Systems-Based Risk Analysis for the NextGen Integration of the Communication, Navigation, and Surveillance System of Systems (S-o-S)

A Thesis

Presented to

the faculty of the School of Engineering and Applied Science

University of Virginia

In partial fulfillment

of the requirements for the degree

Master of Science

By

Bryan R. Lewis

May

2015

APPROVAL SHEET

The thesis

is submitted in partial fu\lfillment of the requirements

for the degree of

Master of Science

Author: Bryan R. Lewis

The Thesis has been read and approved by the examining committee:

Dr. Yacov Y. Haimes

Advisor

Dr. Barry M. Horowitz

Committee Chairman

Dr. Garry M. Jacyna

Mr. Mark Huberdeau

Dr. Michael Smith

Accepted for the school of Engineering and Applied Science:

Dean, School of Engineering and Applied Science

May 2015

Abstract

The Federal Aviation Administration (FAA) is in the transition between the alpha and bravo periods of a long term plan to modernize the National Airspace System (NAS) called NextGen. This plan, currently slated through 2030, sets out to meet four main goals: increase safety, capacity, and efficiency while mitigating environmental impacts of the airspace. One of the many areas of change within NextGen occurs as part of the current Communication, Navigation, and Surveillance (CNS) System of Systems (S-o-S). Currently this system operates semi-autonomously with no explicit dependencies within each system and while it must be used in sync to perform a specific operation, there is no apparent single point of failure for all three systems. Future technologies will move away from this semi-autonomous mode and approach a fully integrated CNS as S-o-S. The lack of opportunities to extensively test these changes to the S-o-S prior to the go-live date creates a need for a way to model and understand possible risks to the S-o-S. This thesis provides a systems-based risk analysis framework for key areas that threaten the operation of the CNS as S-o-S, as well as the safety of the airspace. This thesis will also provide a framework focused on utilizing three different perspectives of a S-o-S, operational, structural, and organization. These different perspectives are used to determine potential risk scenarios and to explore key scenarios that would have the largest negative impact within the CNS. The framework developed in this thesis can be used and applied to other complex emergent Systems of Systems to ensure a systematic and comprehensive risk analysis covering the most critical perspectives of a system. While tradeoff analysis is a key aspect of risk analysis and should not be overlooked in a full risk assessment and management project it is beyond the scope of this thesis. The risk framework builds foundations on which the FAA can make well-informed decisions on the integration of the CNS system of systems within the NextGen Project.

Acknowledgements:

I would like to thank a few of the many people who have helped me along the journey of writing this thesis and whom without it would not have been possible. First and foremost I would like to acknowledge and thank my advisor, Yacov Haimes. Professor Haimes has played many roles throughout the process from research advisor to teacher to mentor. I never knew what an impact Professor Haimes would have throughout my 2 years of courses and research at the University of Virginia. My way of thinking has been radically changed throughout my time here and many of these changes have occurred in total or in part by the positive influence of Professor Haimes. Whether it was our frequent meetings or drives to MITRE Professor Haimes always challenged me to think of problems in a new way and to challenge myself. His insights led well beyond risk analysis to systems thinking and modeling and furthermore to philosophy and life. It has been an incredible journey with Professor Haimes and I cannot thank him enough for the investment he has made in me. I am proud to say that I stand on the shoulders of this giant.

Thank you to Rosemary Shaw, the manager of the Center for Risk Management of Engineering Systems, for all that she has done to help this research and myself over the course of my Masters work. Rosemary has been a bright face in the morning and quick to help whenever I might be in need. There is no doubt that she was vital in my successful completion of this program, both my Thesis and my coursework.

The team from MITRE deserves more thanks than I could possibly give for their help in completing my Thesis. Mark Huberdeau, Frank Willingham, and Deihim Hashemi provided invaluable support from day one of this thesis. The team at MITRE helped guide me to narrow the scope of my work and provide a meaningful path for addressing the risk analysis of CNS Integration. Without their constant steering of the project I would still be lost in the clouds or the weeds. I am thankful for their guidance and approach to the problem at our frequent meetings at MITRE over the past two years.

My committee members, Dr. Barry Horowitz, Dr. Garry Jacyna, Mr. Mark Huberdeau, and Dr. Michael Smith were incredibly helpful in aiming my thesis toward its completion. The discussions

we had during my proposal, and finally my defense, were engaging and thought provoking. These great minds filled my mind with many possible future research topics. Thank you.

I would like to thank my parents, Charlie and Janis Lewis, for their constant love and support throughout this journey. I thank my dad for constantly being a voice of reason and encouragement whenever I was struggling. I thank my mom for her unconditional love, support, and belief in me. Furthermore I would like to thank my sister, Robyn, for her joy and happiness. Never could I call her and not be happy in the moment.

To the other mentors I have learned so much from while at the University of Virginia, I cannot thank you enough. Your words of advice, encouragement, and knowledge were invaluable. Special thanks to Lee Coppock and Saul Yeaton for the time we spent running or riding together meant more to me than you can imagine.

Finally, thank you to the close friends that supported me along the way. Blake Sinyard for showing me how to work hard and do your best, Jack St. Marie for understanding the complex balance of athletics and academics, Sean Keveren for always reminding me I was too stressed and doing fine and Austin McPhillips for giving me a friend to struggle through the job search with.

To the many others who helped along the way, thank you.

Table of Contents

Appendices

Figures

Tables

Part I: Introduction

1. Problem Definition and Motivation

The Federal Aviation Administration (FAA) is currently in a transition between the alpha and bravo phases of a long-term project to modernize the National Airspace System (NAS). The NextGen project utilizes existing and new technologies to meet the four primary goals of the FAA: Improve efficiency, capacity, and safety, while mitigating the environmental effects of the NAS. The NAS is a portion of one of the 16 Critical Infrastructure (CI) Systems (Transportation System Sector) as determined by the Department of Homeland Security (DHS). The Critical Infrastructure is considered as the backbone of the United State's economy, security, and health. The System of Systems that makes up the CI is considered to be so vital to the U.S. that any significant degradation or destruction to any particular system would significantly hamper the nation's security, economy, public health, safety, or a combination of the above [Homeland Security].

The NextGen Project works on improving many areas within the NAS but two main changes can be considered the main drivers of the project: Further utilization of GNSS (Global Navigation Satellite System, also GPS) technology and the integration of the Unmanned Aerial Vehicles (UAVs) into the airspace. Both considerations promise great advances to the current NAS but also come with their own risks. The increased utilization of GPS motivates this project.

Falling under the so-called GPS umbrella, a portion of the NextGen project revolves around the improvements to the current Communication, Navigation, and Surveillance (CNS) System of Systems (S-o-S). The Communication, Navigation, and Surveillance (CNS) System of Systems (S-o-S) is currently operating semi-autonomously. While multiple systems are required to perform a specific operation there is no single point of failure for the S-o-S. The utilization of new technologies, as currently

proposed through the NextGen project, will lead the CNS System of Systems toward a much higher level of integration. In the proposed future there will be significantly more interconnections and interactions across the three main systems involved.

The integration of the CNS as S-o-S from the current separated S-o-S is promised to bring many benefits. That being said such an integration is not without its risks. The extreme caution necessary when dealing with the NAS cannot be understated when considering the actions necessary to complete such a complex integration of an emerging S-o-S. The rate of failure must be so significantly low that it can almost be considered zero before moving forward. Furthermore the change from a system specifically built without a single point of failure to an integrated S-o-S is likely to cause concern among the current decision makers and stakeholders of the NAS.

Currently the FAA is considering multiple configurations for the CNS system, each configuration builds on the prior configuration and moves further toward a fully integrated S-o-S. The three configurations being considered by the FAA are Dynamic RNP, Pairwise Procedures, and Pairwise Procedures coupled with NextGen Safety technology. Each configuration represents a further step toward integration and is further explained in Chapter 3: Technical Understanding of CNS System of Systems.

Without the ability to perform extensive testing of these configurations prior to implementation the FAA must find a way to determine what problems could occur in the completion of this integration. As with any complex and emergent S-o-S there must be a means to determine where these risks may come from and what can be done about them.

To tackle the problem this research explores the level of interconnectedness and interdependency among the three systems, Communication, Navigation, and Surveillance, through three distinct

perspectives of a system: Operational, Structural, and Organizational. Modeling the system by determining interconnections and interdependencies across the CNS as S-o-S through Shared Factors, including shared states, decisions, decision makers, and resources. The research builds on the operational perspective from shared states by determining key risk scenarios and then uncovering the structural vulnerabilities that are inherent to these key risk scenarios. Finally the organizational perspective considers the internal and external organizational changes that may cause further problems to the S-o-S.

This research establishes a methodological approach for analyzing a complex emergent S-o-S integration through these three perspectives: operational, structural, and organizational. The use of shared factors, Risk Filtering, Ranking, and Management (RFRM), and Fault Tree Analysis build the foundation for which this methodology stands on. This assessment of risk lays a modeling foundation that can be used for further analysis with the CNS integration process or for other complex emergent Systems of Systems.

Modeling a complex emergent S-o-S requires an iterative approach that encapsulates these multiple perspectives and representative models. To model the S-o-S it is vital to understand the interconnections, interdependencies, and interactions and the associated risks that occur from the coupling of the CNS. Models should be as simple as possible, yet as complex as required. While the modeling efforts within this thesis does not encompass a full of each system and sub-systems it lays a foundation for which further analysis could be completed as deemed necessary.

The three perspectives provide a unique and systematic approach to considering the interconnections of the S-o-S. Exploring the operational perspective through shared states provides a high level view of the S-o-S in determining interconnections and interdependencies. Studying the structural perspective allows a closer look at key components and key component systems within a

complex S-o-S providing crucial detail within risk analysis. Furthermore, structural interconnections and interdependencies can be discovered and we posit, linked, to the shared factors determined when exploring the operational perspective through shared states. The organizational perspective ensures that a complete model is created that does not leave out changes to the organization and world that the current S-o-S operates. All three are vital to completing a full systematic risk assessment of a complex emergent S-o-S.

While this thesis lacks the information necessary to provide the tradeoffs of the benefits and risks from this integration the modeling framework sets forth a foundation for which to further build such analysis. In combination with further work using this modeling structure and the inclusion of the proposed or determined benefits of the integration the FAA will be able to determine the best course of action to take with regards to the CNS integrations. This these can further provide a framework for further work within the CNS integration but also across any complex emergent S-o-S in question both within the Critical Infrastructure system and outside of the CI system.

2. Literature Review

With the FAA Business Review determining that there is an expected $133 billion of benefit to be gained through changes to the NAS between 2013 and 2030 there is a significant push to increase the efficiency and capacity in the airspace. Furthermore the FAA plans to increase safety while decreasing the environmental affects in hopes of improving overall welfare. The increased utilization of GPS technologies to perform advanced capabilities such as Dynamic Required Navigational Performance (RNP) and Pairwise Procedures represent significant advancements that could lead to such a savings.

The example of the framework provided in this thesis explores the risks with the introduction of the Dynamic Required Navigational Performance configuration. There has been limited work on the

Dynamic RNP capability and while the work that has been completed holds promise there are questions as to its readiness for use in the NAS (Nakamura and Royce 2008, Finkelsztein 2011, and Butchibabu et. al.). Study of the CNS system of systems was done through FAA and MITRE documents and presentations along with meetings with subject matter experts at MITRE held throughout the time of our contract.

The modeling methodology for approaching our risk analysis built on the work of others both on understanding a complex S-o-S and on assessing and managing a complex S-o-S. While many different fields define and understand S-o-S differently (Sage and Cuppan 2001, Sage and Briemer 2007). For this research we build on the properties suggested by Maier (1998).

i. Operational Independence of the Individual Systems
ii. Managerial Independence of the Systems
iii. Geographic Distribution
iv. Emergent Behavior
v. Evolutionary

Recent work from Haimes (2012, 2016), Haimes and Anderegg (2015), Crossely, Held (2008), and Luzeaux, Ruault & Wippler (2011) laid the groundwork for understanding and managing a large scale S-o-S. The breakdown of the organizational prospective into four key factors of vertical, horizontal, external and geographicals was built upon the *The Boundaryless Organization: Breaking the Chains of Organizational Structure* by Ronald Ashkenas.

The work presented by Haimes (2009) in *Risk modeling, assessment, and management* set the foundation for the risk analysis framework such as shared states and risk filtering ranking and management framework. Further work from Haimes (2012), MITRE (2007), and Garvey (2008) further defines the methodology for managing risk in a large scale complex emergent System of Systems. The

FAA's *Safety Management System Manuel (Version 4)* was also used to understand and build on the FAA's current process for safety analysis and risk management process.

The work of Bogdanor (2014) was inspirational in considering the connections between Fault Tree Analysis and Shared Factors. Furthermore his work on GPS timing and S-o-S interconnections and interdependencies provided a jumping off point for my continued work on emergent S-o-S integration with the CNS S-o-S.

3. Technical Understanding of the CNS as System of Systems

The S-o-S for which we will be conducting this risk analysis is comprised of three major systems: Communication (C), Navigation (N), and Surveillance (S) (**Figure 3.1**). Navigation is considered the Pilot's responsibility and is aided by the Flight Management System. The Flight Management System automates many in flight tasks, most notably it includes all components necessary to guide the plane along it's flight plan. This includes the Flight Management Computer, Control Display Unit, and Navigational Aid. Surveillance is considered the Air Traffic Controller's responsibility used to determine aircraft position and spacing within the airspace. Most notably different types of Radar are used to determine positioning but recent advances in GPS technology have increased GPS utilization within the Surveillance system. Surveillance system often includes on ground surveillance as well as in flight surveillance but only in flight surveillance is considered within this thesis. The Communication system represents the connection between the Navigation and Surveillance systems. The Communication system can be divided into Voice Communication and Data Communication sectors, both playing a role in the successful flight of an aircraft.

Currently four separate configurations are being considered with regards to the Communication, Navigation, and Surveillance (CNS) Integration. These four configurations, current configuration,

Dynamic Required Navigational Performance (RNP) configuration, Pairwise Procedures configuration, and the Pairwise Procedures including NextGen Safety Capabilities configuration, are each a step further along the path to integration. This thesis outlines a framework to consider the risks of each configuration but only uses the current and Dynamic RNP configurations as an example of how to approach this problem of complex emerging S-o-S.

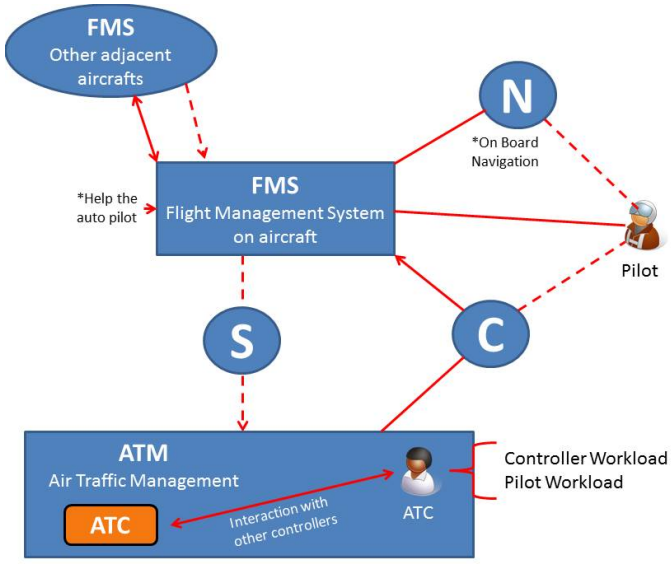


Figure 3.1 – System Model

3.1 Navigation System

The Navigation system is largely considered the pilot's role and responsibility within the NAS. The Navigation system is based around the Flight Management System, which provides the primary navigation, flight planning, and optimized route determination for an aircraft. The Navigation system is then composed of all systems used to perform these actions. Specifically Navigational Aids, the Flight Management Computer coupled to the Control Display Unit (CDU), and the Pilot him/herself (The Avionics Handbook). Of course, other systems can be considered that link to the autopilot function of

the plane. These considerations are left out of this analysis. The navigational aids provide waypoint directions, the computer determines the appropriate path to the waypoint route received from the initial clearance, and the pilot monitors the system and adjusts clearances as necessary. The pilot also has final say in determination of flying by hand or using the autopilot system.

3.1a Current Configuration

The current configuration uses the Flight Management System (FMS) for most navigating in the National Airspace System (NAS). The Flight Management Computer (FMC) collects the flight plan from Air Traffic Control (ATC) prior to leaving the gate. The pilot accepts the clearance and follows ATC instructions for takeoff. After take off the pilot may switch to auto-pilot through the FMS system. The FMS system then uses current Navigational Aids, most often GPS, backed up by radio navigation aids such as Distance Measuring Equipment and VORs. The altitude and spacing is determined by the ATC. The aircraft spacing and required navigational performance (RNP) is determined prior to takeoff. The RNP is a type of performance-based navigation (PBN) that allows the aircraft to fly a path between two 3D-defined points. RNP also refers to a level of performance required for an airspace. These systems do not required the use of the communication or surveillance systems once they have left the gate. Changes in altitude, vectoring, and landing directions are all examples of operations that may require joint use of multiple systems within the CNS, but in the current configuration, neither Communication or Surveillance are required to be working to Navigate within the NAS.

3.1b Dynamic RNP

With the implementation of the Dynamic RNP capability the system will begin the process of integration through need for a new data communication subsystem. The Dynamic Required Navigational Performamne (DRNP) capability enhances present and future Trajectory Based Operations

by expanding RNP operations to live uplink of RNP values on a leg-by-leg basis, radius to fix legs, and fixed radius transitions. The key is the ability to adjust the route or RNP value in time, versus a fixed pre-determined value (Buntin and Dutton). An RNP value is determination of the lateral accuracy of the system. For example, an RNP value of 1, represented in nautical miles (nm), indicates that an aircraft must be within 1nm radius of that position 95% per flight hour, and within a 2nm radius 99.9% per flight hour, as indicated by Figure 3.2 [Dynamic RNP Concept of Operations]. Certain RNP values, such as 0.3, would actually violate current separation standards and require an adjustment to existing standards before gaining expected efficiency and capacity benefits.

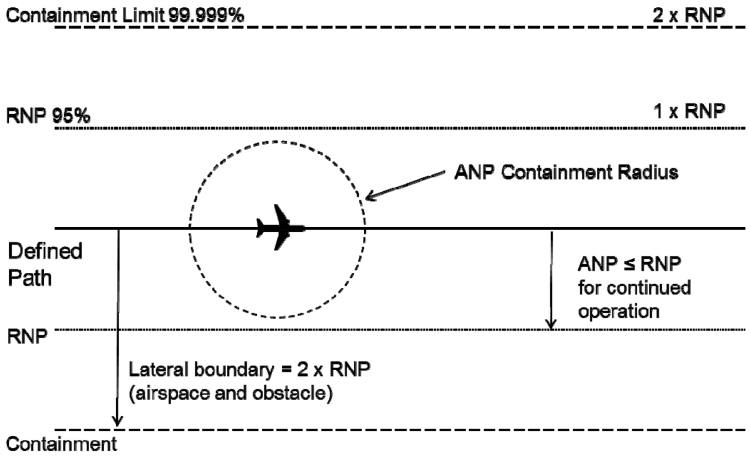


Figure 3.2 – RNP Explanation [Dynamic RNP Concept of Operations]

In order to perform the Dynamic RNP value a DataLink capable of pushing the significantly larger data bites will be required. This will be completed through the use of the Aeronautical Telecommunications Network Baseline 2 (ATN-B2) data communication link.. This begins the integration of the CNS as S-o-S by coupling the Navigation and Communication systems.

The Dynamic RNP capability is being considered for four main applications: Efficient Departure Applications, En Route Rerouting with Metering, Efficient Descent Arrival, and Metroplex situations. As

this Thesis builds a framework for this ambitious risk analysis project our example will only look at the approach phase of flight in regards to Dynamic RNP.

In the terminal airspace, arrivals and departures, Dynamic RNP is expected to provide benefits by better accommodating weather, traffic, special activity airspace as well as gate changes. The automation of the terminal space is expected to provide the many benefits Dynamic RNP promises. Dynamic RNP will allow for the automation of departure runways and routes, departure schedule, path adjustments necessary to meet schedule and metering constraints. The benefits expected include reduced lateral spacing (dependent on policy changes), diminished ground delays, more accurate departure trajectories, and increased fuel efficiency through optimized climb profiles.

The Enroute Phase provides many similar benefits to the terminal environment including the creation of new metered traffic flows to accommodate weather, traffic, and Special Activity Airspaces. One of the ways Dynamic RNP increases efficiency and capacity is the ability for faster aircraft to overtake slower aircraft through RNP offset routes [Buntin, Marc, and John Dutton].

3.1c Pairwise Procedures

Further capabilities will build on this integration, the next consideration, Pairwise Procedures, will require the coupling of all three systems. Advanced Interval Management uses Automatic Dependent Surveillance – Broadcast (ADS-B) to provide precise interval spacing among aircrafts and ATN-B2 to push the large amount of data necessary to make the system work. Current Interval Management is performed by the ATC speaking with the pilot and adjusting their speed and heading through the voice communication system.

