

A System-Theoretic Approach to Risk Analysis

By

Dro J. Gregorian

Sam M. Yoo

Bachelor of Science in Mechanical Engineering
United States Naval Academy, 2010

Master of Science in Engineering Management
Missouri University of Science and Technology, 2017

Bachelor of Science in Engineering Management with Honors
United States Military Academy, 2011

Submitted to the System Design and Management Program
in partial fulfillment of the requirements for the degree of

Master of Science in Engineering and Management
at the
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June 2021

© 2021 Dro J. Gregorian and Sam M. Yoo. All rights reserved.

The author hereby grants to MIT permission to reproduce and to distribute publicly paper and electronic copies of this thesis document in whole or in part in any medium now known or hereafter created.

Signature of Authors

System Design and Management Program
May 1, 2021

Certified by

Nancy Leveson
Department of Aeronautics and Astronautics
Engineering System Lab
Thesis Supervisor

Accepted by

Joan Rubin
Executive Director
System Design and Management Program

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.

This research is based upon work supported by the U.S. Army Combat Capabilities Development Command Aviation & Missile Center (DEVCOM AvMC) under Air Force Contract No. FA8702-15-D-0001. Any opinions, findings, conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of DEVCOM AvMC.

This document is derived from work done for the U.S. Army (and possibly others), it is not the direct product of work done for the U.S. Army. The information provided herein may include content supplied by third parties. Although the data and information contained herein has been produced or processed from sources believed to be reliable, the authors make no warranty, expressed or implied, regarding the accuracy, adequacy, completeness, legality, reliability, or usefulness of any information, conclusions, or recommendations provided herein. Distribution of the information contained herein does not constitute an endorsement or warranty of the data or information provided herein by the U.S. Army, or the U.S. Department of Defense shall be held liable for any improper or incorrect use of the information contained herein and assumes no responsibility for anyone's use of the information. The U.S. Army and U.S. Department of Defense shall not be liable for any claim for any loss, harm, or other damages arising from access to or use of data information, including without limitation any direct, indirect, incidental, exemplary, special, or consequential damages, even if advised of the possibility of such damages. The U.S. Army shall not be liable for any decision made or action taken, in reliance on the information contained herein.

A System-Theoretic Approach to Risk Analysis

by

Dro J. Gregorian and Sam M. Yoo

Submitted to the System Design and Management Program on May 1, 2021 in partial fulfillment of the requirements for the degree of Master of Science in Engineering and Management

ABSTRACT

Traditional safety risk assessment methods focus on component failures instead of the hazards present before the failure occurs. A widespread assessment tool is a risk matrix that measures the probability and severity of a particular risk, focusing heavily on qualitatively assessing the problem and determining its impact categorically through a matrix. The problem with this methodology is that any underlying system components or hazards that somebody cannot quantify are overlooked and may not appear until an accident or performance issue occurs. As a result, most analysis and reporting is conducted after an undesirable event happens, and the lessons-learned are used to prevent future losses.

However, a newer analysis method can identify the hazards and possible scenarios that lead to those losses before they occur. The technique is called System-Theoretic Process Analysis (STPA). STPA utilizes a qualitative approach to analyze the emergent properties of a system by finding unsafe control actions and determining their resultant loss scenarios.

This thesis examines the DoD risk matrix's current use and then leverages STPA to improve the outputs. The authors' research is also widely applicable outside of the DoD. The thesis provides two approaches to apply STPA in risk assessment, but both use a measure of mitigation effectiveness as a proxy for probability. A new STPA-Informed Risk Matrix (SRM) is introduced as an alternative for the MIL-STD-882E risk matrix. By combining the strengths of STPA and traditional risk assessment methods, decision-makers will be more equipped to determine risk levels associated with their projects, specifically concerning system safety. New DoD developmental programs are incredibly complex systems that require risk mitigation at each phase, from design to operation. STPA is applicable and scalable in any phase and yields actionable results that will prevent losses from occurring.

Thesis Supervisor: Nancy Leveson

Title: Professor, Department of Aeronautics and Astronautics

ACKNOWLEDGEMENTS

Writing this thesis was a significant undertaking, and many people deserve thanks for the continual support and guidance throughout the process. The people named here were instrumental to the completion of this work, as were many others.

To Nancy Leveson, our thesis advisor and champion of this topic. Thank you for introducing us to the world of risk matrices. Without your initial guidance and motivation, we would never have embarked upon this journey. Your many hours of feedback and wisdom were instrumental to the completion of this thesis.

The System Safety Lab Group provided educated useful feedback as the authors repeatedly iterated on their earliest ideas. Many thanks go to those members, specifically John Thomas, Bill Young, Michael Schmid, Andrew Kopeikin, Elias Johnson, Justin Poh, Elizabeth Baker, Lawrence Wong, and Adam Munekata

To the members of the MIT Lincoln Lab team that helped support many of the findings and research included in this thesis. Thank you to Amy Alexander, Gabe Elkin, and Emilie Cowen for their enduring contributions to this effort.

To the many individuals who contributed their expert knowledge in discussing their perspectives on risk management, thank you for your time. Your insights helped drive the development of ideas and creative process behind this thesis.

The support of family members was crucial to this thesis's accomplishment, as many long days required their diligent sacrifice and support. To my spouse, Jean Yoo, thank you for being an amazing mom and wife as I conducted research. To my boys Judah and Jordan, I looked forward to seeing you after every long day of work. Thank you for being my incentive to push through the grind. To my heavenly Father, thank you for sustaining me daily in faith.

The support of my mother, father, and brother for allowing me to share ideas and gain some insight from your experiences. Thank you Mom, Baba, and Greg for your help!

The authors are active-duty military officers and must acknowledge that the views expressed in this thesis are our own and do not reflect the official policy or position of the United States Army, United States Navy, the Department of Defense, or the United States Government.

TABLE OF CONTENTS

ABSTRACT.....	3
ACKNOWLEDGEMENTS.....	4
TABLE OF CONTENTS.....	5
LIST OF FIGURES AND TABLES.....	8
LIST OF ACRONYMS	11
1 INTRODUCTION	14
1.1 Motivation	14
1.2 Scope	14
1.3 Research Question.....	14
1.4 Thesis Structure.....	15
2 BACKGROUND: STPA AND RISK MATRICES	16
2.1 STPA Background and Framework	16
2.1.1 STPA Elements.....	17
2.2 The Risk Matrix	18
2.2.1 Risk Terminology	19
2.2.2 Probability/Likelihood	20
2.2.3 Severity/Consequence.....	21
2.3 Strengths and Weaknesses of the Risk Matrix	21
2.3.1 Strengths of the Risk Matrix.....	22
2.3.2 Weaknesses of the Risk Matrix.....	22
2.4 Summary	23
3 RISK POLICIES AND STAKEHOLDER PERSPECTIVES.....	24
3.1 Stakeholder Interviews on Risk.....	24
3.2 Risk Policy Overview.....	25
3.3 Chapter Summary.....	26
4 The STPA-Informed Risk Matrix	27
4.1 Informing Probability Through Mitigation Effectiveness.....	27
4.2 Mitigation Effectiveness Levels.....	32
4.2.1 Reduction Through System Design	33
4.2.2 Detected with Response.....	33
4.2.3 Training and Procedures	36

4.3	Assessing Post-Mitigation Severity	37
4.4	Two Approaches to the STPA-Informed Risk Matrix	39
4.4.1	Scenario-Based Approach.....	39
4.4.2	Hazard-Based Approach	42
4.5	SRM in the DoD Risk Process	45
4.6	Summary	47
5	APPLICATION OF NEW MATRIX TO FUTURE ROTARY-WING AIRCRAFT	48
5.1	STPA of Future Rotary-wing Aircraft Program.....	48
5.1.1	Defining the Purpose of the Analysis	48
5.1.2	Modeling the Control Structure	51
5.1.3	Identify Unsafe Control Actions.....	54
5.1.4	Identify Loss Scenarios.....	55
5.2	Creating the STPA-Informed Risk Matrix.....	56
5.2.1	Scenario-Based Approach.....	56
5.2.2	Hazard-Based Approach	61
5.3	Comparison of the Two Approaches.....	65
5.4	Summary	67
6	CONCLUSION.....	68
6.1	Results and Insights.....	68
6.2	SRM in the Engineering V	70
6.3	Limitations and Future Work	73
6.4	Final Thoughts.....	78
7	APPENDIX.....	79
7.1	STPA Results	79
7.1.1	Loss Table.....	79
7.1.2	Hazard and Sub-Hazard Tables	79
7.1.3	Constraint and Sub-Constraint Tables	81
7.1.4	Responsibilities Table.....	83
7.1.5	Unsafe Control Actions Table	83
7.1.6	Causal Scenarios Table	86
7.2	Complete Risk Assessment	89
7.2.1	Scenario-Based Approach Results.....	89
7.2.2	Hazard-Based Approach Results	99
7.3	DoD Risk Process and Application.....	105

7.3.1	Application in the DoD.....	105
7.3.2	Risk Management Process	105
7.3.3	Risk Assessment Process	110
7.4	DoD Risk Documents.....	110
7.4.1	DoD Instruction 5000.02T, 5000.74, 5000.75, 5000.80, 5000.81	110
7.4.2	Public Law 114-92, National Defense Authorization Act for FY16	111
7.4.3	DoD Instruction 8510.01	111
7.4.4	NIST Special Publication 800-37	112
7.4.5	Air Force Program Risk Management	113
7.4.6	Army Program Risk Management	114
7.4.7	Navy Program Risk Management.....	114
8	REFERENCES	117

LIST OF FIGURES

Figure 2-1: Overview of STPA.....	17
Figure 2-2: Standard Feedback Control Loop	17
Figure 2-3: Program and ESOH Risk Matrices	19
Figure 4-1: Example Risk and Control Matrix	28
Figure 4-2: STPA-Informed Risk Matrix (SRM); MIL-STD-882E Compliant	31
Figure 4-3: Coaxial Helicopter on Left, Single Main Rotor with Tail Rotor Configuration on Right.....	32
Figure 4-4: U.S. Air Force C-130 with External Fuel Tanks.....	33
Figure 4-5: Typical Boeing Aircraft Auxiliary Power Unit Compartment.....	34
Figure 4-6: Honda Blind Spot Information System (BSIS).....	35
Figure 4-7: Image from Toyota's Transparent A-Pillar Patent	36
Figure 4-8: UH-60 Blackhawk Aircrew Trainer.....	37
Figure 4-9: Example Severity Scenario with Mountain Peak.....	38
Figure 4-10: Risk Management Process (Left), Risk Management Framework (Right).....	45
Figure 4-11: Example Risk Monitoring and Trend Matrix.....	46
Figure 4-12: Eight Elements of System Safety Process from MIL-STD-882E.....	46
Figure 5-1: Future Rotary-wing Aircraft High-Level Control Structure	53
Figure 5-2: SRM for UCA 2.0 Series on Flight Control Manipulation	60
Figure 5-3: SRM for Example Sub-Hazards.....	64
Figure 5-4: Causal Scenario-Based Risk Matrix	66
Figure 5-5: Hazard-Based Risk Matrix.....	66
Figure 6-1: STPA-Informed Risk Matrix (SRM); MIL-STD-882E Compliant	69
Figure 6-2: STPA in the Systems Engineering V	70
Figure 6-3: Mitigation Implementation for FRWA Control Structure	72

Figure 6-4: Control Structure Risk State	75
Figure 6-5: Sub-Hazard Groupings.....	76
Figure 6-6: STPA Node Graph	77
Figure 7-1: Ram Air Turbine Generator Risk Matrix Example.....	105
Figure 7-2: Risk and Issue Management Process	106
Figure 7-3: U.S. Army Risk Management Process.....	107
Figure 7-4: Eight Elements of the System Safety Process.....	108
Figure 7-5: MIL-STD-882E Risk Assessment Matrix.....	108
Figure 7-6: Software Safety Criticality Matrix.....	109
Figure 7-7: Relationship Between Risk and SwCI	109
Figure 7-8: RMF and the Defense Acquisition Management System	112
Figure 7-9: NIST 800-37 RMF.....	112
Figure 7-10: NAVAIR System Safety Risk Matrix.....	116

LIST OF TABLES

Table 2-1: Probability Table from MIL-STD-882E	21
Table 2-2: Severity Table from MIL-STD-882E.....	21
Table 3-1: Comparison of DoD Risk Documents.....	26
Table 4-1: Safety Order of Precedence.....	29
Table 4-2: Mitigation Effectiveness Levels.....	30
Table 4-3: Example CPMS Table.....	37
Table 4-4: Steps for Scenario-Based Approach for SRM.....	40
Table 4-5: Hazard and Constraint Formulations.....	42
Table 4-6: Example Sub-Hazard and Sub-Constraint Generation.....	42
Table 4-7: Example Sub-Hazards and Sub-Constraints.....	43

Table 4-8: Steps for Hazard-Based Approach for SRM	44
Table 5-1: Future Rotary-wing Aircraft Losses.....	48
Table 5-2: Future Rotary-wing Aircraft Losses and Sub-losses.....	49
Table 5-3: Future Rotary-wing Aircraft System Hazards.....	50
Table 5-4: Future Rotary-wing Aircraft Constraints	50
Table 5-5: Future Rotary-wing Aircraft Responsibilities	52
Table 5-6: FRWA Unsafe Controls Actions.....	55
Table 5-7: FRWA Causal Scenarios.....	55
Table 5-8: Risk Calculations for Causal Scenarios 2.X.X.....	59
Table 5-9: Sub-Hazards for Aircraft Controllability (H1.0).....	61
Table 5-10: Sub-Constraints for Aircraft Controllability (H1.0).....	62
Table 5-11: Risk Calculations for Sub-Hazards	63
Table 5-12: STPA Mitigation Results Comparison.....	65
Table 7-1: Relationship Between DoDI 5000.02T and New Policy.....	110
Table 7-2: Standard AF Consequence Criteria for Performance	113
Table 7-3: U.S. Navy SYSCOMs and PEOs	115
Table 7-4: Navy Risk Management Frequency and Severity Categories.....	115
Table 7-5: Risk Acceptance Table.....	116

LIST OF ACRONYMS

ACAT	Acquisition Category
AE	Acquisition Enabler
AFPAM	Air Force Pamphlet
APM	Assistant Program/Project/Product Manager
ASA(ALT)	Assistant Secretary of the Army for Acquisition, Logistics, and Technology
ASN	Assistant Secretary of the Navy
BS	Beneficial Stakeholder
CAE	Defense Contract Management Agency
CB	Charitable Beneficiary
CFFC	Commander, Fleet Forces Command
CMC	Command Master Chief Petty Officer
CMES	Combined Mitigation Effectiveness Score
CNO	Chief of Naval Operations
CPMS	Combined Post-Mitigation Severity
CS	Causal Scenario
DARPA	Defense Advanced Research Project Agency
DAU	Defense Acquisition University
DCMA	Component Acquisition Executive
DOD	Department of Defense
DoDI	Department of Defense Instruction
DOT	Department of Transportation
EMD	Engineering & Manufacturing Development
ESOH	Environmental, Safety, and Occupational Health
FAA	Federal Aviation Administration
FMECA	Failure Mode, Effects, and Criticality Analysis
FO	Flight Operator
FRWA	Future Rotary-Wing Aircraft
IEEE	Institute of Electrical and Electronics Engineers
IP	Intellectual Property
ISO	International Standards Organization
IT	Information Technology

LCRM	Life Cycle Risk Management
LOR	Level of Rigor
MCSC	Marine Corps Systems Command
MDA	Milestone Decision Authority
MDAP	Major Defense Acquisition Program
MIL STD	Military Standard
MSA	Materiel Solutions Analysis
N43	Director, Fleet Maintenance
NAVAIR	Naval Air Systems Command
NAVFAC	Naval Facilities Engineering Command
NAVSEA	Naval Sea Systems Command
NAVSUP	Naval Supply Systems Command
NAVWAR	Naval Information Warfare Systems Command
NIST	National Institute of Standards and Technology
OASD	Office of Assistant Secretary of Defense Acquisitions
OASD(A)	Office of the Assistant Secretary of Defense for Acquisition
ORM	Operational Risk Management
PEO	Program Executive Office
PM	Program Manager
PMS	Pre-Mitigation Severity
PPMS	Post-Potential Mitigation Severity
PS	Problem Stakeholder
RAC	Risk Assessment Code
RAC	Risk Assessment Code
RACM	Risk and Control Matrix
RCA	Root Cause Analysis
RIO	Risk, Issue, Opportunity, Management Guide
RMB	Risk Management Board
RMF	Risk Management Framework
RMP	Risk Management Plan
SAE	Service Acquisition Executive
SAR	Selected Acquisition Reports

SE	Systems Engineering
SES	Senior Executive Service
SME	Subject Matter Expert
SML	Senior Material Leader
SOP	Standard Operating Procedure
SRD	Systems Readiness Directorate
SRM	STPA-Risk Matrix
SSCM	Software Safety Criticality Matrix
STPA	System-Theoretic Process Analysis
SwCI	Software Criticality Index
SYSCOM	System Command
TD	Technology Maturation & Risk Reduction
TYCOM	Type Command

THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK

1 INTRODUCTION

This thesis explores the application of the System-Theoretic Process Analysis (STPA) to the standard Department of Defense (DoD) utilized risk matrix as it is applied to systems safety. First, this thesis recommends potential alternatives to the risk matrix that offer a more informative yet concise assessment of risk within a system. It applies the developed approaches to a hypothetical Future Rotary-wing Aircraft (FRWA) as a test case.

By examining the holistic risk environment within complex systems, understanding their key stakeholders, and the strengths/weaknesses of the current risk matrix, the authors develop approaches that incorporate the results of STPA to improve upon the traditional, and often more subjective, risk matrix. This chapter sets the motivation and scope of the overall research. It also introduces the specific research question the authors seek to address and the overall structure of this thesis.

1.1 Motivation

STPA is a new risk analysis technique that can better identify hazards and their associated risks than traditional methods while still fully compliant with DoD Risk Management policy and MIL-STD-882E. Standard risk matrices focus on the assessment of failures rather than hazards. Assessing hazards provides a more comprehensive view of the risk matrix by evaluating the potential for losses rather than component/system failures. Essentially, the current risk matrix using failures only measures reliability and not safety.

In this thesis, the authors develop a method to apply STPA to improve the current risk matrix. The authors aim is to create a more objective, analytical approach that equips decision-makers with the information needed to understand and mitigate risk.

1.2 Scope

This thesis includes the following:

1. Determines how to leverage the STPA methodology to better inform probability and severity assessments for the standard DoD risk matrix for system safety.
2. Develops a comprehensive methodology to create the standard risk matrix using outputs from STPA objectively.
3. Proposes alternative definitions of risk and its evaluation while providing decision-makers with a clear assessment of risk.

To adequately address these areas, the authors focus their analysis on system safety risk and exclude other program risk facets to include traditional cost/schedule factors. Furthermore, this analysis excludes operational/mission risk analysis, which may be better served by the military's existing methodologies, such as Operational Risk Management (ORM). This thesis excludes any new literature beyond January 1, 2021.

1.3 Research Question

The following question helps to frame the approach and define the scope of this thesis:

How can STPA be used to improve the standard DoD risk matrix for systems safety?

1.4 Thesis Structure

This thesis's structure begins with defining the problem of current risk matrices for military acquisition programs, specifically new development efforts, as they inherently hold the most risk. Chapter 2 provides background on STPA and the risk matrix. Chapter 3 provides insights from stakeholder interviews and an overview of relevant DoD policies/guidelines. Chapter 4 introduces the STPA-Informed Risk Matrix (SRM) and two possible approaches to creating it. Chapter 5 shows an in-depth use of the methodologies from Chapter 4 applied to an FRWA program. Finally, Chapter 6 summarizes the research's key points, limitations, and areas for future work.

THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK

2 BACKGROUND: STPA AND RISK MATRICES

This chapter introduces STPA and why it is a valuable analysis approach, particularly for complex systems. Additionally, this chapter provides relevant background information on the DoD risk matrix and its general strengths and weaknesses.

2.1 STPA Background and Framework

STPA is a hazard analysis method designed to determine accident causation holistically. Most traditional hazard and risk analysis tools focus on a series of component failures, where one failure directly relates to the one following or proceeding it. For example, a helicopter's tail rotor cable fails, which leads to a loss of control and resultant crash. This model may have worked well when systems were primarily electromechanical 40-50 years ago, around the time these models were developed. In this period, system flaws could be found, tested, and reviewed before operation when random component failure was the primary failure mode. However, today's extraordinarily complex and software-intensive systems significantly decrease the usefulness of such models focused on component failure. The causes of many accidents today stem from component interactions and not their reliability.

The STPA technique is based on Dr. Nancy Leveson's System-Theoretic Accident Model and Processes (STAMP) and is derived initially from systems theory. Scientists and mathematicians created systems theory in the 1940s to help deal with complex systems. The resulting work would form the basis of systems engineering and safety utilized in the Intercontinental Ballistic Missile (ICBM) and other complex defense systems in the 1950s and 1960s. STPA considers the more widespread causes of mishaps (losses) today to include human operator error, organizational and managerial flaws, unsafe or inadequate software behavior, and component interactions (failures included).

Mishaps often result from interactions among components that violate specific system safety constraints. For example, constraints can require that the aircraft must maintain a minimum distance from the terrain, or weapon arming and firing must never occur inadvertently. Therefore, if the proper constraints are enforced for terrain separation and weapon usage, the system will perform correctly. This approach differs from a component failure analysis that would focus on how often the altitude indicator or weapon status lights will fail. Instead of component failure, the principle of *mitigation effectiveness* is the core concept introduced for the risk analysis methods explored later in this thesis.

STPA is best applied early in developing new systems to design in safety and ensure successful cost/schedule/performance parameters from the beginning. Since STPA does not require a complete design as a precursor or input, using STPA from the start helps avoid the typical costly rework of design flaws identified late in the development or operational phase of a system. STPA can be leveraged as designs are improved and decisions are made throughout the process.

Cybersecurity is another domain that STPA applies to, where safety, cybersecurity, and program goals can be handled in the same manner. Scenarios involving cybersecurity are generated alongside those that influence system safety or program goals, which can be used to develop controls to eliminate or mitigate the potential problems.

Compared to traditional methods that focus on component failure and human error, STPA treats accidents as a control problem. This method scales with system complexity and allows for thorough risk analysis in the early stages of system development. It is meant to seamlessly integrate with the overall architecture and engineering design processes, thus reducing the need for rework at the end of development. Figure 2-1 shows an overview of this method as depicted in the STPA Handbook [1, p. 14].

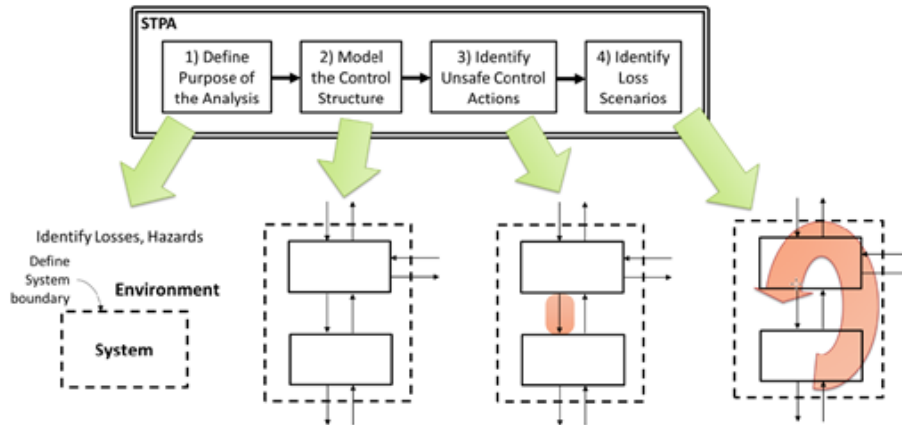


Figure 2-1: Overview of STPA

2.1.1 STPA Elements

A successful analysis relies on identifying four key elements in the STPA process. The first is *Defining the Purpose of the Analysis*. This step includes defining the system boundaries, system environment and identifying any losses or hazards that are to be avoided. Next is *Modeling the Control Structure*. A control structure is a hierarchical view of the controllers and their control interactions. A simple example is shown in Figure 2-2:

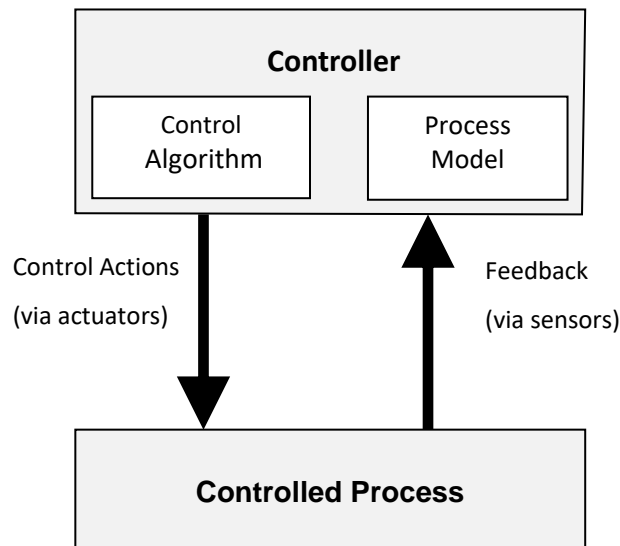


Figure 2-2: Standard Feedback Control Loop

The controllers at the top of the structure are in control of the controlled processes. Arrows represent control actions and feedback, forming a *control-feedback loop*. Generating a diagram detailing all system components and their interactions provides a more straightforward way of visualizing the system's entirety, hierarchy, and control-feedback loops required to enforce safety constraints.

After modeling the system elements in a control structure, *Identifying Unsafe Control Actions* (UCAs) finds what emergent safety problems exist and what worst-case failure modes will result. Emergent behavior does not depend on individual components but rather, the interactions between them [2]. UCAs describe the problems that arise when focusing on control actions instead of individual component performance. Highlighting critical areas and deficient interactions will aid in implementing risk controls. Lastly, *Identifying Loss Scenarios* shows how the UCAs occur and what hazards will result. Compared to other safety analysis methods, the critical difference is that these safety problems emerge from finding the UCAs while remaining less obvious otherwise. A complete example of the STPA process applied to a developmental future aircraft design phase will be shown in Chapter 5.

2.2 The Risk Matrix

The risk matrix is a widely used risk analysis and reporting tool, often incorporated into risk management processes to help decision-makers address risk. The credit for who first derived the risk matrix is debatable. Ale asserts Napoleon first applied a form of the risk matrix based on the likelihood of consequences [3, p. 1]. In 1978, Hussey described a three-dimensional matrix to aid policy decision-makers that he calls the risk matrix [4]. By the late 1980s, the risk matrix had risen to greater prominence within the UK's safety sciences and later the US [5, pp. 83–85].

Today, the risk matrix is a foundational tool of DoD risk management, and project/program managers are required to use it. To understand the risk matrix, one must conceptualize how it fits into the DoD's more extensive acquisition process for developmental projects and the program risk assessment/management processes. The authors acknowledge that there are many ways to interpret and define risk, but this chapter will focus on the DoD's practices.

Risk applied to DoD programs is defined as “potential future events or conditions that may have a negative effect on achieving program objectives for cost, schedule, and performance [6].” This thesis focuses on the system safety-related risks that fall within the “performance” category for DoD program risk. These risks are typically communicated to decision-makers within a risk matrix using two axes: likelihood (probability) between zero and one and the consequence (severity) of the undesired event (See Figure 2-3 Below) [7, p. 101]. The DoD addresses Environmental, Safety, and Occupational Health (ESOH) risk using Military Standard MIL-STD-882E and is primarily a separate assessment process from the program risk described above [7, p. 101].

Both program risk and ESOH risk matrices share similar flaws by focusing on failures rather than hazards and how consequence and likelihood are defined. In most DoD uses, the ordinal scales for rating likelihood and consequence are qualitatively determined (more on this in Chapter 2). Leveson shows how this practice fails to consider more advanced methods to calculate likelihood/consequence and the nuances between categories/boxes within the risk matrix [8].

DoD Acquisition Risk Management Guide

Likelihood	5	IVA	IIIA	IIA	IA
	4	IVB	IIIB	IIB	IB
	3	IVC	IIIC	IIC	IC
	2	IVD	IIID	IIE	ID
	1	IVE	IIIE	IIE	IE
		1	2	3	4
Consequence					

MIL-STD-882E

Probability	A	I	II	III	IV
	B	I	II	III	IV
	C	I	II	III	IV
	D	I	II	III	IV
	E	I	II	III	IV
		I	II	III	IV
Severity					

Note: MIL-STD-882E includes probability level “F” for “eliminated” ESOH risks that are “incapable of occurrence.” ESOH risks with probability level F should not be translated to the DoD Acquisition Risk Management program risk matrix.

Figure 2-3: Program and ESOH Risk Matrices

For further detail on the overall DoD risk assessment process and application of risk matrices with an example, see Appendix Section 7.3.

2.2.1 Risk Terminology

To understand the risk assessment process, it helps to review the DoD's key risk terminology, given that these terms are often defined differently across organizations. The list of terms below is not all-inclusive but covers those used most frequently within the risk assessment.

- **Risk Management:** “the process of identifying, eliminating or mitigating, and accepting residual risk associated with a mission; design of a system, facility, equipment, or process; or their operation.” (DA PAM 385-16) [9, p. 4]
- **Risk:** “potential future event or condition that may have a negative effect on achieving program objectives for cost, schedule, and performance; defined by the probability of an undesired event or condition and the consequences, impact, or severity of the undesired event, were it to occur.” (DoD RIO) [6, p. 11]
- **Risk:** “A combination of the severity of the mishap and the probability that the mishap will occur.” (MIL-STD-882E) [11, p. 7]
- **Mishap:** “An event or series of events resulting in unintentional death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. For the purposes of this Standard, the term “mishap” includes negative environmental impacts from planned events.” (MIL-STD-882E) [11, p. 6]
- **Issue:** “events or conditions with negative effect that have occurred (such as realized risks) or are certain to occur (probability of 1) that should be addressed.” (DoD RIO) [6, p. 3]

- **Opportunity:** “have potential future benefits to the program’s cost, schedule, and/or performance baseline.” (DoD RIO) [6, p. 3]
- **Hazard:** “any real or potential condition that can cause injury, illness, or death to personnel, damage to or loss of a system, equipment or property, or damage to the environment.” (DA PAM 385-16) [9, p. 5]
- **Risk Assessment Code (RAC):** “when severity categories and probability levels are combined, they provide a matrix for assigning a code to the risk associated with a hazard...known as RACs.” (DA PAM 385-16) [9, p. 7]
- **Risk Statement:** “summary of a potential problem that needs to be addressed. The statement communicates the potential adverse event or condition and its consequences on program objectives should the risk be realized. Typically formatted as an “if-then” statement.” (DoD RIO) [6, p. 22-23]

From the above terms, risk-statements are a particularly critical aspect of risk management practice within the DoD and typically take the shape of “if-then” statements. These statements form the basis of better understanding the consequences of a risk if left unmitigated. An excellent example of a risk statement is as follows: *If the program cannot achieve the anticipated structural properties of the wing skin material (uncertain condition) due to the difficulty of controlling processing variables (cause), then the wing design will be 400 pounds heavier or the aircraft maneuvering envelope will be reduced (from 7.0 g [gravitation force] to 6.0 g) (consequences)* [12].

Well-formulated risk statements are necessary for everyone to understand the problem and develop associated mitigations. Many factors contribute to a poorly formulated risk statement. Weak statements often make vague observations, identify issues rather than risks, address uncontrollable areas, define poor execution or quality efforts that should be avoided, or call out an unavoidable event as a risk [12].

2.2.2 Probability/Likelihood

Probability (likelihood) is defined as the probability of an event occurring. This value is derived from quantitative analysis to the maximum extent practical using available engineering and safety data. Despite its basis in factual data, interviews with experts proved that probability could be entirely subjective depending on the program [13]–[35]. Since programs can incorporate experimental components that do not have any reliability data available, program managers would have to make up the failure estimates. The probability level is generally described using a scale from 1-5, ranging from *Eliminated* to *Frequent*. Each probability description has a qualitative definition of the frequency of occurrence. It is worth noting that some programs use probability descriptions with differing definitions or scales to match their needs.

