFuseBoard  
terminal(W) + RFuseBoard terminal(E).RQ33.RCable.RCable.RCable.RCable.RLoad Sharing(W).RLoad Sharing  
(E).RCable.RDistribution Board(West).RDistribution Board(East).RCable.RFuseBoard  
terminal(W).RQ30 + RFuseBoard terminal(E).RCable.RCable.RCable.RCable.RLoad Sharing(W).RQ31.RLoad  
Sharing (E).RCable.RDistribution Board(West).RDistribution Board(East).RCable.RFuseBoard  
terminal(W).RQ30 + RQ32.RCable.RCable.RCable.RLoad Sharing(W).RDistribution  
Board(West).RCable.RFuseBoard terminal(W).RQ30 + RFuseBoard  
terminal(E).RQ33.RCable.RCable.RCable.RQ31.RLoad Sharing (E).RCable.RDistribution Board(East)))

**Reliability distribution for Failure Mode 3 is:**

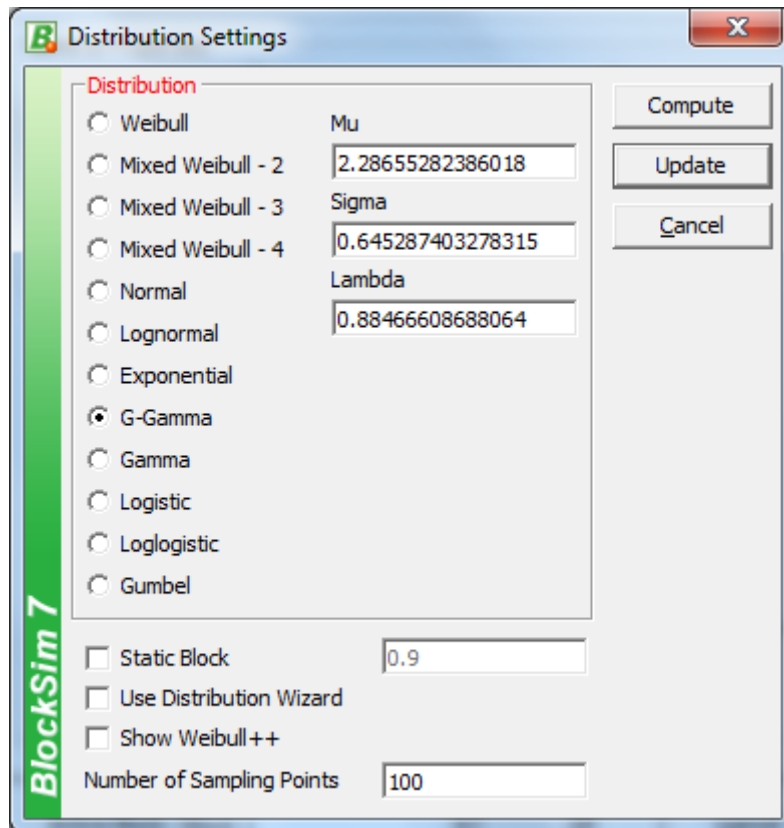


N-3: Shows the distribution that BlockSim recommends for Failure Mode 3.

**The reliability equation for Failure Mode 4 is:**

$$R_s = (\text{RAutomatic Switching System (Standby container)} \cdot R_{x\text{-out-of-4}} (-RQ32 \cdot RFuseBoard$$
  