Advanced IM is enabled by ADS-B that uses ground and flight deck capabilities to provide avionics calculated speeds to the flight deck of another aircraft and uses the information to meet a specific

spacing determined by the Air Traffic Controller (ATC). The main proposed benefit is to improve inter-aircraft spacing precision within the NAS to increase throughput and lead to a reduction in separation standards. This reduction in separation standards is expected to allow an increased flow in the terminal and en route environment (**Figure 3.3**). To perform this capability both ADS-B (Surveillance) and ATN-B2 (Communication) must be working. ADS-B Out provides the lead aircrafts position and speed and using ATN-B2 the follow aircraft who collects the information using ADS-B In. This information creates a time based flow management that allows the follow aircraft to meet the separation distance specified by the ATC.

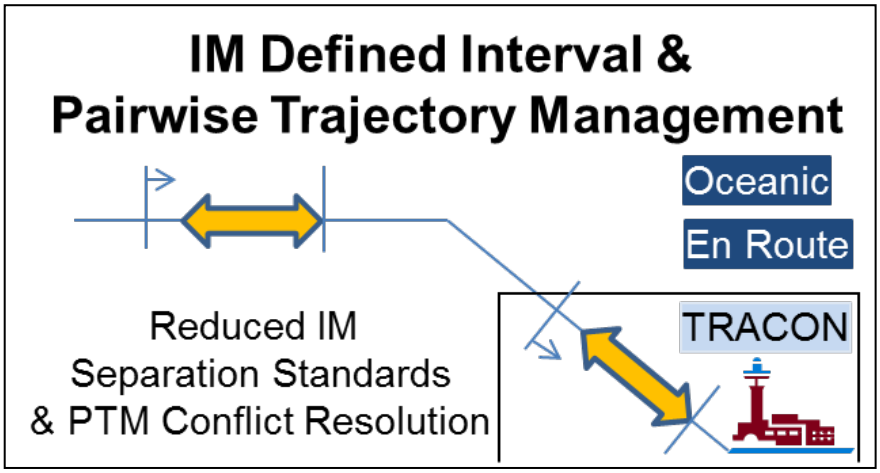


Figure 3.3 [Moertle]

Other capabilities of Advanced IM include the insertion of an aircraft in to the overhead stream and parallel runway approaches (**Figure 3.4 and 3.5**).

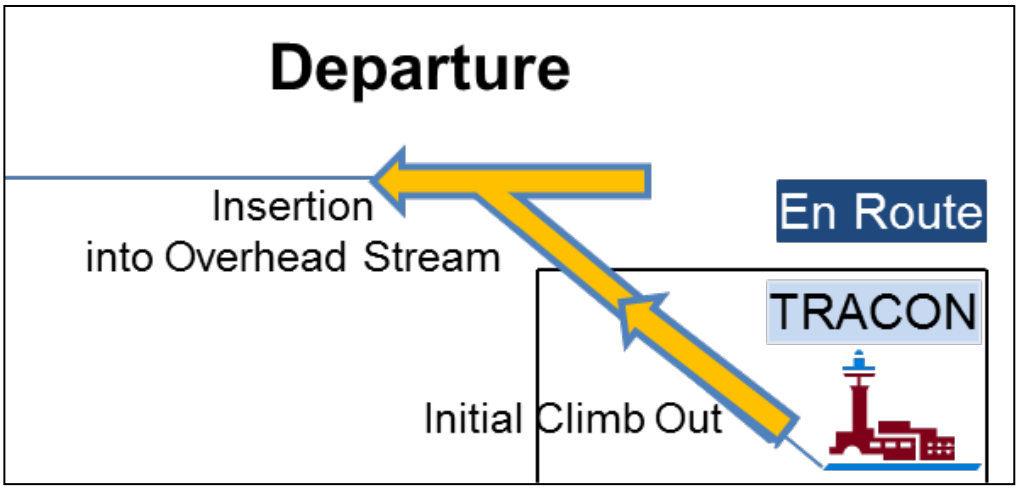


Figure 3.4 [Moertle]

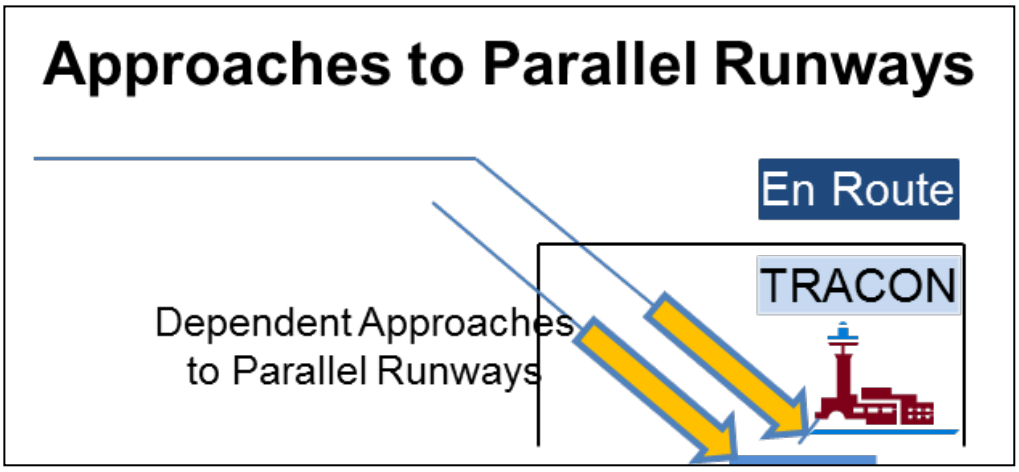


Figure 3.5 [Moertle]

3.2 Surveillance System

The Surveillance System is primarily considered the Air Traffic Controller's responsibility in managing aircraft flow and separation in their designated airspace. The current configuration of the Surveillance system uses a large array of radars. Radars can be divided in to two types: Primary and Secondary. The main differentiator between the two is the Secondary Radar's need for a response from the aircraft to display position on the radarscope while Primary requires no input from the aircraft. A new surveillance technology, Automatic Dependent Surveillance Broadcast (ADS-B), which utilizes GPS, is beginning to be

used in the NAS. ADS-B is an aircraft based surveillance system. The aircraft itself determines its position via satellite position (GPS) and broadcasts it so that that air traffic controllers can track it. The system occurs in the background such that no pilot or ATC input is needed for the function to perform.

The system can further be divided into two sub-sectors: ADS-B In and ADS-B Out. ADS-B Out is the system that sends out the position of the aircraft and is currently seeing some use in the NAS. ADS-B In is the capability of the system to accept the position of other aircrafts using ADS-B. The ADS-B In system will be used to implement the Advanced IM capability discussed previously. ADS-B In is often considered as an integration of the Communication and Surveillance systems as a data communication link is necessary to receive the broadcasts.

While this thesis focuses on the use of ADS-B as an enabling technology for Advanced IM there are many other proposed uses that are not discusses within this paper. These uses can be split to three sections of the airspace: Air-to-Air, Ground-to-Ground, and Air-to-Ground. Advanced IM is included in the Air-to-Air sector but other improvements come from improved low-visibility approaches and enhanced see. Ground-to-Ground improvements come from better taxiway navigation and better surface traffic management from the ATC. ADS-B also provides the ability to increase surveillance coverage in non-radar airspace (Air-to-Ground). While not discussed in detail here the framework provided could well suit a risk analysis of the entire ADS-B implementation.

3.3 Communication System

The Communication system can be separated in to two categories: Voice Communication and Data Communication. The current system relies heavily on Voice Communication between the pilot and air traffic controller. This connection will likely never fully disintegrate but the CNS integration will rely on data communications heavier then it ever has before.

3.3a Current Voice and Data Comm

Currently the voice communication system is accomplished by radio broadcasting and receiving on three major frequencies: UHF, VHF, or HF. The ATC will hand off the pilot when leaving a defined controller airspace. Adjustments to the frequency are required to stay in contact with the controller in the new airspace. Voice Communication is used for many operations within the NAS, most notably, it is used to vector aircrafts to specific approach points. Furthermore voice communication is used to avoid weather, maintain specific separation, ask for and receive altitude corrections, and any other pilot-controller communications.

The current data communication system, Aircraft Communication Addressing and Reporting System (ACARS) is used to push small text data to and from the aircraft. It is completed through a network of ground radio transceivers and a transceiver onboard the aircraft coupled to the Flight Management Computer and its display. The communication is limited to initial flight plan loading, text messages, weather updates, and terminal conditions. Data sent along the ACARS system can be sent by ATC but also sent and received from the airline to determine information regarding delays, weather, and airport changes. The Short Burst Data (SBD) used for the ACARS system will not be viable to send the large amount of data needed for the capabilities described above.

3.3b Aeronautical Telecommunications Network – Baseline 2 (ATN-B2)

The Aeronautical Telecommunications Network – Baseline 2 (ATN-B2) is a new data communication system created to solve this specific problem. ATN-B2 uses a large network of Intermediate Systems or ATN routers to wirelessly transmit large amounts of data quickly and efficiently to the aircrafts originating from any number of different end systems (**Figure 3.6**). The information can be sent over a range of air ground sub networks including VDL-3, VDL-2, SATCOM, and HF). This system will be

necessary to complete many of the NextGen Capabilities the FAA intends to implement. Four major elements will be key for ATN-B2 use in the NextGen environment.

1) Network Mobility - It must be able to transfer data to an aircraft without sender knowledge of the aircraft's location
2) Multiple Links - Simultaneously use the multiple air/ground links that are installed in an aircraft.
3) Data Compression - Account for the low bandwidth air/round data links available today and in the near future that require data compression.
4) Standardization – A standard set of services required by ATS applications and the applications themselves must be compatible worldwide. [Aeronautical Telecommunications Network (ATN)]

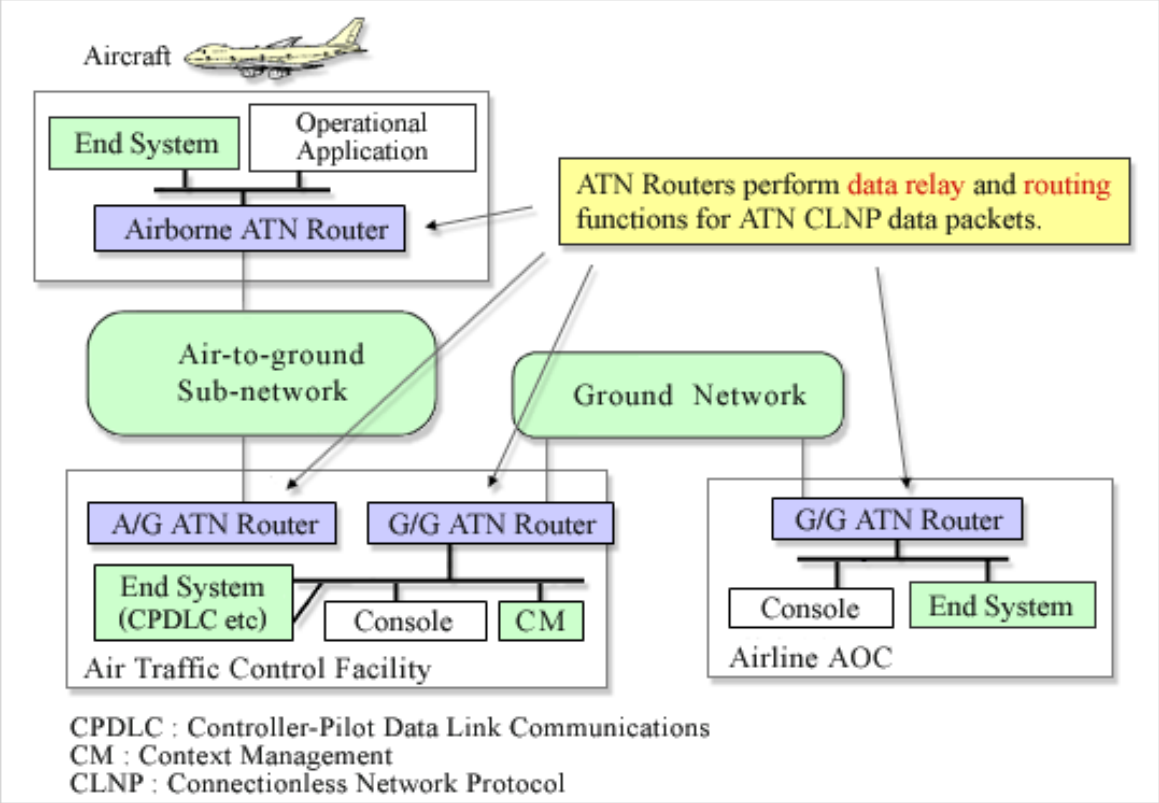


Figure 3.6 – ATN Router System Overview [Oki Electric Industry Co.]

The ATN-B2 DataLink will be part of both the Dynamic RNP and Advanced IM capabilities that will characterize the CNS Integration.

Part II: Methodological Framework

4. Systems Based Methodological Approach to Risk Assessment and Management

The methodology presented through the research for this thesis has three main ideas. First, the need for a systems based iterative approach as presented by the Dynamic Roadmap for Risk Modeling, Planning, Assessment, Management, and Communication (**Figure 4.1**). Second the centrality of state factors (variables, decisions, decision makers, resources) to understanding and modeling the behavior of a complex emergent system of systems (S-o-S). Finally, the methodology presented displays the synergy of three perspectives, operational, structural, and organizational and their unique matching to previously used risk assessment techniques.

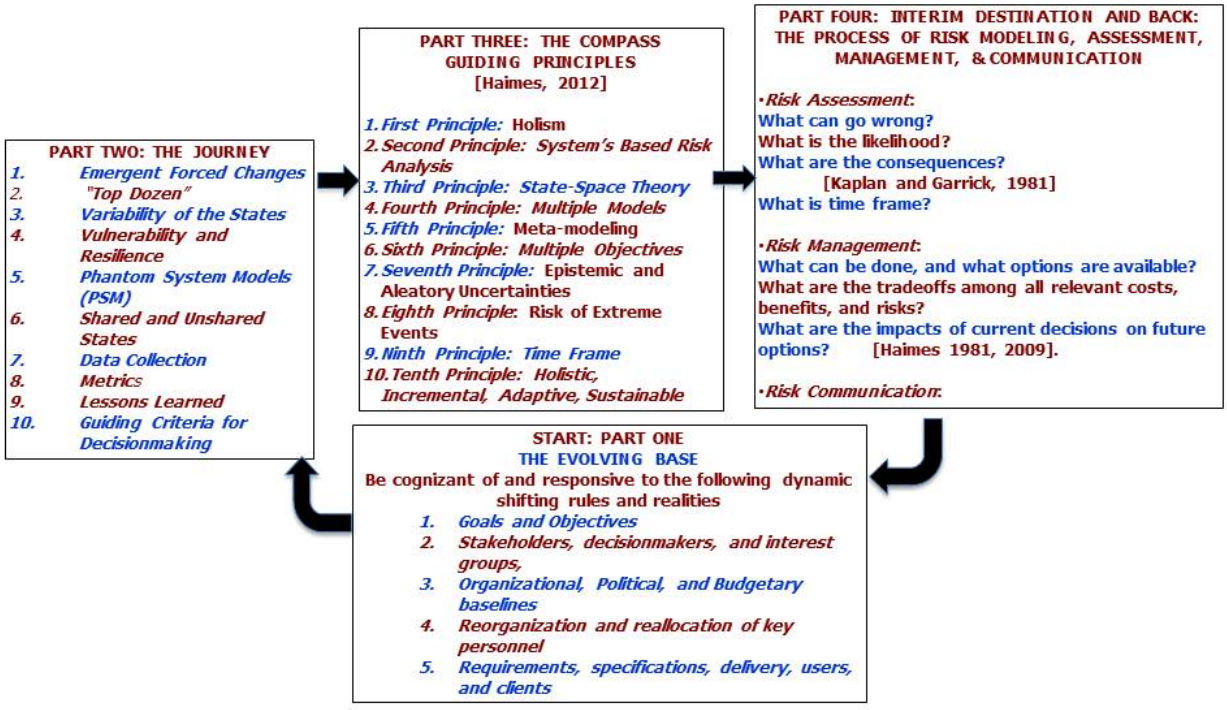


Figure 4.1 [Haimes 2013]

The systems based methodological approach for the research presented here will follow the iterative approach of the Dynamic Roadmap for Risk Modeling, Planning Assessment, Management, and Communication (**Figure 4.1**). The analysis is built on the evolving base. This ensures we are cognizant of and responsive to dynamic realities among the system. Changes could occur to, but are not limited to, goals and objectives, stakeholders, organizations, personnel, and requirements. The Journey includes consideration of Emergent Forced Changes (EFCs) and the reduction of these to a manageable number called the "Top Dozen" or "Dirty Dozen". While required to be exactly 12 the "Dirty Dozen" represent the most important risks, or emergent forced changes of the system. Other keys within the journey include consideration to vulnerability and resilience, shared states, data collection, and metrics. It is also vital to build on lessons learned within the process. Throughout this process the Guiding Principles (Haimes, 2012) provide a compass for a systems based analysis of any emergent system of systems. These key principles are vital to provide a complete and holistic evaluation of the emergent system.

The process leads to the answering of the four questions of risk assessment (Kaplan and Garrick, 1981): (1) what can go wrong? (2) what is the likelihood it would go wrong? (3) what are the consequences? (4) What is the time frame (Haimes 1991)? With these questions addressed, it is necessary to answers an additional set of questions related to risk management presented by Haimes, 1991: (1) What can be done and what option are available? (2) What are the associated trade-offs among all relevant costs, benefits, and risks? (3) What are the impacts of current management decisions on future options? The management portion of this outline was deemed outside the scope and timeframe available for this thesis, but is presented as a vital next step in the future work section of this thesis. Finally all this must be done in a manner that can be communicated to the decision makers and stakeholders involved.

It is vital to understand these are not specific steps to be completed one after another but rather are pieces to a puzzle that must be continually reconsidered and adjusted as needed. Changes to the evolving base could significantly change the analysis and must always be reconsidered and adjusted as lessons are learned and more information is discovered regarding the emergent System of Systems.

Through following this framework for a systems based risk analysis this thesis relied heavily on the centrality of state variables and factors to understand and model the behavior of this complex S-o-S. A complex S-o-S can rarely be well characterized by simple relationships but instead must be understood through the sharing of at least one shared state variable, subsystem, decision, decision maker, or resource. From this idea the interconnections and interdependencies among the Communication, Navigation, and Surveillances systems were developed.

Focusing on these essential states and factors (decisions, decision makers, and resources) we built a foundation for understanding the S-o-S and focused on shared states and factors to discover interconnections and interdependencies across the S-o-S. Shared states represent the operational perspective of the S-o-S and is vital to understanding the basic functionality of the S-o-S. Through our understanding of the system and essential shared states a list of key risk scenarios (Emergent Forced Changes) is proposed. These risk scenarios in part answer the questions “What can go wrong”. Given the timeframe of this research the list of risk scenarios needed to be decreased to be used for this example. To perform this task the Risk Filtering, Ranking, and Management (RFRM) framework was used to determine the most important risk scenarios from the list.

Building on the previous findings of the “dirty dozen” risk scenarios from the RFRM framework fault trees were constructed for the three main cases considered. The fault tree analysis furthers the understanding of the technical and physical elements of the system, adding a structural perspective to the analysis. The fault trees give further insight to the interconnections within the S-o-S and allow for

the discovery of important paths to failure within the proposed S-o-S. It is important to note that while fault tree analysis is normally used to study the reliabilities of a specific component or system within this research it is used to support and build on the synergy between the operational and structural perspectives through interconnections, interdependencies, and shared states (factors).

To conduct a complete analysis for this complex S-o-S through the use of three separate perspectives, operational, structural, and organizational, is necessary. Through shared states (operational) and fault tree analysis (structural) the remaining perspective (organizational) must be considered. While the timeframe of this thesis does not allow an in-depth study of the organizational changes and possible risks that can occur it will outline possible areas for future study.

5. Shared Factors (States, Decisions, Decision Makers, and Resources)

All decisions are made to control (retain or change) the essential states of the system to meet specific desired outputs (goals/objectives), within an acceptable time frame and with acceptable tradeoffs [Haimes, 2009]. With this in mind the essential states, the minimum number of states that can represent the S-o-S in consideration, are vital to understanding and managing a system. Due to the nature of a S-o-S it can be expected that specific interdependencies, interconnections, or other relationships will exist between any two (or more) systems. These connections can be found by utilizing the essential states found and determining which of these states are shared across multiple systems or subsystems.

To further the Shared State analysis other vital parts of the system are included in the research to provide a complete view and understanding of the S-o-S. These include shared decisions, decision-makers, stakeholders, resources, and subsystems. This further investigation in to the interconnections and interdependencies of the systems will allow for a more complete picture of the emergent system.

The identification of these shared factors will serve as a roadmap toward the most important risk scenarios within the S-o-S.