PROBABILITY LEVELS			
Description	Level	Specific Individual Item	Fleet or Inventory
Frequent	A	Likely to occur often in the life of an item.	Continuously experienced.
Probable	B	Will occur several times in the life of an item.	Will occur frequently.
Occasional	C	Likely to occur sometime in the life of an item.	Will occur several times.
Remote	D	Unlikely, but possible to occur in the life of an item.	Unlikely, but can reasonably be expected to occur.
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced in the life of an item.	Unlikely to occur, but possible.
Eliminated	F	Incapable of occurrence. This level is used when potential hazards are identified and later eliminated.	Incapable of occurrence. This level is used when potential hazards are identified and later eliminated.

Table 2-1: Probability Table from MIL-STD-882E

2.2.3 Severity/Consequence

Severity (consequence) is another qualitative component of risk assessment. This element is where brainstorming possible loss scenarios and multi-order effects are necessary to determine the real impact. Once the risks are categorized, they can be assigned a score on a scale of 1-4 to indicate the severity level, ranging from Negligible to Catastrophic. Table 2-2 below shows the mishap result criteria associated with each severity category [11]:

SEVERITY CATEGORIES		
Description	Severity Category	Mishap Result Criteria
Catastrophic	1	Could result in one or more of the following: death, permanent total disability, irreversible significant environmental impact, or monetary loss equal to or exceeding \$10M.
Critical	2	Could result in one or more of the following: permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, reversible significant environmental impact, or monetary loss equal to or exceeding \$1M but less than \$10M.
Marginal	3	Could result in one or more of the following: injury or occupational illness resulting in one or more lost work day(s), reversible moderate environmental impact, or monetary loss equal to or exceeding \$100K but less than \$1M.
Negligible	4	Could result in one or more of the following: injury or occupational illness not resulting in a lost work day, minimal environmental impact, or monetary loss less than \$100K.

Table 2-2: Severity Table from MIL-STD-882E

2.3 Strengths and Weaknesses of the Risk Matrix

Risk matrices are utilized in many organizations to include the DoD, NASA, and the International Organization for Standardization (ISO). They offer a simple visual tool that can help with risk management. One can easily find risk matrices in risk management guides or other management reference books. The widespread use of risk matrices has invited much scrutiny into the merits of the risk matrix itself and called many others to defend the risk matrix as a useful tool. This chapter will discuss the overall strengths and weaknesses of the risk matrix.

2.3.1 Strengths of the Risk Matrix

Risk matrices offer many strengths that make them one of the most widespread risk management tools in use today. The matrices are inherently simple to understand and are often color-coded in red-amber-green scales to indicate low, medium, and high-risk levels. In many circumstances, Talbot states that risk matrices help to people do the following [36]:

- Promote robust discussion (at times more beneficial than the actual risk rating)
- Offer some consistency to prioritizing risks
- Help decision-makers to focus on the highest priority risks
- Show complex risk data in one simple visual

To successfully bring out the best characteristics of risk matrices, Talbot further recommends that users should implement the following [36]:

- Well-defined risk statement
- The robust likelihood and consequence definitions
- A hierarchy of controls to prioritize risk mitigation
- Expected cost/benefit of risk mitigations

Interviews with stakeholders practicing risk management across the DoD confirmed these beneficial aspects of risk matrices in their experience. Additionally, some managers touted it as beneficial since it is universally understood and helps some senior decision-makers quickly focus on and attack higher risks. There is an equal or greater number of shortfalls that others have noted about risk matrices, despite all the strengths highlighted above.

2.3.2 Weaknesses of the Risk Matrix

There are many problems with using a risk matrix to represent safety hazards. These issues drive the need for analysis and improvement to make the risk matrix more useful. Briefly, some of the most glaring weaknesses [8] identified and scrutinized by others include:

- *Lack of Granularity*: prioritizes risk based on overall score instead of providing information to mitigate the risk. Additionally, the ordinal scales oversimplify any calculations that can be made, limiting risk assessment to categorical entries instead of more insightful, data-driven values.
- *Inaccurate Quantitative Analysis*: lack, or abundance, of historical data, can affect likelihood assessments. Low-frequency, catastrophic events may not receive the mitigation prioritization necessary because there is not enough data to suggest the problem may occur, or there is too much data that might suggest a lower failure rate without recognizing the emergent issues of a newer system operating in a different environment.
- *General Heuristic Biases*: evaluating likelihood is subject to various types of psychological biases. The most apparent is confirmation bias where people will focus on information that supports their viewpoint while disregarding anything that may conflict. Another is generating easy scenarios, where people confuse the difficulty of creating a scenario with the actual likelihood of it occurring. Additionally, it is difficult for people to recognize cumulative causes that lead to a mishap because they focus on larger, more

dramatic issues. Lastly, defensive avoidance causes people to reject or downgrade risk that conflicts with other goals (usually financial), leading them to disregard risks because they may require too many resources to mitigate properly.

Risk matrices tend to oversimplify a problem by focusing on the quantitative aspect of a component or system failure instead of addressing the qualitative aspect of risk. The risk matrix exists to convey complex information as succinctly as possible in the form of a numerical value. As a result, some important issues may not be addressed because they cannot be captured numerically. Depending on the risk management document being referenced, there are different standards for calculating final RACs.

Some DoD manuals require multiplying probability and severity, while others use them as a grid coordinate to find a predefined value for that risk. The issue here is the matrix fails to capture depth and nuance in categorizing probability and severity. Despite matrices being similar in appearance, different organizations may have higher or lower resolution for each axis scale. For example, the DoD RIO prescribes a 5x5 matrix, whereas the US Navy uses a 5x4 matrix, which is a subtle difference in visual presentation, yet a potentially impactful difference in terms of classifying and managing risk from a resource allocation perspective. If an organization uses different metrics to classify a risk but uses similar vocabulary from another type of risk matrix, then risk becomes a relative measure based on the risk tolerance of that organization.

Another issue resides in tracking risk over the course of a program's lifetime. Some organizations mandate processes to follow and create tracking plans to manage residual risk and risk burn down. Others perform risk assessments that only capture a snapshot of the program risk at present and do not consider future risk or trends. If there is a disparity between risk management practices between two organizations working on the same program, this can negatively impact cost and schedule while jeopardizing performance for the end user of the product.

2.4 Summary

This section introduced STPA, DoD risk terminology, and key aspects of the risk matrix. The significant strengths and weaknesses of the risk matrix were reviewed so that there is an understanding of the current state of this risk tool. The next chapter will discuss both risk policies and stakeholder perspectives from within the DoD.

THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK

3 RISK POLICIES AND STAKEHOLDER PERSPECTIVES

Stakeholder interviews provide useful insights on how to best improve upon the existing risk matrix and suggest meaningful alternatives. Stakeholders in our context are those who have an interest in an improved risk matrix, or, more broadly speaking, a risk analysis. The stakeholders discussed all have an important role in the realm of risk analysis within the DoD. This chapter also provides a high-level overview of the different risk policies and guidelines used across the DoD today.

3.1 Stakeholder Interviews on Risk

Improving risk analysis methods would not be effective without discussing current practice with stakeholders in different developmental sectors. After conducting 23 interviews with subject matter experts across the DoD, the authors were able to summarize the general sentiment towards risk management and pinpoint some key insights that impact our approach to improvement, specifically with respect to the risk matrix [13]–[35]. Interviewees included system safety engineers, program and project managers, aviation regulatory agencies, defense contractors, aides to Congress, etc...

The most notable issue the authors discovered is a pervasive culture of “pencil-whipping” and resultant lack of follow through with risk management. Interviewees informed the authors that much of the overall risk analysis and management was done for the sake of doing it without any intent to improve the real risk level. Sometimes during quarterly risk meetings or risk review boards that required an update on risk and relevant stakeholders, the presenters would format a briefing that would “make the boss happy.” This cultural problem meant that risk was not being managed properly throughout the life of the program and was treated more as an administrative requirement to meet a deadline.

In this instance, risk managers simply wanted to get the risk analysis done as a “check in the box” instead of taking the time to truly understand the risks involved and the needed mitigations/controls. This mindset segued into the issue of tracking risk at all levels, with a clear snowball effect where the details of risk analysis were lost as risks were presented to program managers. Some organizations created spreadsheets to identify, analyze, and manage risk, however the same concerted effort degraded after a required presentation. After the program ends or the product is manufactured, meaningful risk tracking ceases and product lifecycle issues are harder to trace back to the original design phase risks. As a result, safety issues that surface during operation may not have a traceable ID that would enable designers to address.

Another issue discovered during interviews is the general lack of standardization in approach and metrics for risk management. The authors discovered a significant pattern of miscommunication between organizations. Recalling that the DoD RIO outlines the preferred risk management process while subsequent branch policy reshapes it to suit the needs of a program, it was clear that each organization opted to use their own specialized risk management tools that ranged from specific software to various Excel spreadsheets or PDF forms. While this differentiation is not necessarily a negative indicator, as it allows organizations to tailor risk management to their specific requirements, it can cause a problem when different organizations need to interface with each other regarding risk. If two entities speak different risk languages (i.e., one uses a 4x6 matrix while the other a 5x5, or probability is computed differently, or risks

tracked with varying means), then conflict and disagreement in communicating risk issues and negotiating resources or responsibilities for mitigating risk becomes widespread.

Interviews with stakeholders in PEOs also revealed the use of uniquely tailored Standard Operating Procedures (SOPs) within their programs. For example, the Utility Helicopter and Improved Turbine Engine (ITE) Project Offices under PEO Aviation each utilize their own SOP to address risk. Both SOPs used the same criteria assessment of likelihood but it differs from the DoD RIO standard [37].

Lastly, interviews revealed a noticeable problem in prioritizing risk. Because of the subjective nature of defining probability and severity categories, coupled with a lack of cross-organizational standards, risk planners may disregard seemingly negligible risks that are in fact significant. While this issue can originate from the previously mentioned issues of “pencil-whipping” and non-standardization, it is a separate issue because there is no malintent. Instead, this lack of emphasis on negligible risks is due to a lack of experience or knowledge with handling risk. Contributing to this lack of experience is the worrying lack of guiding tools/methodology for handling risk. If there are no firm standards defining probability and severity, or worse yet, no clear methodology to identifying and mitigating risk, then the onus falls to the system engineer or program manager to create them, which can yield varying results in developing objectively scored RACs, risk prioritization, and risk mitigation plans.

For example, a risk locally defined as “low probability” may receive a low RAC and be placed lower on a list of priorities. However, another organization (e.g., defense contractor) may define “low probability” slightly differently, leading to a different prioritization level from their perspective. Interviews revealed that a clear conversation about risk management methods and language should occur during contract negotiations before any work is started, but rarely does. Rather, the focus of these negotiations tends to emphasize the type of contract (e.g., fixed price or cost-plus), which emphasizes who assumes more of the risk financially during the life of the program. These disparities in risk prioritization (before and during program work) can lead to overlooked safety issues, increases in program cost and schedule, or misunderstanding between two organizations working on managing the same project risk.

Overall, the interviews highlighted three significant shortfalls within the current DoD risk management process. First, the organizational and cultural problem of treating risk management as a “check-the-box” rather than a critical component of program success. Second, the clear lack of a common language, approach, and analysis methodology in terms of identifying and communicating risk. Third, the failure to prioritize risks properly due to a lack of experience/knowledge/methods present within the organization. This thesis seeks to primarily tackle the latter two identified problems with the DoD’s risk management, as culture change is a much more difficult aspect of the risk environment to affect.

3.2 Risk Policy Overview

To understand the current risk matrix landscape, it is important to review how the DoD handles risk. One goal of this thesis is to provide a single unifying methodology across the entire DoD. Interestingly, each branch of service has a different application and process for risk management. Army specific policies will be discussed in the context of three documents AR 70-1, AR 385-30, and DA PAM 385-16. Navy documents primarily reference NAVAIRINST 500.21B and OPNAVINST 5100.24B. Air Force documents reference AFI 63-101 and AFPAM

63-128. More detailed discussion of all documents addressed in Table 3-1 below can be found in Appendix 7.3.

The overarching policy on risk management as it pertains to new development programs is the DoD Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs. Re-published in 2017 to supersede the former DoD Risk Management Guide, this 96-page document serves as the highest-level policy published by the DoD on the topic. Additionally, MIL-STD-882E provides the governing policy on addressing systems safety risk, which is the focus area of this thesis. This section seeks to provide a brief overview of different written documents as it pertains to risk matrix development.

Risk Document	DoDI 5000 Series	DoDI 8510.01	DoD RIO	NIST 800-37	MIL-STD 882E	Army Policies	Air Force Policies	Navy Policies
Risk Matrix Dimensions	N/A	N/A	5x5	N/A	5x4	5x4	5x5	5x4
Policy or Guideline	P	P	P	G	P	P	P	P
Different from RIO terminology?	-	-	-	-	Yes	Yes	Yes	Yes
Prescribe a Risk Methodology?	No	No	Yes	Yes	Yes	Yes	Yes	Yes

Table 3-1: Comparison of DoD Risk Documents

There are some important distinctions regarding risk matrices among the documents the authors reviewed. First is the use of either a 5x5 or 5x4 risk matrix of probability/likelihood and severity/consequence. Table 3-1 shows the differences in risk matrix use today across the three largest branches of the military. Second is whether the documents are from DoD/branch specific policy, or simply a guideline for best practice. The only document that is a suggested best practice is the NIST Special Publication 800-37, which establishes a recommended risk management framework specifically for security and privacy but does not prescribe use of the risk matrix. Lastly, differences in risk terminology and the prescribed risk methodologies exist between the three largest branches of the military and the DoD RIO.

3.3 Chapter Summary

This chapter discussed the insights from 23 key stakeholder interviews involved in risk management within the DoD. The primary interview takeaways highlight a culture of “check-the-box” risk management, lack of standardization/methods, and poor risk prioritization. Additionally, risk documents across the DoD were compared and differences in the use of risk matrices, risk terminology, and methodologies for addressing risk were discovered.

4 THE STPA-INFORMED RISK MATRIX

This chapter focuses on two potential methods to translate the results of an STPA into a risk assessment. Section 4.1 explains the concept of ‘*mitigation effectiveness*’ as a more suitable proxy for probability. Section 4.2 describes levels of mitigation effectiveness and their application in both methods. Section 4.3 discusses the idea of *pre-mitigation* and *post-mitigation severity* for risk mitigation. Section 4.4 covers both methods (scenario and hazard-based), how they inform the final risk matrix, and their strengths and weaknesses. Section 4.5 demonstrates how the authors’ approach to an SRM complements all DoD guidelines.

4.1 Informing Probability Through Mitigation Effectiveness

Rather than treating risk as a component failure problem, risk can be treated as a control problem. Based on the stakeholder interviews conducted in Chapter 3, risk practitioners value concrete and quantifiable methods to assess risk. The DoD often translates risk into a Risk Assessment Code (RAC; e.g., an extreme high risk is ‘1A’ for MIL-STD-882E) or a coordinate grid (e.g., an extreme high risk is a [5,5] risk for program level risk matrices). MIL-STD-882E uses vague, qualitative statements that define frequency of occurrence (see Table 2-2). For STPA to be accepted as a viable alternative to traditional risk assessment methods that focus on reliability, the authors provide methods to translate STPA results into measures of risk.

Probability estimation for new systems is difficult to objectively quantify because it depends on historical data. That data may not exist for systems incorporating autonomy and complex interactions between operators, software, and hardware. Therefore, probability can only be informed by test and evaluation data on the new components and interactions, which may still not accurately depict the true likelihood of a risk event occurring.

If risk managers believe that the chance of a risk occurring is low, they may be biased against dedicating the appropriate resources needed to mitigate a risk. The likelihood of a poorly estimated risk may be quite high, especially for a system utilizing experimental components that do not have failure data readily available. Therefore, more losses may occur in the future because of incorrectly focusing on probability instead of controllability of risk.

Take for example the two battery compartment fires in Boeing’s 787 Dreamliner airplanes in 2013. To save weight on the aircraft, Boeing developed new lithium-ion batteries rather than using a more stable nickel-cadmium battery [38]. Boeing predicted 10 million flight hours between battery failures in their reliability analysis yet both fires occurred in 52,000 flight hours. This example also does not include the three other smoke-related incidents in the battery compartment. Boeing’s experience only shows how something as simple as a battery system’s failed risk assessment could lead to a significant mishap with larger impact (Boeing’s fleet remained grounded for more than four months).

Envision the same scale of potential risks and the need to accurately assess them from the perspective a brand-new advanced aircraft system such as the F-35 Joint Strike Fighter. Some of the unique new systems intended to operate seamlessly together are advanced weapons, degraded visual environment technology, air-launched effects, new propulsion technology, remote autonomous flight, etc... The ability to accurately assess the likelihood of mishaps and risks occurring within any of these systems is an enormously challenging task. The authors demonstrate how it is possible to calculate risk without considering probability.

An alternative and better way to inform probability is to use *mitigation effectiveness* as a proxy. Mitigation effectiveness measures how well a mitigation controls risk, whereas probability just estimates occurrence. By shifting the focus from probability to mitigation effectiveness, risk decision makers can mitigate risks directly instead of fixating on when they will occur.

Risk is currently defined by MIL-STD-882E as “a combination of the severity of the mishap and the probability that the mishap will occur.” Mishap is further defined in MIL-STD-882E as “an event or series of events resulting in unintentional death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. For the purposes of this standard, the term “mishap” includes negative environmental impacts from planned events.”

DA PAM 385-16 defines a hazard as “any real or potential condition that can cause injury, illness, or death to personnel, damage to or loss of a system, equipment or property, or damage to the environment.” Although MIL-STD-882E defines risk as a combination of severity and probability for a mishap, the authors suggest redefining risk by replacing mishap and probability with hazard and mitigation effectiveness respectively in the following way:

Risk: “A combination of the severity of the hazard and the *mitigation effectiveness* in controlling the hazard.”

This definition incorporates the new concept of mitigation effectiveness while remaining true to the intent of MIL-STD-882E.

Mitigation effectiveness is a more useful approach to understanding risk as compared to probability. Some methods, such as the Risk and Control Matrix (RACM), already exist that utilize a similar measure called *control effectiveness*, see Figure 4-1 below [39]:

			Residual Risk Ranking				
Control Effectiveness	Weak or non-existent	5	Very Low	Low	Moderate	High	Critical
	Marginally Adequate	4	Very Low	Low	Moderate	High	Critical
	Adequate	3	Very Low	Very Low	Low	Moderate	High
	Reasonably Strong	2	Very Low	Very Low	Low	Moderate	Moderate
	Strong	1	Very Low	Very Low	Low	Low	Moderate
			1	2	3	4	5
			Very Low	Low	Moderate	High	Critical
			Inherent Risk				

Figure 4-1: Example Risk and Control Matrix

Within the context of this thesis, the primary difference between control effectiveness and mitigation effectiveness is how the effectiveness is informed. Control effectiveness is based on vague, subjective analysis that does not utilize a clear methodology to achieve its results. Conversely, mitigation effectiveness is informed by the results of STPA, a repeatable method that greatly enhances the depth of analysis. Unlike the traditional hazard analysis methods, STPA can start in the concept development stage, before any design exists. This stage of development is also when a preliminary risk matrix is often created.

Like mitigation effectiveness, Leveson describes a measure called “strength of potential controls” and suggests a possible ranking strategy listed below [8].

1. The causal factor can be eliminated through design and high assurance.
2. The occurrence of the causal factor can be reduced or controlled through system design.
3. The causal factor can be detected and mitigated if it does occur through system design or through operational procedures.
4. The only potential controls involve training and procedures.

The above ranking strategy serves as a useful starting point for a closer look into how to assess mitigation effectiveness. Leveson’s “strength of potential controls” is based on the fundamental *Safety Order of Precedence* that is widely accepted in both civilian and government system safety applications. Table 4-1 shows the Safety Order of Precedence below [40, p. 13].

Description	Priority	Definition
Design for Minimum Risk	1	Design to eliminate risks. If the identified risk cannot be eliminated, reduce it to an acceptable level through design selection
Incorporate Safety Devices	2	If identified risks cannot be eliminated through design selection, reduce the risk via the use of fixed, automatic, or other safety design features or devices. Provisions shall be made for periodic functional checks of safety devices.
Provide Warning Devices	3	When neither design nor safety devices can effectively eliminate identified risks or adequately reduce risk, devices shall be used to detect the condition and to produce an adequate warning signal. Warning signals and their application shall be designed to minimize the likelihood of inappropriate human reaction and response. Warning signs and placards shall be provided to alert operational and support personnel of such risks as exposure to high voltage and heavy objects.
Develop Procedures and Training	4	Where it is impractical to eliminate risks through design selection or specific safety and warning devices, procedures and training are used. However, concurrence of authority is usually required when procedures and training are applied to reduce risks of catastrophic, hazardous, major, or critical severity.

Table 4-1: Safety Order of Precedence

The authors suggest using a similar hierarchy to those discussed but also include the ability to assess what is called a ‘*Combined Mitigation Effectiveness Score*’ (CMES), or the impact of a combination of mitigation methods. The use of CMES would replace or inform probability on the standard risk matrix in the form of a new STPA-Informed Risk Matrix (see Figure 4-2 on next page). The term *causal factor* is introduced as the risk identified in the form of causal scenarios generated by STPA. When using the hazard-based approach to develop an SRM, the term *causal factor* is replaced by *sub-hazard*, which will be discussed later in this chapter.

Mitigation Level	Mitigation Description	Mitigation Effectiveness Score (MES)
Eliminated	The casual factor can be eliminated through design or by a specific combination of the below mitigations (proactive).	ELIM
Reduction Through Design	The occurrence of the causal factor can be reduced or controlled through system design (proactive).	3
Detected with Response	The causal factor can be detected and requires a response to mitigate (reactive).	2
Training and Procedures	The causal factor can be mitigated through additional training and procedures (reactive).	1
None	No possible mitigation exists, or mitigation is never applied.	0

Table 4-2: Mitigation Effectiveness Levels

It is important to note that the *safety device* category in Table 4-2 is removed from the mitigation effectiveness levels. The authors believe that safety devices can be incorporated as design features or systems that detect and respond to hazards.

The STPA-Informed Risk Matrix (SRM) is an improved version of the MIL-STD-882E risk matrix. It emphasizes the controllability and mitigation effectiveness of risks over subjective assessments of probability. The scale for CMES ranges from ‘*Least Effective (0)*’ to ‘*Eliminated*’ and depends on the combined impacts of recommended mitigations to address hazards. The ‘*Most Effective (6)*’ category of mitigation effectiveness is reserved for instances where all three levels of mitigation are applied to control a risk that cannot be eliminated (Design + Detection + Training & Procedures = *Most Effective*). All possible combinations of mitigation levels are represented by the scale for CMES in the SRM along the y-axis Table 4-2: Mitigation Effectiveness Levels. Each grouping of CMES also pairs with a probability category from MIL-STD-882E (e.g., *Most Effective* CMES = *Improbable* likelihood for a risk). While the authors prefer to treat mitigation effectiveness as a standalone measure, the association of CMES with probability exists to ensure the developed methodologies comply with MIL-STD-882E, as some organizations may be unwilling to part with probability as their primary measure of risk.

STPA-Informed Risk Matrix						
Least Effective [A]	0					
Somewhat Effective [B]	1					
Moderately Effective [C]	2-3					
Very Effective [D]	4-5					
Most Effective [E]	6					
Eliminated [F]	N/A					
CMES/Prob		1	2	3	4	
	CPMS	Catastrophic	Critical	Marginal	Negligible	
CMES	Least	Somewhat	Moderate	Very	Most	Eliminate
Bins	0	1	2-3	4-5	6	N/A
Probability	Frequent	Probable	Occasional	Remote	Improbable	Eliminate

Figure 4-2: STPA-Informed Risk Matrix (SRM); MIL-STD-882E Compliant

When determining CMES, there are some important assumptions that must be understood. Combined mitigation effectiveness is based on a fundamental assumption that more mitigations of the same level will not provide any additional quantifiable impact to the calculation of CMES. For example, if only two ‘Reduction Through Design (3)’ mitigations were applied to a risk, the final CMES would still be a (3) instead of (6). The quality of the mitigations is most important, not quantity. While there is certainly some merit to the idea that additional mitigations of the same level would provide a positive impact, attempting to summarily quantify that impact is no better than guessing at the probability of risk’s occurrence.

Another assumption is that all mitigations derived from STPA are applied simultaneously, which accounts for their combined effects when applicable. It is possible that a risk planner may not be able to apply all mitigations due to resource limitations or other factors. In these cases, the final risk scores must represent the actual mitigations applied, not the theoretical best-case as is presented in this thesis.

Risk practitioners who apply this methodology correctly will often find that the individual risks identified through STPA can be carefully mitigated (and often eliminated) through thoughtfully developed mitigations. The authors experienced this firsthand while developing mitigations for risks identified in the theoretical FRWA example in Chapter 5.

In some cases, the combined effects of two or more different types may eliminate a risk (yields an *ELIM* score for CMES instead of a numeric score) but fail to do so when applied individually. For example, consider a scenario with an incapacitated pilot in an aircraft. To prevent the loss of the aircraft (and possibly the pilot), the aircraft must be designed to fly with an autonomous mode (*Reduction Through Design*). To know when and how the system should engage the autonomous mode, the system must be able to detect pilot incapacitation and engage the autonomous mode (*Detected with Response*). While the two mitigations are in two distinct mitigation levels and could be independently developed, they work together in this specific context to eliminate the loss of an aircraft and pilot due to pilot incapacitation. STPA helps identify risks and provide the specific context necessary to determine the ideal combinations of mitigations. While there are more nuances within this example that can be elaborated upon, it serves the purpose of showing how multiple combined mitigations can eliminate a specific risk.

4.2 Mitigation Effectiveness Levels

The first aspect to address with the mitigation ranking structure above is additional clarification of the mitigation levels. Later, the discussion on the mitigation effectiveness scores and the impacts of combining mitigation methods is described. The best-case scenario in terms of risk is to eliminate the potential for occurrence completely. When a causal factor (or sub-hazard) identified through STPA can be removed, this means there is zero probability of the risk occurring. Sometimes these types of design changes involve a significant architectural decision and may be more difficult to address in late-stage development. For example, in Figure 4-3 below, if a specific risk involved the loss of tail rotor effectiveness for a helicopter, an effective design would be use of a coaxial rotor system that does not utilize a tail rotor at all [41]-[42].



Figure 4-3: Coaxial Helicopter on Left, Single Main Rotor with Tail Rotor Configuration on Right

One can quickly observe that there would be no possibility of a loss of tail rotor effectiveness after removing the tail rotor from the design. The authors are not suggesting that specific components of a design must be removed to eliminate a causal factor, but the design considerations may be significant to drive the probability of causal factor occurrence to zero. The next preferred mitigation category is to reduce the occurrence of a causal scenario.

4.2.1 Reduction Through System Design

A reduction of risk through system design represents the next best preferred mitigation step when it is otherwise infeasible to eliminate it completely. Elimination of the causal factor/sub-hazard may not be possible based on the current state of the design cycle. A key attribute of this mitigation level is that the design change is meant to *proactively* reduce the occurrence of a causal factor.

An appropriate example of reduction through system design might be causal factors associated with propulsion because of problems with the fuel system (fuel leak, starvation, particulate intrusion, etc.). One possible reduction through system design would be the addition of external fuel tanks to augment the primary fuel system of an aircraft. In the event of a fuel leak or loss of fuel to the primary system for any reason, the aircraft could switch to its reserve external fuel tank source for power. Figure 4-4 below shows an example of a US Air Force C-130 that employs external fuel tanks in its system design [43].



Figure 4-4: U.S. Air Force C-130 with External Fuel Tanks

Additionally, improvements to the fuel system in the form of ballistically tolerant fuel tanks/bladders could represent another effective reduction of the causal factor (fuel leak due to object penetration). It is important to note that regardless of the number of total system design mitigations, the overall net effectiveness is still scored a (3) – the occurrence of the causal factor has been proactively reduced but not eliminated.

Given that it is difficult, if not impossible, to accurately assess the overall reduction in likelihood of a causal factor due to mitigation implementations, the more conservative answer is to accept that some overall reduction has occurred. When a reduction through system design is not feasible, the next best solution is for the system to detect the occurrence of a causal factor and require a response.

4.2.2 Detected with Response

A system that detects the occurrence of a causal factor and responds either automatically or manually (requires operator involvement) to address it ranks as the third best mitigation level, contributing a MES of (2). Unlike the previous mitigation step, design choices here are *reactionary* to the occurrence of a causal factor, which is what lowers the overall mitigation

effectiveness. A simple example of detection with automated response can be illustrated with an engine fire in flight. Many aircraft already have onboard sensors that would inform the pilot if an engine were on fire and automatically engage a fire extinguishing system, such as those used on Boeing airplanes (see Figure 4-5 below) [44].

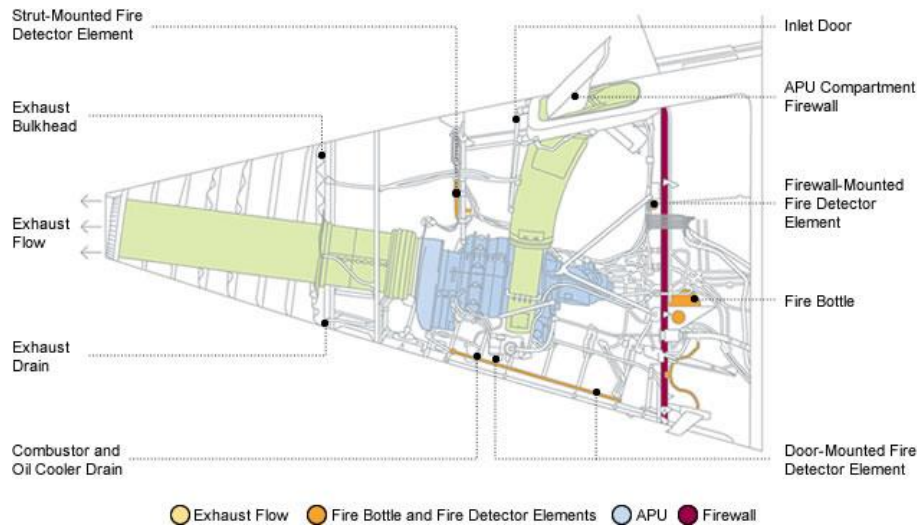


Figure 4-5: Typical Boeing Aircraft Auxiliary Power Unit Compartment

While nothing has changed in terms of system design to reduce the occurrence of an engine fire, Boeing has designed a detection of the causal factor and an appropriate automated response (attempt to extinguish the fire). Because the causal factor's chance of occurrence is unchanged after incorporating these automatic system detection/response features, these mitigations are not as effective as those that might prevent an engine fire to begin with. If automatic response is not possible or preferred, a system that incorporates hazard detection and allows an operator to manually respond is also effective.

In some cases, it may not be feasible for a system design to detect and provide an automated response to a causal factor due to engineering, budgetary, or other constraints, in which case a system that detects and allows for a manual operator response may be another option. Furthermore, there may be instances where a system design cannot reliably detect the occurrence of a causal factor and thus an automated response may not be appropriate due to this issue. Overall, the strength of these reactionary mitigations is weaker than the ones described above through design.

Take for example Honda's Blind Spot Information System (BSIS), a standard safety feature on newer Honda vehicles that provides a manual alert to drivers when an object is occupying the vehicle's blind spot. In this example, the causal factor leading to a loss is the presence of a vehicle in the driver's blind spot. Automotive technology and design choices continue to provide drivers with improved mitigations that reduce the occurrence of losses that result from the 'blind spot' causal factor. Honda's BSIS monitoring is a current example of such design and is achieved using two radar sensors on either side of the vehicle's rear bumper. These sensors scan approximately 10 feet outwards, and 15 feet back from the rear edge of the front doors [45].

While driving, if an object is detected by either radar sensor, the blind spot indicator light located in/near the side mirrors will illuminate. If a turn signal is turned on in the direction of the lane the object is detected in, BSIS will alert the driver with a loud beeping sound until the blind spot has been vacated. If BSIS did more than simply alert the driver when starting to turn into another object occupying his blind spot (e.g., input a steering command to avoid turning into the blind spot entirely), then it would be considered a mitigation that employed a detection with automatic response. To fully mitigate this causal factor with BSIS, the operator of this vehicle must manually control steering commands to avoid turning into another vehicle occupying its blind spot. Additionally, since BSIS may not always properly detect vehicles in the blind spot, the system requires the operator to visually confirm lane changes. Figure 4-6 below shows how BSIS is supposed to operate [46].