terminal(E) · RQ33 · RCable · RCable · RCable · RCable · RCable · RCable · RLoad Sharing(W) · RQ31 · RLLoad Sharing  
(E) · RCable · RDistribution Board(West) · RDistribution Board(East) · RCable · RFuseBoard terminal(W) · RQ30 + RQ32 · RFuseBoard terminal(E) · RQ33 · RCable · RCable · RCable · RCable · RCable · RLLoad  
Sharing(W) · RQ31 · RLLoad Sharing (E) · RCable · RDistribution Board(West) · RDistribution  
Board(East) · RCable · RFuseBoard terminal(W) + RQ32 · RFuseBoard terminal(E) · RQ33 · RCable · RCable · RCable · RCable · RCable · RLLoad Sharing(W) · RLLoad Sharing  
(E) · RCable · RDistribution Board(West) · RDistribution Board(East) · RCable · RFuseBoard terminal(W) · RQ30 + RQ32 · RFuseBoard terminal(E) · RCable · RCable · RCable · RCable · RCable · RLLoad  
Sharing(W) · RQ31 · RLLoad Sharing (E) · RCable · RDistribution Board(West) · RDistribution  
Board(East) · RCable · RFuseBoard terminal(W) · RQ30 + RFuseBoard terminal(E) · RQ33 · RCable · RCable · RCable · RCable · RCable · RLLoad Sharing(W) · RQ31 · RLLoad Sharing  
(E) · RCable · RDistribution Board(West) · RDistribution Board(East) · RCable · RFuseBoard terminal(W) · RQ30 -  
RQ32 · RFuseBoard terminal(E) · RQ33 · RCable · RCable · RCable · RCable · RCable · RLLoad Sharing(W) · RLLoad Sharing  
(E) · RCable · RDistribution Board(West) · RDistribution Board(East) · RCable · RFuseBoard terminal(W) -  
RQ32 · RFuseBoard terminal(E) · RCable · RCable · RCable · RCable · RLLoad Sharing(W) · RQ31 · RLLoad Sharing  
(E) · RCable · RDistribution Board(West) · RDistribution Board(East) · RCable · RFuseBoard terminal(W) - RFuseBoard  
terminal(E) · RQ33 · RCable · RCable · RCable · RCable · RLLoad Sharing(W) · RLLoad Sharing (E) · RCable · RDistribution  
Board(West) · RDistribution Board(East) · RCable · RFuseBoard terminal(W) · RQ30 - RFuseBoard  
terminal(E) · RCable · RCable · RCable · RCable · RLLoad Sharing(W) · RQ31 · RLLoad Sharing (E) · RCable · RDistribution  
Board(West) · RDistribution Board(East) · RCable · RFuseBoard terminal(W) · RQ30 - RQ32 · RCable · RCable · RCable · RLLoad  
Sharing(W) · RDistribution Board(West) · RCable · RFuseBoard terminal(W) · RQ30 - RFuseBoard  
terminal(E) · RQ33 · RCable · RCable · RCable · RQ31 · RLLoad Sharing (E) · RCable · RDistribution  
Board(East) + RQ32 · RCable · RCable · RLLoad Sharing(W) · RDistribution Board(West) · RCable · RFuseBoard  
terminal(W) + RFuseBoard terminal(E) · RQ33 · RCable · RCable · RLLoad Sharing (E) · RCable · RDistribution  
Board(East) + RFuseBoard terminal(E) · RCable · RCable · RQ31 · RLLoad Sharing (E) · RCable · RDistribution  
Board(East) + RCable · RCable · RLLoad Sharing(W) · RDistribution Board(West) · RCable · RFuseBoard  
terminal(W) · RQ30))

**Reliability distribution for Failure Mode 4 is:**



The image shows the 'Distribution Settings' dialog box from BlockSim 7. The dialog has a title bar with the BlockSim logo and a close button. On the left side, there is a vertical green bar with the text 'BlockSim 7'. The main area is titled 'Distribution' in red. It contains a list of distribution types with radio buttons: Weibull, Mixed Weibull - 2, Mixed Weibull - 3, Mixed Weibull - 4, Normal, Lognormal, Exponential, G-Gamma (selected), Gamma, Logistic, Loglogistic, and Gumbel. To the right of these options are input fields for parameters: Mu (2.28655282386018), Sigma (0.645287403278315), and Lambda (0.88466608688064). Below the distribution list, there are three checkboxes: 'Static Block' (unchecked), 'Use Distribution Wizard' (unchecked), and 'Show Weibull++' (unchecked). At the bottom, there is a 'Number of Sampling Points' field set to 100. On the right side of the dialog, there are three buttons: 'Compute', 'Update', and 'Cancel'.

Parameter	Value
Mu	2.28655282386018
Sigma	0.645287403278315
Lambda	0.88466608688064

Static Block: ☐ 0.9

Use Distribution Wizard: ☐

Show Weibull++: ☐

Number of Sampling Points: 100

N-4: Shows the distribution that BlockSim recommends for Failure Mode 4.