Furthermore shared factors represent the operational perspective of a S-o-S. Many different types of perspectives can represent a complex system, we posit that by considering three, operational, structural, and organizational, and connecting these perspectives to proven risk analysis techniques a holistic and complete risk analysis can be undertaken.

5.1 Identification of Shared Factors

From the previous section, the importance of identifying shared factors to improve the understanding of the interconnections and interdependencies amongst systems within a S-o-S provides critical insight to the behavior and workings of the S-o-S. When considering such a complex and large S-o-S such as the CNS it is imperative to parse through the large number of state variables that occur across the S-o-S into a smaller list of essential state variables and factors. This allows for a manageable list that can be beneficial to the analysis at hand. Consider, for example, the state of an aircraft itself, the state of the engine, exterior shell, internal electronics, etc. These may be included as a state of the system given a wide view of the system, but, keeping in mind that the methodology is built to answer the question of risk to integration this further analysis would provide little benefit toward the goal. It is vital to keep models and methodology as simple as possible, but as complex as required.

In providing an example of the methodology the exploration of both the Current Configuration and Dynamic Required Navigational Performance (RNP) Configuration is required. This provides a way to not only learn about the interconnections and interdependencies of the S-o-S but also the changes that are expected to occur from the changes in the shared state variables. It is important not to just note the shared state variables but the changes to the state variables when moving from the Current

Configuration to the Dynamic RNP Configuration. **Tables 5.1-4** represent the essential state variables and their place within the CNS as S-o-S. Those states bolded and italicized represent shared states. **Tables 5.2 and 5.4** indicate not only the system that the state falls under but also the specific subsystem it is related to.

Table 5.1 – Essential State Variables – Current Configuration

States	Communication	Navigation	Surveillance
LF Signal Integrity		✓	
MF Signal Integrity		✓	
HF Signal Integrity	✓		
VHF Signal Integrity	✓	✓	
UHF Signal Integrity (Includes GPS)		✓	✓
SATCOM Signal Integrity	✓		
GPS Signal Integrity		✓	✓
GPS Signal Availability		✓	✓
GPS Signal Accuracy		✓	✓
Radar Signal Integrity			✓
Comprehension	✓		
Plane Authenticity/Identification	✓		✓
Signal Effective Range	✓	✓	✓
Station Authenticity/Identification		✓	
Distance Calculation Accuracy		✓	
Position Drift		✓	
Detection Availability			✓
Navigation System Error - NSE		✓	
Flight Technical Error - FTE (Conformance)	✓	✓	✓

Table 5.2 – Essential State Variables (System View) – Current Configuration

States	Communication	Navigation	Surveillance
LF Signal Integrity		NDB	
MF Signal Integrity		NDB	
HF Signal Integrity	Voice Comm		
VHF Signal Integrity	Voice Comm & ACARS	VOR	
UHF Signal Integrity (Includes GPS)		DME, GPS	ADS-B
SATCOM Signal Integrity	ACARS		
GPS Signal Integrity		PBN, INS, RNAV	ADS-B
GPS Signal Availability		PBN, INS, RNAV	ADS-B
GPS Signal Accuracy		PBN, INS, RNAV	ADS-B
Radar Signal Integrity			SSR, PSR
Comprehension	Voice Comm		
Plane Authenticity/Identification	Voice Comm		SSR
Signal Effective Range	ACARS	VOR, DME, NDB	SSR
Station Authenticity/Identification		NDB, VOR	
Distance Calculation Accuracy		DME	
Position Drift		INS	
Detection Availability			SSR
Navigation System Error - NSE		NDB, VOR, DME, INS	
Flight Technical Error - FTE (Conformance)	All	All	All

Tables 5.1 and 5.2 display the essential states determined, with the help of MITRE, for the current configuration. The shared states are VHF Signal Integrity, GPS Signal Integrity, Availability, and Accuracy, Plane Authenticity, Signal Effective Range, and Flight Technical Error. The importance of VHF Signal Integrity shows a link within the Communication and Navigation. While the systems may not directly

link this shows us a subtle link between the two systems in the current configuration that may not be obvious prior to this analysis. The importance of the GPS signal connects the Surveillance and Navigation systems through Performance Based Navigation and ADS-B surveillance. The signal effective range is actually an essential state across all three systems determining the importance of an aircraft being within range of the systems mentioned.

Table 5.3 – Essential State Variable – Dynamic RNP Configuration

States	Communication	Navigation	Surveillance
HF Signal Integrity	✓	✓	
VHF Signal Integrity	✓	✓	
UHF Signal Integrity		✓	✓
SATCOM Signal Integrity	✓	✓	
GPS Signal Integrity		✓	✓
GPS Signal Availability		✓	✓
GPS Signal Accuracy		✓	✓
Radar Signal Integrity			✓
Comprehension	✓		
Plane Authenticity/Identification	✓		✓
Signal Effective Range	✓	✓	✓
Station Authenticity/Identification		✓	
Distance Calculation Accuracy		✓	
Position Drift		✓	
Detection Availability			✓
Compliance	✓	✓	✓

Table 5.4 – Essential State Variables (System View)– Dynamic RNP Configuration

States	Communication	Navigation	Surveillance
HF Signal Integrity	Voice Comm & ATN-B2	DRNP (FMS)	
VHF Signal Integrity	Voice Comm & ACARS	VOR	
UHF Signal Integrity		DME	ADS-B Out
SATCOM Signal Integrity	ACARS & ATN-B2	DRNP (FMS?)	
GPS Signal Integrity		PBN, INS, RNAV, DRNP	ADS-B Out
GPS Signal Availability		PBN, INS, RNAV, DRNP	ADS-B Out
GPS Signal Accuracy		PBN, INS, RNAV, DRNP	ADS-B Out
Radar Signal Integrity			Radar
Comprehension	Voice Comm		
Aircraft Authenticity/Identification	Voice Comm		SSR
Signal Effective Range	ACARS	VOR, DME	SSR
Station Authenticity/Identification		VOR	
Distance Calculation Accuracy		DME, GPS	
Position Error		INS, DME, GPS	
Detection Availability			SSR
Compliance	All	All	All

Tables 5.3 and 5.4 display the essential states determined, with the help of MITRE, for the Dynamic RNP configuration. It is important to consider changes in the shared essential states from the current configuration. The introduction of Dynamic RNP and its requirement for ATN-B2 brings HF and SATCOM signal integrity to the forefront. While not directly needed for Navigation an adjustment to the HF signal integrity will affect the Navigation system through the data communication link ATN-B2.

The research completed to determine these essential shared states builds a great depth of understanding of each of the systems independently and their interconnections and interdependencies that make up the complex S-o-S. To continue building on this knowledge essential factors and then shared factors were determined. These included decisions, decision makers, and resources within each of the configurations. To further focus this analysis only the approach phase of flight was considered. **Tables 5.5-5.10** display this information, first for the current configuration and then in comparison to the Dynamic RNP configuration.

Table 5.5 – Decisions – Current Configuration

Decision	Communication	Navigation	Surveillance
Tuning of Frequency	Voice Comm	VOR	
Human Information Requests	Voice Comm & ACARS		
System Use		NDB & DME	
INS Correction System		INS, DME, NDB, VOR	
Call Sign Assignment	Voice Comm		SSR
Flight Plan	ACARS, Voice Comm	DME, VOR, INS, & FMC	
Altitude Adjustments	Voice Comm & ACARS		SSR
Weather Aversion	Voice Comm & ACARS		PSR, SSR, ADS-B

Table 5.6 – Essential Decision Makers – Current Configuration

Decision Maker	Communication	Navigation	Surveillance
Pilot	✓	✓	
ATC	✓	✓	✓
Airport		✓	✓
FAA	✓	✓	✓
ICAO	✓	✓	
ARINC	✓		
AAC	✓		
AOC	✓		

Table 5.7 – Essential Resources – Current Configuration

Resource	Communication	Navigation	Surveillance
Radar Sites			✓
NAVAID Site		✓	
Air Traffic Controllers	✓		✓
Pilots	✓	✓	
Airplane	✓	✓	✓
Airport			
Satellites	✓	✓	✓
Navigation Charts (IAP, etc.)		✓	✓
Flight Plans		✓	
Weather Stations	✓	✓	✓
Runways		✓	✓
Flight Management Computer	✓	✓	

Table 5.8 – Decision – Dynamic RNP Configuration – Approach Phase

Decision	Communication	Navigation	Surveillance
Type of Approach			
Instrument Flight Rules	✓	✓	✓
Visual Flight Rules	✓	✓	
Approach System			
ILS		✓	
Vectored Approach	✓		✓
GPS (RNAV) Approach		✓	
VOR Approach		✓	
NDB Approach		✓	
Runway Clearance	✓		
Aircraft Separation	✓		✓
Approach Route	✓	✓	
Holding Pattern	✓	✓	

Figure 5.9 – Decision Makers – Dynamic RNP Configuration – Approach Phase

Decision \ Decision Maker	Pilot	ATC	Airport
Type of Approach			
Instrument Flight Rules	✓	✓	
Visual Flight Rules	✓	✓	
Approach System			
ILS	✓	✓	✓
Vectored Approach	✓	✓	✓
GPS (RNAV) Approach	✓	✓	✓
VOR Approach	✓	✓	✓
NDB Approach	✓	✓	✓
Runway Clearance		✓	✓
Aircraft Separation		✓	
Approach Route	✓	✓	
Holding Pattern		✓	

Table 5.10 – Resources – Dynamic RNP Configuration – Approach Phase

Resource	Communication	Navigation	Surveillance
Radar Sites			✓
DME Substations		✓	
Satellites	✓	✓	
Air Traffic Controllers	✓		✓
Pilots	✓	✓	
Airplane	✓	✓	✓
NACO Charts	✓	✓	✓
Flight Management Computer	✓	✓	
ATN – B2 Receiver/Transceiver	✓		
NAVAID Receiver		✓	
Weather Stations	✓	✓	✓

The previous table provides further insight in to the interconnections and interdependencies across the three systems of Communication, Navigation, and Surveillance. This work provides a means for gaining knowledge of how the system operates currently and how those operations will change and what connections occur with the implementation of Dynamic RNP. While it is vital to understand the connections introduced through ATN-B2 other interdependencies and interconnections that are less obvious show the importance of this work. For consideration aircraft separation is an important decision requiring both the Communication and Navigation systems on line to perform. The weather station resource within the NAS also affects all three systems bringing considerations linked to the stations to the forefront of the analysis.

5.2 Characterizing Interdependencies using Shared Factors

Considering the previous tables (5.1-5.10) the methodology brings to light interconnections and interdependencies among the three systems of Communication, Navigation, and Surveillance. These interconnections can be characterized through shared states and further explored through the use of shared factors. The use of GPS in both the navigation and surveillance systems makes it a vital resource among the CNS and its integrity, availability, and accuracy are vital. VHF signal integrity connects both the communication and navigation systems through the signals use in both voice and data comm (ACARS) as well as VOR navigation. The signal effect range is vital to all three of the systems and indicates the important for complete coverage and understanding of when and where to switch off of one system and on to another. The Dynamic RNP configuration further highlights these shared states and include the importance of HF and SATCOM signal integrity. HF and signal integrity is the crucial state representing the link between communication and navigation through the ATN-B2 data link necessary to perform the capability. These findings are backed up by the shared factors analysis.

5.3 Operational Perspective through Shared Factors

We posit that any complex system of systems can be understood by focusing on three separate perspectives, operational, structural, and organizational and that by benefiting from this breakdown a complete system based risk analysis can be completed. While these perspectives are vital we are not to forget the need for multiple viewpoints within any perspective. For example, when considering the operational perspective one may need to gain insight from many viewpoints and different experts on the operation of the system.

Furthermore we posit that the study of essential states fits perfectly within the operational perspective. We build on the idea that all decisions are made to control (retain or change) the essential

states of the system to meet specific desired outputs (goals/objectives), within an acceptable time frame and with acceptable tradeoffs [Haimes, 2009]. This links the states of the system to the operation of the system, specifically they explore how the system operations, key systems, functionalities, decision makers, decisions, and resources that allow the complex S-o-S to operate smoothly. The discovery of shared states allows us to determine interconnections and interdependencies to further understand how emergent forced changes could affect the smooth operation of the S-o-S. Ultimately the other perspectives (structural and organizational) will be needed to perform a complete risk analysis for any complex S-o-S but the need to understand and determine the interconnections and interdependencies make the operational perspective an obvious starting point for such an analysis.

6. Hierarchical Holographic Modeling (HHM)

To move from an understanding of the system and its interconnections and interdependencies to a risk assessment one must build out risk scenarios and possible emergent forced changes that can occur within the system. To aid in considering the multitude of risks that could occur the use of Hierarchical Holograph Modeling (HHM) [Haimes 1981, 2009] can be implemented. HHM provides a holistic philosophy and methodology used to show the diverse risks inherent to any complex S-o-S and their attributes through multiple perspectives and hierarchies. We believe the more we look the more we will find and the more comprehensive our risk analysis will be. In constructing an HHM it is important to find a multitude of Subject Matter Experts (SMEs) with not only a vast knowledge of the system but a comprehensive knowledge from as many perspectives as possible. While HHM provides a significant aid in determining risks to the system its dependence on Subject Matter Experts made it infeasible for this research. The determination of risk scenarios was done with the helped of shared factors and is explained in the next section. For completeness of the methodology and to highlight HHMs importance

HHM is fully explained and two example HHMs created without the help of a multitude of diverse SME perspectives are shown to provide further understanding (**Figure 6.1-2**).

Holographic refers to the previously mentioned multiple perspectives required for identifying risks to a complex S-o-S. Risks can fall in many categories, including but not limited to, hardware/software, organizational, human, geography or time related, and environmental [Haimes et al. 2002]. This diverse collection of risks expected to be discovered using HHM requires a team with a broad array of experience and knowledge of the S-o-S, or better yet, many teams with each team representing a one of many perspectives. These perspectives are usually listed as the headtopics within an HHM. In **Figure 6.1** the headtopics are Information, Landing System, NAVAID, Approach Procedure, Instrument Approach Procedure, Decision Makers, and Nature.

Hierarchical refers to need to understand not only the many perspectives but also the many levels inherent to any S-o-S. Both high level views and risks and low level risks occur within a S-o-S. It is important to represent both and allow decision makers and stakeholders to steer the analysis in the necessary direction to answer the key risk question being asked. These levels could possibly be represented by management levels, subsystems, geography, or a multitude of other hierarchical representations inherent to a specific S-o-S. These hierarchies are represented by sub-topics, sub-sub-topics and further if necessary underneath the head topics.

HHM combines the holographic methodology with a hierarchical analysis to provide a holistic means to identifying the countless risks from all perspectives and levels within a complex S-o-S. A final key comment regarding HHM is an idea presented by Haimes, once you believe you have won, you have lost. This speaks volumes to the need for risk analysis, especially HHM, to be an iterative process. It is critical that the HHM is not ever considered completed and left aside, it should always be revisited and

adjusted to meet any changes to the system or new ideas that come up throughout the risk analysis process.

Figure 6.1 – Example HHM for Current Configuration

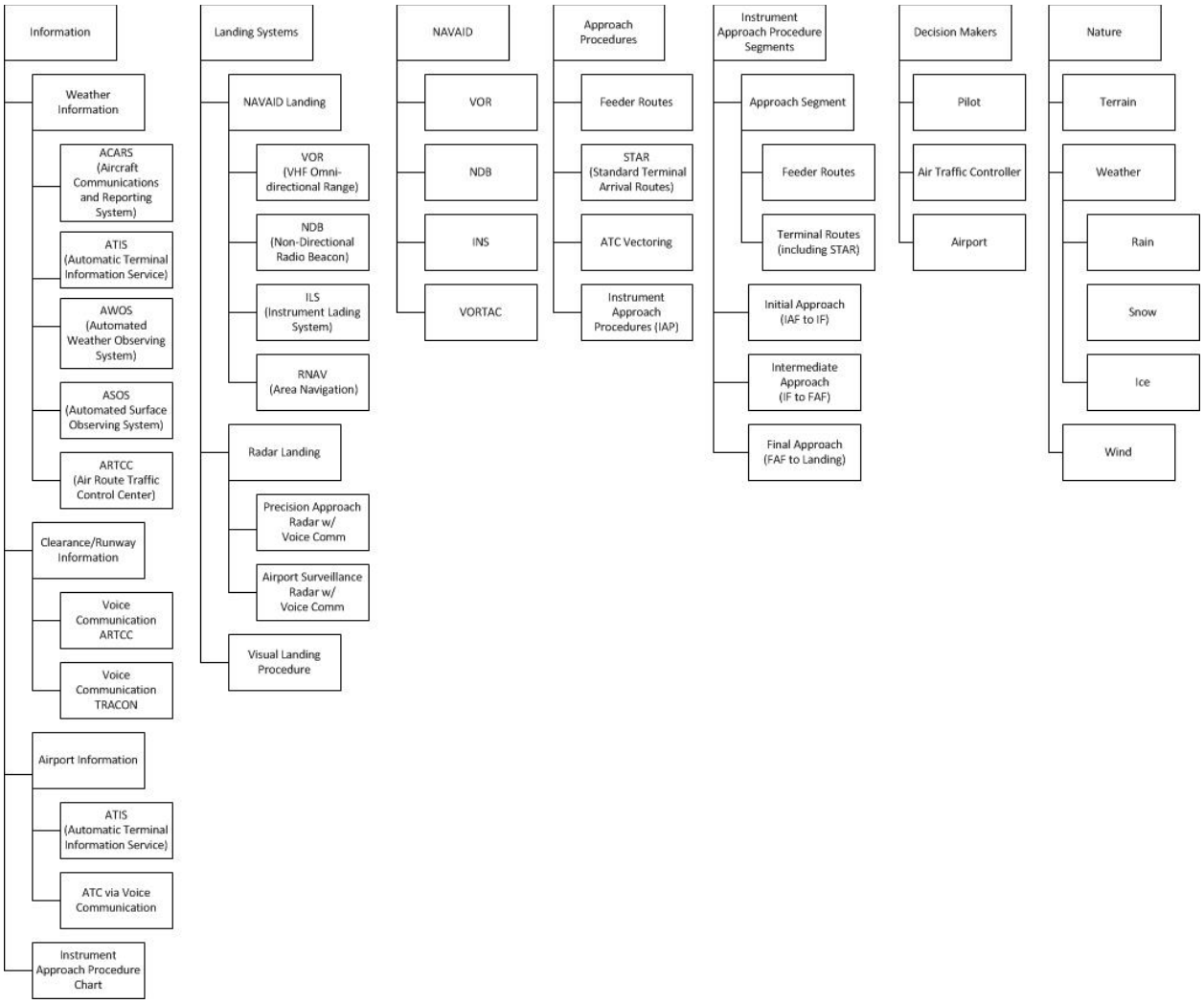
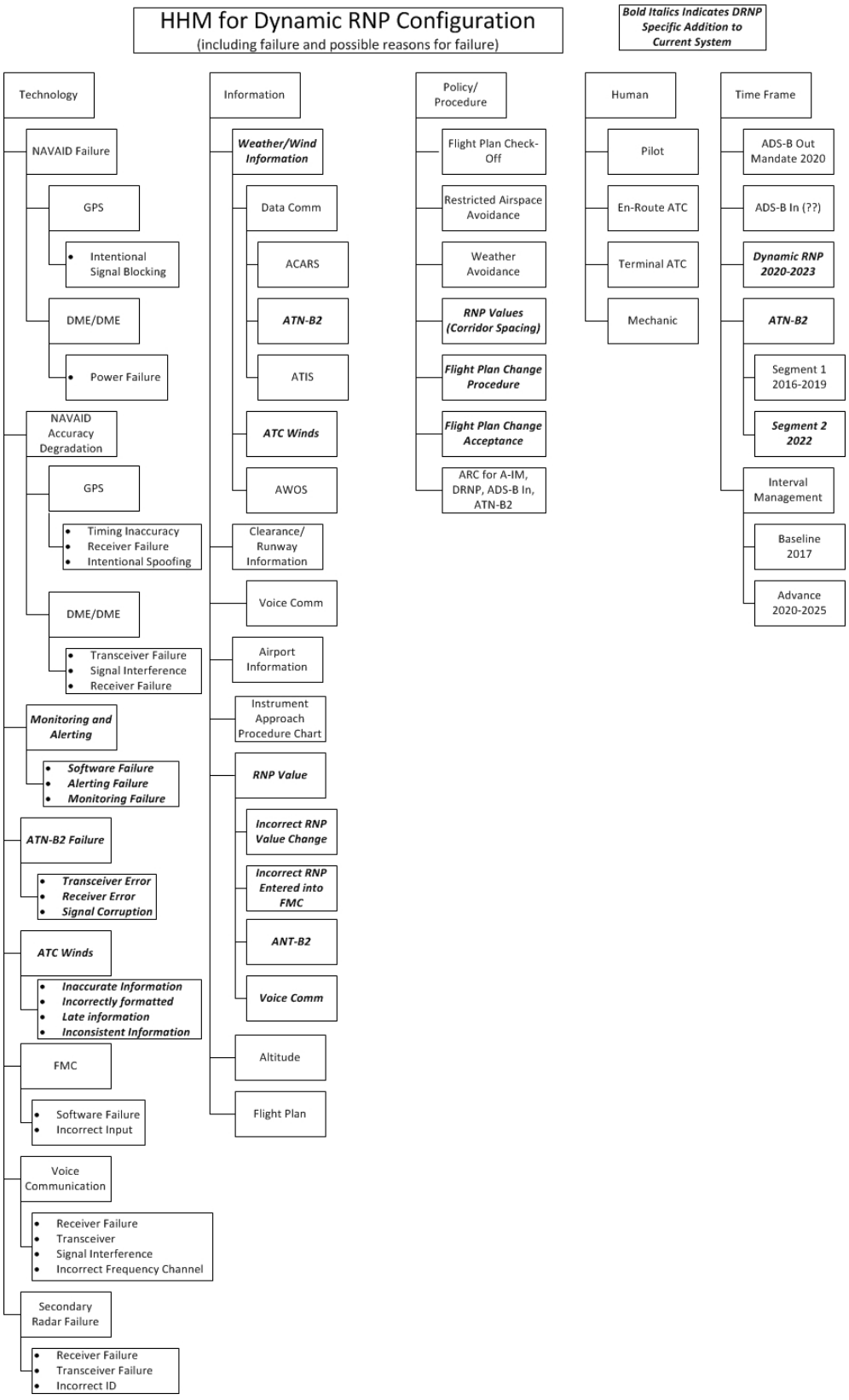


Figure 6.2 – Example HHM for Dynamic RNP Configuration



7. Risk Filtering, Ranking, and Management

Frisk filtering, ranking, and management (RFRM) provides a multistep systematic framework for prioritizing risk management options associated with scenarios regarding large-scale System of Systems [Haimes et al., 2002, Haimes 2009]. The complete framework consists of eight stages but this research applies only a portion of RFRM in order to form a modified RFRM for risk scenarios within an emergent S-o-S where probabilities for the determined risk scenarios may be limited or unavailable altogether. The standard phases include the creation of an HHM (1) Scenario Identification followed by (2) Scenario Filtering based on scope, temporal domain, and level of decision making which would have been completed if possible for this research. Instead of the creation of an HHM and step 2 shared factors and the scope of the project were used to create a list of 10-13 risk scenarios for consideration.