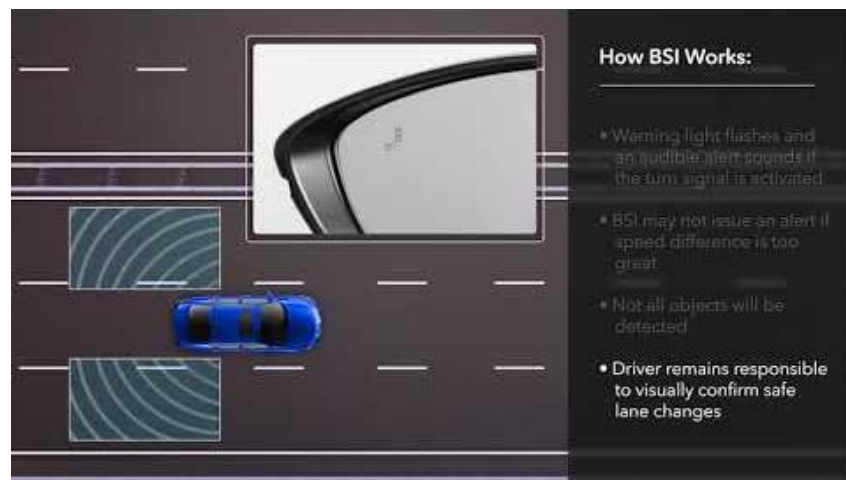


Figure 4-6: Honda Blind Spot Information System (BSIS)

Like the earlier fire extinguishing example, detection and manual response reacts to the presence of a causal factor but does not proactively prevent or eliminate it. One potential design choice to reduce the causal factor might be to design a vehicle with fewer blind spots.

In 2017, Toyota filed a patent that suggested design choices that make the forward blind spot caused by the A-pillars of a car, transparent, offering drivers a full view of their frontal surroundings [46]. The A-pillars frame the windshield on the left and right sides of the dashboard and provide much needed protection in the event of a collision. While this potential design does nothing for the rear blind spots, it does provide valuable removal of 50% of the vehicle's total blind spots, thereby reducing the occurrence of collisions associated with those frontal blind spots. Figure 4-7 below depicts the design mitigation from Toyota's patent [47]. If designing for detection and manual response is not possible (due to various potential reasons), incorporating proper training and procedures represents the final level of mitigation effectiveness and is almost always available to system designers.

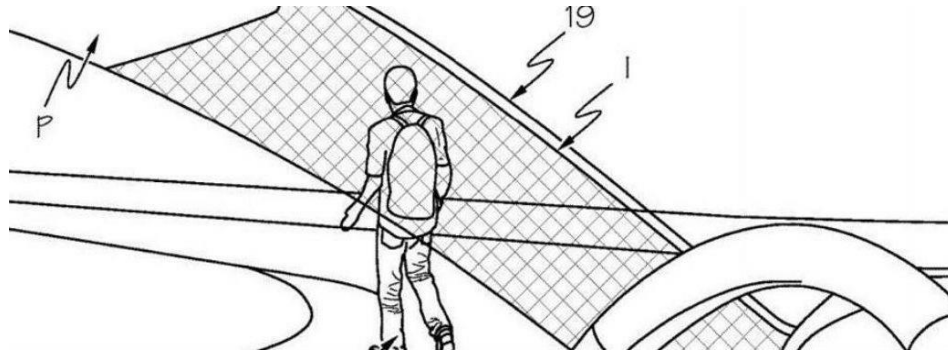


Figure 4-7: Image from Toyota's Transparent A-Pillar Patent

4.2.3 Training and Procedures

While it is only possible to identify what encompasses ‘proper training and procedures’ related to a great number of options, some relevant examples are provided here. In terms of procedures, engineers often develop detailed checklists to help operators reduce working memory load and ensure accuracy in operating the system correctly. Pilots utilize checklists for every aspect of flying from pre-flight through shut down to ensure that they have conducted the numerous required steps to properly execute each phase of aviation operations.

For example, the newer Boeing 787 Dreamliner has 39 high-level checklist steps (not including numerous sub-steps) that pilots must execute from pre-flight to engine start [48]. One could imagine what losses might occur if an inaccuracy existed in the checklist, or if the checklist formatting confused pilots, making it possible to omit or misinterpret a step. The impact of not correctly implementing the proper procedures and its contribution to aviation accidents is well documented in various reports such as those studied by Shappell *et al* [49].

For aviators, proper training is especially important, particularly when responding to emergencies. For example, the Black Hawk Aircrew Trainer (BAT) is a highly immersive training device for the UH60-M aircraft – one of the most flown helicopters in the Army fleet today (Figure 4-8 below) [50]. The flight simulator allows pilots to train in situations and prepare for emergencies that are impossible to simulate in the aircraft [51]. Without such a training tool, pilots of the UH-60M would be far more ill-equipped to safely react to those scenarios.

The purpose of these examples serves only to illustrate how a system might strive to implement the correct training and procedures as a mitigation measure for unsafe scenarios, rather than to provide an exhaustive list of possibilities. If robust training and procedural measures like the UH-60M BAT simulator are selected, then the applied measures can contribute a mitigation effectiveness score of (1).



Figure 4-8: UH-60 Blackhawk Aircrew Trainer

4.3 Assessing Post-Mitigation Severity

To depict the initial risk state of the system, only the *Pre-Mitigation Severity* (PMS) of each risk must be assigned (i.e., before any mitigations are applied, what is the worst-case severity of the risk's resultant loss). PMS is only applied to the severity of the overall pre-mitigated risk, whereas *Post-Potential Mitigation Severity* (PPMS) evaluates the potential impact of each individual mitigation's change to severity. Once PPMS has been determined for each mitigation, the combined impact of all mitigations upon severity can be assessed in a *Combined Post-Mitigation Severity* (CPMS). Note that Pre-Mitigation Severity is usually possible to determine in an early stage of system development.

The CPMS for each risk factor is calculated by finding the *average* of all PPMS scores for a risk and then rounding down to the nearest whole integer (i.e., the worst-case severity outcome). A brief example of how to find CPMS is shown below using Table 4-3, which assumes three hypothetical mitigations (RM01, RM02, and RM03) are applied to Risk # 1. No weighted scaling or other mathematical transformations are applied to CPMS calculations. An assumption is made that each mitigation's impact to severity are equally powerful. The only exception to this determination of CPMS is if an identified risk is eliminated through the applied mitigations, in which case the CPMS defaults to 4 (*Negligible*).

Risk ID	PMS	Mitigation ID	PPMS	CPMS
R1	1	RM01	4	3
		RM02	3	
		RM03	3	

Table 4-3: Example CPMS Table

For $N = \#$ of mitigations

$$CPMS = \frac{\sum_1^N PPMS}{N} \text{ (Round Down to Nearest Whole Integer)}$$

$$\text{From Table 4-3: } CPMS = \frac{(4+3+3)}{3} = \mathbf{3} \text{ (Round Down to Nearest Whole Integer)}$$

For some mitigations, PPMS may not change from the initial PMS. For example, some ‘Reduction Through Design’ mitigations may not reduce severity as these are often proactive measures that help prevent the occurrence of the risk but may not do anything to reduce the severity if the scenario occurred. Consider a new walking path built into a mountain (see Figure 4-9 below), where the risk is falling off the trail and down a steep cliffside [52].

One possible mitigation may be a guard rail that prevents a hiker from falling, which strongly mitigates against falling off the path and its associated losses. However, if a hiker were to fall off the path despite the guard rail, the severity of the risk has not changed as the resultant loss to the individual is most assuredly the same as it is without the guard rail. To take the example a step further, if a safety net were in place alongside the guard rail, this mitigation measure (Reduction Through Design) still proactively prevents the fall and now reduces the severity of the hazard from what could have been ‘*Catastrophic*’ to ‘*Negligible*’ risk.



Figure 4-9: Example Severity Scenario with Mountain Peak

To avoid as much subjective estimation and unintentional bias in application of the PMS/PPMS, the authors recommend a ‘separation of powers.’ The individuals who develop and score mitigation effectiveness should be different from those who assess the PMS/PPMS of each individual mitigation. Ideally, a group of subject matter experts (SMEs) familiar with the system would evaluate the potential impacts to severity. Since many risk factors begin at the highest severity level (*Catastrophic*, 1), there is significant subjectivity in interpretation of risk along the severity axis (from 1 to 4). Hence, a clear separation between those who score mitigation effectiveness and severity helps minimize some of the ‘gaming’ of the quantifiable aspects of the authors’ approaches to risk. Those who develop the mitigations may have a much higher opinion

of how well a measure would impact severity, and therefore should be removed from making severity assessments.

4.4 Two Approaches to the STPA-Informed Risk Matrix

The authors present two possible ways to quantify and prioritize the results of STPA to fit them within the bounds of a standard risk matrix. These methods require a thorough understanding of the authors' suggested use of mitigation effectiveness as a substitute for probability discussed in Section 4.2. The next two sections describe the methodology as well as the strengths and weaknesses of both the scenario and hazard-based approaches to creating an SRM.

4.4.1 Scenario-Based Approach

The scenario-based approach treats risk as all the potential causal scenarios that lead to a loss and their ability to be mitigated. Section 2.2.1 of this thesis discussed the DoD's use of risk-statements in depth, which share many similarities with causal scenarios generated by STPA. Current DoD risk statements are formulated using a detailed "if-then" sentence structure. While not all causal scenarios are written explicitly in that format, causal scenarios describe "the causal factors that can lead to the unsafe control actions and to hazards [1, p. 42]." The causal factors are the "if" portion of a risk statement, and the hazards are the "then" portion. This similarity in how causal scenarios are written allows for straightforward translation into the DoD's method of capturing risks. Furthermore, this supports the authors' assertion that causal scenarios can represent the risks themselves when assessing system safety.

For example, if an analysis yielded 125 causal scenarios, these scenarios would represent the initial number of unique risks that must be mitigated. The initial risk assessment may not fully represent every risk within the system, but it is a starting point as STPA is iterated throughout system development. The full list of initial unmitigated risks can be depicted on an SRM with PMS to show the initial risk state, which will tend to be high overall because each risk will fall within the "*Least Effective*" mitigation effectiveness row of the matrix.

Following an analysis of the system using STPA, the risk practitioners can assess the causal scenarios by developing a list of recommended mitigations for each risk. Each mitigation is assessed a MES using the scale of mitigation effectiveness discussed in Section 4.2. The final CMES will be determined based on the quality (not quantity) and levels of mitigations applied. Additionally, a PPMS is assessed based on the merits of each mitigation's effectiveness alone, and CPMS is then calculated using each PPMS. On the STPA-Informed Risk Matrix, CMES replaces probability along the y-axis and PPMS replaces the standard severity measure on the x-axis.

In real-world applications, it is unlikely that all proposed mitigations would be selected for varying reasons (cost, schedule, difficulty to implement, etc.). However, the new SRM is meant to depict the best possible outcome if risks are addressed more completely. Ultimately, decision makers reviewing a complete SRM must understand the inherent downsides of rejecting specific recommended mitigations and accept the potentially increased level of risk. The final depiction of an SRM is tailorable based on the list of mitigations chosen, and the tradeoffs for including or excluding certain mitigations must be considered (e.g., excluding a particular *detection with response* mitigation might move a risk into a 'High' category based on its

individual contribution to CMES/CPMS). A brief step-by-step overview of this methodology is listed below in Table 4-4:

Scenario-Based Approach	
Step 1	Complete STPA
Step 2	Assess the Pre-Mitigation Severity (PMS) of each casual scenario
Step 3	Generate mitigations to eliminate/control causal scenarios
Step 4	Complete Scoring of CMES/CPMS
Step 5	Plot each causal scenario onto SRM based on CMES/CPMS

Table 4-4: Steps for Scenario-Based Approach for SRM

Upon completion of the five-step process above, the level of granularity of the analysis can be adjusted. For example, decision makers may not want to see a matrix cluttered with hundreds of causal scenarios, which would make identifying areas of concern more challenging. The authors explored a few methods to present a legible and informative SRM.

One method is to plot all causal scenarios onto one SRM. This will show the total system risk in one succinct diagram, affording program managers a high-level view that will aid decision-making and resource allocation. The major downside to this method is that systems with many casual scenarios would yield an extremely cluttered SRM. Ideally, this method would apply to assessments that generate relatively fewer scenarios.

Another method aggregates causal scenarios under their respective UCAs. This representation highlights the control actions that potentially pose the greatest problems for system safety. Additionally, the causal scenarios can then be mapped on the high-level control structure to show which control-feedback loops contain the most risk.

One last method is to group the causal scenarios based on resource requirements. Realistically, applying every mitigation may not be feasible for a design to succeed. Some mitigations may require extensive resource reallocation, prompting formal managerial decisions prior to implementation. Therefore, grouping scenarios based on their implementation requirements will be valuable for decision-makers to assess which mitigations to include or exclude.

4.4.1.1 Strengths and Weaknesses of the Scenario-Based Approach

The scenario-based approach provides multiple strengths in its identification and mitigation of risk. By redefining risk factors as the causal scenarios generated by STPA, risk is captured far more completely than other forms of analysis. Chapter 2 reviewed relevant DoD risk terminology and the DoD RIO’s definition of risk starts as any “potential future event or condition that may have a negative effect...” Causal scenarios capture the potential future events and conditions that can lead to a loss (or negative effect) more analytically and completely than other competing methodologies in use today, such as FMEA or RCA.

Additionally, other methodologies focus on component reliability, which is not the same as safety because of issues that can result from controller interactions. The failure to address the various interactions between a system’s components, software, and controllers significantly

reduces the number of risks identified in the process, which can lead to major losses once the system is in full production and use. Therefore, one of the key strengths of the scenario-based approach is its more comprehensive representation of the potential risks within a developmental system, thereby allowing mitigation of identified risks prior to a system's launch.

Because the scenario-based approach is more comprehensive in capturing risk, some could consider this a weakness. Theoretically, STPA scenario generation can be iterated indefinitely. The true limit is based on the creativity of those conducting the analysis and time available. Generating causal scenarios and identifying a system's risks is time-intensive. However, there is research that shows STPA can be far less time-intensive than other methodologies. One presentation from Yahia and Fawzy on a study involving electric vehicles found methods such as Critical Path Analysis (CPA) and Fault Tree Analysis (FTA) took twice as long and yielded lower quality results than STPA [53].

Additionally, with even a small subset of generated scenarios, it becomes clear that the various types of potential risks exist far beyond the scope of individual system components (e.g., interactions between operators and hardware/software, the various assumptions about human or system behavior, etc...). Therefore, valuable insights can still be gained from a brief, higher-level analysis that generates fewer scenarios yet captures key risk areas that were previously unexplored using methods other than STPA. More scenarios lead to greater understanding of these safety risks within a system. The identification of risks through scenario generation will often be achieved iteratively throughout the engineering and design process, which implies there is no explicit start or stop point in the analysis using this approach.

One feature of this method that serves as both a strength and weakness is how MES and CMES are calculated. The authors chose to utilize a linear scale for mitigation effectiveness levels as opposed to other mathematical distributions. The primary reason for this choice was to simplify the understanding and application of the methodology for the everyday risk practitioner. While the use of other scales for calculating MES and CMES could have been applied (e.g., logarithmic, exponential, etc.), these were considered too cognitively burdensome to apply intuitively. This tradeoff outweighed any potential benefits gained from possibly more appropriate mathematical scales.

For example, a logarithmic scale might have better characterized larger CMES values, particularly if non-linear step values were chosen between mitigation tiers (e.g. 1-5-15 vs. 1-2-3 in mitigation scores). A non-linear scale in mitigation levels also may have been more appropriate under the assumption that one type of mitigation may be far more effective over another. However, it is difficult to state how much more effective various types of mitigations might be. To fully understand and research the real effectiveness of various mitigation levels would be its own thesis topic; therefore the authors chose a simple linear-step scale in assessing mitigation effectiveness until further research definitively proves otherwise.

Another potential weakness with this approach involves possible 'gaming' of the quantitative system developed by the authors. The authors' stakeholder interviews with DoD experts emphasized many experiences with disguising or artificially mitigating risks on a matrix by subjectively downgrading risks that would draw the ire of a higher-level manager. Those individuals with the mindset of avoiding high risks might attempt to use this approach to subjectively calculate CMES and CPMS values that would fit their needs. In such instances, the need for the 'separation of powers' in evaluation mitigation/severity scoring is even greater.

4.4.2 Hazard-Based Approach

The hazard-based approach leverages the causal scenarios from an STPA to generate a complete list of sub-hazards from the original system hazards conceived at the start of the analysis. The sub-hazards are used to “create the behavioral (functional not probabilistic) safety requirements for the various system components, including the software and human operators [1, p. 60].” In this approach, the sub-hazards represent the higher-level mishaps that are to be eliminated or mitigated as risks. The sub-constraints, which are considered synonymous with the controls implemented upon a system, are then formulated for the sub-hazards by using declarative “must” or “must not” statements that dictate ideal controller behavior. The sub-constraints, in conjunction with other system requirements, mitigate the sub-hazards. Leveson and Thomas outline how to formulate hazards and safety constraints using the below format [1, p. 20].

Hazard	<i>System + Unsafe Condition + [Link to Losses]</i>
Safety Constraint	<i>System + Condition to Enforce + [Link to Hazards]</i>

Table 4-5: Hazard and Constraint Formulations

Example Hazard and Safety Constraint:

H-1: <Aircraft> + <violates minimum separation standards> [L-1.0, L-2.0, L-3.0]

SC-1: <Aircraft> + <must satisfy minimum separation standards from other aircraft and objects> [H-1]

Within STPA, refining hazards into sub-hazards is an optional step that is most useful for “large analysis efforts and complex applications [1, p. 21].” While this refinement can occur immediately following the review of high-level hazards, the authors revisit sub-hazard development following completion of causal scenario generation to inform a more complete list. It is highly likely that at least some new sub-hazards would be captured through identification of UCAs and their associated causal scenarios. For example, consider the example hazard and causal scenario below that inform the generation of a new sub-hazard and sub-constraint:

<i>System Hazard 1.0</i>	Aircraft is uncontrollable (manned/unmanned) [L-1.0, L-2.0, L-3.0]
<i>Causal Scenario 1.X.X</i>	Flight operator does not perform data management tasks when entering a new airspace. This could occur if an updated configuration renders the data management tactics, techniques, and procedures that the flight operator is accustomed to, incompatible for proper operation of the system. As a result, the aircraft becomes uncontrollable.
<i>Sub-Hazard 1.1</i>	Aircraft configuration is inappropriate for flight operations [L-1.0, L-2.0, L-3.0]
<i>Sub-Constraint 1.1</i>	Aircraft configuration must be appropriate for flight operations [H-1.1]

Table 4-6: Example Sub-Hazard and Sub-Constraint Generation

Earlier in the analysis, during the refinement of sub-hazards (Step 1 of STPA), a configuration related sub-hazard may not have been identified. The point of this example is to illustrate that there are likely ‘known unknown sub-hazards’ in the early stage of the analysis, which can later be refined with the added granularity provided by robust causal scenario generation from Step 4 of STPA.

While considering the sub-hazards as they relate to causal scenarios, one way to derive the sub-hazards is to ask: What do we need to control to prevent this hazard [1, p. 21]? Another example of breaking down a hazard into sub-hazards is presented below in Table 4-7 [1, p. 21].

System Hazard [H-4]: Aircraft comes too close to other objects on the ground.

Sub-hazards derived from H-4	Example Sub-constraints
H-4.1: Deceleration is insufficient upon landing, rejected takeoff, or during taxiing	SC-4.1: Deceleration must occur within TBD seconds of landing or rejected takeoff at a rate of at least TBD m/s ²
H-4.2: Asymmetric deceleration maneuvers aircraft toward other objects	SC-4.2: Asymmetric deceleration must not lead to loss of directional control or cause aircraft to depart taxiway, runway, or apron
H-4.3: Deceleration occurs after V1 point during takeoff acceleration	SC-4.3: Deceleration must not be provided after V1 point during takeoff

Table 4-7: Example Sub-Hazards and Sub-Constraints

The example sub-hazards in Table 4-7 show how system states related to deceleration could contribute to an aircraft coming too close to the ground and/or other objects. The sub-constraints then provide limitations on system behavior that would prevent the sub-hazard from occurring. It may be impossible to eliminate a sub-hazard by satisfying a sub-constraint, which means it can only be mitigated at best. Note that in this approach, one sub-constraint is generated per sub-hazard under the principle that if the sub-constraint is satisfied, the associated sub-hazard would be eliminated. The alternative would be multiple sub-constraints being implemented to eliminate one sub-hazard, which is not the intended application in this thesis.

Because the hazard-based approach is meant to be used for identifying risk areas at a high-level in complex developmental systems, sub-constraints are often framed as high-level requirements that forgo precise details. As STPA is iterated and deeper levels of analysis are completed, more specific sub-hazards and sub-constraints can be formulated accordingly. Developers also retain the flexibility to address sub-constraints as necessary without constraining themselves throughout the design process.

Mitigations are developed by satisfying the sub-constraints and are scored accordingly. Individual mitigations may satisfy sub-constraints outright, while some sub-constraints may require the combined effects of multiple mitigation levels. It may not be possible to fully satisfy some sub-constraints (e.g., component performance can never truly be guaranteed in the event of failures/malfunctions), but measures can still be taken to mitigate them as effectively as possible.

Additionally, it is important to note that recommended mitigations will create a corresponding change to the control structure by introducing new elements, feedback, control actions, or entirely new control loops that must be analyzed using STPA to ensure that safety and design requirements are met. Analyzing a mitigation's intended impact to the control structure modeled in Step 2 of STPA ensures that recommended mitigations enhance the safety/cybersecurity of the system, rather than introduce new risks. An illustration of the how mitigations influence the control structure is shown later in Chapter 6.

The hazard-based approach is summarized in the following steps:

Hazard-Based Approach	
Step 1	Complete STPA
Step 2	Generate sub-hazards
Step 3	Assess the Pre-Mitigation Severity (PMS) of each sub-hazard
Step 4	Generate sub-constraints
Step 5	Generate mitigations to satisfy each sub-constraint
Step 6	Complete scoring of CMES/CPMS
Step 7	Plot each sub-hazard onto SRM based on CMES/CPMS

Table 4-8: Steps for Hazard-Based Approach for SRM

Note that in STPA, each causal scenario generated will be linked to its associated sub-hazards based on context, which means some scenarios may pair with multiple sub-hazards. Theoretically, eliminating a sub-hazard would eliminate any associated causal scenarios. However, this may not always hold true because some causal scenario may be tied to other sub-hazards that cannot be fully eliminated. The causal scenarios themselves serve to challenge how effectively mitigations (sub-constraints) prevent the associated losses or mitigate their impact.

4.4.2.1 Strengths and Weaknesses of the Hazard-Based Approach

Because the hazard-based approach shares many similarities with the scenario-based approach, many of the same strengths and weaknesses are applicable. This section will primarily focus on the attributes unique to this specific approach that have not already been discussed.

One of the key strengths of the hazard-based approach is that it allows hazards to be considered and mitigated without requiring an individual to think of every conceivable or emergent causal scenario, as multiple causal scenarios may fall under the same sub-hazard. This process helps speed up the risk evaluation process without sacrificing depth of analysis. To achieve this speed and fidelity in the risk analysis, the assumption is that a sufficient baseline STPA with causal scenario generation has been achieved to drive the refinement of a thorough sub-hazard list.

The hazard-based approach effectively aggregates the risks into sub-hazard groupings, where every conceivable causal scenario is theoretically captured by an applicable sub-hazard. The previously discussed scenario-based approach may be too granular and demand a high cognitive load when presenting system risk analysis to someone unfamiliar with STPA. In contrast, the higher-level view presented by the sub-hazards on an SRM reduces the cognitive demand by presenting overall system risk at a more interpretable level.

The hazard-based approach includes some weaknesses. While sub-hazards can be developed following a review and approval of a high-level hazards (approximately 7-10), a full STPA is still recommended to generate a more comprehensive list of sub-hazards. Therefore, the approach to identifying and mitigating risks is still as work intensive as the scenario-based approach, although the overall time required for a quality assessment of risk is arguably less. Provided that a complete STPA has been conducted with an appropriate level of causal scenario

generation, it is unlikely that developing additional causal scenarios would yield the addition of many new sub-hazards.

Another weakness of the hazard-based approach is that it provides diminishing returns for lower-level applications of STPA. The approach is best suited for large and complex systems, where the continual discovery, refinement, and mitigation of sub-hazards is meaningful. More detailed and specific applications of STPA (e.g., aircraft landing gear system) vs. higher level applications (e.g., autonomous aircraft) are likely to provide less value as the importance of identifying and mitigating sub-hazards may not even be necessary (provided the initial list of higher system hazards adequately represents the specific system). The hazard-based approach was originally conceptualized and tested on a large and complex developmental system and may not be suitable for more detailed analyses depicting specific sub-systems.

4.5 SRM in the DoD Risk Process and the RMF

Whether the scenario-based approach or hazard-based approach is used for risk analysis, the risk assessment process is in accordance with all DoD policies and regulations regarding risk management discussed in Chapter 3. The DoD RIO and MIL-STD-882E help inform the overall risk assessment process, while the RMF (both the DoD and NIST perspectives) address risk assessment more specifically for information and cybersecurity. While the authors developed this methodology as an exploration for how the DoD could improve risk assessment for new developmental programs, the methodology can be extended to any application to include organization, cybersecurity, or information systems. The risk assessment process according to the RIO and the RMF from the NIST are both shown below:

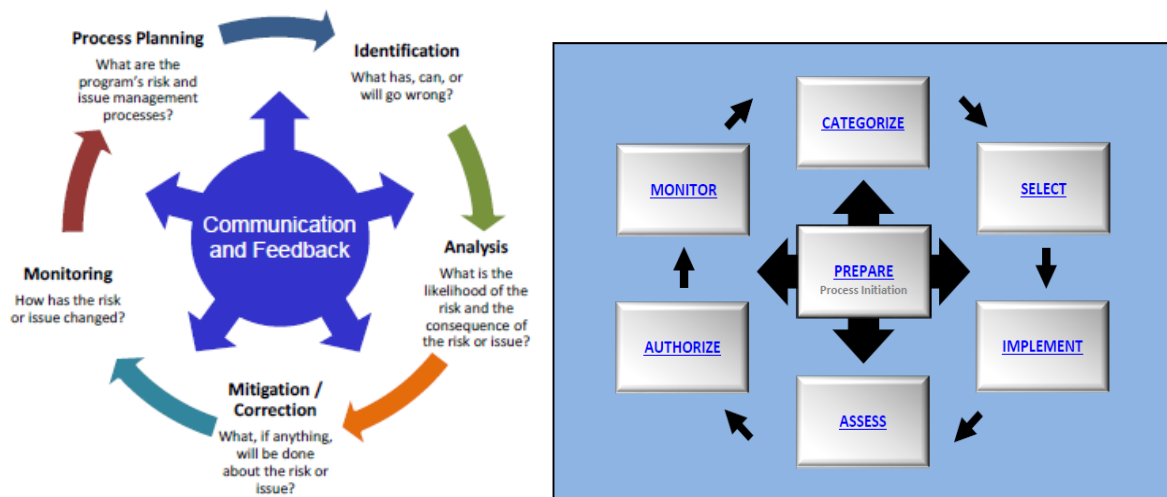


Figure 4-10: Risk Management Process (Left), Risk Management Framework (Right)

Three of the steps of the risk management process from the DoD RIO are *risk identification, analysis, and mitigation/correction*. The scenario/hazard-based approaches using STPA thoroughly satisfy the requirements of these three steps. In terms of *process planning*, STPA and the creation of the SRM represent the formal processes to document the overall approach (as opposed to traditional hazard analysis methodologies). *Risk monitoring* answers the question of how are the risk mitigation plans working? While the approaches to creating an SRM in Section 4.4 showed the best-case representation of risk mitigation, the system will need to be

continuously monitored through subsequent iterations of STPA to evaluate the true mitigation effectiveness (or *probability*) of mitigations applied to risks. The DoD RIO continues to recommend use of a risk matrix for risk monitoring with an example shown in Figure 4-11 below [6, p. 38].

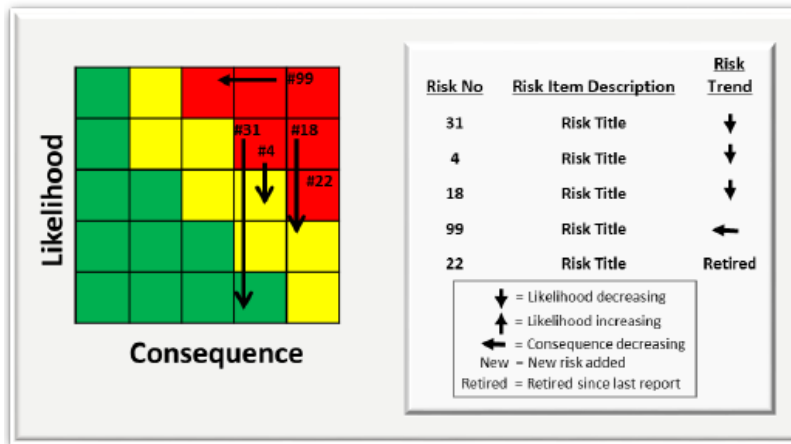


Figure 4-11: Example Risk Monitoring and Trend Matrix

MIL-STD-882E includes an eight-step process to managing system safety and risk that ties into the DoD RIO risk management process and use of the risk matrix. Again, STPA and the SRM fully represent Element 1, or the system safety approach used. Elements 2-5 are captured using STPA and applying mitigations as shown by the authors' approaches. Element 6-8 are satisfied by continuously monitoring the identified risks using STPA as the system progresses in its life cycle.

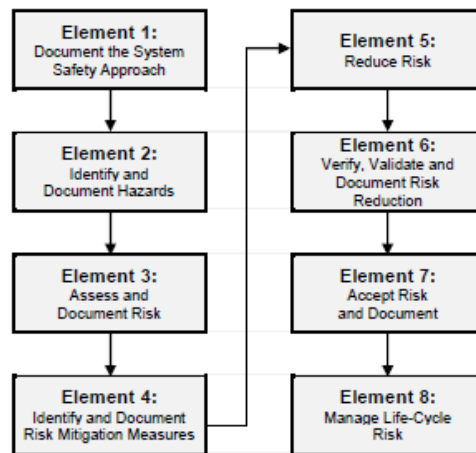


Figure 4-12: Eight Elements of System Safety Process from MIL-STD-882E

The primary takeaway from this Section is to show how the authors' developed risk approaches nest thoroughly within all government regulations, policies, and frameworks for risk, safety, and cybersecurity management. The authors' assessment of these documents in Chapter 3 show that the SRM can provide an improved, standardized, objective approach to risk

management within the DoD. The DoD stands to benefit from applying the SRM to their respective methods for enhanced hazard analysis and control.

4.6 Summary

This chapter served as an exploration of the possible methods to measure and assess risk using the results of STPA. The concepts of *mitigation effectiveness*, *potential post-mitigation severity*, and scoring for each are explained. Two methods are derived that leverage STPA: the scenario-based approach and the hazard-based approach. The scenario-based approach delves into specific causal scenarios and uses *mitigation effectiveness* as a proxy for probability. The hazard-based approach provides a higher view of risk while utilizing the depth of analysis from STPA with an emphasis on sub-hazard identification and sub-constraint development. Section 4.5 showed how the SRM nests within the higher DoD guidance for risk management processes.

While the authors do not claim to have solved the problem of perfect risk identification and assessment, this work establishes the first effort to translate STPA into an interpretable risk identification and mitigation method that is compliant with MIL-STD-882E and DoD policy.

THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK

5 APPLICATION OF NEW MATRIX TO FUTURE ROTARY-WING AIRCRAFT

To demonstrate the different approaches to risk assessment using STPA that were explained in the previous chapter, the authors will apply the methods to a hypothetical future rotary wing aircraft (FWRA) program. This chapter is not meant to demonstrate how to do a complete STPA, and the authors suggest readers reference the STPA Handbook for additional guidance. A future aircraft program is almost always a complex, multi-billion-dollar system that is attempting to achieve novel design goals with specific requirements (e.g., F-35 Joint Strike). Inherently, there is a significant amount of risk to analyze for such a large-scale new system.

Unfortunately, for a new developmental system that relies on a new architecture and advanced components, estimations of reliability and failure modes are unlikely to address the emergent risks. Utilizing STPA to intelligently design the right controls early in the design phase, while iterating the process for continual refinement, helps mitigate risks and prevent future losses. In this chapter, the STPA methodology is used to inform the risk assessment process to achieve more objective results.