To provide an in depth and useful analysis of the most important risks to the system a (4) multicriteria evaluation was performed for each of the risk scenarios (this research has skipped over phase III, bi-criteria filtering, due to the unknown likelihoods within our emergent S-o-S). This phase of RFRM provide a means for filtering the risks through their ability to defeat the three defense properties of a system: resilience, robustness, and redundancy. Scenarios able to defeat these properties are considered more severe and are selected for further analysis through fault trees. Once again the use of subject matter experts is vital to provide understanding and rankings as to a specific scenarios ability to defeat the defense properties of a system.

While the constraints of this research lead to the creation of a modified RFRM framework limited to a highly focused effort on stage 4 (mulicriteria evaluation) the remaining eight steps could provide great help in filtering and ranking further risks. An in depth explanation of the remaining steps not covered here can be found chapter 7 of *Risk Modeling, Assessment, and Management* by Yacov Y. Haimes. The remaining four steps are (5) quantitative ranking, using the cardinal version of the MIL-STD 882 Risk

Matrix, (6) Risk Management, (7) safeguarding against missing critical items, and (8) operational feedback. These remaining steps focus on the importance of an iterative process key to any risk analysis. While not performed directly through RFRM this research was performed in a holistic and iterative process to determine any necessary changes due to changes in scope, process, or to the S-o-S itself.

7.1 Defining Risk Scenarios

While an ideal risk analysis, similar to the one presented here, would define risk scenarios through the constructing of an HHM with the help of a multitude of experts with many different perspectives of the system or system of systems, the constraint on subject matter expets (SMEs) and time created a need for an alternative process. For this process we exploited the knowledge we gained from shared states and factors to come up with our own "dirty dozen" list of top risk scenarios for further consideration. Two lists were created, one for the current configuration and another for the Dynamic RNP configuration both focusing on the approach phase of flight (**Table 7.1**).

Table 7.1 – Risk Scenarios for CNS as S-o-S Integration (Approach Phase)

Current Configuration	Dynamic RNP Configuration
1.1 NAVAID or GPS Outage	2.1 NAVAID or GPS Outage
1.2 NAVAID or GPS Accuracy Degradation	2.2 NAVAID or GPS Accuracy Degradation
1.3 Radar Outage	2.3 Monitoring and Alerting Failure
1.4 Voice Comm Failure	2.4 ATN-B2 Failure
1.5 Instrument Landing System Failure	2.5 Weather Information Failure
1.6 Incorrect Airport Information	2.6 Flight Management Computer Failure
1.7 Incorrect Understanding of Instructions	2.7 Instrument Landing System Failure
1.8 Incorrect Weather Information	2.8 Voice Comm Outage
1.9 Incorrect Plane Authentication/ Identification	2.9 Incorrect Understanding of Instructions
1.10 Flight Technical Error	2.10 Radar Outage
	2.11 Incorrect Plane Authentication or Identification
	2.12 Flight Technical Error

Taking cues from the important shared factors discussed in section 5.1 and from knowledge gleamed from our understanding of the S-o-S and discussions with team at MITRE the previous list was created. The importance and shared states of VHF Signal Integrity, GPS Signal Integrity, Availability, and Accuracy show the obvious need to consider outages to the systems involved to be considered leading to the risk scenarios 1.1, 1.2, 1.4, 1.5, 2.1, 2.2, 2.7 and 2.8. Also the explicit state of flight technical error leads to risk scenario 1.10 and 2.12. Further connections found from shared states specific to the Dynamic RNP connection such as HF and SATCOM signal integrity and its importance to ATN-B2 and the Dynamic RNP configuration lead to risk scenarios 2.4, and 2.6.

The remaining scenarios build on knowledge gained throughout the discovery of shared states. The consideration of Radar Outages (1.3 and 2.10) come from the understanding that with the introduction of Dynamic RNP and ADS-B many current radar systems will be decommissioned possibly leading to a lack of necessary coverage. Monitoring and alerting (2.3) is a key safety aspect built in to Dynamic RNP to ensure the pilot, crew, and ATC are aware of the plane's current performance ability. The remaining scenarios are information based and push to discover if certain information or lack thereof will cause significant problems as the change to Dynamic RNP occurs.

7.2 Prioritizing Risk Scenarios through Multi-criteria Filtering

To gain further insight into the risk scenarios proposed and determine which scenarios are key and deserve further analysis we take advantage of the fourth stage of RFMR: multi-criteria filtering. Multi-criteria filtering takes advantage of a system's 3 defense properties of a system, redundancy resilience and robustness, to discover the key risk areas within any system. Exploring further within these defense properties of a system we utilize 11 specific characteristics to gain insight in to the severity of the risks within any specific scenario: (1) un-detectability; (2) uncontrollability; (3) multiple paths to failure; (4) irreversibility; (5) duration of effects; (6) cascading effects; (7) operating environment; (8) wear and tear; (9) Hardware/Software/Human/Organizational Interfaces; (10) complexity; and (11) design immaturity.

Each scenario is then given an associated qualitative risk severity rating of high, medium, or low. (Full explanation of each of the eight specific characteristics and specific definitions of high, medium, or low can be found in Appendix D). These characteristics do not ensure a catch all for every system. While we believe this is a fairly comprehensive set across many systems it is possible, and likely, that adjustments will need to be made to cover the S-o-S in question.

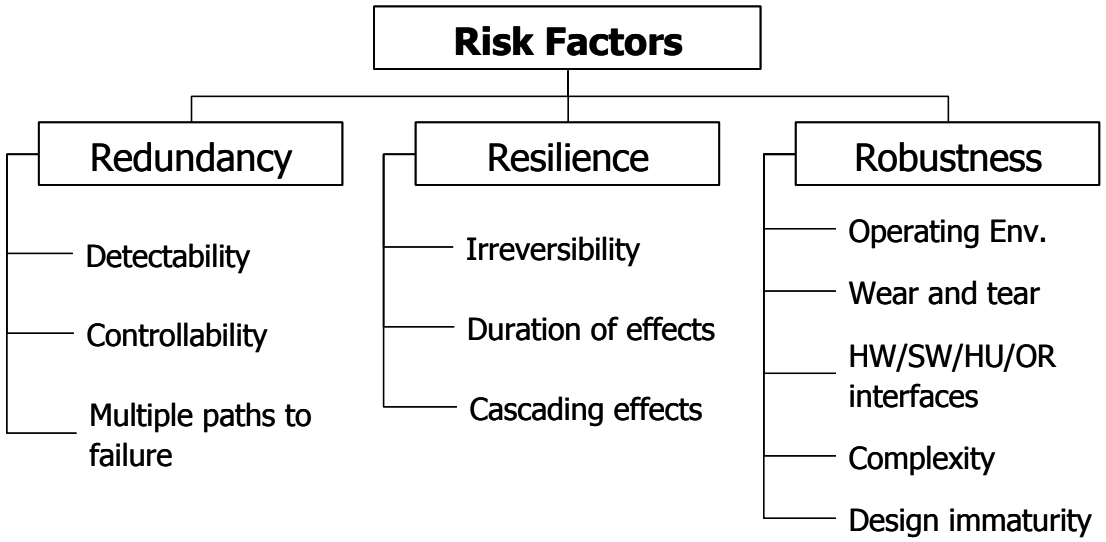


Figure 7.1 – Breakdown of Characteristics into 3 defense properties of a system

Drawing on the risk scenarios determined in section 7.1 (**Table 7.1**) a multi-criteria analysis was performed. To complete the analysis the help of subject matter experts (SMEs) were provided by MITRE. Each SME was provided an introduction to the CNS integration problem, a powerpoint explaining the need for RFRM and its benefits to the problem at hand, as well as an excel spreadsheet to fill in the necessary responses (high, medium, or low) for each scenario and each characteristic. In order to fulfill a broad perspective and understanding of the risks involved with our chosen scenarios each expert was asked to complete a spreadsheet with consideration to both the current configuration and the dynamic RNP configuration. Furthermore, two types of risks were considered, both safety and value risk. Safety risk relates specifically to the possibility of risks to health, such as increased probability of

incursions while value risk relates to interferences to the system that could cause economic losses such as loss of capacity within the airspace. These separate perspectives, safety and value, allow us to keep in line with the FAAs goals for NextGen of increased safety, capacity, and efficiency. A sample of the spreadsheet is shown in **Figure 7.2** with completed spreadsheets with all characteristics, scenarios, and SME responses available in Appendix A. Each column separated by a dashed line represents a different SME's response to the specific characteristic and risk scenario being considered. The three SME's all provided their own area of expertise and a different perspective of the system. Mr. Steve Osbourne provided an ATC perspective, Mr. Gerry McNeil has previous pilot experience and is a navigation expert, Dr. Monticone is a communications expert.

Column 1: Mr. Steve Osbourne – ATC Perspective
Column 2: Mr. Gerry McNeil – Nav Expert / Pilot Experience
Column 3: Dr. Monticone – Comm Expert

Current Configuration - Safety - Approach Phase of Flight

Event / Criteria	NAVAID or GPS Outage		NAVAID or GPS Accuracy Degradation		Radar Failure		Voice Comm Failure		
Expert	1	2	1	2	1	2	1	2	3
Undetectability									
Uncontrollability									
Multiple Paths to Failure									
Irreversibility									

Figure 7.2 – Sample RFRM Multi-Criteria Spreadsheet

When compiling the three SME spreadsheets a means of determining which characteristics and scenarios were most important had to be determined. We emphasized any characteristic with which two or more experts ranked as medium or higher as well as any scenarios that were ranked medium by

one expert in seven or more of the characteristics. This provides both for agreement in areas to hold weight as well as for an expert in a specific field to trump the answers of others that may not have as much knowledge or experience in that specific area. The scenarios that met these criteria are bolded and highlighted in the tables shown in **Appendix A**.

For the current configuration Radar Failure and Incorrect Understanding of Instructions were both marked by two experts as medium. Radar Failure met the criteria with consideration to the operating environment characteristic within safety perspective and for both operating environment, duration of effects, and irreversibility in regards to value perspective. Incorrect understanding of instructions was ranked medium in reversibility and cascading effects as well as receiving seven medium ratings from Mr. Steve Osbourne. Incorrect understanding of instructions was ranked medium in all characteristics other than wear and tear by Mr. Steve Osbourne. Finally voice communication failure was ranked medium by all three experts for both duration of effects and cascading effects within the value perspective. This left four scenarios for further considerations: Radar Failure, Voice Comm Failure, Incorrect Weather Information and Incorrect Understanding of Instructions. Upon further discussion with the team and in keeping with the mantra that our analysis should answer specific questions Incorrect Weather Information and Incorrect Understanding of Instructions were dropped as they will not be affected by the integration of CNS.

For the Dynamic RNP configuration Monitoring and Alerting Failure, ATN-B2 failure, Flight Management Computer Failure, Radar Outage and NAVAID or GPS Outage/Degradation were highlighted. Radar outage and NAVAID or GPS Outage/Degradation were only highlighted in concerns for the value of the system. Mr. Steve Osbourne ranked seven or more characteristics as medium in NAVAID or GPS Outage/Degradation, Monitoring and Alerting failure, and Flight Management Computer failure requiring note although other experts did not rank them as highly. Dr. Monticone similarly

focused on the ATN-B2 failure although others seem less concerned. Radar outage was the one scenario ranked medium for Cascading Effects and Operating Environment by two or more experts.

Gleaming from the advice and further discussion with the MITRE team and the MITRE SMEs the following scenarios were considered further: NAVAID/GPS Outage, Monitoring and Alerting Failure, Flight Management Computer Failure, Voice Comm Failure, and Radar Outage. This provides a significantly more manageable list to build our analysis on. While some scenarios were expected, Voice Comm Failure and Radar Outages would likely have been left off a risk analysis not completed using the methodology presented here.

8. Fault Tree Analysis

Building upon the shared factors and previously determined risk scenarios, fault tree analysis can be implemented to determine how a specific risk scenario could occur. Fault Tree Analysis builds understanding of the structural/cyber-physical dimension of the emerging S-o-S. The Fault Tree shows specific commonalities, interdependencies, interconnectedness, and other relationships among the structural/cyber physical dimension of the systems and subsystems comprising the S-o-S [U.S. Nuclear Regulatory Commission, 1981, Haimes, 2009].

With the large number of components within the CNS System of Systems each with its own unique reliability we must determine the overall reliability of the system. The Fault Tree provides a systematic and quantitative process that can be used to view the reliability of the S-o-S. In the possible, and likely, case that probabilities are unavailable for an emerging S-o-S, such as the case with future configurations of the CNS Fault Tree can still outline key interconnections and interdependencies vital to the S-o-S. For further study without probabilities Event Tree Analysis can be used alongside Fault Tree to build a process of the failure to present the timeline of events of a failed system.

We define reliability as the conditional probability that the system will perform its expected functions throughout a specific time interval, given that it was functioning at a specific time (t_0). In this sense, fault tree analysis provides a systematic and quantitative process that can be used to view the reliability of the system-of-systems. Utilizing the components shown in **Figure 8.1** can help us determine the reliability of the system. The reliability is defined as the probability that the system operates correctly throughout a specific interval in time given that it was operating correctly at t=0. These systems can be connected in two ways, through OR gates or AND gates shown in **Figure 8.1**. When connected via an OR gate, or in series, either event occurring causes the prior event to occur. When connected via an AND gate, or in parallel, all events must occur in order to cause the prior event to occur.

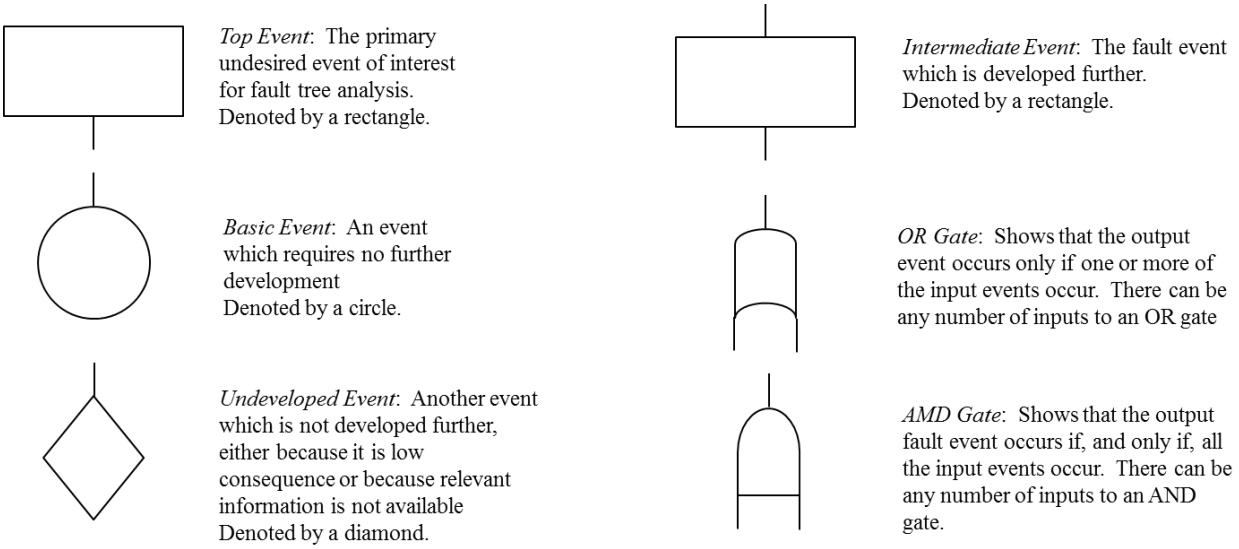


Figure 8.1 [U.S. Nuclear Regulatory Commission, 1981]

This difference between the two gates is explained using Figure 8.2. Top Event 1 would occur (the system would fail) if either Event A or Event B occurred. Systems in series are in general less reliable and can be represented in Boolean Algebra with a "+". Top Event 2 would occur (the system would fail) if

and only if **both** Event C and Event D occurred. Systems in parallel are in general more reliable and can be represented in Boolean Algebra with a "•".

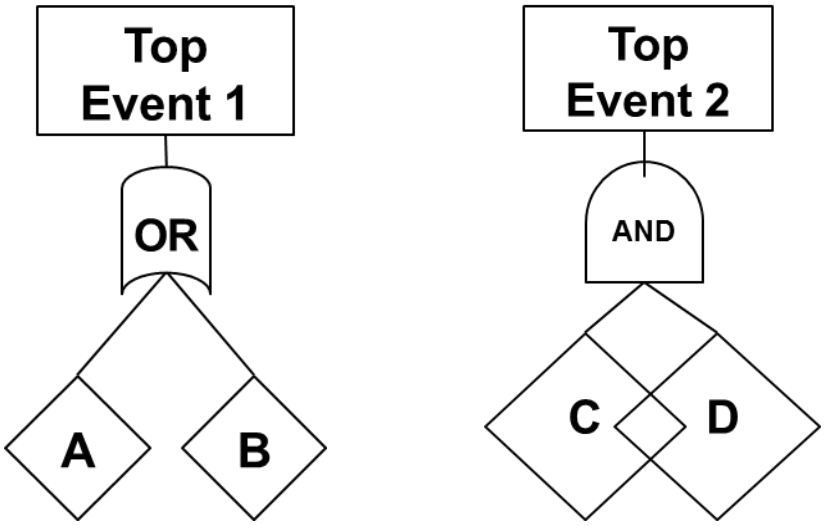


Figure 8.2 – Fault Tree Analysis "AND" and "OR" Gate Example

The goal of Fault Tree is to identify potential weaknesses and interconnections within a system, or the members of the fault tree that would cause a system's failure. Finding the critical paths to failure through minimal cut sets builds on this idea. A minimal cut sets is defined as the smallest combination of component failures, which if they occur, will cause the top event to occur. In other words, they are a combination of events in parallel that if all fail the event will occur. This set is vital in determining the key influencers of the event being considered and provide a key set of events that will have a dramatic influence on the S-o-S.

A preliminary simple fault tree can be characterized as shown in **Figure 8.3**. The focus here is a large scale view of how a Dynamic Required Navigational Performance (RNP) capability could fail. The model may be further applied to address specific risk scenarios as needed. Each Fault Tree will provide valuable insight into the interdependencies and interconnections that could possibly lead to the specific risk scenarios we are exploring.