5.1 STPA of Future Rotary-wing Aircraft Program

5.1.1 Defining the Purpose of the Analysis

The analysis begins by defining the system boundary and operating environment. Usually, a performance specifications document outlines the objectives the stakeholders want to meet for their program. The theoretical purpose of the FRWA is to conduct combat missions in hostile locations, minimize potential harm to people and equipment within its operating environment, and maintain security of critical information. The FRWA is intended to be an optionally manned aircraft capable of operating fully or semi-autonomously in accordance with the technology trends of the future. Without consideration of detailed design specifications, the authors can still examine the controls that would enable an FRWA to operate safely. While the general purpose and boundaries of the analysis may seem broad, there is enough context to conduct a high-level STPA that provides valuable insights for a developmental FRWA program.

With the purpose and boundaries defined, the next step is to generate possible losses and hazards that will guide the rest of the analysis. A *loss* is something of value to a stakeholder that would be unacceptable to lose (i.e., loss of life, environmental pollution, loss of reputation, etc.). Consequently, there are a few losses that can result from the system's purpose and stakeholder values:

System Losses	
ID	Description
L1.0 – Human Loss	Loss of life or permanent total disability
L2.0 – Material Loss	Loss or damage to aircraft or equipment
L3.0 – Mission Loss	Loss of tactical mission
L4.0 – Critical Information Loss	Loss of critical information

Table 5-1: Future Rotary-wing Aircraft Losses

It is important to note that these losses are not in a specific hierarchical order and do not necessarily reflect priority. The stakeholders determine the relative importance of losses based on their own value assessments. Additionally, losses can be divided into sub-losses. These can provide granularity in assessing more detailed aspects of each loss. Table 5-2 shows one example of subdividing the higher system losses in accordance with the severity categories shown in MIL-STD-882E:

System Losses			
ID		Description	Severity
L1.0 - Human Loss	L1.0	Loss of life or permanent total disability	1
	L1.1	Permanent partial disability; injury that results in hospitalization	2
	L1.2	Injury resulting in lost workdays	3
	L1.3	Injury not resulting in lost workdays	4
L2.0 - Material Loss	L2.0	Loss or damage to aircraft or equipment (>\$1mil)	1
	L2.1	Major damage to aircraft/equipment (<\$1mil, >\$200k)	2
	L2.2	Serious damage to aircraft/equipment (<\$200k, >\$10k)	3
	L2.3	Minor damage to aircraft/equipment (<\$10k, >\$2k)	4
L3.0 - Mission Loss	L3.0	Loss of tactical mission that significantly affects strategic mission	1
	L3.1	Complete loss of tactical mission	2
	L3.2	Partial tactical mission loss	3
	L3.3	Minor tactical mission degradation	4
L4.0 - Critical Information Loss	L4.0	Loss of very important critical information	1
	L4.1	Loss of important critical information	2
	L4.2	Loss of somewhat important critical information	3
	L4.3	Loss of unimportant critical information	4

Table 5-2: Future Rotary-wing Aircraft Losses and Sub-losses

The *severity* column in this table is pertinent to determining the PPMS of each loss outlined in Chapter 4. The sub-loss descriptions and associated severity values can be adjusted based on stakeholder preferences or removed completely if the intent is to conduct STPA without applying the authors’ risk methodologies. To streamline tracking and identification of losses, ‘Loss IDs’ are assigned to each loss. Since an initial STPA examines the high-level control structure of the FRWA system, further analyses could be conducted for other aspects of the program (e.g., program management and organizational structure). Assigning Loss IDs at the start of the analysis allows for proper traceability (losses trace to hazards, hazards trace to constraints, etc.) as the analysis may reveal additional losses and hazards later. The next step in the analysis is to refine the high-level hazards.

A *hazard* is defined as a “system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss [4, p. 9].” The goal is to identify a

system *state* (instead of a component *failure*) that if left unmitigated would result in a loss. An important distinction between hazards and losses is that the effects of hazards can be mitigated through the application of suitable controls, whereas losses are outside the scope of control. Additionally, hazards can contribute to more than one loss, which requires additional notations to maintain traceability. Hazard specification can be summarized using the following format:

$$\text{Hazard Specification} = \text{System} + \text{Unsafe Condition} + [\text{Link to Loss}]$$

Describing hazards in this manner will prevent the common mistake of identifying causes of hazards rather than the hazards themselves. The high-level hazards for the FRWA are below:

System Hazards		
ID	Description	Loss Link
H1.0	Aircraft is Uncontrollable (Manned/Unmanned)	L1.0, L2.0, L3.0
H2.0	Structural Integrity of Aircraft is Violated	L1.0, L2.0, L3.0
H3.0	Minimum Aircraft Separation Standards are Violated	L1.0, L2.0, L3.0
H4.0	Aircraft Environment is Harmful to Human Performance	L1.0
H5.0	Aircraft Operations Cause Collateral Damage or Friendly Fire	L1.0, L2.0, L3.0
H6.0	Aircraft is Unable to Conduct Mission Tasks	L1.0, L2.0, L3.0
H7.0	Critical Information is Compromised	L3.0, L4.0

Table 5-3: Future Rotary-wing Aircraft System Hazards

Each of these hazardous states and associated losses are preventable with proper controls. Constraints are then constructed and traced back to the hazards. A constraint is created by determining the necessary functionality to prevent a hazard. A simpler way of describing a constraint (desired function) is that it is the inverse of a hazard (undesired function). Table 5-4 below shows a list of high-level constraints linked to their associated hazards for the FRWA.

System Constraints		
ID	Description	Hazard Link
C1.0	Aircraft Must Remain Controllable During Manned/Unmanned Operations	H1.0
C2.0	Aircraft Structural Integrity Must Be Maintained	H2.0
C3.0	Aircraft Must Satisfy Minimum Separation Standards from Moving or Fixed Objects	H3.0
C4.0	Aircraft Environment Must Be Suitable for Mission Performance	H4.0
C5.0	Collateral Damage/Friendly Fire Must Be Prevented	H5.0
C6.0	Aircraft Must Be Able to Perform Combat Mission Tasks	H6.0
C7.0	Critical Information Must Be Protected	H7.0

Table 5-4: Future Rotary-wing Aircraft Constraints

New losses, hazards, and constraints may need to be included since unsafe control interactions may surface as the analysis progresses. Next, the analysis can investigate controller responsibilities, control interactions, and modeling of the system control structure.

5.1.2 Modeling the Control Structure

The next step of STPA is modeling the high-level, hierarchical control structure for the FRWA program. A *hierarchical control structure* is “a system model that is composed of feedback control loops. An effective control structure will enforce *constraints* on the behavior of the overall system [1, p. 22].” Control loops capture the relationships between different elements within the system and allow for a clear model of what controls exist and whether they perform the necessary constraints to prevent hazards. Generally, the control structure starts at an abstract level and is iteratively refined to grasp more detail of the system. A complete control structure requires the inclusion of Controllers, Control Actions, Feedback, Inputs/Outputs from Components, Process Models, and Controlled Processes.

The following is a list of the FRWA controllers and their subsequent *responsibilities*. The responsibilities involve providing control actions and receiving feedback, thus creating the control-feedback loops of the overall control structure:

1. **Higher Mission Authority (HMA)**: higher-level command authority for the operators of the FRWA, likely a superior officer/supervisor.
2. **Air Traffic Control (ATC)**: air traffic coordination entity, civilian or military.
3. **Operator(s)**: designates human operator(s) that control the FRWA. Operators may be located inside the aircraft or operate remotely from a Ground Control Station or another future aircraft. The Operator also controls the advanced teaming features with other future aircraft. The generic term ‘operator’ is employed since teaming may be operated by a non-FRWA operator.
4. **Maintenance and Preflight**: those responsible to ensure FRWA configured and ready to execute a specific mission.
5. **Advanced Teaming Control**: autonomous agent that dynamically optimizes the employment of the team of multiple FRWA to coordinate mission execution. This may be implemented as a centralized or a decentralized controller.
6. **Aircraft Software Enabled Controller (ASEC)**: autonomous agent that controls the aircraft subsystems. It consists of a Mission Systems controller and an Air Vehicle Systems controller.
7. **Aircraft Subsystems**: include combat, navigation, communication, propulsion control, flight control, and environmental systems.

With the controllers and their responsibilities defined, the control structure depicts the initial control-feedback loops necessary for the system to function. Process models generate a list of control actions that will be analyzed in the next step of STPA. Each *control action* describes how the controller performs some function over an actuator within the vertical hierarchy of control flow. Black arrows represent control actions, red arrows represent feedback, and dashed lines imply an informational exchange. Informational exchanges are instances where components inside or outside the system boundary provide inputs and outputs that affect operation, but do not necessarily control any aspect of the system. Figure 5-1 below shows the FRWA control structure.

System Responsibilities

ID	Description	
R1.0 – Higher Mission Authority	R1.1	Defines or convey the rules of engagement before a mission
	R1.2	Defines mission parameters such as objectives, configurations, and priorities
	R1.3	Provides mission execution updates and approvals to FRWA during the mission
R2.0 – Air Traffic Control (ATC)	R2.1	Controls aircraft flight paths within an airspace structure
R3.0 – Aircraft Operator	R3.1	Controls aircraft
	R3.2	Performs attack when commanded
	R3.3	Performs reconnaissance when commanded
	R3.4	Performs self-defense when necessary
	R3.5	Executes commands sent by HMA
	R3.6	Protects mission-critical information
R4.0 – Maintenance and Pre-Flight	R4.1	Configures the Aircraft Software Enabled Controller for the mission (ex: program mission parameters, update MOSA firmware)
	R4.2	Configures Aircraft Subsystems for the mission
	R4.3	Conducts the FRWA preflight before takeoff
	R4.4	Maintains the FRWA
	R4.5	Secures critical FRWA data
R5.0 – Advanced Teaming Control	R5.1	Aggregates shared combat data to determine up-to-date status of available FRWA resources and mission tasks
	R5.2	Generates an optimized task allocation of the FRWA resources to accomplish mission tasks subject to defined parameters
R6.0 – Aircraft Software- Enabled Controller (ASEC)	R6.1	Integrates Operator commands to control aircraft subsystems
	R6.2	Provides assisted decision making to the Operator
	R6.3	Ensures system health
	R6.4	Ensures system security
	R6.5	Changes aircraft environment
	R6.6	Enforces limitations of Operator commands
R7.0 – Aircraft Subsystems	R7.1	Executes Operator and ASEC provided commands
	R7.2	Enforces limitations of Operator override commands
	R7.3	Protects mission-critical systems

Table 5-5: Future Rotary-wing Aircraft Responsibilities

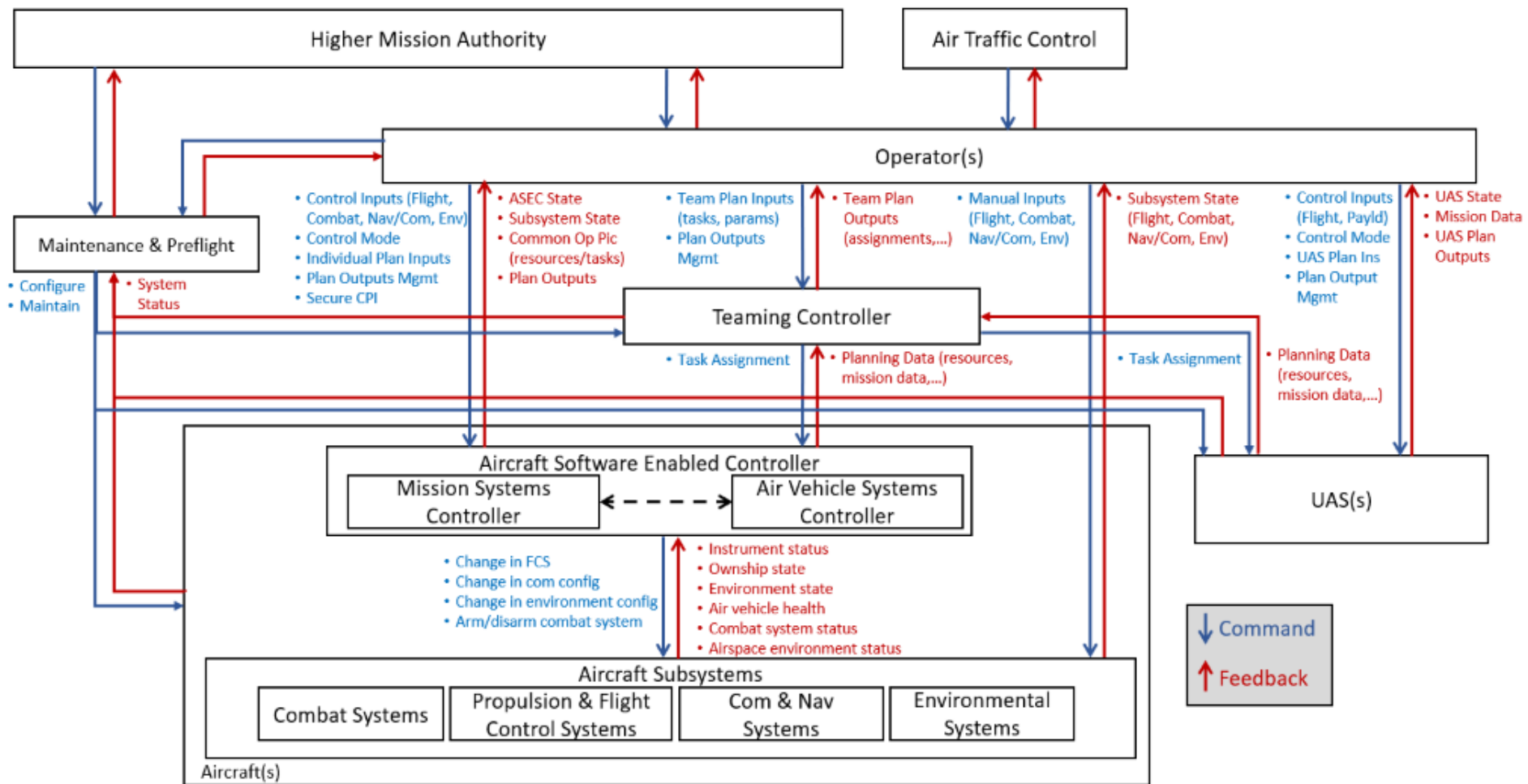


Figure 5-1: Future Rotary-wing Aircraft High-Level Control Structure

Each of the controllers in Figure 5-1 can be deconstructed into more detailed components. For example, the Operator(s) controller encompass both manned and unmanned configurations. The unmanned configuration could consist of a human operator using a remote-control station to send commands to the ASEC within the physical aircraft. Conversely, the system could be manned, which entails one or two pilots physically occupying the aircraft and providing commands to the ASEC via some pilot-vehicle interface (controls, switches, and displays). Future iterations of STPA would represent controllers in more detail as the design of the system begins to move beyond the initial concept theory.

To highlight the risk assessment approaches developed in Chapter 4, the remainder of the analysis in this chapter is limited to the control interactions between the Operator and the Aircraft Software-Enabled Controllers (ASEC). With the control structure created and responsibilities outlined, the next step is to identify the possible unsafe control actions within the system.

5.1.3 Identify Unsafe Control Actions

Unsafe control actions (UCAs) are defined as control actions that will lead to a hazard in a worst-case environment [1, p. 35]. There are four possible ways a control action can be considered unsafe and lead to a hazard:

1. Not providing the control action causes the hazard.
2. Providing the control action causes the hazard.
3. Providing a control action too early, too late, or out of order causes the hazard.
4. Providing a control action for too long or short a time causes the hazard.

Each control action is listed in a table with columns for each of the four cases. All UCAs contain five elements, which appear in the table:

$$UCA = Source + Type + Control Action + Context + [Hazard Link]$$

Using this format, here is a list of the high-level UCAs for a specific control action within the Operator to ASEC control loop:

Control Action	UCA ID	Not providing the control action causes hazard	Hazard Link	UCA ID	Providing the control action causes hazard	Hazard Link
Operator manipulates flight controls <i>(any input related to maintaining safety of flight)</i>	2.0	Operator does not make aircraft control inputs during manned aircraft operation during critical phases of flight	H01, H02, H03, H06	2.3	Operator makes aircraft control inputs when aircraft is in autonomous operation	H01, H02, H03, H06
	2.1	Operator does not make aircraft control inputs when aircraft is disengaged from autonomous mode	H01, H02, H03, H06	2.4	Operator makes improper aircraft control inputs during critical phases of flight	H01, H02, H03
	2.2	Operator cannot make aircraft control inputs during an emergency while the aircraft is in autonomous mode	H01, H02, H03, H06			
	UCA ID	Providing a control action too early, too late, or out of order causes hazard	Hazard Link	UCA ID	Providing a control action for too long or short a time causes hazard	Hazard Link
	2.5	Operator makes aircraft control inputs too early prior during critical phases of flight	H01, H02, H03, H06	2.8	Operator maintains aircraft control inputs for too long during critical phases of flight	H01, H02, H03, H06

	2.6	Operator makes aircraft control inputs too early before autonomous mode is disengaged	H01, H02, H03, H06	2.9	Operator maintains aircraft control inputs for too short a time during critical phases of flight	H01, H02, H03, H06
	2.7	Operator makes aircraft control inputs too late during critical phases of flight	H01, H02, H03, H06			H01, H02, H03, H06

Table 5-6: FRWA Unsafe Controls Actions

These examples highlight only some of possible ways UCAs can occur and do not cover every possible case for FRWA. Additionally, these UCAs do not guarantee that the hazard will result, but instead emphasizes what may happen in a worst-case scenario. These UCAs will provide the basis for the causal scenarios generated and analyzed in the next section. A complete list of all UCAs for FRWA can be found in the Appendix.

5.1.4 Identify Loss Scenarios

The next step is to identify the causal scenarios that can lead to a hazard (UCA) and therefore to a loss. Generally, the scenarios involve control flaws of some kind, which can include unsafe controller behavior, inadequate feedback or informational exchange, issues in the control path, flawed process models, flawed control algorithms, failures in the controlled process, and other things. The analysis between the Operator and the ASEC control loop identified 67 loss scenarios. However, this does not indicate the analysis is complete, nor does it represent every possible scenario. A complete STPA analysis would include independent review and validation of the analysis. Two causal scenarios are presented below as examples:

UCA	Causal Scenario	Refinement
2.0 – Operator does not make aircraft control inputs during manned aircraft operation during critical phases of flight. [H1.0, H2.0, H3.0, H6.0]	CS 2.0.1 - Operator is incapacitated by enemy fire, injury, illness and leans onto the controls accidentally activating them. As a result, the aircraft can become uncontrollable.	<ul style="list-style-type: none"> • The Operator is hit by enemy fire and subjected to a fatal or incapacitating injury. • The Operator becomes airsick due to physiological factors or extreme maneuvering to evade enemy fire. • The Operator experiences a sudden onset of extreme pain due to an undetected health condition.
	2.0.3 - Operator receives poor or inadequate feedback from flight controls and does not make necessary control inputs during a critical mode of flight, as a result the aircraft becomes uncontrollable.	<ul style="list-style-type: none"> • The indication of a fire does not illuminate properly, so the Operator does not perform the emergency procedure. • The altitude indicator is obstructed by dust or debris and reads incorrectly, causing the Operator to not set sufficient power during landing. • The control actuators for a flight surface fail without indication, so the Operator is unable to respond with the correct control inputs.

Table 5-7: FRWA Causal Scenarios

The first scenario describes a situation where the Operator becomes incapacitated for a myriad of different reasons. The second covers an example of inadequate controller feedback

causing the pilot to lose control of the aircraft. If either scenario occurs, UCA 2.0 will occur where the Operator does not make the control inputs during critical phases of flight. Consequently, Hazards 1.0, 2.0, 3.0, or 6.0 may occur. The *refinement* column provides more information about how a situation can unfold. This information might be provided by a SME who is familiar with the details that could lead to loss scenarios. For a complete list of all causal scenarios and their effects on UCAs, refer to the Appendix.

Due to the iterative nature of STPA, causal scenarios can be refined as the analysis progresses. Since they inform design decisions, it is expected that any changes in design may eliminate causal scenarios while creating new ones. The point of creating these scenarios is to suggest how unsafe control actions can occur and how to mitigate them as early as possible in the design phase.

5.2 Creating the STPA-Informed Risk Matrix

With the initial STPA complete, the authors' proposed risk mitigation techniques are demonstrated through a tangible example. The goal of this section is to show each method's effectiveness and compare their results.

5.2.1 Scenario-Based Approach

The scenario-based approach provides the most detail in risk assessment in comparison with the other methods explored by the authors. With STPA for the FRWA complete, the next step is to assess PMS and create mitigations that will eliminate or control the occurrence of the causal risk factors. For example, consider the causal scenarios that cause affect in-flight controllability (CS 2.X.X).

Causal Scenario 2.0.1 describes a situation where the FO is incapacitated, leans on the flight controls, and the aircraft becomes uncontrollable. The PMS is assessed to be *catastrophic* (1), thus requiring some pertinent mitigations with corresponding mitigation effectiveness scores (MES).

Three recommended mitigations (RMs) were determined to control this issue: RM01, RM02, and RM03 ($N=3$). RM01 entails a pilot monitoring system ($MES=2$), RM02 outlines a remote-control design feature ($MES=3$), and RM03 describes an autonomous flight control system ($MES=3$). Therefore, totaling the highest values of each mitigation level results in a CMES of 5 (*Very Effective*). Additionally, each of these mitigations are assessed to reduce severity to 4 (*Negligible*) when applied individually, resulting in a PPMS of 4.

$$CPMS = \frac{\sum_1^3 PPMS}{3} = \frac{4+4+4}{3} = 4 .$$

However, in this example, the authors assess that this scenario can be eliminated when all mitigations are applied simultaneously. Therefore, the final CMES is *ELIM* while the PPMS is still 4.

CS 2.0.2 describes the FO having an incorrect mental model of the state of the flight control systems and loses control of the aircraft. There are three proposed mitigations: RM08, RM12, and RM04 ($N=3$). RM08 ($MES=2$) is an advanced detection and alerting system, RM12 ($MES=2$) is an emergency response system, and RM04 ($MES=1$) details better training and procedures. Therefore, totaling the highest values of each mitigation level results in a CMES of 3

(*Moderately Effective*). For PPMS, RM08 is assessed to reduce severity to *Negligible (4)*, RM12 to *Marginal (3)*, and RM04 to *Critical (2)*. Therefore, the resulting PPMS is *Marginal (3)*.

$$CPMS = \frac{\sum_1^3 PPMS}{3} = \frac{4+3+2}{3} = 3 .$$

This process is repeated for each causal scenario until all have been assigned CMES and PPMS scores. Table 5-8 shows a selection of causal scenarios and their associated mitigations/scores using this method:

THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK

Causal Scenario		PMS	RM ID	Recommended Mitigation	MES	CMES	PPMS	CPMS
CS 2.0.1	Operator is incapacitated by enemy fire, injury, illness and leans onto the controls accidentally activating them. As a result, aircraft can become uncontrollable.	1	RM01	Aircraft monitors pilot health/posture/attention and automatically engages autonomous mode when Operator is incapacitated/task saturated/inattentive/fixated; system can also alert and allow a remote operator to take control	ELIM	ELIM	4	4
			RM02	Aircraft can be remotely controlled while in manned configuration			4	
			RM03	Aircraft can autonomously execute specific flight maneuvers (e.g. return to base, climb/descend to specific altitudes, fly a specific straight-and-level profile, formation flight, reroute to designated airspace); maintains all structural limitations			4	
CS 2.0.2	Operator mental model of aircraft flight control systems conflicts with reality and Operator does not make the necessary manual inputs during a critical mode of flight. As a result, the aircraft becomes uncontrollable. (e.g. executing an emergency procedure incorrectly because the Operator does not understand the relationships between subsystems)	1	RM08	Aircraft health systems monitor aircraft performance, alert Operator when unsafe scenarios are approaching (e.g., engine health in danger, airframe integrity compromised, combat system malfunctions/loss of effectiveness, etc.)	2	3	4	3
			RM12	Emergency response system detects problems and alerts the Operator, awaits Operator input, and automatically engages if outside the time window allotted for Operator action	2		3	
			RM04	Operator trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1		2	
CS 2.0.3	Operator receives poor or inadequate feedback from flight controls and does not make necessary control inputs	1	RM05	Design salient PVI alerts to the Operator that combine audio, visual, and haptic feedback. An alerting schema/framework should be created utilizing context-specific alerts appropriate to the severity of the situation.	3	5	3	3

	during a critical mode of flight. As a result, the aircraft becomes uncontrollable. (e.g. Operator does not get a FIRE light in the event of an engine fire and does not execute the proper emergency procedures)		RM08	Aircraft health systems monitor aircraft performance, alert Operator when unsafe scenarios are approaching (e.g., engine health in danger, airframe integrity compromised, combat system malfunctions/loss of effectiveness, etc.)	2		3	
			RM12	Emergency response system detects problems and alerts the Operator, awaits Operator input, and automatically engages if outside the time window allotted for Operator action	2		3	
CS 2.0.4	Operator becomes saturated with mission tasks and does not respond to aircraft alerts, as a result the aircraft violates minimum separation standards during formation flight (e.g. Operator is performing mission tasks and does not realize aircraft is drifting too close to other aircraft within formation and collides with friendly aircraft)	1	RM03	Aircraft can autonomously execute specific flight maneuvers (e.g. return to base, climb/descend to specific altitudes, fly a specific straight-and-level profile, formation flight, reroute to designated airspace); maintains all structural limitations	ELIM	ELIM	4	4
			RM01	Aircraft monitors pilot health/posture/attention and automatically engages autonomous mode when Operator is incapacitated/task saturated/inattentive/fixated; system can also alert and allow a remote operator to take control			4	
			RM21	Aircraft geospatial awareness systems (GPS, proximity sensors, transponder, etc.) provide position data in relation to terrain, airspace, aircraft, known enemy positions, and other obstacles that alerts the Operator if safety thresholds are breached. Real-time airspace update service that can relay dynamically changing airspace/battlespace information to participating aircraft; data is pulled from high level server every X minutes to provide information to operators			4	
CS 2.0.5	Operator commands a flight control input, but it is not received because of faulty wiring/hardware malfunction in the fly-by-wire system (e.g. Operator tries to correct trim of aircraft but tail rotor control does not receive signal)	1	RM14	Design redundant architecture for all critical control components to ensure proper operation (e.g. wireless signal equipment, control linkages, onboard wiring)	3	3	3	3

Table 5-8: Risk Calculations for Causal Scenarios 2.X.X

In the last step, the causal scenarios are plotted on the STPA-Informed Risk Matrix (SRM) and their risk scores can be calculated. The matrix below in Figure 5-2 depicts the risks for all causal scenarios related to flight control inputs:

Flight Control Manipulation Risks					
Least [A]	0				
Somewhat [B]	1				
Moderate [C]	2-3		2.1.1, 2.3.1, 2.4.2,	2.0.2, 2.0.5, 2.5.1,	
Very [D]	4-5		2.4.1, 2.7.3, 2.7.4, 2.8.1,	2.0.3, 2.8.3,	
Most [E]	6		2.8.2,	2.5.2, 2.5.3, 2.9.2, 2.9.3,	
Eliminated [F]	N/A	2.0.1, 2.0.4, 2.2.1, 2.6.1, 2.7.1, 2.7.2, 2.8.4, 2.9.1,			
CMES		1	2	3	4
	CPMS	Catastrophic	Critical	Marginal	Negligible

Figure 5-2: SRM for UCA 2.0 Series on Flight Control Manipulation

For the full risk analysis using the scenario-based approach, reference Appendix Section 7.2, which contains the calculations and risk profiles for each UCA series analyzed within the Operator to ASEC control loop. The application of this approach only shows the causal scenarios for one UCA series. While more control loops were analyzed during the overall STPA and many more scenarios were generated, the authors chose to illustrate the results using a selected portion of the analysis.

The authors opted to plot all causal scenarios based on UCAs to avoid clutter. Reference the Appendix Section 7.2 to see an example of all scenarios plotted on one SRM. It is possible that an analysis of a completely different system may yield hundreds of scenarios, necessitating a different approach to aggregating and visualizing risk. However, the previous point is less significant as many risk managers typically choose to only see several of the highest risks on a matrix.

Overall, the scenario-based approach leverages STPA’s depth of analysis and generates a useful informed risk matrix from which planners can comprehensively assess the risk within the system based on mitigation effectiveness. The matrix is aligned with MIL-STD-882E for familiarity and the risk definitions remain unchanged. As discussed in Chapter 4, the CMES scale allows for translation to probability if desired. This similarity allows for easier implementation by providing a familiar risk matrix informed by a complete STPA.

5.2.2 Hazard-Based Approach

The hazard-based approach provides a higher-level risk assessment while using the depth of analysis provided by STPA causal scenarios generation. Following the methodology described in Section 4.4.2, the first step after completing STPA is to capture sub-hazards using the context of the causal scenarios.

Table 5-9 below contains the sub-hazards generated from all the causal scenarios linked to system hazard H1.0: *Aircraft is Uncontrollable (Manned/Unmanned)* and will serve as the primary example. Note that the sub-hazards shown are only from the analysis of the FO-ASEC control loop and is not representative of all potential sub-hazards within the system.

System Hazards			
ID	Description		Loss Link
H1.0 - Aircraft is Uncontrollable (Manned/Unmanned)	H1.1	Insufficient control inputs during manned flight	L1.0, L2.0, L3.0
	H1.2	Insufficient control inputs during unmanned flight	L1.0, L2.0, L3.0
	H1.3	Controller/hardware feedback is inadequate/incorrect to maintain controllability	L1.0, L2.0, L3.0
	H1.4	Aircraft controllability is susceptible to enemy action	L1.0, L2.0, L3.0
	H1.5	Improper exchange of control authority during flight operations	L1.0, L2.0, L3.0
	H1.6	Configuration is inappropriate for flight operations	L1.0, L2.0, L3.0
	H1.7	Aircraft safety measure prevent controllability during flight operations	L1.0, L2.0, L3.0

Table 5-9: Sub-Hazards for Aircraft Controllability (H1.0)

Each sub-hazard is listed and linked to its corresponding loss. It is important to note that these sub-hazards are generated based on the causal scenarios, so each scenario is linked to the most relevant sub-hazard.

Overall, there were 67 causal scenario that were grouped into 39 sub-hazards. The specific scenario to sub-hazard pairings can be found in Appendix Section 7.2. This process captures the depth of STPA without analyzing each individual causal scenario directly based on specific contextual details. The next step is to create sub-constraints and link them to sub-hazards, as demonstrated in Table 5-10 below.

System Constraints

ID	Description	Hazard Link	
C1.0 - Aircraft Remains Controllable During Manned/Unmanned Operations	C1.1	Control inputs must be adequate to maintain aircraft controllability for manned flight	H1.1
	C1.2	Control inputs must be adequate to maintain aircraft controllability for unmanned flight	H1.2
	C1.3	Controller/hardware feedback must be adequate to maintain controllability	H1.3
	C1.4	Aircraft control architecture must not be susceptible to enemy action	H1.4
	C1.5	Control authority for flight systems must be properly exchanged	H1.5
	C1.6	Configuration must be appropriate for flight operations	H1.6
	C1.7	Aircraft safety measures must not affect controllability during flight operations	H1.7

Table 5-10: Sub-Constraints for Aircraft Controllability (H1.0)

These constraints are designed to specify the ideal behavior of the system through recommended mitigations to prevent the sub-hazards from occurring. Next, risk calculations are complete in the same manner as the scenario-based method. Using C1.2 as an example, recommendations are required to ensure aircraft controllability can be maintained during unmanned flight.

First, the PMS is assessed to be *Catastrophic (1)*. Three recommended mitigations (RMs) were determined to combat this issue: RM02, RM03, and RM04 ($N=3$). RM02 outlines a remote-control design feature ($MES=3$), RM03 describes an autonomous flight control system ($MES=3$), and RM04 outlines training and procedures ($MES=1$). Therefore, totaling the highest values of each mitigation level results in a CMES of 4 (*Very Effective*). For PPMS, RM02 is assessed to reduce severity to *Negligible (4)*, RM03 to *Marginal (3)*, and RM04 to *Marginal (3)*.

$$CPMS = \frac{\sum_1^3 PPMS}{3} = \frac{4+3+3}{3} = 3 .$$

Therefore, the final CMES is *Very Effective (4)* and the PPMS is *Marginal (3)*.

Another example is shown for C3.2, which involves maintaining minimum separation standards from intangible entities (e.g., airspace). The PMS for this sub-hazard is *Catastrophic (1)*. There are two proposed mitigations: RM21 and RM04 ($N=2$). RM21 ($MES=ELIM$) is an advanced geospatial awareness system, and RM04 ($MES=1$) outlines better training and procedures. Totaling the values of each mitigation level results in a CMES of *ELIM* because one of the RMs can eliminate the sub-hazard. For PPMS, RM21 is assessed to reduce severity to *Negligible (4)* and RM04 to *Marginal (3)*.

Therefore, the resulting PPMS is *Marginal (3)*.

$$CPMS = \frac{\sum_1^2 PPMS}{2} = \frac{4+3}{2} = 3 \text{ (rounded down) .}$$

The final CMES is *ELIM* while the CPMS is still *Marginal (3)*. Table 5-11 highlights a few more examples of this method.

Constraint		Hazard Link	CS Link	PMS	RM ID	Recommended Mitigation	MES	CMES	PPMS	CPMS
C1.2	Control inputs must be adequate to maintain aircraft controllability for unmanned flight	H1.2	2.2.1, 2.6.1, 2.7.3, 2.8.2, 2.9.2, 3.5.1,	1	RM02	Aircraft can be remotely controlled while in manned configuration	3	4	4	3
					RM03	Aircraft can autonomously execute specific flight maneuvers (e.g. return to base, climb/descend to specific altitudes, fly a specific straight-and-level profile, formation flight, reroute to designated airspace); maintains all structural limitations	3		3	
					RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1		3	
C3.2	Aircraft must satisfy separation standards for intangible entities	H3.2	2.8.3, 3.0.1, 3.0.2, 3.3.1, 3.4.1, 5.5.1,	1	RM21	Aircraft geospatial awareness systems (GPS, proximity sensors, transponder, etc.) provide position data in relation to terrain, airspace, aircraft, known enemy positions, and other obstacles that alerts the FO if safety thresholds are breached. Real-time airspace update service that can relay dynamically changing airspace/battlespace information to participating aircraft; data is pulled from high level server every X minutes to provide information to operators	ELIM	ELIM	4	3
					RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1		3	
C1.3	Controller/hardware feedback must be adequate to maintain controllability	H1.3	2.0.3, 2.6.1, 2.7.3, 2.8.4, 2.9.1, 3.5.1,	1	RM05	Design salient PVI indications/alerts with high polling rates that combine audio, visual, and haptic feedback. An alerting schema/framework should be created utilizing context-specific alerts appropriate to the severity of the situation.	3	5	4	3
					RM08	Aircraft health systems monitor aircraft performance, alert FO when unsafe scenarios are approaching (e.g. engine health in danger, airframe integrity compromised, combat system malfunctions/loss of effectiveness, etc.)	2		3	

Table 5-11: Risk Calculations for Sub-Hazards

With CMES and CPMS calculated, the sub-hazards are plotted on the SRM:

Sub-Hazard Risks					
Least [A]	0				
Somewhat [B]	1				
Moderate [C]	2-3				
Very [D]	4-5			1.2, 1.3	
Most [E]	6				
Eliminated [F]	N/A	3.2			
CMES		1	2	3	4
	CPMS	Catastrophic	Critical	Marginal	Negligible

Figure 5-3: SRM for Example Sub-Hazards

These sub-hazards are just a few select example to show how calculations work for different MES, CMES, and PPMS scores. For the complete risk calculations for all sub-hazards, refer to the Appendix Section 7.2.

The hazard-based approach provides a higher view of the potential safety issues within the system while taking advantage of the detailed context provided by the causal scenarios. The ‘CS Link’ column shows which scenarios link to sub-hazards and sub-constraints. This helps traceability in determining how recommendations can affect sub-hazards and scenarios alike. It is possible that a sub-hazard can be eliminated through proper constraint satisfaction, yet some associated causal scenarios could still occur because they are linked to multiple different sub-hazards.

For example, CS 3.5.1 is linked to sub-hazards H1.2 and H1.3. Appropriate mitigations were able to eliminate H1.2, yet H1.3 was only able to achieve a CMES of 5. This means that CS3.5.1 could still occur despite only one of its linked sub-hazards being eliminated. As with the scenario-based method, the same cluttering issues can arise when plotting all hazard groups onto

one matrix. The key benefit with this approach is that hazards are meant to be generalized, which helps account for most, if not all, causal scenarios that could occur. The simplest way to combat crowding on the matrix is to ensure the sub-hazard list is succinct and reflects undesirable system states rather than causes. Additionally, only the highest risk or most difficult to mitigate sub-hazard groups may be shown on the risk matrix.

5.3 Comparison of the Two Approaches

Comparing and contrasting the methods above yield some interesting insights. The scenario and hazard-based methods convey more useful information as shown in the comparison chart in Table 5-12 below.

	Scenario-Based		Hazard-Based	
Mitigation Effectiveness	67 scenarios		39 hazards	
ELIM	30	43%	16	41%
6	6	9%	10	26%
5	12	17%	4	10%
4	5	7%	4	10%
3	12	17%	5	13%
2	1	1%	0	0%
1	1	1%	0	0%

Table 5-12: STPA Mitigation Results Comparison

The chart categorizes scenarios and hazards by their final CMES. Interestingly, both methods eliminated approximately 40% of causal scenarios and hazards. It appears there is more of a spread to ‘mitigation effectiveness’ that result in lower CMES scores for the scenario-based approach, whereas the sub-hazards were grouped at higher scores. There were no hazards that scored less than a CMES of three, which means that a recommended design change would satisfy a constraint and thus eliminate the sub-hazard. However, this only shows half of the risk analysis since severity is not considered at this point. The SRMs below (Figures 5-4 and 5-5) convey the risk matrix using the scenario and hazard-based approaches.

THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK

All Causal Scenarios					
Least [A]	0				
Somewhat [B]	1		4.4.1,		
Moderate [C]	2-3		2.1.1, 2.3.1, 2.4.2,	2.0.2, 2.0.5, 2.5.1, 4.0.2, 6.2.2, 6.3.1,	3.2.1, 4.0.3, 4.6.2, 5.3.1,
Very [D]	4-5	4.1.2, 7.0.1,	2.4.1, 2.7.3, 2.7.4, 2.8.1, 3.0.1, 4.2.1, 5.0.2, 7.1.1,	2.0.3, 2.8.3, 4.0.4, 4.6.1, 5.1.1, 6.4.1, 7.1.3,	
Most [E]	6		2.8.2,	2.5.2, 2.5.3, 2.9.2, 2.9.3, 4.3.1,	
Eliminated [F]	N/A	2.0.1, 2.0.4, 2.2.1, 2.6.1, 2.7.1, 2.7.2, 2.8.4, 2.9.1, 3.0.2, 3.1.1, 3.3.1, 3.4.1, 3.5.1, 4.0.1, 4.1.1, 4.5.1, 5.0.1, 5.2.1, 5.4.1, 5.5.1, 5.6.1, 6.0.1, 6.1.1, 6.2.1, 6.5.1, 7.0.2, 7.1.2, 7.1.4, 7.1.5, 7.1.6,			
CMES		1	2	3	4
	CPMS	Catastrophic	Critical	Marginal	Negligible

Figure 5-4: Causal Scenario-Based Risk Matrix

All Sub-Hazards					
Least [A]	0				
Somewhat [B]	1				
Moderate [C]	2-3			4.4, 4.5, 6.1, 6.3,	
Very [D]	4-5			1.2, 1.3, 2.3, 2.4, 3.3, 4.1, 6.7, 6.10,	
Most [E]	6		6.2, 6.4, 7.4, 7.5,	1.4, 2.1, 4.2, 5.1, 5.2, 6.8,	
Eliminated [F]	N/A	1.1, 1.5, 1.6, 2.2, 3.1, 3.2, 3.4, 4.3, 5.3, 6.5, 6.6, 6.9, 7.1, 7.2, 7.3, 7.6,			
CMES		1	2	3	4
	CPMS	Catastrophic	Critical	Marginal	Negligible

Figure 5-5: Hazard-Based Risk Matrix

The scenario-based risks are more spread out compared to the hazard-based risks among risk categories on the matrix. Because of their detailed nature, risk planners can see the severities of individual scenarios. In contrast, the hazard-based matrix shows a more consolidated view of risk. This appears to suggest that the hazard-based approach may overgeneralize severity by causing CPMS to be more centrally distributed compared to the spread of the scenario based-approach.

The results from this risk analysis can be viewed from different perspectives. The first is that the sub-hazards serve to encompass the scenarios, making it simpler to mitigate the hazardous states directly without diving into the specific context of how those system states will occur. Figuratively speaking, instead of risk planners putting out numerous small fires, they are focusing their efforts on fewer large fires. This approach is ideal for a high-level view of risk because it is easier to make broader changes to satisfy safety constraints earlier in the design process before certain aspects of the system architecture are decided during design reviews.

Another perspective is that the sub-hazards may overshadow some of the specific issues that require more concentrated attention. The authors encountered some causal scenarios that were solved with lower levels of mitigation effectiveness but would lose the specific contextual details of these problems when they are grouped into sub-hazards. Understanding every possible scenario and how to mitigate it provides the context necessary to make very detailed design changes that affect specific elements of the control structure.

However, this level of detail comes at the cost of missing larger emergent issues that may arise when multiple scenarios are grouped together. Patterns and coupling of control actions may not be as obvious when viewed from the detailed perspective of causal scenarios. With either perspective, both approaches offer a concrete way to translate the results of STPA into risk. Both approaches help inform risk managers, who can decide which risk mitigation methods work best for their specific level of risk assessment.

5.4 Summary

This section covered the STPA for a theoretical FRWA system and the resultant risk assessment using the methodologies developed by the authors. Because STPA is an iterative process, the losses, hazards, and constraints may change as the designers mitigate risks. Eventually, all system designs need to move forward in development, at which point certain design changes may no longer be feasible. STPA and the risk assessment approaches presented will help designers find and mitigate any risks along the way.

The scenario-based approach provided the authors with a detailed look at risks within the context of causal scenarios. The concept of mitigation effectiveness proved to be effective in representing system risk based on the quality of controls. The hazard-based approach provided another useful risk assessment approach at a higher level of abstraction. The hazard-based approach yielded interpretable results that program managers and system engineers would find insightful and was informed by a complete STPA analysis.

Each approach provides designers with a perspective of risk that they can then address with early design changes or formulate a mitigation plan to address the risk later in the engineering process. When the approaches are used appropriately and in the right context, they can produce actionable results for organizations to manage risk.

6 CONCLUSION

The authors have demonstrated multiple ways to translate the results of STPA into a thorough risk assessment process. The methods proposed in this thesis were applied to a hypothetical FRWA and would benefit from being tested on other use cases. In particular, the scenario and hazard-based approaches to generating an STPA-Informed Risk Matrix stand to benefit from additional testing, verification, and validation by risk managers within the DoD. The authors hope that the research presented in this thesis can serve better risk practices in any organization where risk matrices are used.

Because cultural change is a slow, tedious process for any organization (particularly the DoD), it is important to make incremental changes with a larger goal in mind. The larger goal in this context is to provide risk analysis tools that decision makers can use to make more informed choices. Any new way to better understand or visualize risk should be welcomed. The proposed approaches do not fundamentally change the definitions provided by standard risk publications but instead add value from the in-depth STPA method.

6.1 Results and Insights

This thesis used the STPA hazard-analysis methodology to better inform the current DoD risk matrix. The results of the analysis addressed the research question raised in Section 1.3, with the summarized answer provided below:

PRIMARY RESEARCH QUESTION:

How can STPA be applied to improve the standard DoD risk matrix for systems safety?

The authors explored two possible methodologies to apply STPA to improve the standard DoD risk matrix for systems safety. The scenario-based approach requires a complete STPA and classifies the causal scenarios as the risk factors to be eliminated or mitigated. The authors introduce the concept of *mitigation effectiveness* as a proxy for *likelihood* in the risk matrix. This concept built upon existing standard accepted practices such as the Safety Order of Precedence for mitigations and introduced the impacts of combined mitigations of different types (*design vs. detection vs. training/procedures*) into a Combined Mitigation Effectiveness Score (CMES). The authors also introduced how to assess Post-Potential Mitigation Severity (PPMS) and Combined Post-Mitigation Severity (CPMS) when more than one mitigation level was applied. Evaluating each individual risk using CMES/CPMS provided a granular perspective on risk with the emphasis on controlling risk rather arbitrarily estimating its likelihood. A blank SRM is shown below in Figure 6-1.

Sub-Hazard Risks					
Least [A]	0				
Somewhat [B]	1				
Moderate [C]	2-3				
Very [D]	4-5				
Most [E]	6				
Eliminated [F]	N/A				
CMES		1	2	3	4
	CPMS	Catastrophic	Critical	Marginal	Negligible

Figure 6-1: STPA-Informed Risk Matrix (SRM); MIL-STD-882E Compliant

The hazard-based approach was the second method developed to translate STPA into a risk matrix. This method uses causal scenarios to generate sub-hazards, which are considered the higher-level risks to be mitigated and plotted on an SRM. Each sub-hazard requires an associated sub-constraint (safety requirement) that helps guide the development of mitigations to eliminate/control the occurrence of hazardous system states. This approach uses the same scoring methods introduced with CMES/CPMS before plotting sub-hazards onto an SRM.

Both the scenario and hazard-based approaches highlight the best-case outcomes for mitigation effectiveness/severity assuming all sub-constraints/mitigations are addressed to their fullest extent. However, the option remains to assess worst-case outcomes in case program managers cannot implement every single mitigation due to resource limitations. The hazard-based approach provides a higher-level look at a system's risk that still uses the detailed context from causal scenarios to drive safety requirements and mitigation development.

Although both approaches were useful from different aspects, the authors believe the hazard-based approach represents the best method to inform a risk matrix using STPA. The benefit of the hazard-based approach for DoD system development is that it yields tangible safety and cybersecurity requirements. Many current DoD projects fail to address thorough safety and cybersecurity requirements and instead focus on other, more performance-centric

goals (e.g., speed, power, endurance, etc.). Risk managers would benefit from the application of this methodology as it focuses more on controlling risks as opposed to estimating risk. Additionally, all approaches developed by the authors enable the translation of mitigation effectiveness into likelihood as a superior way to quantify risk estimation.

The authors’ research focused on adapting STPA into the current DoD risk matrix. If unbounded by the confines of the risk matrix, STPA could be applied to help visualize risk in potentially more intuitive and interpretable ways. Section 6.3 on limitations and future work will introduce some of the authors’ preliminary ideas on risk visualization.

6.2 SRM in the Engineering V

With STPA complete and the risks assessed using one of the two discussed approaches, the next step (if developing a new system) is to apply the results to the design process. The goal is to refine designs and make them as safe as possible before committing substantial time and resources, where hasty efforts can result in costly re-work later in the process.

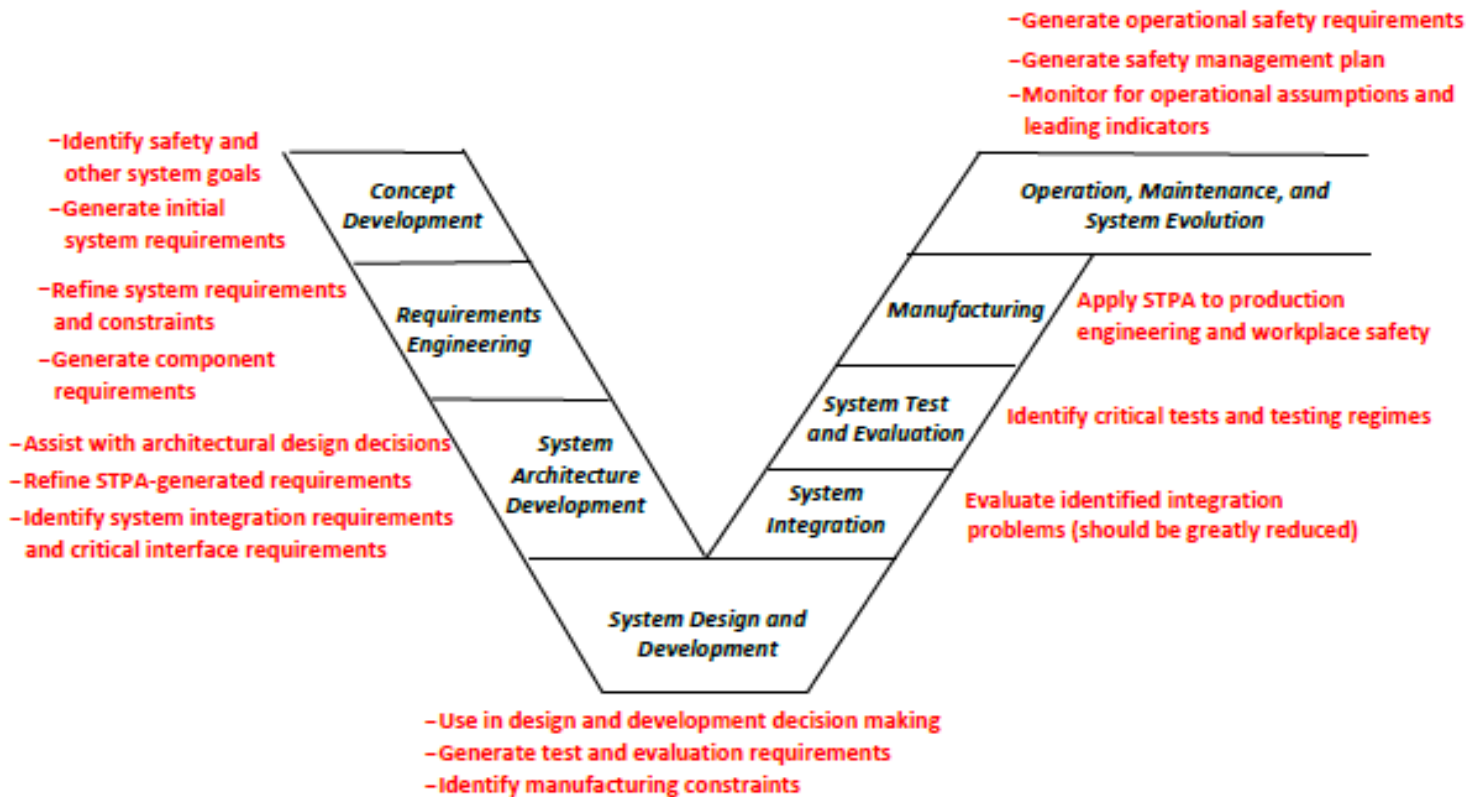


Figure 6-2: STPA in the Systems Engineering V

The STPA Handbook offers a blueprint for how the analysis can fit into the design process as shown above in Figure 6-2 [1, p. 54]. Ideally, STPA needs to be conducted at the beginning of the process to have the greatest impact on system architecture. The later that STPA is applied, the less proactive design changes can be made.

For the case of a FRWA, a high-level STPA will help inform which aspects of the architecture need to be refined based on their apparent contributions to loss as defined by the stakeholders. The authors' analysis highlighted different risk areas that can be mitigated before the preliminary and critical design reviews.

For a program that can cost billions of dollars in development, proper risk reduction is crucial in saving costs associated with late-stage design changes. Figure 6-3 below provides an example of how a few recommended mitigations would be applied to a high-level conceptual control structure for an FRWA. This diagram shows the changes that RMs can have on the control structure, providing a more insightful look at risk assessment from the perspective of the associated controls/feedback. The control structure can then be updated and another iteration of STPA can be conducted to determine the safety of the planned mitigations. The next iteration may prove that the RMs were safe and effective with the risks mitigated appropriately.

However, it is also possible that several new UCAs and causal scenarios may be discovered that require further mitigation to control risks introduced by a new recommended mitigation. The control structure will then go through further refinement until the program manager and safety engineers are satisfied with the system risk state and can progress to the next phase in design. The authors' proposed methods to assess risk complement STPA's iterative nature, allowing design decisions to be made early and often.

RM01

**New Feedback:
Operator
Monitoring/**

RM02

**New Control:
Remote Operation
While Manned**

RM03

**New Control:
Autonomous
Aircraft Control
Inputs**

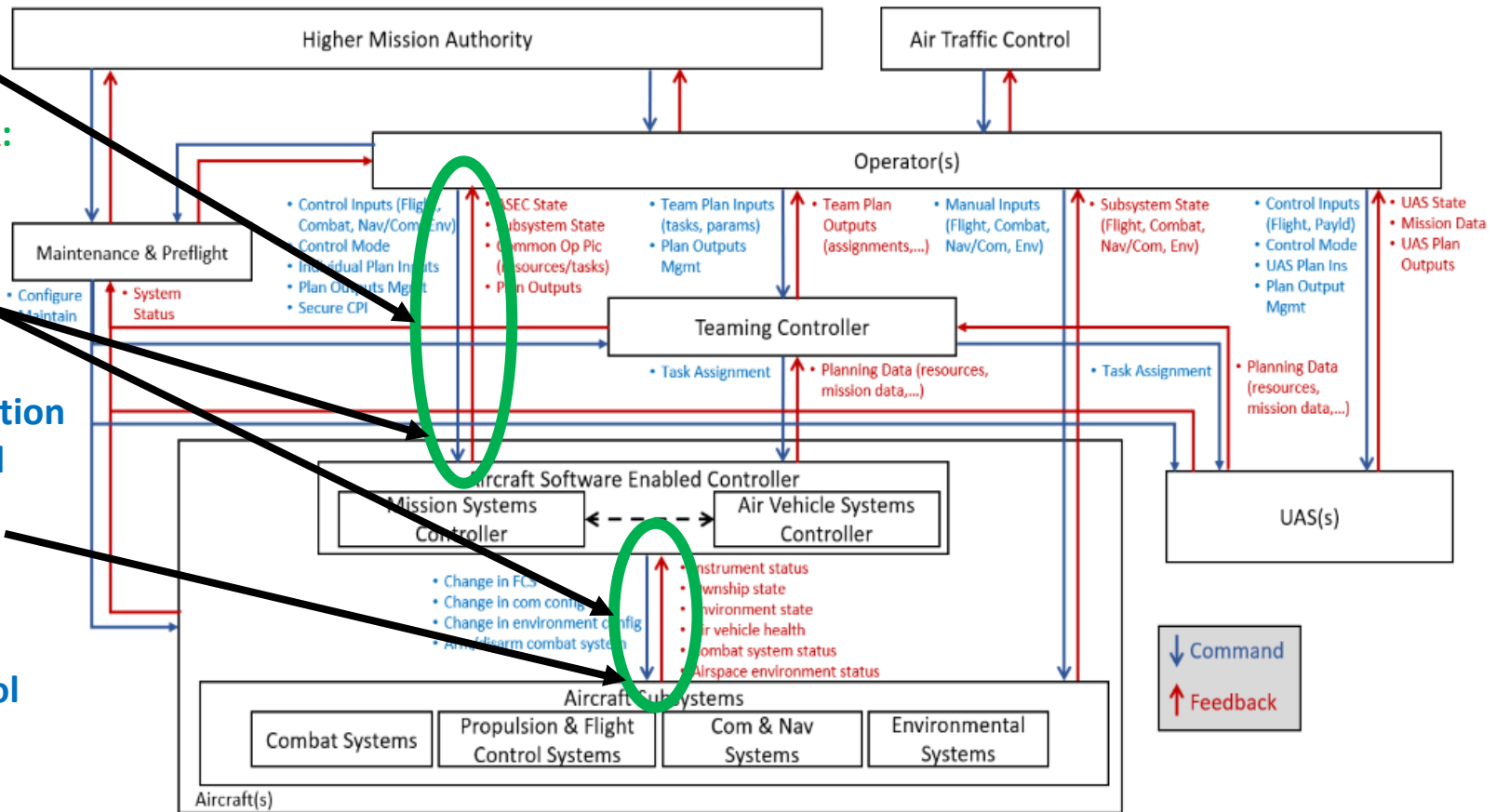


Figure 6-3: Mitigation Implementation for FRWA Control Structure

6.3 Limitations and Future Work

Some important limitations were introduced as the authors attempted to scope the boundaries of their research to the time and resources available. This section will review some of the major limitations of the research presented by the authors, along with various recommendations for areas of future work.

The authors chose to selectively consider system safety and cybersecurity risks above other types (e.g., organizational, privacy, supply chain, cost/schedule, etc.). While many other types of risks are involved within complex developmental systems, the authors framed many of their concepts, such as *mitigation effectiveness*, on addressing safety and cybersecurity. While the approaches developed by the authors will theoretically work on anything that STPA can be applied to, the methodologies are unproven on more abstract applications, such as focused efforts on organizational risk. Future research could be conducted to apply the authors' scenario or hazard-based approaches on systems that do not seek to manage risk for safety/cybersecurity as their primary objective.

Another area for future work would be to show how the SRM could evolve after multiple iterations of STPA on the same system. The authors' demonstration of their approaches was applied at a higher level of system abstraction that would certainly yield more specified requirements and recommendations if time were available to iterate the analysis. For instance, system sub-constraints and their associated recommended mitigations may yield more functional and directed layers of sub-constraints/recommendations. Cabosky shows in her recent thesis how iterating STPA uncovers different valuable recommendations as the analysis goes through subsequent levels of refinement [54]. In terms of risk mitigation and monitoring, iterative STPA would help demonstrate how recommended mitigations would alter the system's control structure to either eliminate or control risk from system design to operation.

Another limitation of the authors' work is that it was not possible to evaluate how well these risk analysis methods performed in comparison to other traditional hazard analysis techniques. While much research exists to support STPA as a more effective (if not equivalent) hazard analysis approach, the authors applied their research to a hypothetical FRWA that did not allow for a comparing and contrasting to another traditional, externally generated risk assessment. A valuable verification of the authors' work would be to apply either the scenario or hazard-based approach to a DoD program still in the developmental/prototype phase and compare the risk assessment from a safety/cybersecurity perspective to those conducted by both government and contractor entities.

To make the transition from the standard risk matrix to the new methodology as seamless as possible, it is important to create a new way to present information in an intuitive fashion without compromising its effectiveness. Because STPA inherently generates a list of control actions that can be sorted by risk score, these risks help formulate the new matrix. However, a table is not necessarily the most conducive way to present risk to a wider audience. Instead, the authors suggest a more visual presentation that is easily interpreted by those with less STPA and risk management experience.

Figure 6-4 below illustrates a possible way to convey the risk state for each control feedback loop on the control structure. This visualization allows for easy identification of risk areas and their relationships within the system. The controllers and loops can be color-coded to

represent risk states based on severity and mitigation effectiveness. Additionally, as new ideas are implemented, control structures can be placed in chronological order to catalog the historical design changes.

Another method is to show sub-hazard groupings as they relate to losses, as seen in Figure 6-5 below. The groupings can be useful for high-level planners to make initial risk assessments and decide where to focus resources early in the design process. One last concept would be to display all the elements of a complete STPA (losses, hazards, UCAs, and causal scenarios) as a node graph, as seen in Figure 6-6 below. This graph helps viewers conceptualize how each element affects and traces to one another. Color coding can also help identify which elements contribute most to the risk state of the system.

Because STPA focuses on control interactions, the level of complexity of the system will dictate the difficulty in representing the risk of various control actions. New risk visualization techniques may help managers and engineers understand what they need to focus on and how to allocate resources for their projects. Different techniques may be suited to depict different aspects of the analysis. The goal is to assist the decision making by project managers and by the system design teams.

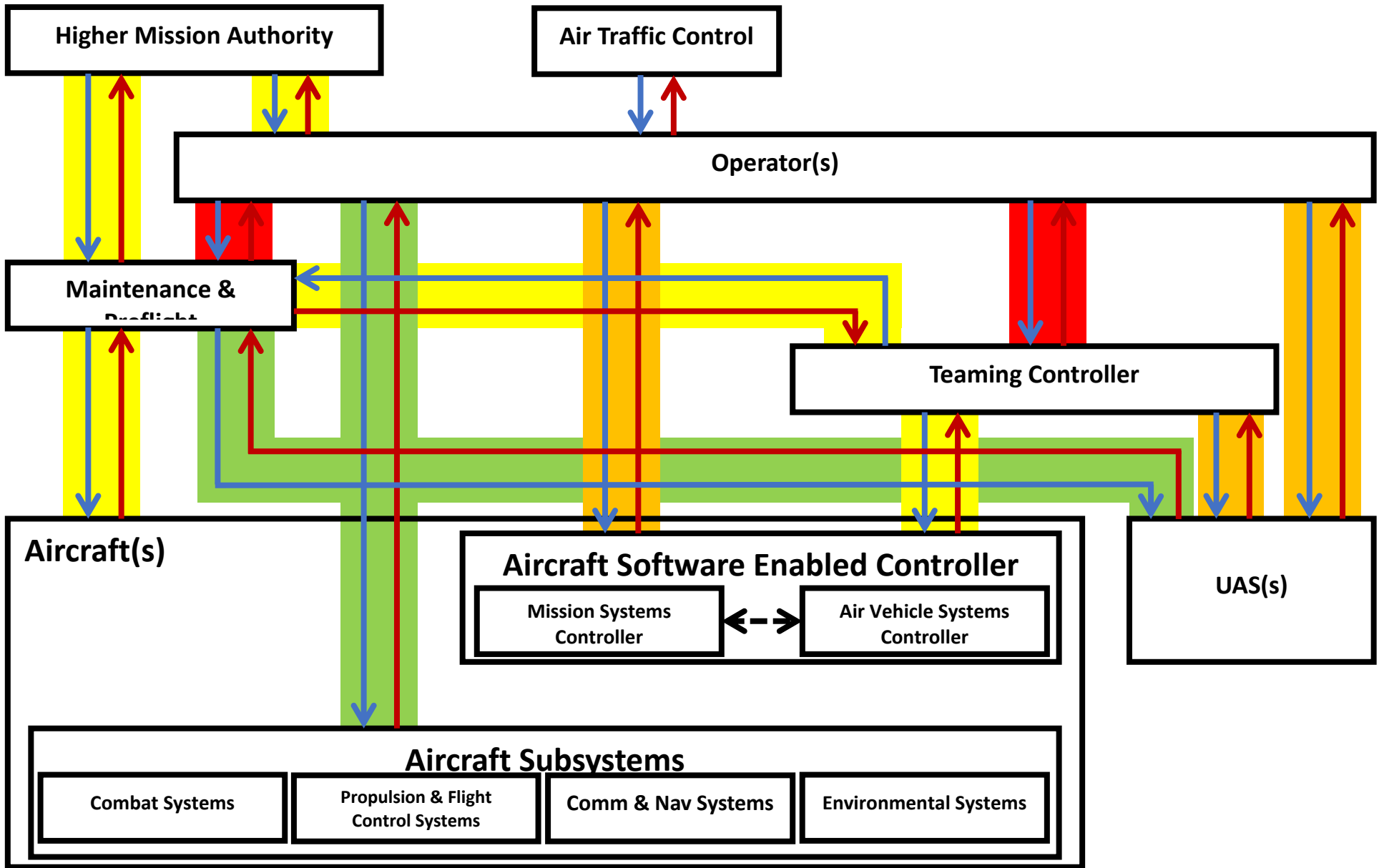


Figure 6-4: Control Structure Risk State

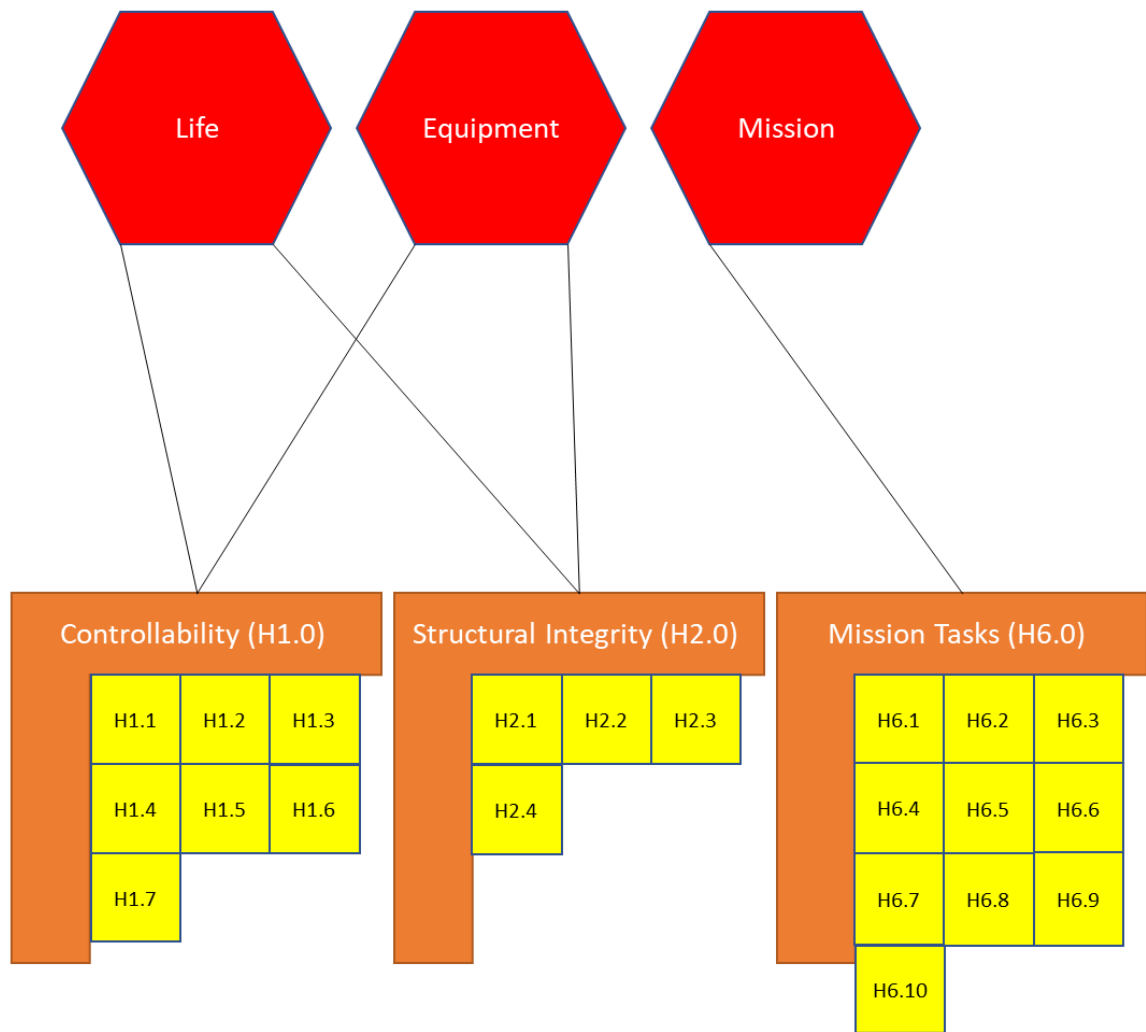
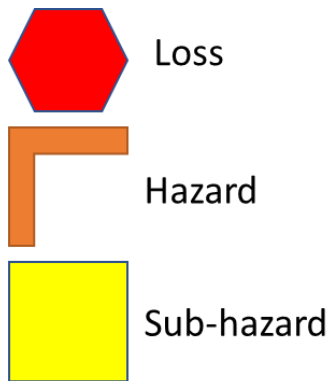