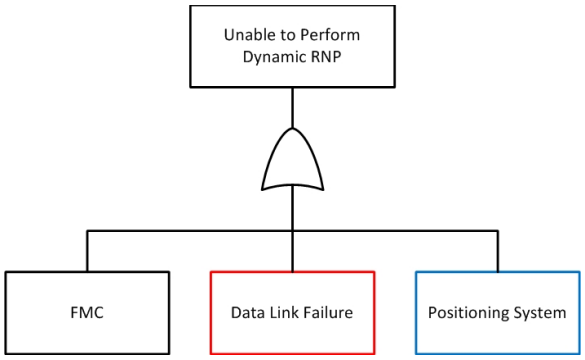


Figure 8.3 – Simple Dynamic RNP Fault Tree

8.1 Dynamic RNP Overview Analysis

When considering the key risk scenarios determined through the modified RFRM multi-criteria evaluation with the help of MITRE subject matter experts, NAVAID/GPS Outage, Monitoring and Alerting Failure, Flight Management Computer Failure, Voice Comm Failure, and Radar Outage, it was understood that the first three were the key components to the dynamic RNP capability. Therefore it was decided that a fault tree analysis could build off of the fault tree suggested in **Figure 8.3** with further consideration to the three main systems, Flight Management Computer (FMC), Data Link, and Positioning System would provide the necessary understanding for our analysis and a minimal cut set could be determined.

Each system, the Flight Management Computer, Data Link System, and Positioning System make up the minimal cut set of the simple fault tree presented in **Figure 8.3**. To build on this understanding each of the three systems had their own fault tree built and expanded to find a minimal cut set for each system, FMC (**Figure 8.4**), Data Link (**Figure 8.5**), and Positioning (**Figure 8.6**). These gave a more comprehensive understanding of the structural perspective of the Dynamic RNP system, and therefore the CNS as S-o-S Integration.

The fault tree for the Flight management Computer (**Figure 8.4**) shows two important subsystems vital to the health of the FMC. One of the main benefits of Dynamic RNP is its use of a monitoring and alerting system to inform the pilot to problems within the system and with the possible inability to perform the RNP value required for a specific airspace. As these events, System Error and Monitoring and Alerting Failure, are connected with an AND gate, it will take failures to both events to cause the top event to occur. The OR gates represented below both the Systems Error and Monitoring and Alerting Failure Events mean that the minimal cut sets are made up of the many combinations of sub-events underneath System Error and Monitoring and Alerting Failure. For example, one minimal cut set is Incorrect Acceptance of Clearance and Software Failure; another would be Incorrect RNP Value Input and an Alerting Failure. The Significance of the minimal cut set and the synergy between this structural perspective and the operational perspective is provided in Section 10.

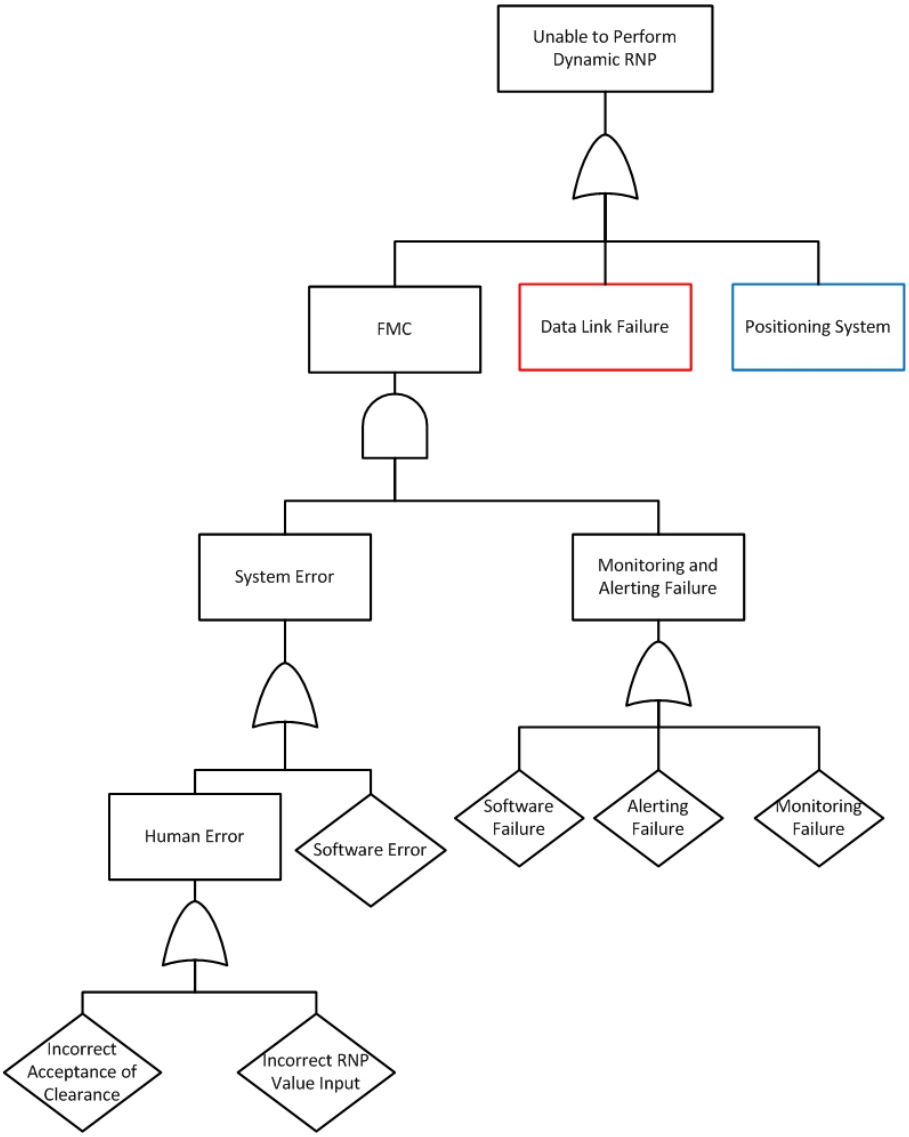


Figure 8.4 – Flight Management Computer Fault Tree

The Fault Tree for the Data Link system (**Figure 8.5**) is similarly built from that of the FMC with two main data links available to perform Dynamic RNP. While ATN-B2 is the main system, Dynamic RNP can operate through a slightly decreased mode through the FANS 1/A data link. This means the minimal cut set is determined by the failure of both the ATN-B2 and FANS 1/A data link. The ATN-B2 system can be brought down by failures in Ground End System, Routers, the on plane receiver, or a combination of all signals failing at once. The FANS 1/A system can similarly be brought down by failures within the Radio Transceiver Network, AFEPS, DataLink System, the on plane receiver or a combination of all signal types failing at once. This means the minimal cut set is determined by any combination of these failures. For example a possible minimal cut set is the failure of an ATN route coupled with the FANS 1/A on plane receiver failing.

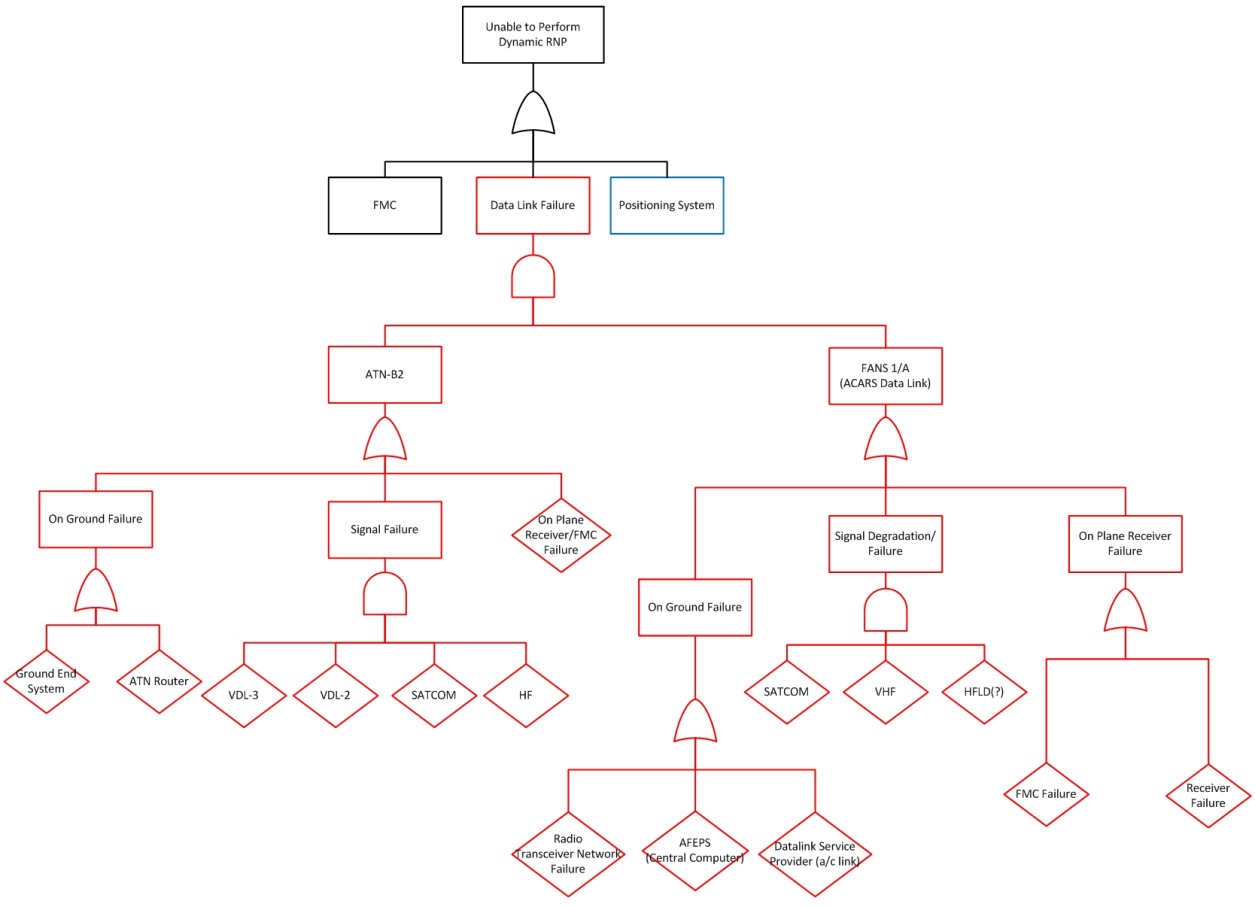


Figure 8.5 – Data Link Failure Fault Tree

Once again the Positioning System fault tree (Figure 8.6) continues the theme of two main subsystems for the use of the Dynamic RNP capability. GPS (GNSS) is considered the main positioning system for Dynamic RNP due to its incredible accuracy but DME/DME is also being considered as it has proven to be accurate enough for most all RNP needs. Again the minimal cut set is determined by a failure to both the DME/DME and GPS systems. Therefore, the all minimal cut sets can be determined through the combination of a failure mode of DME/DME and of GPS. For example, a possible minimal cut set is given by insufficient power within DME/DME system and a Satellite failure among the GPS system.

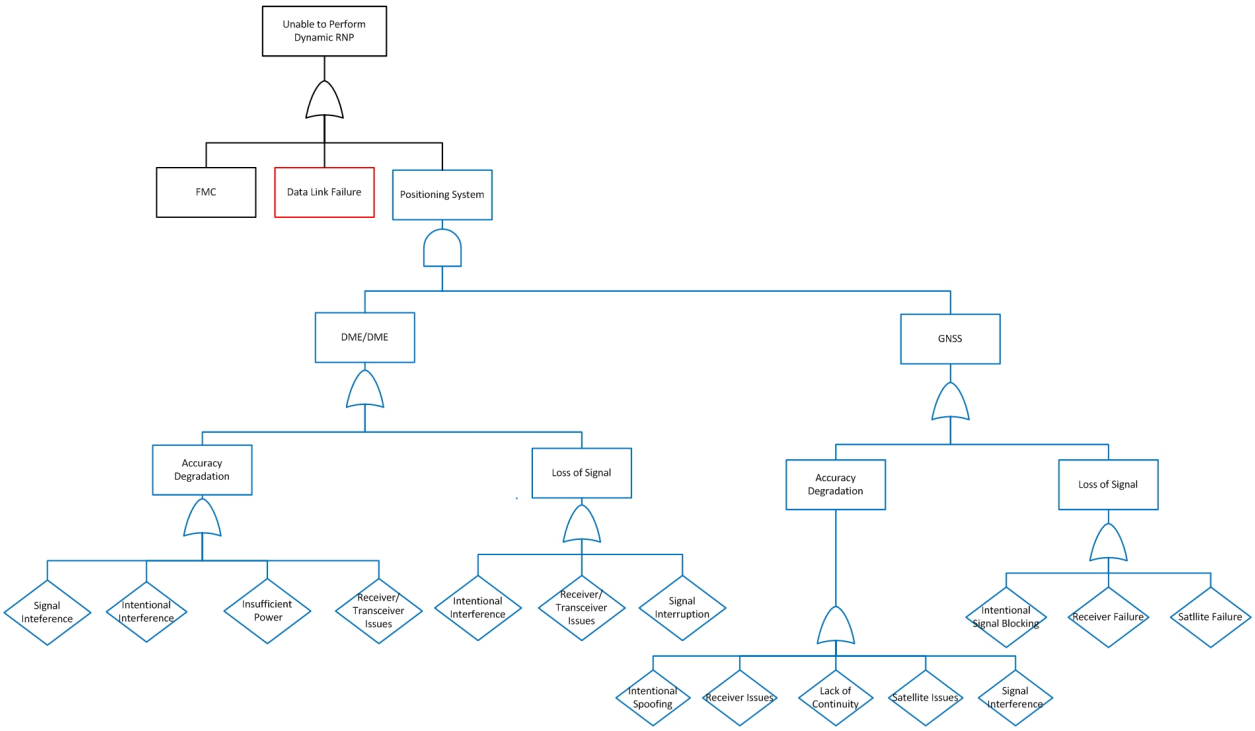


Figure 8.6 – Positioning System Fault Tree

Beyond the further analysis considered through the synergy of shared factors (operational perspective) and fault tree analysis (structural) perspective there are two main takeaways form these work. There has been discussion regarding the use of both FANS 1/A and ATN-B2. The current plan is

that ATN-B2 will be used as the primary system with FANS 1/A only for Oceanic and other remote operations. This Fault Tree shows the key benefits to using both within the key Communication systems of the DRNP capability. Similarly there are clear benefits to the enabling of both GPS and DME/DME for the key Navigation system of the DRNP capability. For this reason both are considered within the Fault Tree as AND gates.

The Fault Tree Analysis builds on the prior work using shared states and determines minimal cut sets within the S-o-S. The provided minimal cut sets help further show interconnections and interdependencies within the S-o-S that will play a key role in system failure. While reliabilities for each part of the system would be helpful there is still much information to be gained from the determination of interconnections and interdependencies. Also, while not utilized within this research, Bogdanor (2014) lays out a helpful way to deal with the lack of probabilities through the use of event trees, discussed in brief in Section 9. This work pulls together the pieces that began with the collection of shared states, decisions, and resources and builds toward the identification of critical sources of risk resulting from the integration of CNS. The Fault Tree and Minimal Cut Sets further our understanding and insight into the interconnectedness and interdependencies among CNS. This task continues the process of identifying critical emerging sources of risk due to the integration CNS.

8.2 Dynamic RNP Scenario Specific Analysis

Although some of the risk scenarios determined through the RFRM multi-criteria evaluation were built in to one fault tree and outlined in Section 8.1, the following sections study the specific risk scenarios presented by Radar Outages and Voice Communication Failures.

8.2b Radar Outage

We begin the analysis of the other key risk scenarios with radar outage. Two main radar systems are currently used within the National Airspace System (NAS), Primary Radar and Surveillance (Secondary) Radar. Primary Radar uses standard Doppler radar procedures while Surveillance Radar actually sends a signal to a transponder on a plane that replies to the interrogator to obtain location. Both are used to determine aircraft location. Surveillance Radar has the distinct advantage of providing the radarscope with the plane's identification credentials automatically with its response. For a failure to the system to occur both radar types must fail.

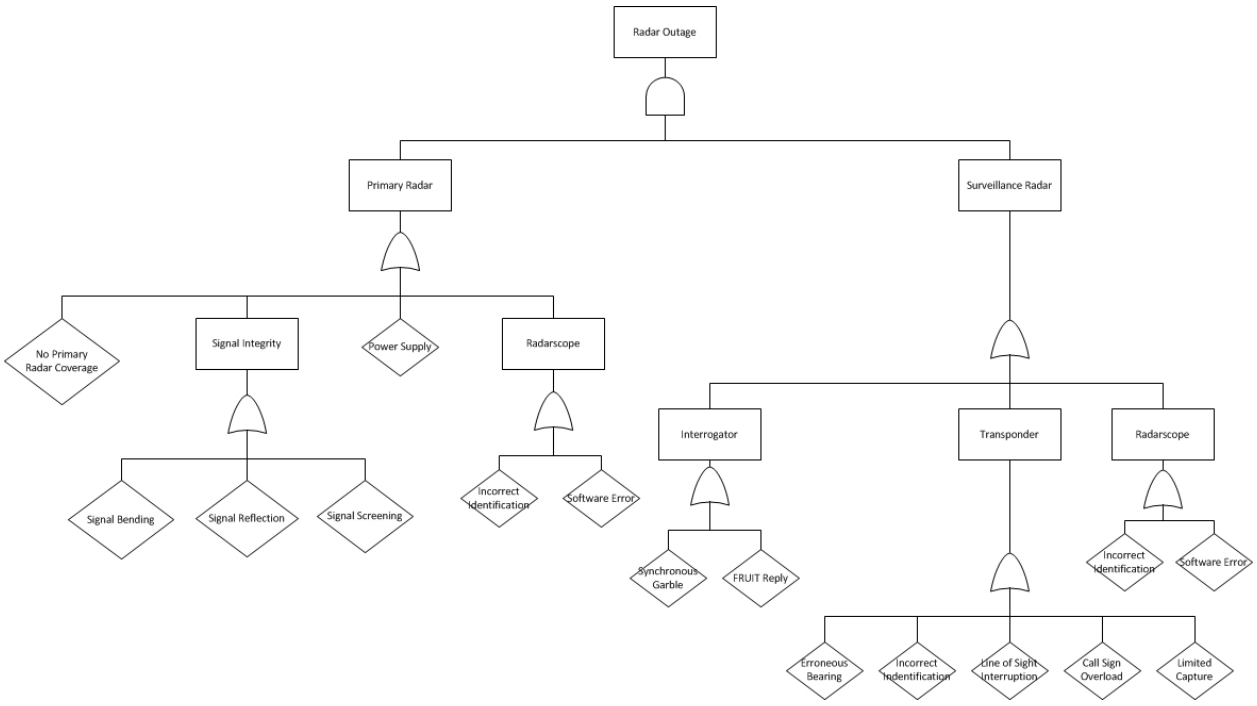


Figure 8.7 – Radar Outage Fault Tree

The fault tree shows few redundancies among the system but it should be considered the oftentimes multiple radars cover larger or more important airspaces such as the terminal airspace (TRACON). The minimal cut set can be represented by any combination of events within primary radar and surveillance area branches of the fault tree. It should be mentioned that the failure of primary

radar at this point in time is consider almost negligible. After completing the fault tree further questions were asked as to the importance of this risk scenario since the fault tree was not incredible beneficial. The real question and worry with Radar Outage occurs with the introduction of ADS-B and the possible disbanding of current radars to decrease maintenance costs. These worries fall within the organizational perspective and will be study as such.

8.2c Voice Communication Failure

The Voice Communication is currently the main link between the air traffic controller and the pilot in the current configuration. The pilot will switch from air traffic controller to air traffic controller as he moves through the airspace. Voice communication is used for clearances, altitude changes, vectoring, as well as any other necessary communication. The real problem within the voice communication system occurs not with a brief outing but an extended outage.