Figure 6-5: Sub-Hazard Groupings

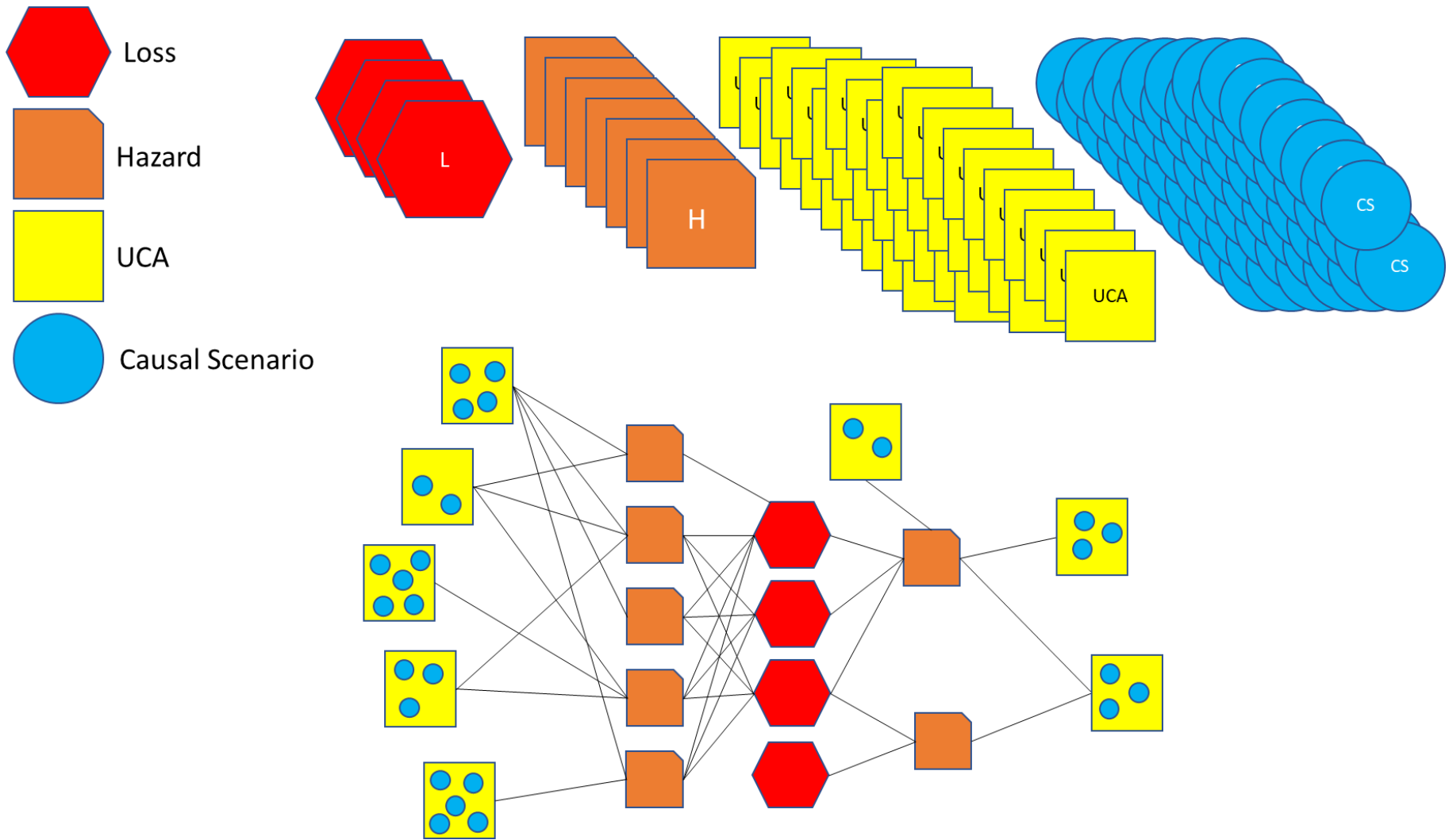


Figure 6-6: STPA Node Graph

6.4 Final Thoughts

The authors explored better ways to manage risk within the context of STPA by focusing on quantifying the results based on the notion that risk is intuitively a math problem. After months of research and many attempts to translate STPA into risk, the authors think they provided a meaningful step in the right direction that de-emphasizes reliability and focuses on mitigation effectiveness, or how well risks can be controlled. Hundreds of hours of interviews with key stakeholders revealed that current risk assessment processes were often ineffective and ill-informed, especially when estimating probability.

By bridging existing literature on the priority and types of mitigation techniques (e.g., System Safety Order of Precedence) and building upon ideas presented by safety experts, the authors introduced their idea of *combined mitigation effectiveness scores* (CMES). CMES helped assess how well risks were addressed by considering the combinatorial effects of different levels of risk mitigation, and their impact on overall *mitigation effectiveness*. Additionally, the authors provided a way to assess severity in the form of post-potential mitigation severity, which evaluates the best and worst-case outcomes depending on the applied mitigations. With both axes of the risk matrix informed by STPA, the risk assessment process now benefits from objective analysis of component interactions instead of subjectively determining how failure rates contribute to risk.

This thesis serves as a guide for further research into new risk analysis techniques. Leveraging the STPA methodology provided significant improvements to current risk evaluation practices, and the authors hope that others can improve upon these ideas to better represent system safety risk.

7 APPENDIX

This section contains the complete STPA results and the complete risk analyses explored in Chapter 5.

7.1 STPA Results

7.1.1 Loss Table

System Losses and Sub-Losses			
ID		Description	Severity
L1.0 - Human Loss	L1.1	Loss of life or permanent total disability	1
	L1.2	Permanent partial disability; injury that results in hospitalization	2
	L1.3	Injury resulting in lost work days	3
	L1.4	Injury not resulting in lost work days	4
L2.0 - Material Loss	L2.1	Loss or damage to aircraft or equipment (>\$1mil)	1
	L2.2	Major damage to aircraft/equipment (<\$1mil, >\$200k)	2
	L2.3	Serious damage to aircraft/equipment (<\$200k, >\$10k)	3
	L2.4	Minor damage to aircraft/equipment (<\$10k, >\$2k)	4
L3.0 - Mission Loss	L3.1	Loss of tactical mission that significantly affects strategic mission	1
	L3.2	Complete loss of tactical mission	2
	L3.3	Partial tactical mission loss	3
	L3.4	Minor tactical mission degradation	4
L4.0 - Critical Information Loss	L4.1	Loss of very important critical information	1
	L4.2	Loss of important critical information	2
	L4.3	Loss of somewhat important critical information	3
	L4.4	Loss of unimportant critical information	4

7.1.2 Hazard and Sub-Hazard Tables

System Hazards		
ID	Description	Loss Link
H1.0	Aircraft is Uncontrollable (manned/unmanned)	L1.0, L2.0, L3.0
H2.0	Structural Integrity of Aircraft is Violated	L1.0, L2.0, L3.0

H3.0	Minimum Aircraft Separation Standards are Violated	L1.0, L2.0, L3.0
H4.0	Aircraft Environment is Harmful to Human Performance	L1.0
H5.0	Aircraft Operations Cause Collateral Damage or Friendly Fire	L1.0, L2.0, L3.0
H6.0	Aircraft is Unable to Conduct Mission Tasks	L1.0, L2.0, L3.0
H7.0	Critical Information is Compromised	L3.0, L4.0

System Hazards and Sub-Hazards

ID		Description	Loss Link
H1.0 - Aircraft is Uncontrollable (Manned/ Unmanned)	H1.1	Operator is incapacitated during flight	L1.0, L2.0, L3.0
	H1.2	Control inputs are inadequate during unmanned flight	L1.0, L2.0, L3.0
	H1.3	Controller/hardware feedback is inadequate/incorrect to maintain controllability	L1.0, L2.0, L3.0
	H1.4	Component performance impacts controller functions	L1.0, L2.0, L3.0
	H1.5	Enemy action compromises controllability	L1.0, L2.0, L3.0
	H1.6	Operator task saturation/fixation/inattention	L1.0, L2.0, L3.0
	H1.7	Improper exchange of control authority	L1.0, L2.0, L3.0
	H1.8	Configuration is inappropriate for flight operations	L1.0, L2.0, L3.0
H2.0 - Structural Integrity of Aircraft is Violated	H2.1	Inadequate health data collection/reporting	L1.0, L2.0, L3.0
	H2.2	Inadequate control algorithms allow maneuvers to exceed structural limitations	L1.0, L2.0, L3.0
	H2.3	Operator task saturation/fixation/inattention	L1.0, L2.0, L3.0
	H2.4	Operator's mental model of control inputs is incorrect	L1.0, L2.0, L3.0
	H2.5	Enemy action compromises structural integrity	L1.0, L2.0, L3.0
	H2.6	Component performance impacts structural integrity	L1.0, L2.0, L3.0
H3.0 - Minimum Aircraft Separation Standards are Violated	H3.1	Operator task saturation/fixation/inattention	L1.0, L2.0, L3.0
	H3.2	Operators violate separation standards for intangible entities	L1.0, L2.0, L3.0
	H3.3	Operators violate separation standards for tangible entities	L1.0, L2.0, L3.0
	H3.4	Control algorithm for flight maneuvers violates separation standards during autonomous flight	L1.0, L2.0, L3.0
H4.0 - Aircraft Environment is Harmful to Human Performance	H4.1	Component performance impacts internal aircraft environment	L1.0
	H4.2	Mission flight profile impacts internal aircraft environment	L1.0
	H4.3	Aircraft ergonomics have negative effects on operator health	L1.0
	H4.4	Aircraft environment is susceptible to enemy action	L1.0
	H4.5	Feedback to environmental controllers is incorrect/inadequate	L1.0
H5.0 - Aircraft Operations Cause Collateral Damage or Friendly Fire	H5.1	Operators cause collateral damage/friendly fire due to incorrect/inadequate feedback	L1.0, L2.0, L3.0
	H5.2	Friendly assets/non-combatants are within mission system envelopes during system engagement	L1.0, L2.0, L3.0
	H5.3	Inadvertent operation of mission systems	L1.0, L2.0, L3.0
H6.0 - Aircraft is Unable to Conduct Mission Tasks	H6.1	Mission system configuration is inappropriate for mission requirements	L1.0, L2.0, L3.0
	H6.2	Miscommunication between controllers during mission	L1.0, L2.0, L3.0
	H6.3	Insufficient clearance to conduct mission	L1.0, L2.0, L3.0

	H6.4	Enemy action interferes with mission tasks	L1.0, L2.0, L3.0	
	H6.5	Operator's mental model of mission tasks is incorrect	L1.0, L2.0, L3.0	
	H6.6	Inadvertent operation of mission systems	L1.0, L2.0, L3.0	
	H6.7	Improper exchange of control authority	L1.0, L2.0, L3.0	
	H6.8	Operators cannot conduct mission tasks due to incorrect/inadequate feedback	L1.0, L2.0, L3.0	
	H6.9	Environmental factors reduce mission system performance	L1.0, L2.0, L3.0	
	H6.10	Mis-prioritization of mission tasks	L1.0, L2.0, L3.0	
	H6.11	Component performance impacts controller functions	L1.0, L2.0, L3.0	
	H6.12	Operator task saturation/fixation/inattention	L1.0, L2.0, L3.0	
	H7.0 - Critical Information is Compromised	H7.1	Critical information-related equipment is insufficient at securing critical information	L3.0, L4.0
		H7.2	Critical information is unable to be secured by Operator	L3.0, L4.0
		H7.3	Communication is not encrypted sufficiently to protect critical information	L3.0, L4.0
H7.4		Reception of critical information control signals is insufficient when handling critical information	L3.0, L4.0	
H7.5		Critical information is not protected against enemy action	L3.0, L4.0	
H7.6		Critical information is inadvertently compromised	L3.0, L4.0	

7.1.3 Constraint and Sub-Constraint Tables

System Constraints		
ID	Description	Hazard Link
C1.0	Aircraft Must Remain Controllable During Manned/Unmanned Operations	H1.0
C2.0	Aircraft Structural Integrity Must Be Maintained	H2.0
C3.0	Aircraft Must Satisfy Minimum Separation Standards from Moving or Fixed Objects	H3.0
C4.0	Aircraft Environment Must Be Suitable for Mission Performance	H4.0
C5.0	Collateral Damage/Friendly Fire Must Be Prevented	H5.0
C6.0	Aircraft Must Be Able to Perform Combat Mission Tasks	H6.0
C7.0	Critical Information Must Be Protected	H7.0

System Constraints and Sub-Constraints			
ID	Description		Hazard Link
Aircraft Must Remain Controllable During	C1.1	Control inputs must be adequate to maintain aircraft controllability for manned flight	H1.1
	C1.2	Control inputs must be adequate to maintain aircraft controllability for unmanned flight	H1.2
	C1.3	Controller/hardware feedback must be adequate to maintain controllability	H1.3

Manned/Unmanned Operations	C1.4	Aircraft control architecture must not be susceptible to enemy action	H1.4
	C1.5	Control authority for flight systems must be properly exchanged	H1.5
	C1.6	Configuration must be appropriate for flight operations	H1.6
	C1.7	Aircraft safety measures must not affect controllability during flight operations	H1.7
C2.0 - Aircraft Structural Integrity Must Be Maintained	C2.1	Maintenance procedures/health data collection must be adequate to maintain structural integrity	H2.1
	C2.2	Control algorithms must prevent maneuvers from exceeding structural limitations	H2.2
	C2.3	Controller/hardware feedback must be adequate to maintain structural integrity	H2.3
	C2.4	Aircraft structural design must not be susceptible to enemy action	H2.4
C3.0 - Aircraft Must Satisfy Minimum Separation Standards from Moving or Fixed Objects	C3.1	Control inputs must be adequate to maintain separation standards for manned flight	H3.1
	C3.2	Aircraft must satisfy separation standards for intangible entities	H3.2
	C3.3	Aircraft must satisfy separation standards for tangible entities	H3.3
	C3.4	Control algorithm for flight maneuvers must maintain separation standards during autonomous flight	H3.4
C4.0 - Aircraft Environment Must Be Suitable for Mission Performance	C4.1	Component performance must maintain safe aircraft environment	H4.1
	C4.2	Aircraft must be properly configured for assigned mission flight profiles	H4.2
	C4.3	Aircraft ergonomics must be sufficient for FO health/performance	H4.3
	C4.4	Aircraft environment must not be susceptible to enemy action	H4.4
	C4.5	Environmental controller feedback must be sufficient for Operator performance	H4.5
C5.0 - Collateral Damage/Friendly Fire Must Be Prevented	C5.1	Mission system operation must be sufficient in preventing collateral damage/friendly fire	H5.1
	C5.2	Friendly assets/non-combatants must remain outside mission system envelopes during system engagement	H5.2
	C5.3	Mission systems must not be unintentionally operated	H5.3
C6.0 - Aircraft Must Be Able to Perform Combat Mission Tasks	C6.1	Mission system configuration must be appropriate for mission requirements	H6.1
	C6.2	Communication between controllers must be sufficient for mission task requirements	H6.2
	C6.3	Clearance must be sufficient to conduct mission	H6.3
	C6.4	Mission tasks must not be affected by enemy action	H6.4
	C6.5	Mission systems must not be inadvertently operated	H6.5
	C6.6	Control authority for mission systems must be properly exchanged	H6.6
	C6.7	Mission system feedback must be sufficient during flight	H6.7
	C6.8	Environmental factors must not reduce mission system performance	H6.8
	C6.9	Mission tasks must be prioritized by controllers	H6.9
	C6.10	Component performance must not impact mission system controller functions	H6.10
C7.0 - Critical Information Must Be Protected	C7.1	Critical information-related equipment must be able to secure critical information	H7.1
	C7.2	System must be able to secure critical information when FO is unable	H7.2
	C7.3	Communications/signals must be sufficiently encrypted to protect critical information	H7.3
	C7.4	Control signal reception must be sufficient when handling critical information	H7.4
	C7.5	Critical information must be protected against enemy action	H7.5
	C7.6	Critical information must not be inadvertently compromised	H7.6

7.1.4 Responsibilities Table

System Responsibilities		
Responsibility ID	Responsibility Description	
R1.0 – Higher Mission Authority	R1.1	Defines or convey the rules of engagement before a mission
	R1.2	Defines mission parameters such as objectives, configurations, and priorities
	R1.3	Provides mission execution updates and approvals to FRWA during the mission
R2.0 – Air Traffic Control (ATC)	R2.1	Controls aircraft flight paths within an airspace structure
R3.0 – Aircraft Operator	R3.1	Controls aircraft
	R3.2	Performs attack when commanded
	R3.3	Performs reconnaissance when commanded
	R3.4	Performs self-defense when necessary
	R3.5	Executes commands sent by HMA
	R3.6	Protects mission-critical information
R4.0 – Maintenance and Pre-Flight	R4.1	Configures the Aircraft Software Enabled Controller for the mission (ex: program mission parameters, update MOSA firmware)
	R4.2	Configures Aircraft Subsystems for the mission
	R4.3	Conducts the FRWA preflight before takeoff
	R4.4	Maintains the FRWA
	R4.5	Secures critical FRWA data
R5.0 – Advanced Teaming Control	R5.1	Aggregates shared combat data to determine up-to-date status of available FRWA resources and mission tasks
	R5.2	Generates an optimized task allocation of the FRWA resources to accomplish mission tasks subject to defined parameters
R6.0 – Aircraft Software-Enabled Controller (ASEC)	R6.1	Integrates Operator commands to control aircraft subsystems
	R6.2	Provides assisted decision making to the Operator
	R6.3	Ensures system health
	R6.4	Ensures system security
	R6.5	Changes aircraft environment
	R6.6	Enforces limitations of Operator commands
R7.0 – Aircraft Subsystems	R7.1	Executes Operator and ASEC provided commands
	R7.2	Enforces limitations of Operator override commands
	R7.3	Protects mission-critical systems

7.1.5 Unsafe Control Actions Table

Control Action	UCA ID	Not providing the control action causes hazard	Hazard Link	UCA ID	Providing the control action causes hazard	Hazard Link
	1.0	HMA does not provide mission authorization to FO when aircraft is inside valid engagement zone	H5.0, H6.0	1.1	HMA provides mission authorization to FO when aircraft is inside valid engagement zone	H5.0

HMA sends mission-related commands and grants authorizations to FO	UCA ID	Providing a control action too early, too late, or out of order causes hazard	Hazard Link	UCA ID	Providing a control action for too long or short a time causes hazard	Hazard Link
	1.3	HMA provides mission authorization to FO before receiving latest battlespace intelligence information	H5.0, H6.0			
	1.4	HMA provides mission authorization to FO too late and aircraft leaves valid engagement zone	H5.0, H6.0			
Control Action	UCA ID	Not providing the control action causes hazard	Hazard Link	UCA ID	Providing the control action causes hazard	Hazard Link
FO manipulates flight controls (any input related to maintaining safety of flight)	2.0	FO does not make aircraft control inputs during manned aircraft operation during critical phases of flight	H1.0, H2.0, H3.0, H6.0	2.3	FO makes aircraft control inputs when aircraft is in autonomous operation	H1.0, H2.0, H3.0, H6.0
	2.1	FO does not make aircraft control inputs when aircraft is disengaged from autonomous mode	H1.0, H2.0, H3.0, H6.0	2.4	FO makes improper aircraft control inputs during critical phases of flight	H1.0, H2.0, H3.0
	2.2	FO cannot make aircraft control inputs during an emergency while the aircraft is in autonomous mode	H1.0, H2.0, H3.0, H6.0			
	UCA ID	Providing a control action too early, too late, or out of order causes hazard	Hazard Link	UCA ID	Providing a control action for too long or short a time causes hazard	Hazard Link
	2.5	FO makes aircraft control inputs too early prior during critical phases of flight	H1.0, H2.0, H3.0, H6.0	2.8	FO maintains aircraft control inputs for too long during critical phases of flight	H1.0, H2.0, H3.0, H6.0
	2.6	FO makes aircraft control inputs too early before autonomous mode is disengaged	H1.0, H2.0, H3.0, H6.0	2.9	FO maintains aircraft control inputs for too short a time during critical phases of flight	H1.0, H2.0, H3.0, H6.0
	2.7	FO makes aircraft control inputs too late during critical phases of flight	H1.0, H2.0, H3.0, H6.0			H1.0, H2.0, H3.0, H6.0
Control Action	UCA ID	Not providing the control action causes hazard	Hazard Link	UCA ID	Providing the control action causes hazard	Hazard Link
FO performs data management (all tasks associated with managing flight that are not mission-specific; e.g. fuel management, weather checks, navigation, radio communication)	3.0	FO does not perform data management when entering a new airspace	H3.0, H5.0, H6.0, H7.0	3.1	FO performs data management during critical phases of flight	H1.0, H2.0, H3.0, H6.0
				3.2	FO performs data management during critical phases of mission	H5.0, H6.0, H7.0
	UCA ID	Providing a control action too early, too late, or out of order causes hazard	Hazard Link	UCA ID	Providing a control action for too long or short a time causes hazard	Hazard Link
	3.3	FO performs data management too late after entering a new airspace	H3.0, H5.0, H6.0, H7.0	3.5	FO performs data management for too long during critical phases of mission	H5.0, H6.0, H7.0
	3.4	FO performs data management too early before entering a new airspace	H3.0, H5.0, H6.0, H7.0			
Control Action	UCA ID	Not providing the control action causes hazard	Hazard Link	UCA ID	Providing the control action causes hazard	Hazard Link
FO engages attack systems	4.0	FO does not engage attack-related systems when inside a valid engagement zone	H6.0	4.1	FO engages attack-related systems unintentionally outside of valid engagement zone	H5.0, H6.0
	UCA ID	Providing a control action too early, too late, or out of order causes hazard	Hazard Link	UCA ID	Providing a control action for too long or short a time causes hazard	Hazard Link
	4.2	FO engages attack-related systems too late after entering a valid engagement zone	H5.0, H6.0	4.5	FO leaves attack-related systems engaged for too long while inside valid engagement zone	H5.0, H6.0
	4.3	FO engages attack-related systems before entering a valid engagement zone	H5.0, H6.0	4.6	FO inside valid engagement zone for too short of a time while conducting attack	H5.0, H6.0

	4.4	FO engages attack related systems out of sequence inside a engagement zone	H5.0, H6.0			
Control Action	UCA ID	Not providing the control action causes hazard	Hazard Link	UCA ID	Providing the control action causes hazard	Hazard Link
FO engages reconnaissance systems	5.0	FO does not engage aircraft reconnaissance systems after entering mission area	H6.0	5.1	FO engages aircraft reconnaissance systems inside mission area when hostile electronic warfare systems are active	H06
				5.2	FO engages reconnaissance systems while engaging attack and/or self-defense systems within mission area	H06
	UCA ID	Providing a control action too early, too late, or out of order causes hazard	Hazard Link	UCA ID	Providing a control action for too long or short a time causes hazard	Hazard Link
	5.3	FO engages aircraft reconnaissance systems too late when entering a mission area	H6.0	5.5	FO leaves aircraft reconnaissance systems engaged for too long after exiting a mission area	H6.0
	5.4	FO engages aircraft reconnaissance systems too early before entering a mission area	H3.0, H4.0, H5.0, H6.0	5.6	FO disengages aircraft reconnaissance systems before necessary when inside a mission area	H6.0
Control Action	UCA ID	Not providing the control action causes hazard	Hazard Link	UCA ID	Providing the control action causes hazard	Hazard Link
FO engages threat countermeasure systems (TCMs)	6.0	FO does not engage threat countermeasure systems before entering hostile territory	H6.0	6.1	FO engages threat countermeasure systems unintentionally before entering hostile territory	H5.0, H6.0
				6.2	FO engages threat countermeasure systems but aircraft does not to respond/receive inputs after entering hostile territory	H6.0
	UCA ID	Providing a control action too early, too late, or out of order causes hazard	Hazard Link	UCA ID	Providing a control action for too long or short a time causes hazard	Hazard Link
	6.3	FO engages threat countermeasure systems too late when within hostile territory	H6.0	6.4	FO leaves threat countermeasure systems engaged for too long after exiting hostile territory	H5.0, H6.0
				6.5	FO disengages threat countermeasure systems before exiting hostile territory	H6.0
Control Action	UCA ID	Not providing the control action causes hazard	Hazard Link	UCA ID	Providing the control action causes hazard	Hazard Link
FO executes secure critical information procedures	7.0	FO does not execute secure procedure of critical information within the aircraft when aircraft is operating in mission area	H6.0, H7.0	7.1	FO executes secure procedure of critical information during critical phases of mission, but procedures are ineffective	H6.0, H7.0
	UCA ID	Providing a control action too early, too late, or out of order causes hazard	Hazard Link	UCA ID	Providing a control action for too long or short a time causes hazard	Hazard Link
	7.2	FO executes secure critical information procedure too late before operating in mission area	H6.0, H7.0	7.3	FO executes secure critical information procedure but is stopped too soon before operating in mission area	H6.0, H7.0
Control Action	UCA ID	Not providing the control action causes hazard	Hazard Link	UCA ID	Providing the control action causes hazard	Hazard Link
FO verifies preflight checks are complete and configuration is appropriate for mission	8.0	FO does not verify preflight checks and configuration before operating the aircraft	H1.0, H2.0, H4.0, H6.0	8.1	FO verifies preflight checks and configuration incorrectly before operating aircraft	H1.0, H2.0, H4.0, H6.0
	UCA ID	Providing a control action too early, too late, or out of order causes hazard	Hazard Link	UCA ID	Providing a control action for too long or short a time causes hazard	Hazard Link

8.2	FO verifies preflight checks and configuration before aircraft is ready for operation	H1.0, H2.0, H4.0, H6.0	8.4	FO takes too long to verify preflight checks and configuration before the mission	H1.0, H2.0, H4.0, H6.0
8.3	FO verifies preflight checks and configuration too late before mission	H1.0, H2.0, H4.0, H6.0			

7.1.6 Causal Scenarios Table

CS ID	Causal Scenario	PMS
CS 2.0.1	FO is incapacitated by enemy fire, injury, illness and leans onto the controls accidentally activating them. As a result, aircraft can become uncontrollable.	1
CS 2.0.2	FO mental model of aircraft flight control systems conflicts with reality and FO does not make the necessary manual inputs during a critical mode of flight. As a result, the aircraft becomes uncontrollable. (e.g. executing an emergency procedure incorrectly because the FO does not understand the relationships between subsystems)	1
CS 2.0.3	FO receives poor or inadequate feedback from flight controls and does not make necessary control inputs during a critical mode of flight. As a result, the aircraft becomes uncontrollable. (e.g. FO does not get a FIRE light in the event of an engine fire and does not execute the proper emergency procedures)	1
CS 2.0.4	FO becomes saturated with mission tasks and does not respond to aircraft alerts, as a result the aircraft violates minimum separation standards during formation flight (e.g. FO is performing mission tasks and does not realize aircraft is drifting too close to other aircraft within formation and collides with friendly aircraft)	1
CS 2.0.5	FO commands a flight control input, but it is not received because of faulty wiring/hardware malfunction in the fly-by-wire system. As a result, the aircraft becomes uncontrollable. (e.g. FO tries to correct trim of aircraft but tail rotor control does not receive signal)	1
CS 2.1.1	FO cannot make aircraft control inputs when the aircraft is disengaged from autonomous mode due to enemy spoofing the autonomous control signal during the transition to manual control. As a result, the aircraft becomes uncontrollable.	1
CS 2.2.1	Safety interlocks malfunction and disconnect the FO's physical inputs to the fly-by-wire system. The aircraft is in autonomous mode and does not allow the FO the make necessary aircraft control inputs during an in-flight emergency. As a result the aircraft becomes uncontrollable.	1
CS 2.3.1	FO is spatially disoriented and inaccurately believes that the aircraft autonomous mode is malfunctioning. FO makes a flight control input which results into violation of minimum separation standards.	1
CS 2.4.1	FO remotely sends control signal to aircraft, but it is block/jammed and not received. Remote FO was commanding an aggressive maneuver of the airframe when enemy jamming blocks the remote signal from stopping the aircrafts last maneuver command. As a result, aircraft structural integrity is violated.	1
CS 2.4.2	FO executes a faulty mental model of a flight procedure and does not control the aircraft properly during an emergency, resulting in a loss of main engine power. As a result, structural integrity of the aircraft is violated. (e.g. pilot does not execute a recovery maneuver properly and crashes the aircraft)	1
CS 2.5.1	FO does not recall the flight parameters for working operation of flight systems and makes certain flight inputs too early. As a result, the aircraft becomes uncontrollable. (e.g. FO attempt to engage autopilot function too soon before establishing the correct flight profile [speed/attitude])	1
CS 2.5.2	FO initiates a flight maneuver too early based on a signal/indication relayed from the ASEC. As a result, the structural integrity is violated. [e.g. VSI/radar altimeter indications inform FO that aircraft is descending more rapidly than reality during DVE, FO overtorques aircraft in response]	1
CS 2.5.3	FO commands ASEC to perform an autonomous flight procedure and the command is not received or executed fully by the ASEC, as a result the FO conducts the procedure too soon. As a result, aircraft structural integrity is violated. (e.g. automated landing mode engaged, landing gear are not fully extended and aircraft is not ready to land but FO lands without gears extended)	1
CS 2.6.1	FO does not receive feedback that the autonomous mode is fully disengaged because the alert he received was dismissed earlier on in the flight and the FO forgets that partial autonomy is still active. The FO then initiates a high/low power maneuver with flight controls, which results in unexpected control inputs as they conflict with the partial autonomy. As a result, the aircraft becomes uncontrollable.	1
CS 2.7.1	FO becomes fixated on a mission task and enters a delayed aircraft control input. As a result, the structural integrity of the aircraft is violated. (e.g. FO commands a high-power maneuver while task saturated and delays finishing the maneuver)	1
CS 2.7.2	FO relegates autonomous control of FRWA to another FO, who does not fully absorb necessary information from the transition and enters a delayed aircraft command. As a result, the aircraft becomes uncontrollable (e.g. FRWA is fuel low, but new FO delays sending refuel signal to aircraft and aircraft is forced to land in hostile territory)	1