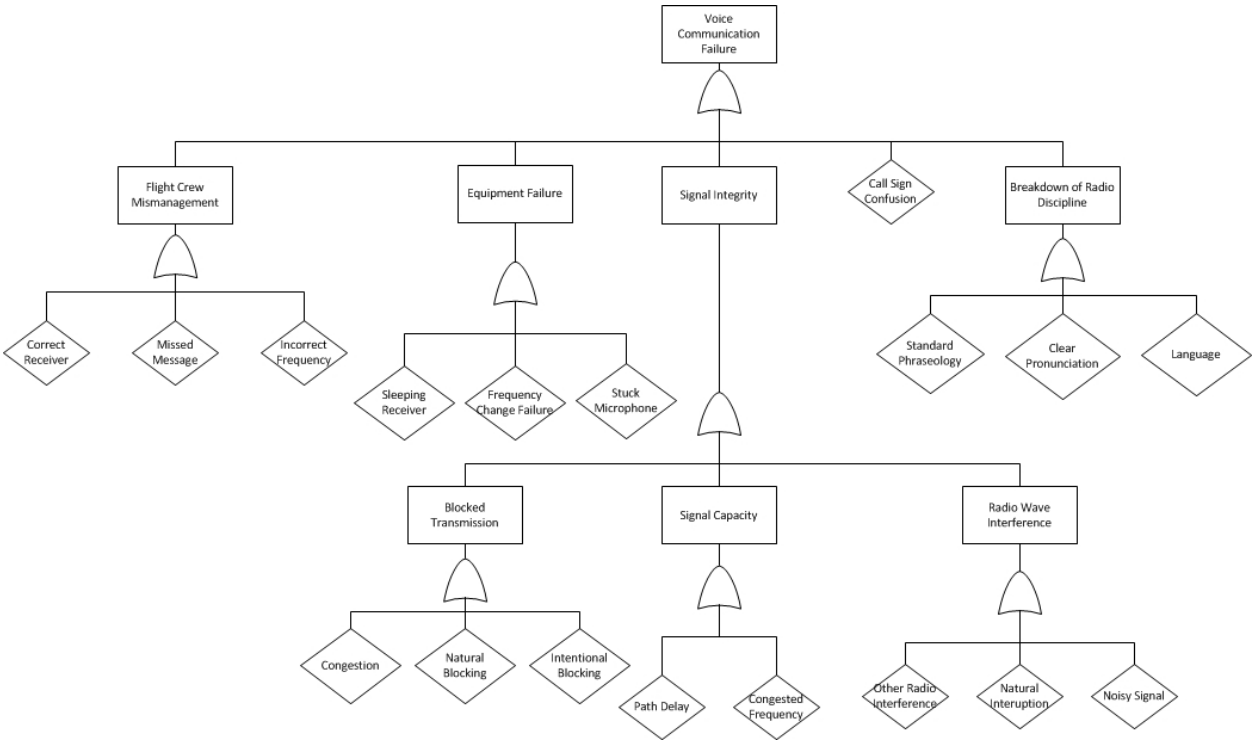


Figure 8.8 – Voice Communication Fault Tree

The voice communication system has many points of fault throughout the system. Two key faults exist, mechanical fault and human error. Often mechanical faults are fixed within a reasonable time frame but a human error can have large and lasting affects within the NAS. The question to be answered for the CNS integration is if the human error factor will be decreased with the introduction of data communication? If so, will technological failures occur at a greater rate offsetting any decrease of human factor error in voice communication? The answer to these questions must be answered but may not be possible until the implementation of the ATN-B2 datalink. It should be stated that this unknown factor raises questions as to the timeframe of limiting voice communication. It is likely the FAA will continue the use of Voice Comm until this questions can be answered.

9. Event Tree Analysis

The fault tree analysis presented in the previous section exhibits the failure modes of key systems and scenarios within the CNS integration but the use of probabilities and reliabilities were not used due to the lack of information for this emergent S-o-S. While fault tree analysis still provides a great deal of understanding regarding the interconnections and interdependencies within a complex S-o-S through the minimal cut set. While not used for this research Event Tree Analysis is another tool that can be useful in similar situations where probabilities are not available. Furthermore, event tree analysis incorporates a notion of time frame associated with the risk events along the path to total system failure.

This technique, developed by Bogdanor (2014), can be reviewed in full in Section 4.4 of his Thesis, *Risk Analysis of GPS-Dependent Communications Critical Infrastructure Utilized by the US Electric Power Grid*. Event Tree Analysis follows a chronological order of events beginning with some initiating event. At each stage a success or failure may be possible leading to different options at the next stage and eventually to all possible outcomes that can occur after the initiating event. If probabilities are available

it is possible to use the analysis to determine the likelihood of all possible outcomes through the use of the law of total probability and the assumption of the independence of the likelihood of failure at each stage.

In certain situations this technique may provide another tool to be used to explore risk events and scenarios especially when the timeline of events is critical or when probabilities are missing. The technique provides a unique and new perspective that has had great success in other risk analysis projects. While not used within this research it should be consider as a valuable tool within the overall framework and methodology that is presented here for work on complex and emergent systems of systems.

An example of event tree analysis from Bogdanor (2014) is shown below in **Figure 9.1** to further understanding of what the teqhnique looks like within a real world example.

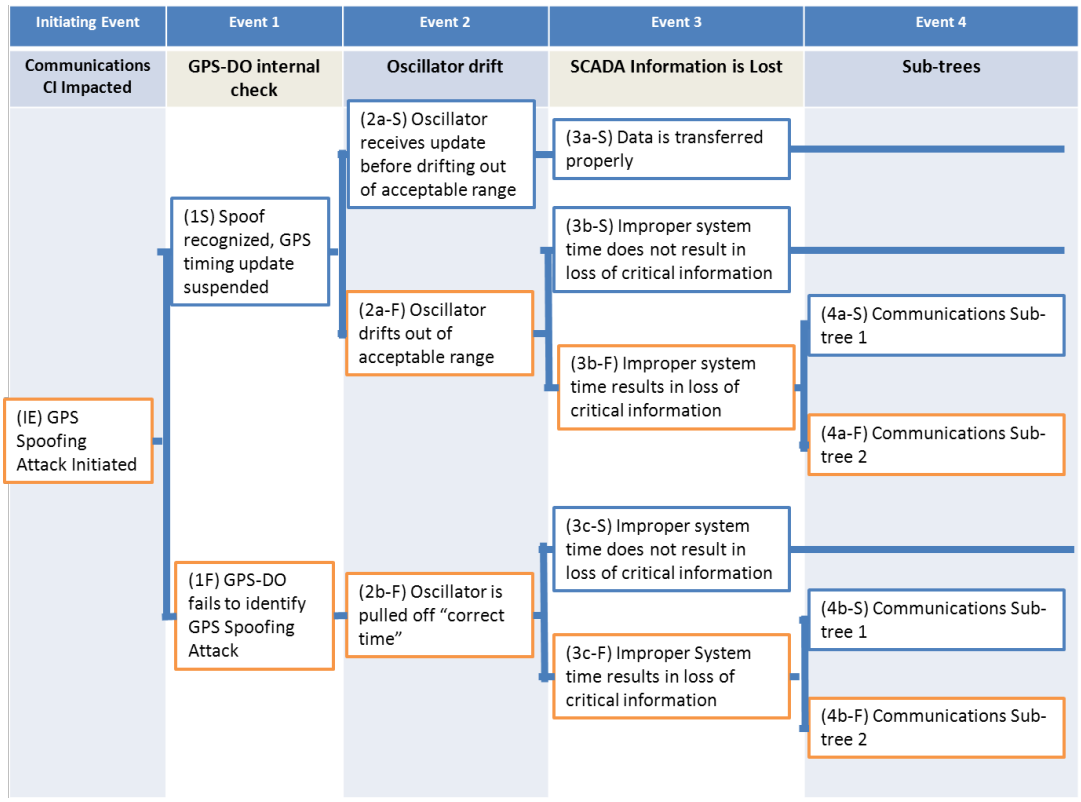


Figure 9.1 – Event Tree Example: GPS Spoofing Attack vs. Communication CI Event Tree [Bogdanor]

10. Synergy of Operational and Structural Perspectives

In the process of performing this analysis we found a synergy between the operational and structural perspectives used throughout the risk analysis. It was apparent that these two perspectives were more than separate perspectives but were closely linked. Further study found these connections built in to the already established tools of shared factors and fault tree analysis. It was often found that components that represented the minimal cut set in Fault Tree were closely linked to the shared factors discovered at the beginning of this analysis.

10.1: Shared States (Factors)

As discussed previously shared factors play a primary role in finding the interdependencies and interconnections among systems and subsystems that help lead to the determination of risk scenarios to be further considered. The usefulness of shared states can be expanded to further aid our risk assessment and management by considering decisions and Emergent Forced Changes (EFCs), both internal and external, affecting the S-o-S. This operational/Decision Making human interface innate to shared factors provides a beneficial perspective for analysis.

Any decision within a complex S-o-S is likely to have far reaching and possibly unknown effects on the system as a whole. Shared factors provide a way to understand where the effects of any decision will cause possible changes to the current way in which a S-o-S operates. Knowledge of all shared factors provides a means of understanding the interconnections and interdependencies of a S-o-S that may be used to understand how decisions affecting one factor affect the other sub-systems within a complex S-o-S.

Similarly, the effects of EFCs can be understood utilizing shared factors to determine how they make their way through a S-o-S. Effects on any specific factor caused by an EFC can be tracked by that specific

factor's connections to other systems within the S-o-S. These insights are invaluable in determining the importance of a specific EFC and their long term effects on the system. Continually utilizing shared states can allow stakeholders to effectively manage not only previously considered EFCs but new EFCs that occur without prior consideration significantly shortening the time to manage any significant risk to the S-o-S.

10.2: Fault Tree Analysis

While Shared States provide great insight into the effects of decisions and EFCs on a S-o-S through their interconnections and interdependencies Fault Tree Analysis (FTA) looks at the structural/cyber-physical connectedness among a complex S-o-S. As discussed above FTA is used to determine a minimal cut set for a specific system, capability, or process (Top Event) within the S-o-S. This minimal cut set determines the key structural/cyber-physical components within the S-o-S that leads to a failure of the top event. Utilization of probabilities or Event Tree can bring further understanding to the system.

Fault Tree is best at providing an understanding of the physical connections that form within the S-o-S. With the creation of a minimal cut set it can be determined what physical elements of a system are key to its continued function. Those elements can then be linked within the specific fault tree or to their occurrence within another system's minimal cut set.

10.3: The Synergy between Fault Tree and Shared Factors

With shared factors and fault tree analysis both providing a way to discover interconnections and interdependencies of a S-o-S within risk analysis it is reasonable to consider the synergy of these two techniques. On one hand shared factors consider the risks presented through functional/operational and time frame considerations emanating from decisions made within S-o-S and EFCs. On the other

hand Fault Tree Analysis considers structural / cyber-physical dimension of the S-o-S and how the reliability of each piece affects the system or subsystem in consideration.

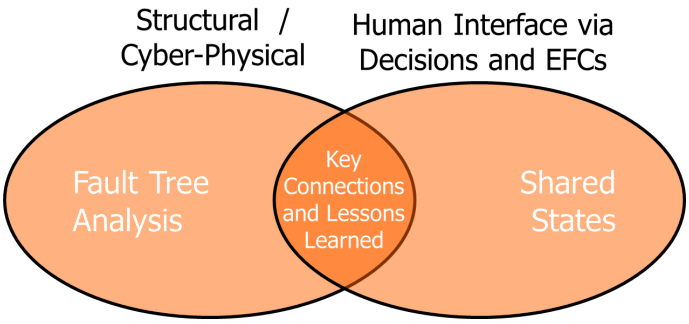


Figure 10.1 – Synergy of Structural and Operational Perspectives

It is natural to then consider if there is a link among the shared factors discovered and the minimal cut sets determined through FTA. To find such a connection the minimal cut sets found through Fault Tree Analysis are crosschecked with the shared factors found previously. It is expected to find at least one factor that stems from the members within a minimal cut set. This connection bridges the gap between the structural/cyber physical makeup of the system and the functional/operation and timeframe considerations built upon to form the list of shared factors.

An example of this can be found within the FAA's NextGen project where they are considering the integration of the CNS as S-o-S. The shared states and Fault Tree used to show the connection is shown below in the Appendix. We will consider the failure of the Dynamic RNP capability with consideration to shared factors and a Fault Tree. Within the DataLink branch of the Fault Tree the minimal cut sets include a member of both the ATN-B2 system and FANS 1/A system. With that consideration, where can we find shared factors affecting these systems? The Flight Management Computer (FMC) is required to properly ensure completion of any communication for the aircrafts DRNP capability and represents a vital shared resource. Looking at the Positioning System the key factors include signal integrity, receiver integrity, and the flight management computer. These three states show up as part of the minimal cut

set within both the DME/DME configuration and GNSS configuration of the positioning system. These interconnections are linked using both Shared Factors and Fault Tree analysis providing further valuable information to the interconnections and interdependencies of this S-o-S.

This brief example can show the beautiful link of shared factors and fault tree analysis in determining connections among S-o-S that can be used to prepare for EFCs and make key decisions in a systems future operation. This synergy provides a beautiful connection of two seemingly separate Risk Analysis techniques.

11. Organizational Perspective

The great synergy between Fault Tree Analysis and Shared Factors must be further considered within their organizational environment. While a great deal can of knowledge be gained from the interconnections and interdependencies found through FTA and Shared Factors the organizational environment can significantly change how the S-o-S operates. Any S-o-S is bound to the organization which it operates within. A multitude of factors within an organization can greatly change the operation of a system causing adjustments throughout the analysis.

Taking from the work of Ashkenas et. al. in *The Boundaryless Organization: Breaking the Chains of Organizational Structure* we posit that one should consider four main areas within an organization must be considered in order to have a comprehensive analysis. There are vertical considerations, which represents the different levels and ranks of people, horizontal considerations, representing the different functions and disciplines across an organization, external considerations, representing the interaction of the organization to the outside world such as supplies, customers, regulators, etc., and finally geographic considerations [Ashkenas et. al., 1995]. All these pieces greatly affect the S-o-S and the interconnections and interdependencies determined using Fault Tree Analysis and Shared Factors.

A full integration of the S-o-S must include changes that will be made across a diverse and complex organization such as the FAA. Some possible effects on each consideration are discussed further.

1. ***Vertical*** – With the implementation of new technology the FAA must consider effects to the current vertical structure of the system. How will management of the airspace change? What will the changing role of Air Traffic Controllers, Pilots, and Airport Managers effect the S-o-S. Will there be a change in the structure of command due to these knew technologies and capabilities?
2. ***Horizontal*** – The FAA must consider the changes in boundaries as they consider these new technologies. For example, the boundary between UAVs, Commercial, and General Aviation. How will it affect this emergent S-o-S?
3. ***External*** – The FAA operates in a complex environment with many stakeholders representing many areas of the airspace. Some key stakeholders that need to be considered in the decision making process include Airlines, Pilots, Airports, Air Traffic Controllers, General Aviation, UAVs and their infrastructure and personnel,
4. ***Geographical*** – While the FAA creates rules and decision for the United States the current airspace is no doubt a global one. Decisions made and possible EFCs can be influenced by the decisions made by other aviation administrations across the globe [Ashkenas et. al, 1995].

Further building on the work of interconnections and interdependencies of FTA and Shared Factors one can benefit from the understanding of the organizational structure and changes necessary to complete the S-o-S. Each portion of the analysis provides and unique view and perspective that helps build to a final understanding of the S-o-S. Without the hard work in determining structural / cyber physical (FTA) and operational (STA) interconnections there is no use in considering organizational changes as there is no way to understand how those changes would propagate throughout the S-o-S.

12. Overview of Operational, Structural, and Organizational Perspectives

There is a clear synergy between the interdependencies and interconnectedness of a S-o-S found from two separate perspectives in Fault Tree Analysis and Shared Factors. Fault Tree Analysis finds and builds on interdependencies and interconnections found through the structural/cyber-physical dimension of the S-o-S while Shared Factors takes advantage of the Operational/Decision-Making dimension. Both provide a great deal of useful information that lead to an effective risk assessment and management of complex emergent S-o-S. Furthermore the analysis would be incomplete without consideration of organizational effects, vertical, horizontal, external, and geographic. We posit that by incorporating these three separate but connected perspectives a well thought out systems based methodology is presented within this thesis.

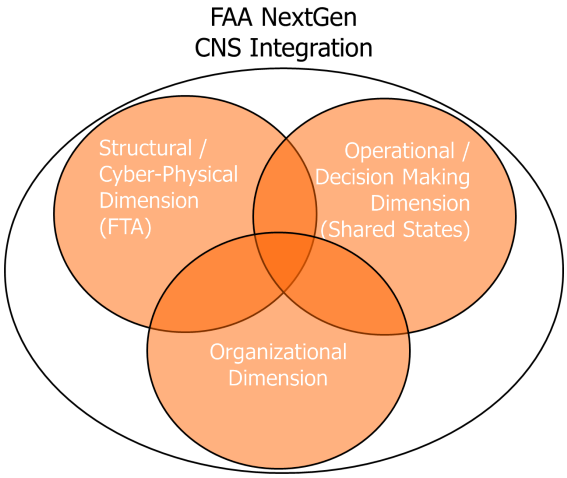


Figure 12.1 – Three Necessary Perspectives of a Complex S-o-S

The structural and operational dimensions share many close links and build a wealth of knowledge in regards to the S-o-S and its interconnections and interdependencies for this integration but the organizational perspective ensures that the work holds over time. A well thought out analysis using only two perspectives could fall greatly short if unforeseen changes to the organizational structure appear. With this in mind the three perspectives shown here are vital to our systematic modeling framework.

Part III: Summary and Conclusions

13. Key Challenges

Of the numerous challenges associated with this thesis research, managing the large scope of the project, finding information on an emerging system, and then managing the complexity of the S-o-S mark the key challenges that had to be overcome for this study to be successful. With a large initial scope covering four different configurations and five separate phases of flight (take-off, en-route, approach, paired approach, and missed approach) an appropriate scope had to be found. Along with the determination of scope there were many levels of the system to consider. Oftentimes our scope and analysis were overwhelming in the details of specific system inner workings, other times there were not enough details to perform a proper risk assessment.

Gaining knowledge and insight within complex and emergent system of systems is vital; and a significant amount of information was gleamed from technical documents and subject matter experts in lieu of an unavailable database. The process of determining shared factors aided in this process but the meticulous process required to determine the appropriate shared factors cannot be overlooked. We believe our work overcame this lack of data, and it is appropriate to perform a proper systematic risk analysis; however there is no perfect substitute for data on any particular system. As it is possible with emergent systems there may not be a means to collect this data until after the "go-live" date for these capabilities ever increasing the need for a holistic systematic risk analysis for the CNS Integration.

Moreover each of the Communication, Navigation, and Surveillance systems are, in their own right, inherently complex S-o-S with many subsystems and components meeting the operational goal of each main system. This complexity represents a significant challenge. In overcoming this challenge to modeling and management a great amount of technical knowledge and understanding had to be gained

of the CNS as S-o-S to provide a satisfactory risk analysis. Even so, a complete and thorough understanding of the entire system was well beyond the scope of this thesis, and we leaned on the help of subject-matter experts to fill in information as needed. The initial push to determine essential factors in this analysis provided the main means for gaining a technical and operational understanding of each of the systems involved, communication, navigation, and surveillance.

14. Summary of Contributions

This research builds a systems-based holistic methodology to address the emergent forced changes and then the risks that may occur when integrating a complex and emergent S-o-S. The methodology is built on a foundation of well-established risk methodology and forms a framework which considers the synergy of the operational and structural perspectives to such a S-o-S through shared factors and fault-tree analysis. The research outlines this synergy and the connections that are expected to be discovered between the two separate yet connected systems-based risk analysis methodologies. Furthermore the work encourages a holistic view by overlaying an organizational view to any S-o-S integration. Without all three perspectives represented the analyst would leave himself open to missing a vital aspect to the system that could negatively affect future decisions and options based on current decisions made without regards to the three perspectives.

These three perspectives, operational, structural, and organizational, were built on the shoulders of previously established risk methodologies. The operational perspective was studied using extensive research to determine essential states and factors that described and represented the S-o-S [Haimes 2009]. These factors and the knowledge gleamed from the study allowed for the determination of key risk scenarios in the absence of a completed HHM. Using a modified Risk Filtering, Ranking, and Management method these risk scenarios were filtered to determine the key scenarios that should be further analyzed [Haimes 2009]. These key scenarios were then treated to a structural perspective.

Through fault tree analysis these different systems were studied at the structural level to determine key interconnections and interdependencies through their minimal cut set. The minimal cut set then showed a synergy with the essential shared factors determined in the initial study of the system [U.S. Nuclear Regulatory Commission, 1981]. This synergy represents the interaction between the two perspectives, operational and structural.

Finally with significant study on the operational and structural perpsectives completed a brief discussion of the organizational perspective was presented [Ashkenas et. al., 1995]. While thorough study could not be completed within the timeframe of this research the suggestions presented build a stepping stone for further research on this perspective. The organizational perspective will be vital in fully understanding the complex S-o-S.

15. Recommendations for Future Work

First and foremost a significant study of the organizational perspective of this S-o-S would provide a great benefit to the CNS Integration project. Any study spent on further investigation to the organizational changes coming due to the integration would provide immense value to the team. These organizational realignment could significantly impact the findings presented here through changes in policy, rules and regulations, management hierarchy, training times, or a multitude of other organizational factors.

While this research covered a portion of the CNS Integration, it is only a small portion compared with the entire project. Initially there was consideration to provide a comprehensive analysis across four configurations, (i) current, (ii) dynamic RNP, (iii) pairwise procedure, and (iv) pairwise procedure coupled with NextGen safety protocol. Not only are four configurations important to the NextGen Integration but each configuration can be further divided in to the different phases of flight, departure,

en-route, and approach with each phase of flight relying on different systems and procedures to meet a specific objective. Each phase and configuration presents new challenges and risks to such an integration. The methodology here should lay a solid groundwork to begin such analysis but the large scope of such an undertaking will take much more research in the coming years.

16. References

1. "Aeronautical Telecommunications Network (ATN)." FAA William J. Hughes Technical Center, n.d. Web. 18 Nov. 2014. <http://www.tc.faa.gov/its/cmd/visitors/data/ACT-300/atn.pdf>.
2. A.P. Sage and C.D. Cuppan, On the systems engineering and management of systems of systems and federation of systems, Inform Knowledge Syst Management 2(4), (2001), 325-345
3. A.P. Sage and S.M Biemer, Processes for systems family architecting, design and integration, IEEE Syst J 1(1) (2007), 5-16
4. Ashkenas, Ronald N. The Boundaryless Organization: Breaking the Chains of Organizational Structure. San Francisco: Jossey-Bass, 1995. Print.
5. Bogdanor, Josh M. "Risk Analysis of GPS-Dependent Communications Critical Infrastructure Utilized by the US Electric Power Grid." Thesis. University of Virginia, 2014. Print.
6. Buntin, Marc, and John Dutton. DRNP Fg2 Briefing 1-22-14 Final. N.p. PDF.
7. Butchibabu, Abhizna, Midkiff, Alan, Kendra, Andrew, Hansman R. John, and Chandra C. Divya. “Analysis of Safety Reports Involving Area Navigation and Required Navigational Performance Procedures”. International Conference on Human-Computer Interaction in Aeronautics (HCI-Aero), Cape Canaveral, FL, 3-5 November 2010.
8. D. Luzeaux, J.R. Ruault & J.L. Wippler, "Complex Systems and Systems of Systems Engineering", ISTE Ltd and John Wiley & Sons Inc, 2011
9. Federal Aviation Administration. March 27, 2014. Dynamic Required Navigational Performance Preliminary Concept of Operations.
10. Finkelsztein, Daniel M. 4d Dynamic Required Navigation Performance Final Report. Hampton, Va.: National Aeronautics and Space Administration, Langley Research Center, 2011.
11. Garvey, P. R., 2008, Analytical Methods for Risk Management: A Systems Engineering Perspective, Chapman-Hall/CRC-Press, Taylor & Francis Group (UK), Boca Raton, London, New York, ISBN: 1584886374.
12. Haimes, Y.Y., 1981, Hierarchical holographic modeling, *IEEE Transactions on Systems, Man, and Cybernetics* **11**(9): 606-617.
13. Haimes, Y.Y., Modeling and Managing Interdependent Complex Systems of Systems, 2016, Submitted to John Wiley & Sons, New York, New York.
14. Haimes, Yacov Y. "On the Complex Definition of Risk: A Systems-Based Approach." Risk Analysis 29.12 (2009): 1647-654.

15. Haimes, Y. Y. (2009). Risk modeling, assessment, and management. 3rd ed. Hoboken, NJ: John Wiley & Sons.
16. Haimes, Y. Y. (1991), Total Risk Management. Risk Analysis, 11: 169–171.
17. Held, J.M.,The Modelling of Systems of Systems, PhD Thesis, University of Sydney, 2008
18. "Homeland Security." *What is Critical Infrastructure?* N.p. Web. 13 Mar. 2015. < http://www.dhs.gov/what-critical-infrastructure>
19. Kaplan, S. and Garrick, B. J. (1981), On The Quantitative Definition of Risk. Risk Analysis, 1: 11–27.
20. Moertle, Peter, Katkin, Rafe, Karen Viets, Bill Penhallegon and Randy Bone. *Advanced Interval Management Overview*. [PowerPoint Slides]. March 4, 2014.
21. M.W. Maier, Architecting principle for systems-of-systems, Syst Eng 1(4) (1998), 267-284
22. Nakamura, David, and William Royce. "Operational Benefits of Performance-Based Navigation." Boeing, 2008. Web. 2 Dec. 2014.
23. Oki Electric Industry Co., Ltd., March 29, 2003. "ATN Router Overview". < https://www.oki.com/jp/SSC/ITS/eng/image/atn200303.pdf >
24. Safety Management System Manual Version 4.0. N.p.: FAA Air Traffic Organization Safety and Technical Training, 1 Sept. 2014. PDF.
25. The MITRE Institute, September 1, 2007, "MITRE Systems Engineering (SE) Competency Model, Version 1," pp. 10, 41–42.
26. Walter, Randy. "Flight Management System." The Avionics Handbook. Boca Raton: CRC, 2001. N. pag. Print.
27. U.S. Nuclear Regulatory Commission, 1981, *Fault Tree Handbook*, NUREG-81/0492.

Appendix A. Multi-Criteria Analysis SME Tables

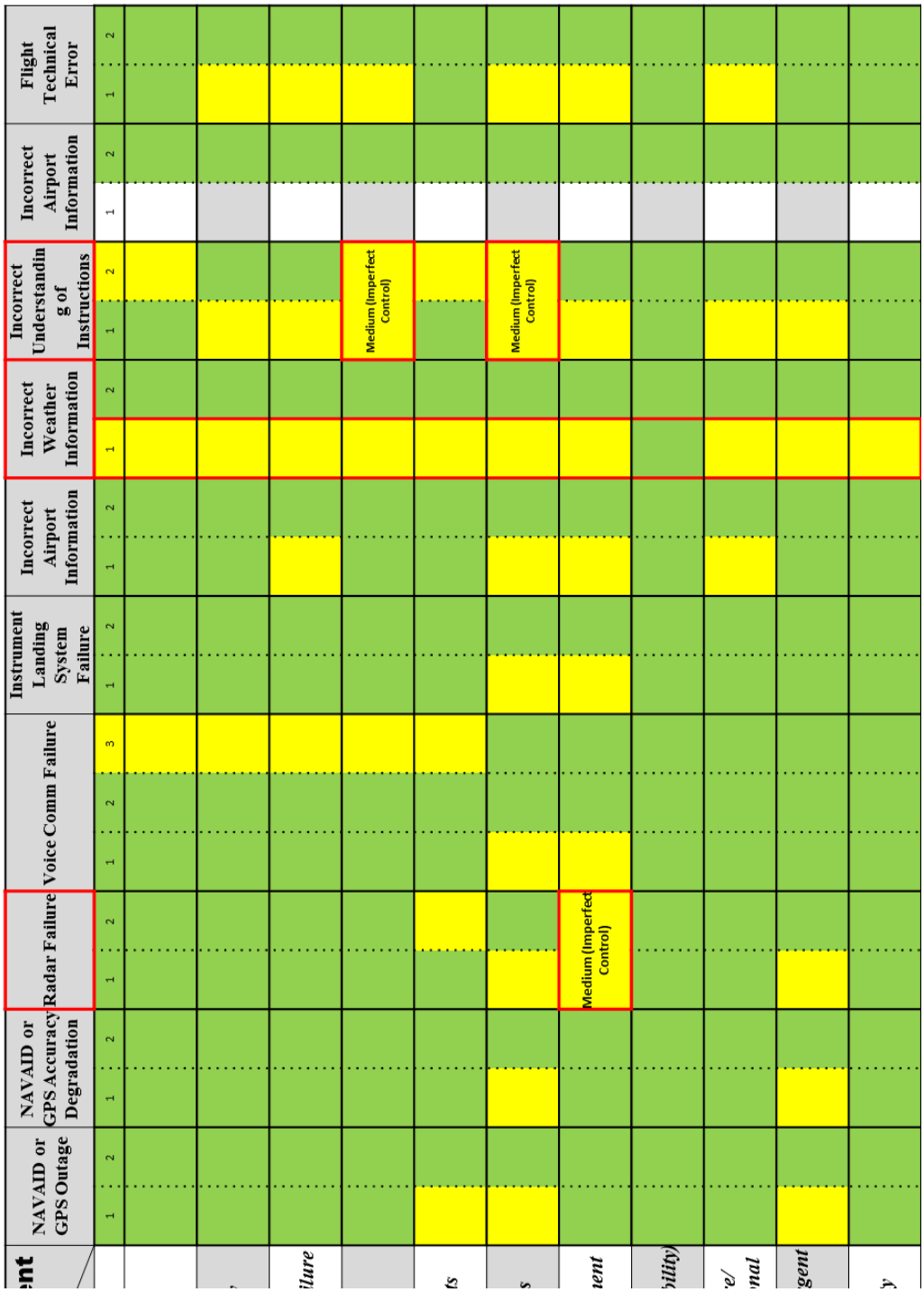


Figure A.1

Medium High

Column 2: Mr. Gerry McNeil – Nav Expert / Pilot Experience
Column 3: Dr. Monticone – Comm Expert

Current Configuration - Value - Approach Phase of Flight

	NAVAID or GPS Outage		NAVAID or GPS Accuracy Degradation		Radar Failure		Voice Comm Failure			Instrument Landing System Failure		Incorrect Airport Information		Incorrect Weather Information		Incorrect Understanding of Instructions		Incorrect Airport Information		Flight Technical Error	
nion	1	2	1	2	1	2	1	2	3	1	2	1	2	1	2	1	2	1	2	1	2
ility																					
bility																					
o Failure																					
lity																					
Effects							Medium (Imperfect Control)														
ffects					Medium (Imperfect Control)		Medium (Imperfect Control)														
ronment																					
Durability)																					
ftware/ izational																					
emergent rs																					
nturity																					

Figure A.2

Medium High

Column 2: Mr. Gerry McNeil – Nav Expert / Pilot Experience
Column 3: Dr. Monticone – Comm Expert