CS 2.7.3	FRWA delays transmitting a feedback signal to the FO through ASEC, the FO is unable to react in the proper amount of time. As a result, the aircraft becomes uncontrollable	1
CS 2.7.4	FO has a set amount of time to respond to an aircraft emergency but is delayed in the aircraft control input. As a result, the structural integrity of the aircraft is violated. (e.g. engine experiences a fire, FO does not deploy firefighting system in time and smoke fills the cockpit).	1
CS 2.8.1	FO loses situational awareness/task saturated and makes an input for too long. As a result, structural integrity of the aircraft is violated. (e.g. during instrument takeoff, pilot continues climb because they become disoriented from lack of visual references).	1
CS 2.8.2	FO does not properly understand aircraft systems and their associated checklist commands. Flight training did not adequately prepare the FO with environmental structural/limitations of the aircraft and the FO holds inputs (collective – power demand) for too long. As a result, the aircraft becomes uncontrollable. (e.g. FO demands too much power from the system to climb a terrain feature under hot weather and overtorques the aircraft)	1
CS 2.8.3	FO maintains a control input for too long because ASEC provides a delayed indication. As a result, the aircraft violates minimum separation standards. (e.g. vertical speed indicator lags, therefore the pilot holds a climb for too long violating minimum separation standards)	1
CS 2.8.4	FO holds an input for too long because the ASEC does not provide feedback that the input was received. As a result, the aircraft becomes uncontrollable. (e.g. fly-by-wire connections between PVI and HW fail, so the pilot continues to hold a climb with no effect)	1
CS 2.9.1	FO loses situational awareness/task saturated and makes an input for too short. As a result, the aircraft becomes uncontrollable. (e.g. pilot becomes distracted by mission management and stop providing flight control inputs)	1
CS 2.9.2	FO does not understand aircraft systems/checklists, holding inputs for too short. As a result, the aircraft becomes uncontrollable. (e.g. FO holds incorrect nose attitude during landing and has a hard landing)	1
CS 2.9.3	FO maintains a control input for too short a time because ASEC provides an incorrect indication. The ASEC does not process the aircraft's health monitoring sensor feedback in time when the FO was conducting a combat maneuver due to a hard reset of the primary flight computer. As a result, structural integrity is violated.	1
CS 3.0.1	FO does not recognize when he has entered new enemy-controlled airspace because he is relying on outdated airspace information and does not communicate his identity through proper transponder signal or other communications. The FO does not have the latest friendly intelligence that established the current operating airspace as hostile with a 'no-fly designation' due to enemy jamming of FRWA's over-the-horizon communication capability. As a result, minimum separation standards are violated.	1
CS 3.0.2	FO does not perform data management tasks when entering a new airspace. This could occur if an updated configuration renders the data management TTPs that the FO is accustomed to incompatible for proper operation of the system. As a result, minimum separation standards are violated.	2
CS 3.1.1	FO receives a system alert that draws his attention to perform a data management task during formation flight under manual control. As a result, the aircraft violates minimum separation standards.	1
CS 3.2.1	ASEC receives conflicting information inputs from multiple FOs due to misidentification of tracks and is unable to discern the status of a contact detected by the reconnaissance systems. As a result, the aircraft is unable to perform mission tasks. (e.g. one FO identifies a track as hostile, while another identifies it as neutral/friendly)	1
CS 3.3.1	FO uploads flight way points too late into the mission execution because he does not believe that they are outdated (however mission dynamics have changed). As a result, the aircraft violates minimum separation standards. (e.g. remote pilot is too slow to update automated flight plan after recognizing his mission data is outdated, aircraft enters enemy airspace)	1
CS 3.4.1	FO updates transponder code and radio frequency too early before entering a new airspace because he wants to complete the data management tasks in advance and is engaged by friendly forces that have recently entered the AO that believe no friendly aircraft are operating in the area. As a result, the aircraft violates minimum separation standards.	1
CS 3.5.1	FO performs data management for too long because the ASEC is not relaying the appropriate status feedback, which draws the FO's attention away from manual flight control too long and the aircraft enters an unusual attitude. As a result, the aircraft is uncontrollable. [e.g. FO attempts to update his flight plan but the system does not adequately inform the pilot of the status and is distracted from flying the aircraft]	1
CS 4.0.1	FO does not receive adequate feedback from the targeting system because not enough of the on-board sensors can provide target information. The FO does not have any other sensors outside of the FRWA that he can rely on as the sole operational asset with the target identification capabilities in the area and does not engage the attack systems. As a result, the aircraft is unable to conduct mission tasks.	2
CS 4.0.2	FO does not attack target because the FO is unaware of engaged system safety interlocks preventing the arming of onboard weaponry. Safety of flight system (e.g. weight-on-wheel switch) prevents arming of weapons, thus preventing FO from engaging attack systems. As a result, the aircraft is unable to conduct mission tasks.	2

CS 4.0.3	Attack system believes aircraft is within Engagement Zone (EZ), but FO knows this to be false because of environmental conditions outside the aircraft he is observing that the ASEC is not aware of, so the FO does not release the weapon. [e.g. FO observes that his wingman is inside the weapon danger zone but the system shows the aircraft inside a safe area, so the FO chooses not to fire]. As a result, the aircraft is unable to conduct mission tasks.	3
CS 4.0.4	FO does not attack target because he believes another asset is conducting the attack based on a radio miscommunication. Inadequate teaming/ communication causes confusion in attack orders and priority and the acquired target may not be engaged when necessary. As a result, the aircraft is unable to conduct mission tasks.	2
CS 4.1.1	FO engages attack system despite inadequate feedback from data management systems within FRWA because friendly intelligence assets inform the FO that the area is clear to engage. As a result this leads to an unsafe attack and aircraft operations cause collateral damage or friendly fire.	1
CS 4.1.2	FO leaves weapon system armed after an attack because they intend to conduct an attack shortly on a new passing run, but never engages the intended target and forgets to disarm the system leading to a negligent discharge later in the flight while FO engages attack control. This results in an attack an EZ. As a result, aircraft operations cause collateral damage or friendly fire.	1
CS 4.2.1	FO performs attack late due to coordination issues with remote designator. FO is ready to perform attack, but remote designator loses communication due to jamming and cannot reliably designate target at moment of attack. FO needs to reposition/reconduct attack procedures. As a result, the aircraft is unable to conduct mission tasks.	2
CS 4.3.1	FO begins attack prior to entering valid Engagement Zone (EZ) because he believes the target is inside the correct EZ based on incorrect sensor feedback received from a ground force operator. As a result, aircraft operations cause collateral damage or friendly fire.	1
CS 4.4.1	FO does not perform attack procedure correctly because of an incorrect mental model [e.g. they skipped steps in a checklist based on use of an outdated checklist because they did not have the latest version prior to flight], resulting in ineffective targeting acquisition and/or unintended weapons release. As a result, the aircraft is unable to conduct mission tasks.	2
CS 4.5.1	FO cannot perform attack because armed weapons lose effectiveness. The attack systems are armed for too long during the mission because the FO loses awareness that they were engaged far earlier in the flight, which leads to battery drain/gimbal misalignment, preventing an effective attack at a later time. As a result, the aircraft is unable to conduct mission tasks.,	3
CS 4.6.1	FO disengages attack system before conducting attack. FO disarms targeting system because of exchange of FO targeting responsibility to another target controller and does not re-engage the on-board targeting system before conducting follow-on attack. As a result, the aircraft is unable to conduct mission tasks.	3
CS 4.6.2	FO does not receive adequate feedback from attack and reconnoiter systems that a target has been eliminated because of system limitations [e.g. beyond line of sight] and disengages attack system prior to target being completely destroyed. The FO believes the target was destroyed based on ordinance used for target and subsequently disengages the attack systems. When target resurfaces from sensor data, the FO is not able to attack quickly enough due to disarmament of the attack systems earlier. As a result, the aircraft is unable to conduct mission tasks.	3
CS 5.0.1	FO does not receive feedback from ATC with regard to location of mission area because ATC does not have the latest intelligence and does not engage reconnaissance systems, resulting in a loss of target identification. As a result, the aircraft is unable to conduct mission tasks.	1
CS 5.0.2	FO is in vicinity of equipment within mission area that generates electromagnetic interference (EMI) and does not engage reconnaissance systems because he knows they may not function properly near EMI sources. As a result, the aircraft is unable to conduct mission tasks.	1
CS 5.1.1	FO engages reconnaissance systems inside mission area but systems are jammed/spoofed by enemy EW assets, which prevents them from functioning properly. As a result, the aircraft is unable to conduct mission tasks.	1
CS 5.2.1	FO engages reconnaissance systems to maintain battlespace situational awareness while simultaneous conducting an attack or performing self-defense, causing the ASEC to misprioritize command signals. This can degrade specific mission system performance if the ASEC is unable to filter through the commands quickly enough, which may result in a loss of mission for one or both tasks.	2
CS 5.3.1	FO engages reconnaissance systems while entering mission area, but the ASEC is slow to initialize the systems. e.g. the cooldown period for FLIR, warm up for radar, time syncing required to enter battlespace management networks, etc. As a result, the aircraft is unable to conduct mission tasks.	2
CS 5.4.1	FO engages reconnaissance systems accidentally while on ground in a friendly area due to inadvertent activation and causes radiation harm to nearby personnel or equipment. As a result, aircraft operations cause collateral damage or friendly fire.	3
CS 5.5.1	FO leaves reconnaissance systems engaged after exiting mission area because he still believes he is operating within the mission airspace, which enables the enemy to track location of aircraft through broadcasted signals from aircraft. As a result, the minimum aircraft separation standards are violated.	2
CS 5.6.1	FO believes they are outside a mission area due to conflicting feedback from ATC and disengages reconnaissance systems too soon, leading to missed target opportunities, intel, and teaming coordination. As a result, the aircraft is unable to conduct mission tasks.	2
CS 6.0.1	FO misses the checklist step to engage TCM due to increasing cognitive load from mission tasks and the aircraft does not automatically launch effective countermeasures when engaged by enemy air defense assets. As a result, the aircraft is unable to conduct mission tasks.	1

CS 6.1.1	FO unintentionally engages TCMs due to a similarity in the control for a separate mission task before entering hostile territory. TCMs are then triggered by a false alarm (high safety but low reliability detection system) and expend flares that provide position intelligence to hostile scouts in a neighboring area, leading to an aborted mission for the FRWA which required the utmost stealth. As a result, the aircraft is unable to conduct mission tasks.	1
CS 6.2.1	FO engages TCM systems, but ASEC computers are powering back-up following an in-flight reboot due to a malfunction diagnosed by the operator. The TCM systems do not engage (e.g. pilot sends command to deploy chaff via PVI, but the self-defense computer is still restarting so the signal is not relayed). As a result, the aircraft is unable to conduct mission tasks.	1
CS 6.2.2	FO commands TCM systems to engage but signals to ASEC are jammed/spoofed. There is a problem engaging TCM systems and aircraft cannot defend against enemy air defense. As a result, the aircraft is unable to conduct mission tasks.	1
CS 6.3.1	FO receives incoming notification of enemy air threat but does not react in time to engage additional TCMs due to low resolution feedback [i.e. insufficient detail to adequately respond to the threat] from the alert system and the aircraft does not defend itself to the fullest extent and is damaged by enemy air defense assets. As a result, the aircraft is unable to conduct mission tasks.	1
CS 6.4.1	FO leaves TCMs engaged for too long and prematurely expends entire countermeasure inventory. As a result, the aircraft is no longer able to perform self-defense and conduct mission tasks.	1
CS 6.5.1	FO disengages TCMs before leaving hostile territory because FO believes he is outside of enemy threat range due to incorrect mental model of hostile systems maximum engagement range. The FRWA is then engaged by enemy air defense system when TCMs are off. As a result, the aircraft is unable to conduct mission tasks.	1
CS 7.0.1	FO commands ASEC to secure mission data, but ASEC does not perform operation correctly (power loss/spoofing/signal interception). As a result, information security is compromised.	1
CS 7.0.2	FO is incapacitated and cannot secure mission data (e.g. pilot(s) is killed in crash and cannot zeroize mission systems so adversary can recover secure information). As a result, critical information is compromised.	1
CS 7.1.1	ASEC receives conflicting commands from FOs to load mission data. Another FO has taken temporary control of the FRWA before another FO takes over. Confusion over ongoing control authority ensues and a misunderstanding related to whether or not the appropriate mission data was loaded earlier on in the flight results in mission data that is compromised because enemy assets are able to decipher mission information from the unsecured communication. As a result, critical information is compromised	1
CS 7.1.2	FO believes mission data is secure but feedback is incorrect (e.g. when loading a mission plan, FO receives a false indication of secure comms because the system does not recognize/alert the FO if cryptographic keys are outdated or not, and makes what the FO believes are secure radio calls over unencrypted channels), which results in a loss of critical information.	2
CS 7.1.3	FO inputs commands to secure mission data to ASEC but commands are not received (e.g. spoofing/jamming prevents commands from being received during remote operation)	2
CS 7.1.4	ASEC secures mission data when not commanded by FO (e.g. enemy spoofing signals trigger zeroization of data without command from FO), which results in a loss of critical mission information related to targets and grid coordinates needed to conduct the mission. As a result, critical information is compromised	2
CS 7.1.5	FO does not update mission-related critical information correctly because he has a faulty mental model of when the update is supposed to occur. As a result, critical information is compromised (e.g. crypto rollover does not occur at the time believed by the FO and causes radio transmissions to become unencrypted and vulnerable to enemy intelligence)	1
CS 7.1.6	FO secures mission data by mistake (e.g. pilot(s) engages zeroize function unintentionally due to lack of a safeguard/safety interlock on the control activation). As a result, critical information is compromised.	2

7.2 Complete Risk Assessment

7.2.1 Scenario-Based Approach Results

Causal Scenario	PMS	RM ID	Recommended Mitigation	MES	CMES	PPMS	CPMS
-----------------	-----	-------	------------------------	-----	------	------	------

CS 2.0.1	FO is incapacitated by enemy fire, injury, illness and leans onto the controls accidentally activating them. As a result aircraft can become uncontrollable.	1	RM01	Aircraft monitors pilot health/posture/attention and automatically engages autonomous mode when FO is incapacitated/task saturated/inattentive/fixated; system can also alert and allow a remote operator to take control	ELIM	ELIM	4	4
			RM02	Aircraft can be remotely controlled while in manned configuration			4	
			RM03	Aircraft can autonomously execute specific flight maneuvers (e.g. return to base, climb/descend to specific altitudes, fly a specific straight-and-level profile, formation flight, reroute to designated airspace); maintains all structural limitations			4	
CS 2.0.2	FO mental model of aircraft flight control systems conflicts with reality and FO does not make the necessary manual inputs during a critical mode of flight. As a result the aircraft becomes uncontrollable. (e.g. executing an emergency procedure incorrectly because the FO does not understand the relationships between subsystems)	1	RM08	Aircraft health systems monitor aircraft performance, alert FO when unsafe scenarios are approaching (e.g. engine health in danger, airframe integrity compromised, combat system malfunctions/loss of effectiveness, etc.)	2	3	4	3
			RM12	Emergency response system detects problems and alerts the FO, awaits FO input, and automatically engages if outside the time window allotted for FO action	2		3	
			RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1		2	
CS 2.0.3	FO receives poor or inadequate feedback from flight controls and does not make necessary control inputs during a critical mode of flight. As a result the aircraft becomes uncontrollable. (e.g. FO does not get a FIRE light in the event of an engine fire and does not execute the proper emergency procedures)	1	RM05	Design salient PVI indications/alerts with high polling rates that combine audio, visual, and haptic feedback. An alerting schema/framework should be created utilizing context-specific alerts appropriate to the severity of the situation.	3	5	3	3
			RM08	Aircraft health systems monitor aircraft performance, alert FO when unsafe scenarios are approaching (e.g. engine health in danger, airframe integrity compromised, combat system malfunctions/loss of effectiveness, etc.)	2		3	
			RM12	Emergency response system detects problems and alerts the FO, awaits FO input, and automatically engages if outside the time window allotted for FO action	2		3	
CS 2.0.4	FO becomes saturated with mission tasks and does not respond to aircraft alerts, as a result the aircraft violates minimum separation standards during formation flight (e.g. FO is performing mission tasks and does not realize aircraft is drifting too close to other aircraft within formation and collides with friendly aircraft)	1	RM03	Aircraft can autonomously execute specific flight maneuvers (e.g. return to base, climb/descend to specific altitudes, fly a specific straight-and-level profile, formation flight, reroute to designated airspace); maintains all structural limitations	ELIM	ELIM	4	4
			RM01	Aircraft monitors pilot health/posture/attention and automatically engages autonomous mode when FO is incapacitated/task saturated/inattentive/fixated; system can also alert and allow a remote operator to take control			4	
			RM21	Aircraft geospatial awareness systems (GPS, proximity sensors, transponder, etc.) provide position data in relation to terrain, airspace, aircraft, known enemy positions, and other obstacles that alerts the FO if safety thresholds are breached. Real-time airspace update service that can relay dynamically changing airspace/battlespace information to participating aircraft; data is pulled from high level server every X minutes to provide information to operators			4	
CS 2.0.5	FO commands a flight control input, but it is not received because of faulty wiring/hardware malfunction in the fly-by-wire system. As a result, the aircraft becomes uncontrollable. (e.g. FO tries to correct trim of aircraft but tail rotor control does not receive signal)	1	RM14	Design redundant architecture for all critical control components to ensure proper operation (e.g. wireless signal equipment, control linkages, onboard wiring)	3	3	3	3
CS 2.1.1	FO cannot make aircraft control inputs when the aircraft is disengaged from autonomous mode due to enemy spoofing the autonomous control signal during the transition to manual control. As a result, the aircraft becomes uncontrollable.	1	RM06	Design the autonomous control system to be jam and spoof resistant	3	3	2	2
CS 2.2.1	Safety interlocks malfunction and disconnect the FO's physical inputs to the fly-by-wire system. The aircraft is in autonomous mode and does not allow the FO the make necessary aircraft control inputs during an in-flight emergency. As a result the aircraft becomes uncontrollable.	1	RM07	Provide FO with direct control of hardware that bypasses ASEC and/or allows FO to reset system (circuit breaker panels, kill switches, etc)	ELIM	ELIM	4	4
			RM12	Emergency response system detects problems and alerts the FO, awaits FO input, and automatically engages if outside the time window allotted for FO action			4	
CS 2.3.1	FO is spatially disoriented and inaccurately believes that the aircraft autonomous mode is malfunctioning. FO makes a flight control input which results into violation of minimum separation standards.	1	RM08	Aircraft health systems monitor aircraft performance, alert FO when unsafe scenarios are approaching (e.g. engine health in danger, airframe integrity compromised, combat system malfunctions/loss of effectiveness, etc.)	2	3	2	2
			RM21	Aircraft geospatial awareness systems (GPS, proximity sensors, transponder, etc.) provide position data in relation to terrain, airspace, aircraft, known enemy positions, and other obstacles that alerts the FO if safety thresholds are breached. Real-time airspace update service that can relay dynamically changing	3		2	

				airspace/battlespace information to participating aircraft; data is pulled from high level server every X minutes to provide information to operators				
			RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1		3	
CS 2.4.1	FO remotely sends control signal to aircraft, but it is block/jammed and not received. Remote FO was commanding an aggressive maneuver of the airframe when enemy jamming blocks the remote signal from stopping the aircrafts last maneuver command. As a result, aircraft structural integrity is violated.	1	RM06	Design the autonomous control system to be jam and spoof resistant	3		2	
			RM08	Aircraft health systems monitor aircraft performance, alert FO when unsafe scenarios are approaching (e.g. engine health in danger, airframe integrity compromised, combat system malfunctions/loss of effectiveness, etc.)	2	5	2	2
			RM12	Emergency response system detects problems and alerts the FO, awaits FO input, and automatically engages if outside the time window allotted for FO action	2		2	
			RM29	Design high assurance communications network (similar to GPS satellites) that provides multiple paths to send and receive control signals to aircraft	3		3	
CS 2.4.2	FO executes a faulty mental model of a flight procedure and does not control the aircraft properly during an emergency, resulting in a loss of main engine power. As a result, structural integrity of the aircraft is violated. (e.g. pilot does not execute a recovery maneuver properly and crashes the aircraft)	1	RM08	Aircraft health systems monitor aircraft performance, alert FO when unsafe scenarios are approaching (e.g. engine health in danger, airframe integrity compromised, combat system malfunctions/loss of effectiveness, etc.)	2		3	
			RM12	Emergency response system detects problems and alerts the FO, awaits FO input, and automatically engages if outside the time window allotted for FO action	2	3	2	2
			RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1		3	
CS 2.5.1	FO does not recall the flight parameters for working operation of flight systems and makes certain flight inputs too early. As a result, the aircraft becomes uncontrollable. (e.g. FO attempt to engage autopilot function too soon before establishing the correct flight profile [speed/attitude])	1	RM08	Aircraft health systems monitor aircraft performance, alert FO when unsafe scenarios are approaching (e.g. engine health in danger, airframe integrity compromised, combat system malfunctions/loss of effectiveness, etc.)	2	3	3	3
			RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1		3	
CS 2.5.2	FO initiates a flight maneuver too early based on a signal/indication relayed from the ASEC. As a result, the structural integrity is violated. [e.g. VSI/radar altimeter indications inform FO that aircraft is descending more rapidly than reality during DVE, FO overtorques aircraft in response]	1	RM14	Design redundant architecture for all critical control components to ensure proper operation (e.g. wireless signal equipment, control linkages, onboard wiring)	3		4	
			RM08	Aircraft health systems monitor aircraft performance, alert FO when unsafe scenarios are approaching (e.g. engine health in danger, airframe integrity compromised, combat system malfunctions/loss of effectiveness, etc.)	2	6	3	3
			RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1		3	
CS 2.5.3	FO commands ASEC to perform an autonomous flight procedure and the command is not received or executed fully by the ASEC, as a result the FO conducts the procedure too soon. As a result, aircraft structural integrity is violated. (e.g. automated landing mode engaged, landing gear are not fully extended and aircraft is not ready to land but FO lands without gears extended)	1	RM08	Aircraft health systems monitor aircraft performance, alert FO when unsafe scenarios are approaching (e.g. engine health in danger, airframe integrity compromised, combat system malfunctions/loss of effectiveness, etc.)	2		3	
			RM14	Design redundant architecture for all critical control components to ensure proper operation (e.g. wireless signal equipment, control linkages, onboard wiring)	3	6	4	3
			RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1		3	
CS 2.6.1	FO does not receive feedback that the autonomous mode is fully disengaged because the alert he received was dismissed earlier on in the flight and the FO forgets that partial autonomy is still active. The FO then initiates a high/low power maneuver with flight controls, which results in unexpected control inputs as they conflict with the partial autonomy. As a result the aircraft becomes uncontrollable.	1	RM08	Aircraft health systems monitor aircraft performance, alert FO when unsafe scenarios are approaching (e.g. engine health in danger, airframe integrity compromised, combat system malfunctions/loss of effectiveness, etc.)		ELIM	4	4
			RM05	Design salient PVI indications/alerts with high polling rates that combine audio, visual, and haptic feedback. An alerting schema/framework should be created utilizing context-specific alerts appropriate to the severity of the situation.			4	
CS 2.7.1	FO becomes fixated on a mission task and enters a delayed aircraft control input. As a result, the structural integrity of the aircraft is violated. (e.g. FO commands a high-power maneuver while task saturated and delays finishing the maneuver)	1	RM08	Aircraft health systems monitor aircraft performance, alert FO when unsafe scenarios are approaching (e.g. engine health in danger, airframe integrity compromised, combat system malfunctions/loss of effectiveness, etc.)		ELIM	4	4
			RM10	ASEC detects delay in FO inputs and switches aircraft to autonomous mode if no input is made within a certain timeframe			4	

			RM01	Aircraft monitors pilot health/posture/attention and automatically engages autonomous mode when FO is incapacitated/task saturated/inattentive/fixated; system can also alert and allow a remote operator to take control			4	
CS 2.7.2	FO relegates autonomous control of FRWA to another FO, who does not fully absorb necessary information from the transition and enters a delayed aircraft command. As a result, the aircraft becomes uncontrollable (e.g. FRWA is fuel low, but new FO delays sending refuel signal to aircraft and aircraft is forced to land in hostile territory)	1	RM08	Aircraft health systems monitor aircraft performance, alert FO when unsafe scenarios are approaching (e.g. engine health in danger, airframe integrity compromised, combat system malfunctions/loss of effectiveness, etc.)	ELIM	ELIM	4	4
			RM32	Design flight/mission control systems to ensure appropriate control authority/information exchanges between controllers that satisfy required conditions for handoff			4	
			RM05	Design salient PVI indications/alerts with high polling rates that combine audio, visual, and haptic feedback. An alerting schema/framework should be created utilizing context-specific alerts appropriate to the severity of the situation.			4	
CS 2.7.3	FRWA delays transmitting a feedback signal to the FO through ASEC, the FO is unable to react in the proper amount of time. As a result the aircraft becomes uncontrollable	1	RM05	Design salient PVI indications/alerts with high polling rates that combine audio, visual, and haptic feedback. An alerting schema/framework should be created utilizing context-specific alerts appropriate to the severity of the situation.	3	5	3	2
			RM10	ASEC detects delay in FO inputs and switches aircraft to autonomous mode if no input is made within a certain timeframe	2		2	
			RM29	Design high assurance communications network (similar to GPS satellites) that provides multiple paths to send and receive control signals to aircraft	3		3	
CS 2.7.4	FO has a set amount of time to respond to an aircraft emergency but is delayed in the aircraft control input. As a result, the structural integrity of the aircraft is violated. (e.g. engine experiences a fire, FO does not deploy firefighting system in time and smoke fills the cockpit).	1	RM12	Emergency response system detects problems and alerts the FO, awaits FO input, and automatically engages if outside the time window allotted for FO action	2	5	3	2
			RM08	Aircraft health systems monitor aircraft performance, alert FO when unsafe scenarios are approaching (e.g. engine health in danger, airframe integrity compromised, combat system malfunctions/loss of effectiveness, etc.)	2		2	
			RM05	Design salient PVI indications/alerts with high polling rates that combine audio, visual, and haptic feedback. An alerting schema/framework should be created utilizing context-specific alerts appropriate to the severity of the situation.	3		2	
CS 2.8.1	FO loses situational awareness/task saturated and makes an input for too long. As a result, structural integrity of the aircraft is violated. (e.g. during instrument takeoff, pilot continues climb because they become disoriented from lack of visual references).	1	RM08	Aircraft health systems monitor aircraft performance, alert FO when unsafe scenarios are approaching (e.g. engine health in danger, airframe integrity compromised, combat system malfunctions/loss of effectiveness, etc.)	2	5	3	2
			RM05	Design salient PVI indications/alerts with high polling rates that combine audio, visual, and haptic feedback. An alerting schema/framework should be created utilizing context-specific alerts appropriate to the severity of the situation.	3		2	
			RM10	ASEC detects delay in FO inputs and switches aircraft to autonomous mode if no input is made within a certain timeframe	2		3	
CS 2.8.2	FO does not properly understand aircraft systems and their associated checklist commands. Flight training did not adequately prepare the FO with environmental structural/limitations of the aircraft and the FO holds inputs (collective – power demand) for too long. As a result the aircraft becomes uncontrollable. (e.g. FO demands too much power from the system to climb a terrain feature under hot weather and overtorques the aircraft)	1	RM05	Design salient PVI indications/alerts with high polling rates that combine audio, visual, and haptic feedback. An alerting schema/framework should be created utilizing context-specific alerts appropriate to the severity of the situation.	3	6	2	2
			RM08	Aircraft health systems monitor aircraft performance, alert FO when unsafe scenarios are approaching (e.g. engine health in danger, airframe integrity compromised, combat system malfunctions/loss of effectiveness, etc.)	2		3	
			RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1		3	
CS 2.8.3	FO maintains a control input for too long because ASEC provides a delayed indication. As a result, the aircraft violates minimum separation standards. (e.g. vertical speed indicator lags, therefore the pilot holds a climb for too long violating minimum separation standards)	1	RM08	Aircraft health systems monitor aircraft performance, alert FO when unsafe scenarios are approaching (e.g. engine health in danger, airframe integrity compromised, combat system malfunctions/loss of effectiveness, etc.)	2	5	3	3
			RM05	Design salient PVI indications/alerts with high polling rates that combine audio, visual, and haptic feedback. An alerting schema/framework should be created utilizing context-specific alerts appropriate to the severity of the situation.	3		4	
			RM10	ASEC detects delay in FO inputs and switches aircraft to autonomous mode if no input is made within a certain timeframe	2		3	
			RM21	Aircraft geospatial awareness systems (GPS, proximity sensors, transponder, etc.) provide position data in relation to terrain, airspace, aircraft, known enemy positions, and other obstacles that alerts the FO if safety thresholds are breached. Real-time airspace update service that can relay dynamically changing	3		2	

				airspace/battlespace information to participating aircraft; data is pulled from high level server every X minutes to provide information to operators					
CS 2.8.4	FO holds an input for too long because the ASEC does not provide feedback that the input was received. As a result, the aircraft becomes uncontrollable. (e.g. fly-by-wire connections between PVI and HW fail, so the pilot continues to hold a climb with no effect)	1	RM14	Design redundant architecture for all critical control components to ensure proper operation (e.g. wireless signal equipment, control linkages, onboard wiring)	3	ELIM	ELIM	4	4
			RM08	Aircraft health systems monitor aircraft performance, alert FO when unsafe scenarios are approaching (e.g. engine health in danger, airframe integrity compromised, combat system malfunctions/loss of effectiveness, etc.)				4	
			RM03	Aircraft can autonomously execute specific flight maneuvers (e.g. return to base, climb/descend to specific altitudes, fly a specific straight-and-level profile, formation flight, reroute to designated airspace); maintains all structural limitations				4	
CS 2.9.1	FO loses situational awareness/task saturated and makes an input for too short. As a result, the aircraft becomes uncontrollable. (e.g. pilot becomes distracted by mission management and stop providing flight control inputs)	1	RM08	Aircraft health systems monitor aircraft performance, alert FO when unsafe scenarios are approaching (e.g. engine health in danger, airframe integrity compromised, combat system malfunctions/loss of effectiveness, etc.)		ELIM	ELIM	4	4
			RM01	Aircraft monitors pilot health/posture/attention and automatically engages autonomous mode when FO is incapacitated/task saturated/inattentive/fixated; system can also alert and allow a remote operator to take control				4	
			RM05	Design salient PVI indications/alerts with high polling rates that combine audio, visual, and haptic feedback. An alerting schema/framework should be created utilizing context-specific alerts appropriate to the severity of the situation.				4	
CS 2.9.2	FO does not understand aircraft systems/checklists, holding inputs for too short. As a result, the aircraft becomes uncontrollable. (e.g. FO holds incorrect nose attitude during landing and has a hard landing)	1	RM08	Aircraft health systems monitor aircraft performance, alert FO when unsafe scenarios are approaching (e.g. engine health in danger, airframe integrity compromised, combat system malfunctions/loss of effectiveness, etc.)	2	6	6	3	3
			RM05	Design salient PVI indications/alerts with high polling rates that combine audio, visual, and haptic feedback. An alerting schema/framework should be created utilizing context-specific alerts appropriate to the severity of the situation.	3			3	
			RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1			3	
CS 2.9.3	FO maintains a control input for too short a time because ASEC provides an incorrect indication. The ASEC does not process the aircraft's health monitoring sensor feedback in time when the FO was conducting a combat maneuver due to a hard reset of the primary flight computer. As a result, structural integrity is violated.	1	RM14	Design redundant architecture for all critical control components to ensure proper operation (e.g. wireless signal equipment, control linkages, onboard wiring)	3	6	6	2	2
			RM08	Aircraft health systems monitor aircraft performance, alert FO when unsafe scenarios are approaching (e.g. engine health in danger, airframe integrity compromised, combat system malfunctions/loss of effectiveness, etc.)	2			3	
			RM05	Design salient PVI indications/alerts with high polling rates that combine audio, visual, and haptic feedback. An alerting schema/framework should be created utilizing context-specific alerts appropriate to the severity of the situation.	3			2	
			RM21	Aircraft geospatial awareness systems (GPS, proximity sensors, transponder, etc.) provide position data in relation to terrain, airspace, aircraft, known enemy positions, and other obstacles that alerts the FO if safety thresholds are breached. Real-time airspace update service that can relay dynamically changing airspace/battlespace information to participating aircraft; data is pulled from high level server every X minutes to provide information to operators	3			2	
			RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1			3	
CS 3.0.1	FO does not recognize when he has entered new enemy-controlled airspace because he is relying on outdated airspace information and does not communicate his identity through proper transponder signal or other communications. The FO does not have the latest friendly intelligence that established the current operating airspace as hostile with a 'no-fly designation' due to enemy jamming of FRWA's over-the-horizon communication capability. As a result, minimum separation standards are violated.	1	RM09	Navigation/communication system notify and request confirmation from FO when entering/leaving airspace to automatically adjust radio frequencies and transponder codes	2	5	5	2	2
			RM21	Aircraft geospatial awareness systems (GPS, proximity sensors, transponder, etc.) provide position data in relation to terrain, airspace, aircraft, known enemy positions, and other obstacles that alerts the FO if safety thresholds are breached. Real-time airspace update service that can relay dynamically changing airspace/battlespace information to participating aircraft; data is pulled from high level server every X minutes to provide information to operators	3			2	
			RM22	Aircraft must automatically send identity/position messages to friendly forces when entering a new airspace, conducting mission tasks, experiencing in-flight emergencies, etc. (e.g. BlueForce Tracker, Link-16 messages)	3			4	