Dynamic RNP Configuration - Safety - Approach Phase of Flight

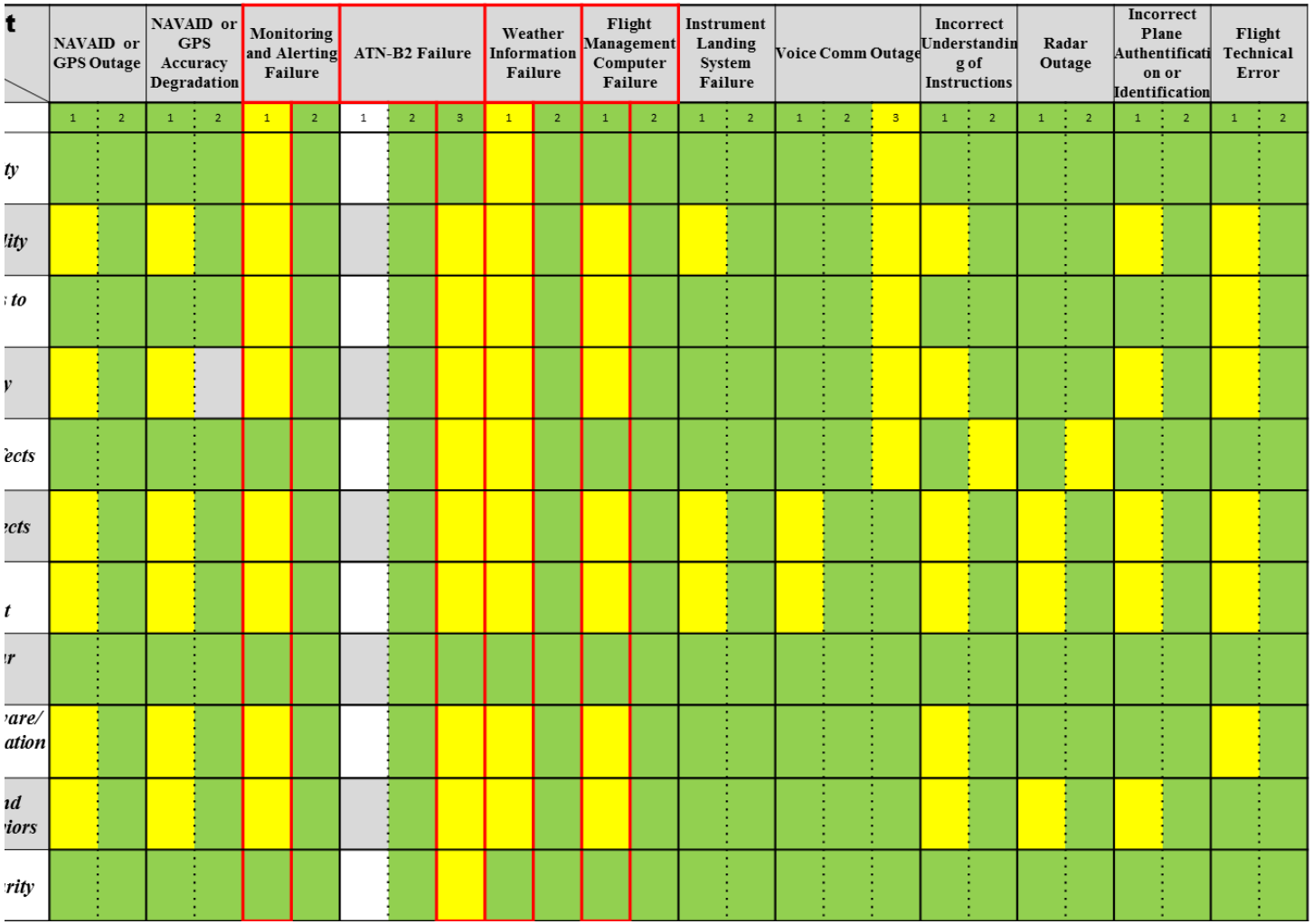


Figure A.3

Column 3: Dr. Monticone – Comm Expert

Dynamic RNP Configuration - Value - Approach Phase of Flight

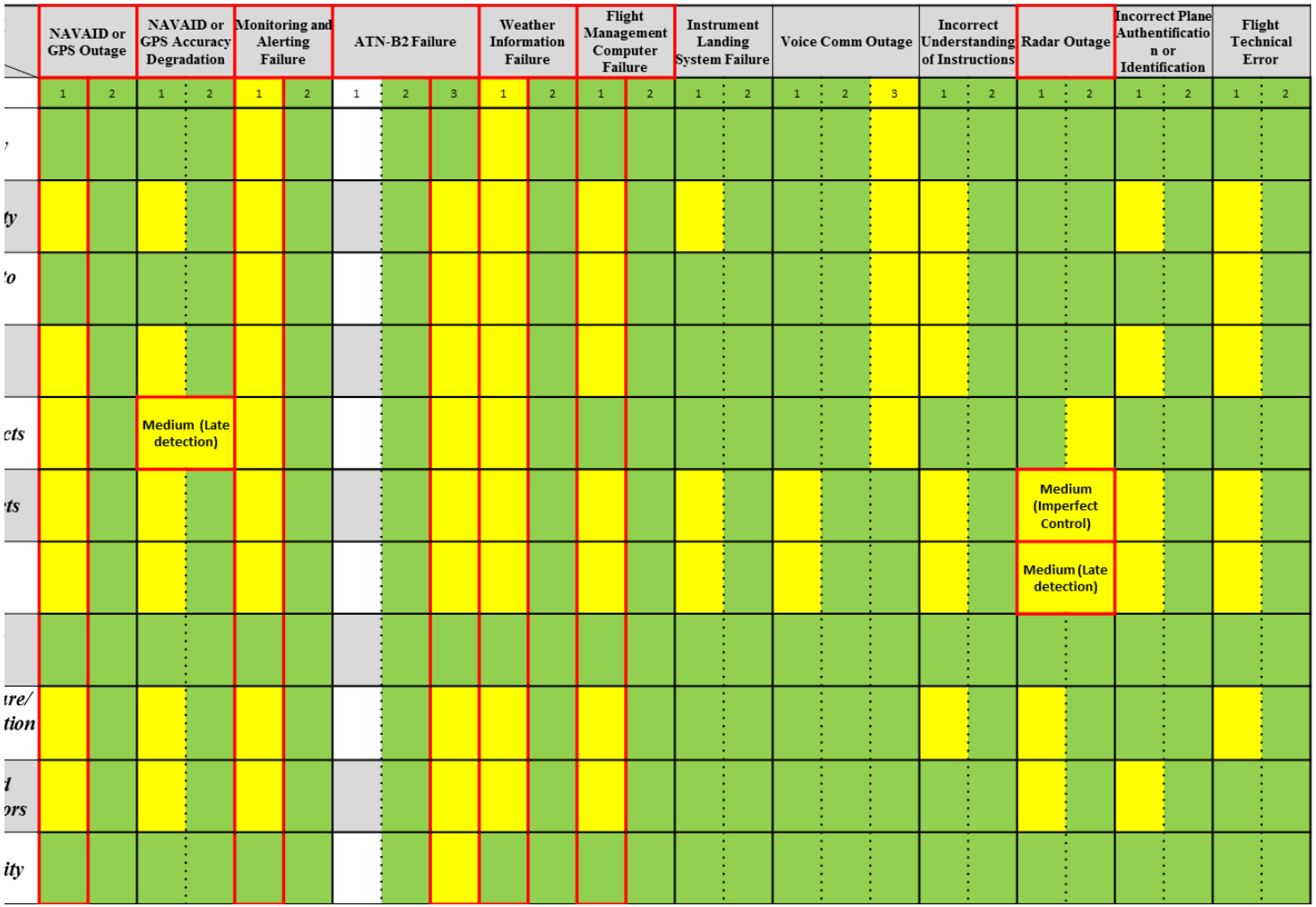


Figure A.4

Appendix B. Full Page Fault Tree Figures

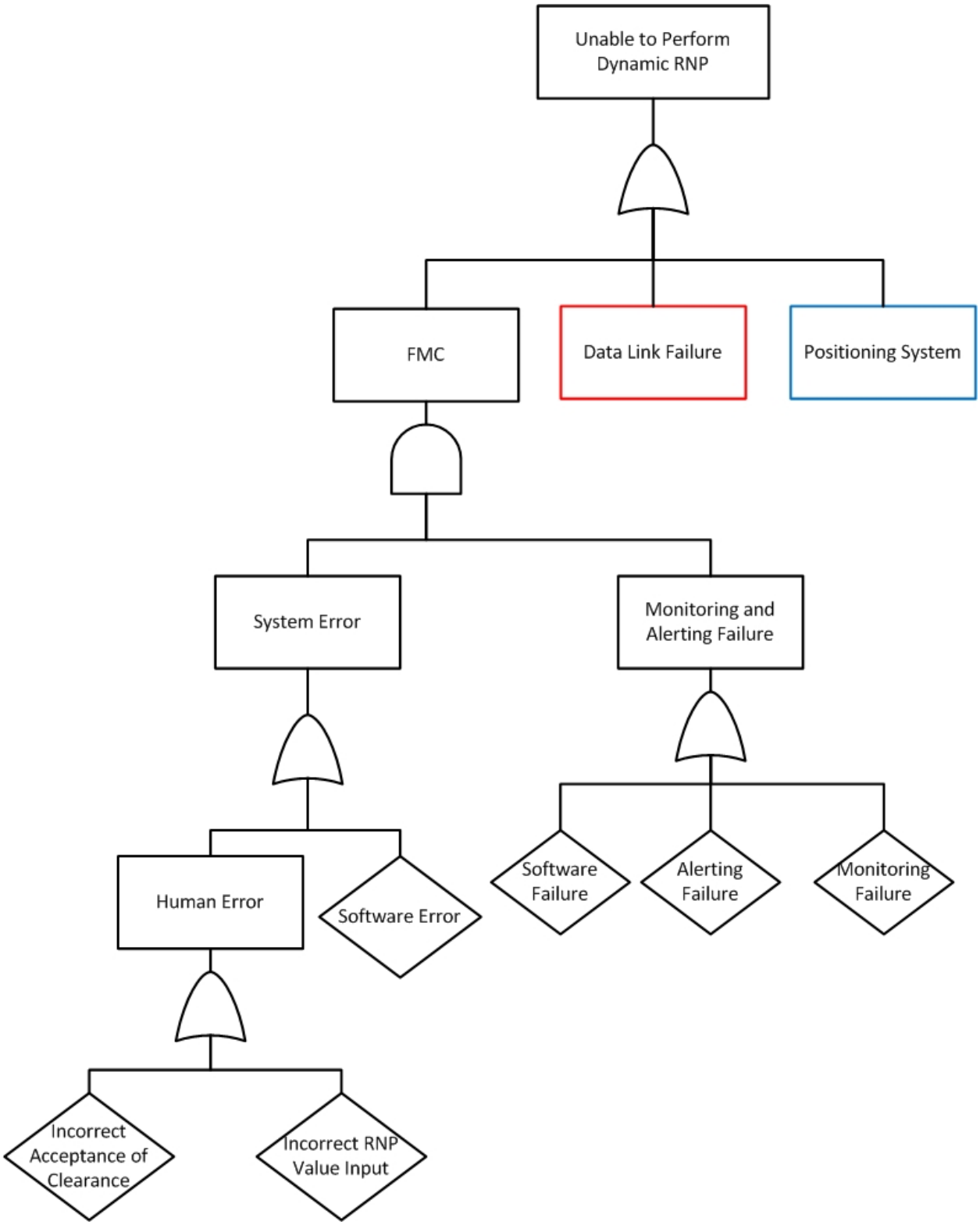


Figure B.1 – Flight Management Computer Fault Tree

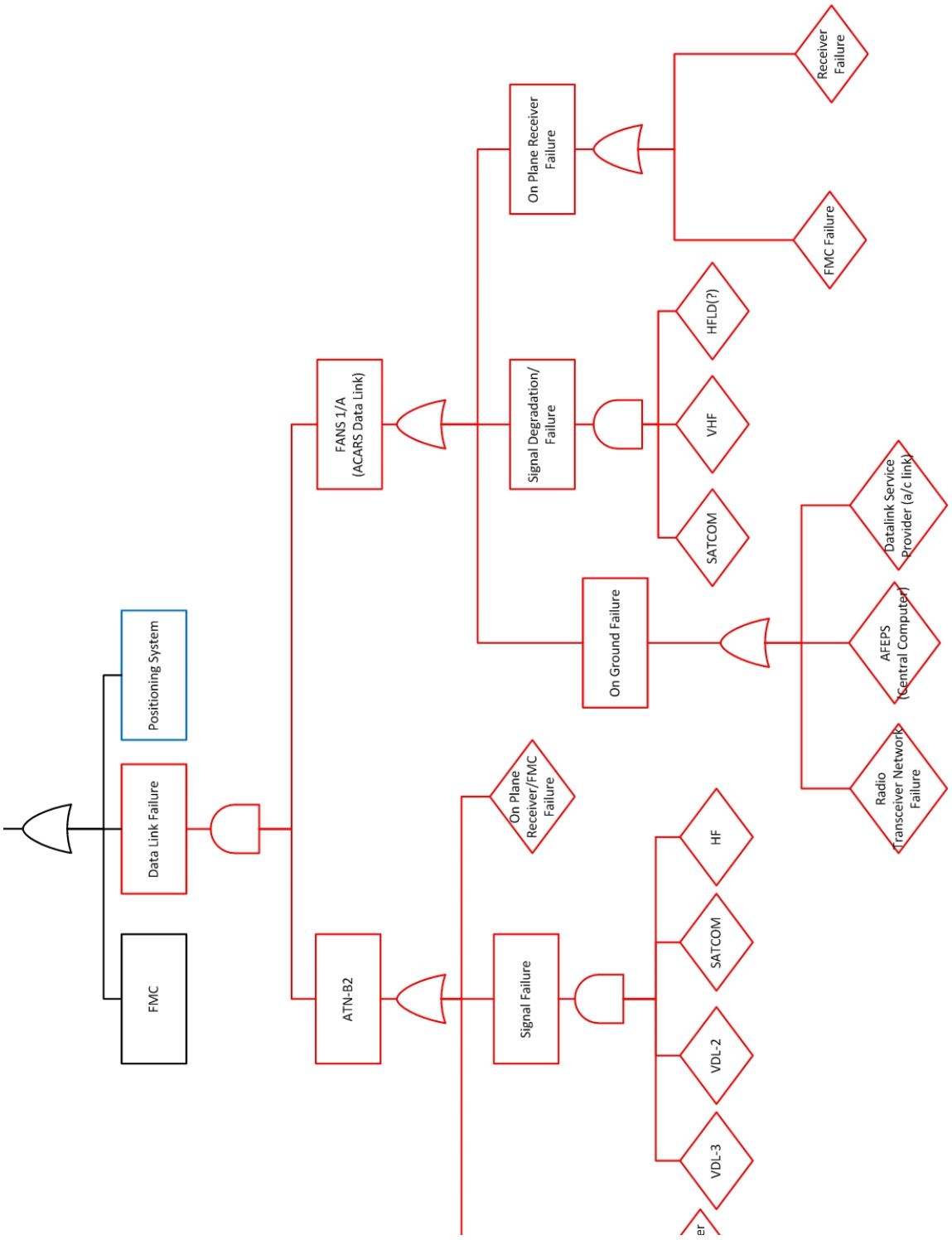

FMC
Positioning System
Data Link Failure
ATN-B2
FANS 1/A (ACARS Data Link)
Signal Failure
On Plane Receiver/FMC Failure
Signal Degradation/ Failure
On Plane Receiver Failure
On Ground Failure
HF
SATCOM
VDL-2
VDL-3
HFLD(?)
VHF
SATCOM
Receiver Failure
FMC Failure
Datalink Service Provider (a/c link)
AFEPS (Central Computer)
Radio Transceiver Network Failure

Figure B.2

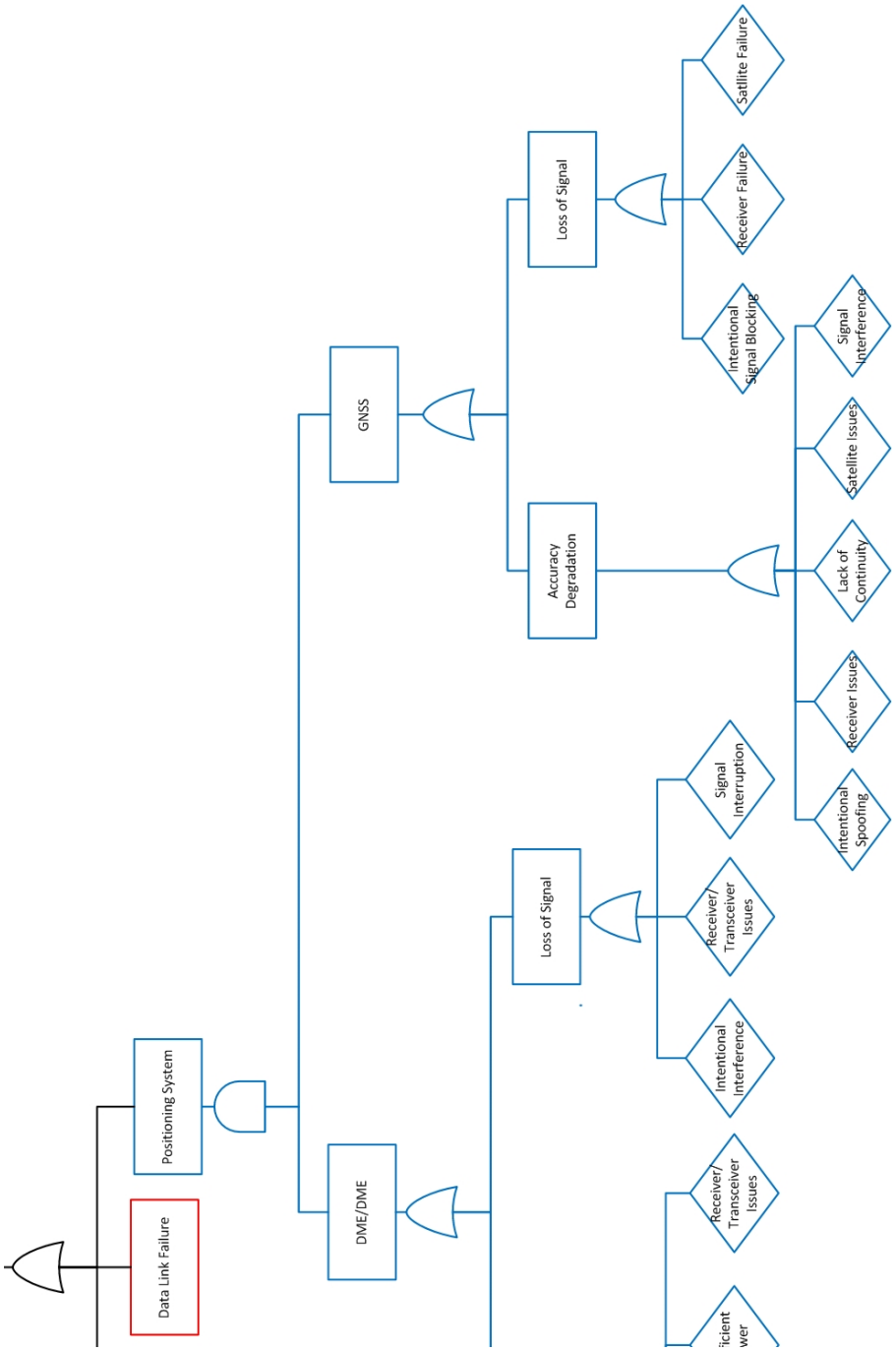

Data Link Failure
Positioning System
DME/DME
GNSS
Loss of Signal
Accuracy Degradation
Satlite Failure
Receiver Failure
Intentional Signal Blocking
Signal Interference
Satellite Issues
Lack of Continuity
Receiver Issues
Intentional Spoofing
Loss of Signal
Signal Interruption
Receiver/ Transceiver Issues
Intentional Interference
Receiver/ Transceiver Issues

Figure B.3

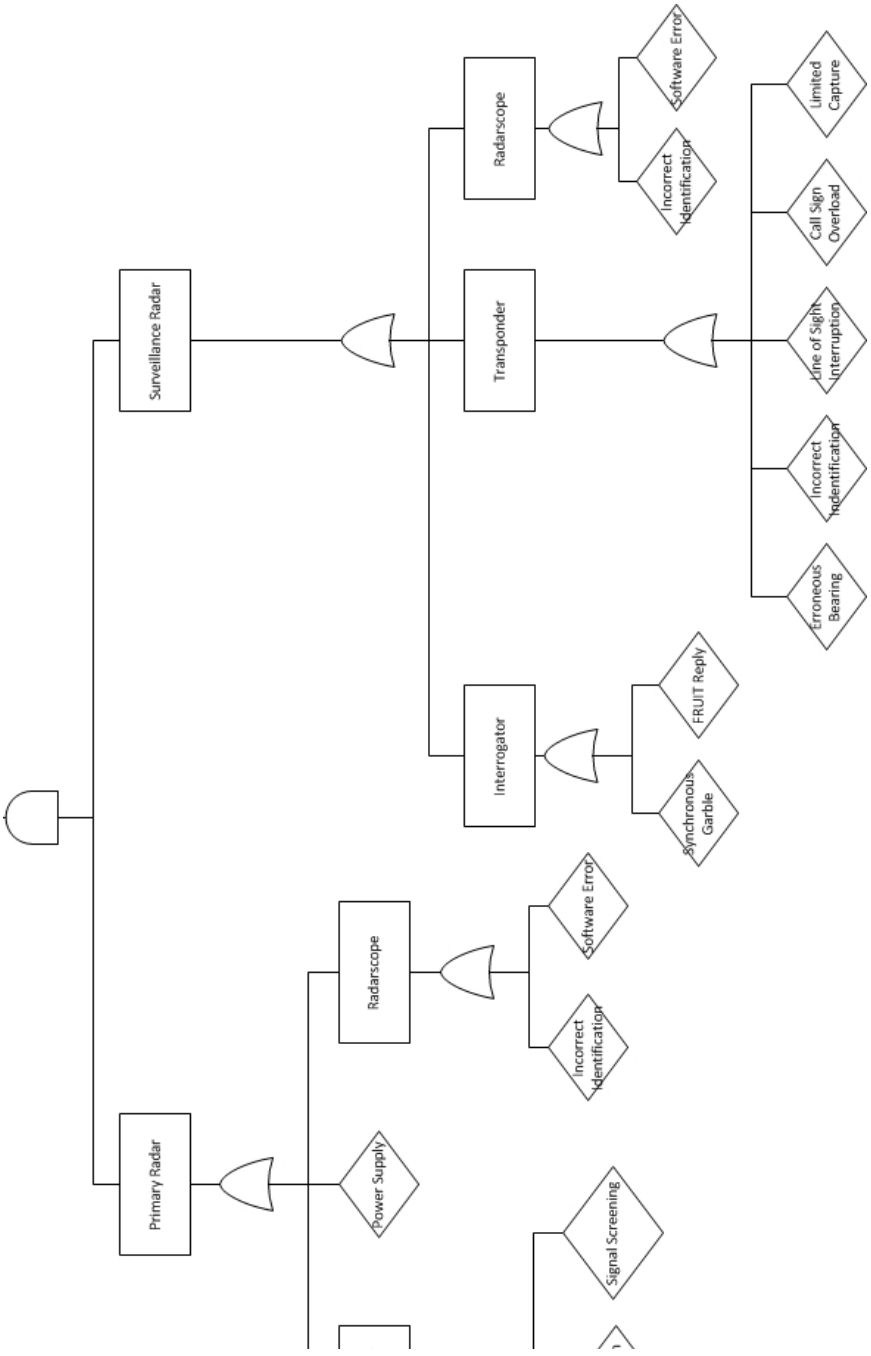

Surveillance Radar
Primary Radar
Radarscope
Transponder
Interrogator
Radarscope
Software Error
Incorrect Identification
Limited Capture
Call Sign Overload
Line of Sight Interruption
Incorrect Identification
Erroneous Bearing
FRUIT Reply
Synchronous Garble
Software Error
Incorrect Identification
Power Supply
Signal Screening

Figure B.4

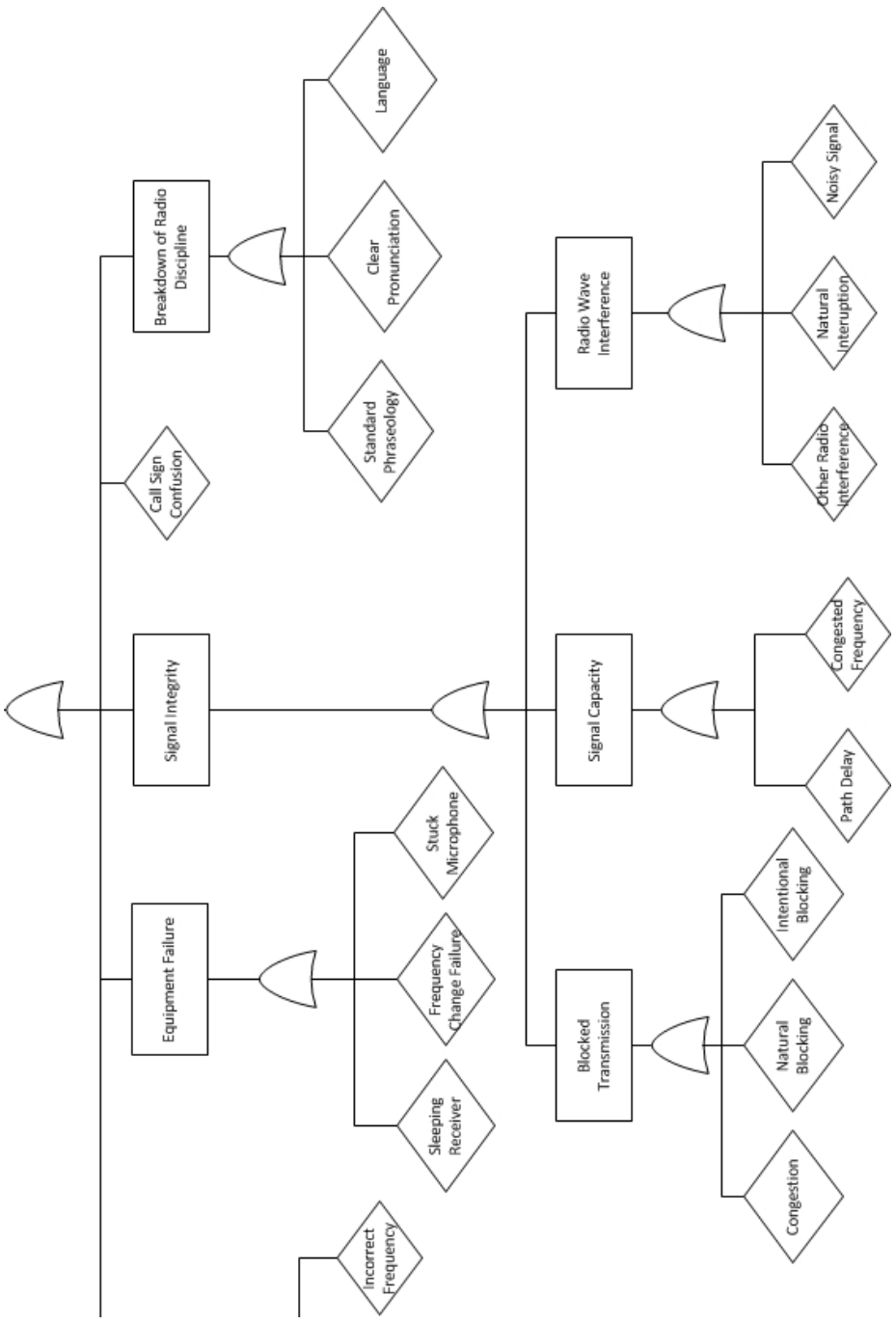

Signal Integrity
Equipment Failure
Incorrect Frequency
Sleeping Receiver
Frequency Change Failure
Stuck Microphone
Call Sign Confusion
Breakdown of Radio Discipline
Standard Phraseology
Clear Pronunciation
Language
Signal Capacity
Blocked Transmission
Congestion
Natural Blocking
Intentional Blocking
Path Delay
Congested Frequency
Radio Wave Interference
Other Radio Interference
Natural Interuption
Noisy Signal

Figure B.5

Appendix C. Acronyms Abbreviations

AAC	Airline Administrative Control
ACARS	Aircraft Communications and Reporting System
ADS-B	Automatic Dependent Surveillance - Broadcast
AOC	Aeronautical Operational Control
ARINC	Aeronautical Radio, Inc.
ASOS	Automated Surface Observing System
ASR	Airport Surveillance Radar
ATIS	Automatic Terminal Information System
ATN-B2	Aeronautical Telecommunication Network Baseline 2
AWOS	Automated Weather Observing System
CNS	Communication, Navigation, and Surveillance
DME	Distance Measuring Equipment
DRNP	Dynamic Required Navigational Performance
FAA	Federal Aviation Administration
FANS	Future Air Navigation System
FMC	Flight Management Computer
FMS	Flight Management System
HHM	Hierarchical Holographic Modeling
ICAO	International Civil Aviation Organization
ILS	Instrument Landing System
INS	Inertial Navigation System
NDB	Non Directional Radio Beacon
NAS	National Airspace System
PAR	Precision Approach Radar
PBN	Performance Based Navigation
RNAV	Area Navigation
RNP	Required Navigational Performance
RFRM	Risk Filtering, Ranking, and Management
S-o-S	System of Systems
SME	Subject Matter Expert
SSR	Secondary Surveillance Radar
TRACON	Terminal Radar Approach Control Facilities
VOR	VHF Omni-Directional Range

Appendix D. RFRM Characteristics

1. **Undetectability** - refers to the redundancy of modes by which the initial events of a scenario can be discovered before harm occurs to the system. High undetectability represents a threat that is undetectable, medium refers to late detection or a risk that is hard to detect, while low represents an early and easy detection.

2. **Uncontrollability** refers to the redundancy of controlling modes by which it is possible to take action or make an adjustment to prevent harm to the system. High uncontrollability represents a risk scenario that is uncontrollable, while a low rating represents an easily controlled scenario. Medium represents a scenario falling between high and low dependent on a SME's judgement.

3. **Multiple paths to failure** indicates that there are multiple and possibly unknown ways for the events of a scenario to harm the system, such as circumventing safety devices. If there are many ways in which the system can fail following the initiating event, then the risk level here is deemed high. A low rating is given when there is only one path in which the system can fail. Medium represents a scenario falling between high and low dependent on a SME's judgement.

4. **Irreversibility** indicates a scenario in which the adverse condition cannot be returned to the initial, operational (pre-event) condition. A high rating represents a scenario that cannot be returned to any percentage of the original operating state. A medium rating represents the ability to return to a degraded mode of the original state while low is the full return to the original operating condition.

5. **Duration of effects** indicates a scenario which would have a long duration of adverse consequences. A high risk level is given when the duration of effects is long, while low risk is given when the effects are of short duration.

6. **Cascading effects** indicates a scenario where the effects of an adverse condition readily propagate to other systems or subsystems, i.e., cannot be contained. For example, a Dynamic RNP failure on one plane could have effects on the operational state of other aircraft in the same airspace. If there are many potential cascading effects the scenario is ranked high while few cascading effects receive a low ranking.

7. **Operating environment** indicates a scenario that results from external stressors. High risk events represent scenarios that are very sensitive to the environment in which it operates. Changes to the operating are likely to cause problems to the current operation of the system. Low risk represents scenarios where the environment can greatly change without changes to the operation of the system.

8. **Wear and tear** indicates a scenario that results from use, leading to degraded performance. High risk is given to systems that receive large amounts of wear and tear and will have to be maintained and fixed often. Low risk systems are not significantly affected by normal wear and tear.

9. **HW/SW/HU/OR** (Hardware, Software, Human, and Organizational) interfaces indicates a scenario in which the adverse outcome is sensitive to interfaces among diverse subsystems (e.g., human and hardware). High risk scenarios are those scenarios that are very sensitive to the interfaces among hardware, software, human, and organizational pieces within a system. Low risk scenarios lack the significant sensitive to such interfaces.

10. **Complexity/emergent behaviors** indicate a scenario in which there is a potential for system-level behaviors that are not anticipated from knowledge of components and the laws of their interactions. High risk systems occur with complex S-o-S that are not fully understood due to their complexity or emergent design. Low risk systems represent simple systems which are well understood.

11. **Design Maturity** indicates a scenario in which the adverse conditions are related to the newness of a design or other lack of concept proof. Low risk is given to systems that have taken precautions and incorporate diverse redundancy with tried and tested methods. High risk is given to systems that have not yet received ample attention to cover all possible risk scenarios and of which no tried and well tested method have been created to defend the system from emergent forced changes.