CS 3.0.2	FO does not perform data management tasks when entering a new airspace. This could occur if an updated configuration renders the data management TTPs that the FO is accustomed to incompatible for proper operation of the system. As a result, minimum separation standards are violated.	2	RM33	Aircraft must be able to detect and validate software and hardware configuration changes and notify operator. FO must acknowledge and verify all configuration prior to operation	ELIM		4	3
			RM21	Aircraft geospatial awareness systems (GPS, proximity sensors, transponder, etc.) provide position data in relation to terrain, airspace, aircraft, known enemy positions, and other obstacles that alerts the FO if safety thresholds are breached. Real-time airspace update service that can relay dynamically changing airspace/battlespace information to participating aircraft; data is pulled from high level server every X minutes to provide information to operators	3	ELIM	3	
CS 3.1.1	FO receives a system alert that draws his attention to perform a data management task during formation flight under manual control. As a result, the aircraft violates minimum separation standards.	1	RM03	Aircraft can autonomously execute specific flight maneuvers (e.g. return to base, climb/descend to specific altitudes, fly a specific straight-and-level profile, formation flight, reroute to designated airspace); maintains all structural limitations	ELIM	ELIM	4	4
			RM21	Aircraft geospatial awareness systems (GPS, proximity sensors, transponder, etc.) provide position data in relation to terrain, airspace, aircraft, known enemy positions, and other obstacles that alerts the FO if safety thresholds are breached. Real-time airspace update service that can relay dynamically changing airspace/battlespace information to participating aircraft; data is pulled from high level server every X minutes to provide information to operators			4	
			RM01	Aircraft monitors pilot health/posture/attention and automatically engages autonomous mode when FO is incapacitated/task saturated/inattentive/fixated; system can also alert and allow a remote operator to take control			4	
CS 3.2.1	ASEC receives conflicting information inputs from multiple FOs due to misidentification of tracks and is unable to discern the status of a contact detected by the reconnaissance systems. As a result, the aircraft is unable to perform mission tasks. (e.g. one FO identifies a track as hostile, while another identifies it as neutral/friendly)	1	RM13	Design control logic that aids in task prioritization, detects and prevents conflicting mission commands, and provides feedback indicating which control responsibilities are under ASEC/teaming control	3	3	4	4
CS 3.3.1	FO uploads flight way points too late into the mission execution because he does not believe that they are outdated (however mission dynamics have changed). As a result, the aircraft violates minimum separation standards. (e.g. remote pilot is too slow to update automated flight plan after recognizing his mission data is outdated, aircraft enters enemy airspace)	1	RM21	Aircraft geospatial awareness systems (GPS, proximity sensors, transponder, etc.) provide position data in relation to terrain, airspace, aircraft, known enemy positions, and other obstacles that alerts the FO if safety thresholds are breached. Real-time airspace update service that can relay dynamically changing airspace/battlespace information to participating aircraft; data is pulled from high level server every X minutes to provide information to operators	ELIM	ELIM	4	4
			RM09	Navigation/communication system notify and request confirmation from FO when entering/leaving airspace to automatically adjust radio frequencies and transponder codes			4	
CS 3.4.1	FO updates transponder code and radio frequency too early before entering a new airspace because he wants to complete the data management tasks in advance and is engaged by friendly forces that have recently entered the AO that believe no friendly aircraft are operating in the area. As a result, the aircraft violates minimum separation standards.	1	RM09	Navigation/communication system notify and request confirmation from FO when entering/leaving airspace to automatically adjust radio frequencies and transponder codes	ELIM	ELIM	4	4
CS 3.5.1	FO performs data management for too long because the ASEC is not relaying the appropriate status feedback, which draws the FO's attention away from manual flight control too long and the aircraft enters an unusual attitude. As a result, the aircraft is uncontrollable. [e.g. FO attempts to update his flight plan but the system does not adequately inform the pilot of the status and is distracted from flying the aircraft]	1	RM05	Design salient PVI indications/alerts with high polling rates that combine audio, visual, and haptic feedback. An alerting schema/framework should be created utilizing context-specific alerts appropriate to the severity of the situation.	3	ELIM	4	4
			RM03	Aircraft can autonomously execute specific flight maneuvers (e.g. return to base, climb/descend to specific altitudes, fly a specific straight-and-level profile, formation flight, reroute to designated airspace); maintains all structural limitations			4	
			RM01	Aircraft monitors pilot health/posture/attention and automatically engages autonomous mode when FO is incapacitated/task saturated/inattentive/fixated; system can also alert and allow a remote operator to take control			4	
CS 4.0.1	FO does not receive adequate feedback from the targeting system because not enough of the on-board sensors can provide target information. The FO does not have any other sensors outside of the FRWA that he can rely on as the sole operational asset with the target identification capabilities in the area and	2	RM26	Design targeting system that compiles track and target information through sensor fusion (optical, IR, radar, force tracker, etc.) to meet attack criteria	3	ELIM	4	4

	does not engage the attack systems. As a result, the aircraft is unable to conduct mission tasks.							
CS 4.0.2	FO does not attack target because the FO is unaware of engaged system safety interlocks preventing the arming of onboard weaponry. Safety of flight system (e.g. weight-on-wheel switch) prevents arming of weapons, thus preventing FO from engaging attack systems. As a result, the aircraft is unable to conduct mission tasks.	2	RM07	Provide FO with direct control of hardware that bypasses ASEC and/or allows FO to reset system (circuit breaker panels, kill switches, etc)	3	3	3	3
CS 4.0.3	Attack system believes aircraft is within Engagement Zone (EZ), but FO knows this to be false because of environmental conditions outside the aircraft he is observing that the ASEC aware of , so the FO does not release the weapon. [e.g. FO observes that his wingman is inside the weapon danger zone but the system shows the aircraft inside a safe area, so the FO chooses not to fire]. As a result, the aircraft is unable to conduct mission tasks.	3	RM21	Aircraft geospatial awareness systems (GPS, proximity sensors, transponder, etc.) provide position data in relation to terrain, airspace, aircraft, known enemy positions, and other obstacles that alerts the FO if safety thresholds are breached. Real-time airspace update service that can relay dynamically changing airspace/battlespace information to participating aircraft; data is pulled from high level server every X minutes to provide information to operators	3	2	4	4
CS 4.0.4	FO does not attack target because he believes another asset is conducting the attack based on a radio miscommunication. Inadequate teaming/ communication causes confusion in attack orders and priority and the acquired target may not be engaged when necessary. As a result, the aircraft is unable to conduct mission tasks.	2	RM13	Design control logic that aids in task prioritization, detects and prevents conflicting mission commands, and provides feedback indicating which control responsibilities are under ASEC/teaming control	3	4	3	3
CS 4.1.1	FO engages attack system despite inadequate feedback from data management systems within FRWA because friendly intelligence assets inform the FO that the area is clear to engage. As a result this leads to an unsafe attack and aircraft operations cause collateral damage or friendly fire.	1	RM26	Design targeting system that compiles track and target information through sensor fusion (optical, IR, radar, force tracker, etc.) to meet attack criteria	3	ELIM	4	4
CS 4.1.2	FO leaves weapon system armed after an attack because they intend to conduct an attack shortly on a new passing run, but never engages the intended target and forgets to disarm the system leading to a negligent discharge later in the flight while FO engages attack control. This results in a weapons release outside of a EZ. As a result, aircraft operations cause collateral damage or friendly fire.	1	RM08	Aircraft health systems monitor aircraft performance, alert FO when unsafe scenarios are approaching (e.g. engine health in danger, airframe integrity compromised, combat system malfunctions/loss of effectiveness, etc.)	2	5	1	1
			RM24	Design incremental control logic that prevents unintentional activation/deactivation of mission controls, such as those associated with weapons, self-defense, and reconnaissance	3		1	
CS 4.2.1	FO performs attack late due to coordination issues with remote designator. FO is ready to perform attack, but remote designator loses communication due to jamming and cannot reliably designate target at moment of attack. FO needs to reposition/reconduct attack procedures. As a result, the aircraft is unable to conduct mission tasks.	2	RM26	Design targeting system that compiles track and target information through sensor fusion (optical, IR, radar, force tracker, etc.) to meet attack criteria	3	4	2	2
CS 4.3.1	FO begins attack prior to entering valid Engagement Zone (EZ) because he believes the target is inside the correct EZ based on incorrect sensor feedback received from a ground force operator. As a result, aircraft operations cause collateral damage or friendly fire.	1	RM08	Aircraft health systems monitor aircraft performance, alert FO when unsafe scenarios are approaching (e.g. engine health in danger, airframe integrity compromised, combat system malfunctions/loss of effectiveness, etc.)	2	6	3	3
			RM21	Aircraft geospatial awareness systems (GPS, proximity sensors, transponder, etc.) provide position data in relation to terrain, airspace, aircraft, known enemy positions, and other obstacles that alerts the FO if safety thresholds are breached. Real-time airspace update service that can relay dynamically changing airspace/battlespace information to participating aircraft; data is pulled from high level server every X minutes to provide information to operators	3		3	
			RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1		3	
			RM26	Design targeting system that compiles track and target information through sensor fusion (optical, IR, radar, force tracker, etc.) to meet attack criteria	3		3	
CS 4.4.1	FO does not perform attack procedure correctly because of an incorrect mental model [e.g. they skipped steps in a checklist based on use of an outdated checklist because they did not have	2	RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1	1	2	2

	the latest version prior to flight], resulting in ineffective targeting acquisition and/or unintended weapons release. As a result, the aircraft is unable to conduct mission tasks.							
CS 4.5.1	FO cannot perform attack because armed weapons lose effectiveness. The attack systems are armed for too long during the mission because the FO loses awareness that they were engaged far earlier in the flight, which leads to battery drain/gimbal misalignment, preventing an effective attack at a later time. As a result, the aircraft is unable to conduct mission tasks.,	3	RM24	Design incremental control logic that prevents unintentional activation/deactivation of mission controls, such as those associated with weapons, self-defense, and reconnaissance	3	ELIM	3	3
			RM08	Aircraft health systems monitor aircraft performance, alert FO when unsafe scenarios are approaching (e.g. engine health in danger, airframe integrity compromised, combat system malfunctions/loss of effectiveness, etc.)	ELIM		4	
CS 4.6.1	FO disengages attack system before conducting attack. FO disarms targeting system because of exchange of FO targeting responsibility to another target controller and does not re-engage the on board targeting system before conducting follow-on attack. As a result, the aircraft is unable to conduct mission tasks.	3	RM13	Design control logic that aids in task prioritization, detects and prevents conflicting mission commands, and provides feedback indicating which control responsibilities are under ASEC/teaming control	3	4	4	3
			RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1		3	
CS 4.6.2	FO does not receive adequate feedback from attack and reconnoiter systems that a target has been eliminated because of system limitations [e.g. beyond line of sight] and disengages attack system prior to target being completely destroyed. The FO believes the target was destroyed based on ordinance used for target and subsequently disengages the attack systems. When target resurfaces from sensor data, the FO is not in a position to attack quickly enough due to disarmament of the attack systems earlier. As a result, the aircraft is unable to conduct mission tasks.	3	RM26	Design targeting system that compiles track and target information through sensor fusion (optical, IR, radar, force tracker, etc.) to meet attack criteria	3	3	4	4
CS 5.0.1	FO does not receive feedback from ATC with regard to location of mission area because ATC does not have the latest intelligence and does not engage reconnaissance systems, resulting in a loss of target identification. As a result, the aircraft is unable to conduct mission tasks.	1	RM21	Aircraft geospatial awareness systems (GPS, proximity sensors, transponder, etc.) provide position data in relation to terrain, airspace, aircraft, known enemy positions, and other obstacles that alerts the FO if safety thresholds are breached. Real-time airspace update service that can relay dynamically changing airspace/battlespace information to participating aircraft; data is pulled from high level server every X minutes to provide information to operators	ELIM	ELIM	4	4
CS 5.0.2	FO is in vicinity of equipment within mission area that generates electromagnetic interference (EMI) and does not engage reconnaissance systems because he knows they may not function properly near EMI sources. As a result, the aircraft is unable to conduct mission tasks.	1	RM08	Aircraft health systems monitor aircraft performance, alert FO when unsafe scenarios are approaching (e.g. engine health in danger, airframe integrity compromised, combat system malfunctions/loss of effectiveness, etc.)	2	5	1	2
			RM30	Design critical mission systems and computers to be hardened against EMI	3		3	
CS 5.1.1	FO engages reconnaissance systems inside mission area but systems are jammed/spoofed by enemy EW assets, which prevents them from functioning properly. As a result, the aircraft is unable to conduct mission tasks.	1	RM06	Design the autonomous control system to be jam and spoof resistant	3	4	3	3
CS 5.2.1	FO engages reconnaissance systems to maintain battlespace situational awareness while simultaneously conducting an attack or performing self-defense, causing the ASEC to misprioritize command signals. This can degrade specific mission system performance if the ASEC is unable to filter through the commands quickly enough, which may result in a loss of mission for one or both tasks.	2	RM13	Design control logic that aids in task prioritization, detects and prevents conflicting mission commands, and provides feedback indicating which control responsibilities are under ASEC/teaming control	ELIM	ELIM	4	4
CS 5.3.1	FO engages reconnaissance systems while entering mission area, but the ASEC is slow to initialize the systems. e.g. the cooldown period for FLIR, warm up for radar, time syncing required to enter battlespace management networks, etc. As a result, the aircraft is unable to conduct mission tasks.	2	RM27	Design mission systems with X seconds startup period and implement sensor feedback to alert the pilot of readiness status	3	3	4	4
CS 5.4.1	FO engages reconnaissance systems accidentally while on ground in a friendly area due to inadvertent activation, and causes radiation harm to nearby personnel or equipment. As a	3	RM08	Aircraft health systems monitor aircraft performance, alert FO when unsafe scenarios are approaching (e.g. engine health in danger, airframe integrity compromised, combat system malfunctions/loss of effectiveness, etc.)	2	ELIM	3	3

	result, aircraft operations cause collateral damage or friendly fire.		RM24	Design incremental control logic that prevents unintentional activation/deactivation of mission controls, such as those associated with weapons, self-defense, and reconnaissance	ELIM		4	
			RM21	Aircraft geospatial awareness systems (GPS, proximity sensors, transponder, etc.) provide position data in relation to terrain, airspace, aircraft, known enemy positions, and other obstacles that alerts the FO if safety thresholds are breached. Real-time airspace update service that can relay dynamically changing airspace/battlespace information to participating aircraft; data is pulled from high level server every X minutes to provide information to operators	3		3	
CS 5.5.1	FO leaves reconnaissance systems engaged after exiting mission area because he still believes he is operating within the mission airspace, which enables the enemy to track location of aircraft through broadcasted signals from aircraft. As a result, the minimum aircraft separation standards are violated.	2	RM21	Aircraft geospatial awareness systems (GPS, proximity sensors, transponder, etc.) provide position data in relation to terrain, airspace, aircraft, known enemy positions, and other obstacles that alerts the FO if safety thresholds are breached. Real-time airspace update service that can relay dynamically changing airspace/battlespace information to participating aircraft; data is pulled from high level server every X minutes to provide information to operators	ELIM	ELIM	4	3
			RM08	Aircraft health systems monitor aircraft performance, alert FO when unsafe scenarios are approaching (e.g. engine health in danger, airframe integrity compromised, combat system malfunctions/loss of effectiveness, etc.)			4	
			RM24	Design incremental control logic that prevents unintentional activation/deactivation of mission controls, such as those associated with weapons, self-defense, and reconnaissance	3		3	
CS 5.6.1	FO believes they are outside a mission area due to conflicting feedback from ATC and disengages reconnaissance systems too soon, leading to missed target opportunities, intel, and teaming coordination. As a result, the aircraft is unable to conduct mission tasks.	2	RM21	Aircraft geospatial awareness systems (GPS, proximity sensors, transponder, etc.) provide position data in relation to terrain, airspace, aircraft, known enemy positions, and other obstacles that alerts the FO if safety thresholds are breached. Real-time airspace update service that can relay dynamically changing airspace/battlespace information to participating aircraft; data is pulled from high level server every X minutes to provide information to operators	ELIM	ELIM	4	3
			RM08	Aircraft health systems monitor aircraft performance, alert FO when unsafe scenarios are approaching (e.g. engine health in danger, airframe integrity compromised, combat system malfunctions/loss of effectiveness, etc.)			4	
			RM24	Design incremental control logic that prevents unintentional activation/deactivation of mission controls, such as those associated with weapons, self-defense, and reconnaissance	3		3	
CS 6.0.1	FO misses the checklist step to engage TCM due to increasing cognitive load from mission tasks and the the aircraft does not automatically launch effective countermeasures when engaged by enemy air defense assets. As a result, the aircraft is unable to conduct mission tasks.	1	RM23	Ensure ASEC alerts FO prior to entering hostile airspace if threat countermeasures are not engaged. System automatically activates the threat countermeasures systems if alert is not acknowledged by the FO without manual confirmation	ELIM	ELIM	4	4
CS 6.1.1	FO unintentionally engages TCMs due to a similarity in the control for a separate mission task before entering hostile territory. TCMs are then triggered by a false alarm (high safety but low reliability detection system) and expend flares that provide position intelligence to hostile scouts in a neighboring area, leading to an aborted mission for the FRWA which required the utmost stealth. As a result, the aircraft is unable to conduct mission tasks.	1	RM24	Design incremental control logic that prevents unintentional activation/deactivation of mission controls, such as those associated with weapons, self-defense, and reconnaissance	ELIM	ELIM	4	4
			RM21	Aircraft geospatial awareness systems (GPS, proximity sensors, transponder, etc.) provide position data in relation to terrain, airspace, aircraft, known enemy positions, and other obstacles that alerts the FO if safety thresholds are breached. Real-time airspace update service that can relay dynamically changing airspace/battlespace information to participating aircraft; data is pulled from high level server every X minutes to provide information to operators			4	
CS 6.2.1	FO engages TCM systems, but ASEC computers are powering back-up following an in-flight reboot due to a malfunction diagnosed by the operator. The TCM systems do not engage (e.g. pilot sends command to deploy chaff via PVI, but the self-defense computer is still restarting so the signal is not relayed). As a result, the aircraft is unable to conduct mission tasks.	1	RM43	Design aircraft TCM systems to be able to operate independently from ASEC in event of ASEC failure	ELIM	ELIM	4	4
			RM07	Provide FO with direct control of hardware that bypasses ASEC and/or allows FO to reset system (circuit breaker panels, kill switches, etc)			4	
CS 6.2.2	FO commands TCM systems to engage, but signals to ASEC are jammed/spoofed. There is a problem engaging TCM systems and aircraft cannot defend against enemy air defense. As a result, the aircraft is unable to conduct mission tasks.	1	RM06	Design the autonomous control system to be jam and spoof resistant	3	3	3	3
			RM07	Provide FO with direct control of hardware that bypasses ASEC and/or allows FO to reset system (circuit breaker panels, kill switches, etc)	3		3	

CS 6.3.1	FO receives incoming notification of enemy air threat but does not react in time to engage additional TCMs due to low resolution feedback [i.e. insufficient detail to adequately respond to the threat] from the alert system and the aircraft does not defend itself to the fullest extent and is damaged by enemy air defense assets. As a result, the aircraft is unable to conduct mission tasks.	1	RM31	Design critical flight components to be ballistically tolerant (e.g. fuel system, rotors, control linkages, etc.)	3	3	3	3
			RM44	Design TCM sensors that are high fidelity/reliability without blind spots with effective coverage overlap.	3		3	
CS 6.4.1	FO leaves TCMs engaged for too long and prematurely expends entire countermeasure inventory. As a result, the aircraft is no longer able to perform self-defense and conduct mission tasks.	1	RM24	Design incremental control logic that prevents unintentional activation/deactivation of mission controls, such as those associated with weapons, self-defense, and reconnaissance	3	4	3	3
			RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1		3	
CS 6.5.1	FO disengages TCMs before leaving hostile territory because FO believes he is outside of enemy threat range due to incorrect mental model of hostile systems maximum engagement range. The FRWA is then engaged by enemy air defense system when TCMs are off. As a result, the aircraft is unable to conduct mission tasks.	1	RM21	Aircraft geospatial awareness systems (GPS, proximity sensors, transponder, etc.) provide position data in relation to terrain, airspace, aircraft, known enemy positions, and other obstacles that alerts the FO if safety thresholds are breached. Real-time airspace update service that can relay dynamically changing airspace/battlespace information to participating aircraft; data is pulled from high level server every X minutes to provide information to operators	ELIM	ELIM	4	4
			RM08	Aircraft health systems monitor aircraft performance, alert FO when unsafe scenarios are approaching (e.g. engine health in danger, airframe integrity compromised, combat system malfunctions/loss of effectiveness, etc.)			4	
CS 7.0.1	FO commands ASEC to secure mission data, but ASEC does not perform operation correctly (power loss/spoofing/signal interception). As a result, information security is compromised.	1	RM16	ASEC detects any information security faults and relays them to FO (e.g. critical information not loaded correctly, crypto keys not rolling over at correct time, attempted jamming/spoofing, etc.)	2	5	1	1
			RM06	Design the autonomous control system to be jam and spoof resistant	3		1	
			RM14	Design redundant architecture for all critical control components to ensure proper operation (e.g. wireless signal equipment, control linkages, onboard wiring)	3		1	
CS 7.0.2	FO is incapacitated and cannot secure mission data (e.g. pilot(s) is killed in crash and cannot zeroize mission systems so adversary can recover secure information). As a result, critical information is compromised.	1	RM15	Data management system detects an emergency and purges critical information automatically (i.e. remote aircraft crash, incapacitated operator, etc.)	ELIM	ELIM	4	4
			RM01	Aircraft monitors pilot health/posture/attention and automatically engages autonomous mode when FO is incapacitated/task saturated/inattentive/fixated; system can also alert and allow a remote operator to take control			4	
CS 7.1.1	ASEC receives conflicting commands from FOs to load mission data. Another FO has taken temporary control of the FRWA before another FO takes over. Confusion over ongoing control authority ensues and a misunderstanding related to whether or not the appropriate mission data was loaded earlier on in the flight results in mission data that is compromised because enemy assets are able to decipher mission information from the unsecured communication. As a result, critical information is compromised	1	RM16	ASEC detects any information security faults and relays them to FO (e.g. critical information not loaded correctly, crypto keys not rolling over at correct time, attempted jamming/spoofing, etc.)	2	5	3	2
			RM13	Design control logic that aids in task prioritization, detects and prevents conflicting mission commands, and provides feedback indicating which control responsibilities are under ASEC/teaming control	3		2	
CS 7.1.2	FO believes mission data is secure but feedback is incorrect (e.g. when loading a mission plan, FO receives a false indication of secure comms because the system does not recognize/alert the FO if cryptographic keys are outdated or not, and makes what the FO believes are secure radio calls over unencrypted channels), which results in a loss of critical information.	2	RM16	ASEC detects any information security faults and relays them to FO (e.g. critical information not loaded correctly, crypto keys not rolling over at correct time, attempted jamming/spoofing, etc.)	ELIM	ELIM	4	4
CS 7.1.3	FO inputs commands to secure mission data to ASEC but commands are not received (e.g. spoofing/jamming prevents commands from being received during remote operation)	2	RM16	ASEC detects any information security faults and relays them to FO (e.g. critical information not loaded correctly, crypto keys not rolling over at correct time, attempted jamming/spoofing, etc.)	2	5	3	3
			RM06	Design the autonomous control system to be jam and spoof resistant	3		3	
CS 7.1.4	ASEC secures mission data when not commanded by FO (e.g. enemy spoofing signals trigger zeroization of data without command from FO), which results in a loss of critical mission information related to targets and grid coordinates needed to	2	RM20	Design safety interlock to prevent inadvertent zeroization of critical information	ELIM	ELIM	4	3
			RM18	Require a manual input from FO to verify/confirm recommended system response for all critical information related functions			4	
			RM06	Design the autonomous control system to be jam and spoof resistant			3	

	conduct the mission. As a result, critical information is compromised								
CS 7.1.5	FO does not update mission-related critical information correctly because he has a faulty mental model of when the update is supposed to occur. As a result, critical information is compromised (e.g. crypto rollover does not occur at the time believed by the FO and causes radio transmissions to become unencrypted and vulnerable to enemy intelligence)	1	RM16	ASEC detects any information security faults and relays them to FO (e.g. critical information not loaded correctly, crypto keys not rolling over at correct time, attempted jamming/spoofing, etc.)	ELIM	ELIM	4	4	
			RM18	Require a manual input from FO to verify/confirm recommended system response for all critical information related functions			4		
CS 7.1.6	FO secures mission data by mistake (e.g. pilot(s) engages zeroize function unintentionally due to lack of a safeguard/safety interlock on the control activation). As a result, critical information is compromised.	2	RM20	Design safety interlock to prevent inadvertent zeroization of critical information	ELIM	ELIM	4	4	
			RM18	Require a manual input from FO to verify/confirm recommended system response for all critical information related functions			4		

7.2.2 Hazard-Based Approach Results

Constraint		Hazard Link	Scenario Link	PMS	RM ID	Recommended Mitigation	MES	CMES	PPMS	CPMS
C1.1	Control inputs must be adequate to maintain aircraft controllability for manned flight	H1.1	2.0.1, 2.0.2, 2.0.5, 2.2.1, 2.5.1, 2.7.3, 2.8.2, 2.9.2, 3.5.1,	1	RM01	Aircraft monitors pilot health/posture/attention and automatically engages autonomous mode when FO is incapacitated/task saturated/inattentive/fixated; system can also alert and allow a remote operator to take control	ELIM	ELIM	4	3
					RM14	Design redundant architecture for all critical control components to ensure proper operation (e.g. wireless signal equipment, control linkages, onboard wiring)			3	
					RM03	Aircraft can autonomously execute specific flight maneuvers (e.g. return to base, climb/descend to specific altitudes, fly a specific straight-and-level profile, formation flight, reroute to designated airspace); maintains all structural limitations			3	
C1.2	Control inputs must be adequate to maintain aircraft controllability for unmanned flight	H1.2	2.2.1, 2.6.1, 2.7.3, 2.8.2, 2.9.2, 3.5.1,	1	RM02	Aircraft can be remotely controlled while in manned configuration	3	4	4	3
					RM03	Aircraft can autonomously execute specific flight maneuvers (e.g. return to base, climb/descend to specific altitudes, fly a specific straight-and-level profile, formation flight, reroute to designated airspace); maintains all structural limitations	3		3	
					RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1		3	
C1.3	Controller/hardware feedback must be adequate to maintain controllability	H1.3	2.0.3, 2.6.1, 2.7.3, 2.8.4, 2.9.1, 3.5.1,	1	RM05	Design salient PVI indications/alerts with high polling rates that combine audio, visual, and haptic feedback. An alerting schema/framework should be created utilizing context-specific alerts appropriate to the severity of the situation.	3	5	4	3
					RM08	Aircraft health systems monitor aircraft performance, alert FO when unsafe scenarios are approaching (e.g. engine health in danger, airframe integrity compromised, combat system malfunctions/loss of effectiveness, etc.)	2		3	
C1.4	Aircraft control architecture must not be susceptible to enemy action	H1.4	2.0.1, 2.1.1	1	RM06	Design the autonomous control system to be jam and spoof resistant	3	6	3	2
					RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1		3	
					RM01	Aircraft monitors pilot health/posture/attention and automatically engages autonomous mode when FO is incapacitated/task saturated/inattentive/fixated; system can also alert and allow a remote operator to take control	2		2	
					RM02	Aircraft can be remotely controlled while in manned configuration	3		2	
					RM03	Aircraft can autonomously execute specific flight maneuvers (e.g. return to base, climb/descend to specific altitudes, fly a specific straight-and-level profile, formation flight, reroute to designated airspace); maintains all structural limitations	3		3	
					RM31	Design critical flight components to be ballistically tolerant (e.g. fuel system, rotors, control linkages, etc.)	3		3	
C1.5	Control authority for flight systems must be properly exchanged	H1.5	2.7.2,	1	RM01	Aircraft monitors pilot health/posture/attention and automatically engages autonomous mode when FO is incapacitated/task saturated/inattentive/fixated; system can also alert and allow a remote operator to take control	2	ELIM	2	3

					RM32	Design flight/mission control systems to ensure appropriate control authority/information exchanges between controllers that satisfy required conditions for handoff	ELIM		4	
C1.6	Configuration must be appropriate for flight operations	H1.6		2	RM33	Aircraft must be able to detect and validate software and hardware configuration changes and notify operator. FO must acknowledge and verify all configuration prior to operation	ELIM	ELIM	4	3
					RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1		3	
C1.7	Aircraft safety measures must not affect controllability during flight operations	H1.7		1	RM07	Provide FO with direct control of hardware that bypasses ASEC and/or allows FO to reset system (circuit breaker panels, kill switches, etc)	3	3	2	2
					RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1		2	
C2.1	Maintenance procedures/health data collection must be adequate to maintain structural integrity	H2.1		1	RM08	Aircraft health systems monitor aircraft performance, alert FO when unsafe scenarios are approaching (e.g. engine health in danger, airframe integrity compromised, combat system malfunctions/loss of effectiveness, etc.)	2	6	4	3
					RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1		2	
					RM05	Design salient PVI indications/alerts with high polling rates that combine audio, visual, and haptic feedback. An alerting schema/framework should be created utilizing context-specific alerts appropriate to the severity of the situation.	3		3	
C2.2	Control algorithms must prevent maneuvers from exceeding structural limitations	H2.2	2.4.1, 2.4.2, 2.5.3, 2.7.1, 2.7.4,	2	RM03	Aircraft can autonomously execute specific flight maneuvers (e.g. return to base, climb/descend to specific altitudes, fly a specific straight-and-level profile, formation flight, reroute to designated airspace); maintains all structural limitations	ELIM	ELIM	4	4
C2.3	Controller/hardware feedback must be adequate to maintain structural integrity	H2.3	2.4.1, 2.5.2, 2.5.3, 2.7.1, 2.7.4, 2.8.1, 2.9.3,	2	RM05	Design salient PVI indications/alerts with high polling rates that combine audio, visual, and haptic feedback. An alerting schema/framework should be created utilizing context-specific alerts appropriate to the severity of the situation.	3	5	2	2
					RM08	Aircraft health systems monitor aircraft performance, alert FO when unsafe scenarios are approaching (e.g. engine health in danger, airframe integrity compromised, combat system malfunctions/loss of effectiveness, etc.)	2		2	
C2.4	Aircraft structural design must not be susceptible to enemy action	H2.4		1	RM08	Aircraft health systems monitor aircraft performance, alert FO when unsafe scenarios are approaching (e.g. engine health in danger, airframe integrity compromised, combat system malfunctions/loss of effectiveness, etc.)	2	5	3	3
					RM31	Design critical flight components to be ballistically tolerant (e.g. fuel system, rotors, control linkages, etc.)	3		3	
C3.1	Control inputs must be adequate to maintain separation standards for manned flight	H3.1	2.0.4, 2.3.1, 2.8.3, 3.0.2, 3.4.1,	1	RM01	Aircraft monitors pilot health/posture/attention and automatically engages autonomous mode when FO is incapacitated/task saturated/inattentive/fixated; system can also alert and allow a remote operator to take control	ELIM	ELIM	4	4
					RM05	Design salient PVI indications/alerts with high polling rates that combine audio, visual, and haptic feedback. An alerting schema/framework should be created utilizing context-specific alerts appropriate to the severity of the situation.	3		4	
C3.2	Aircraft must satisfy separation standards for intangible entities	H3.2	2.8.3, 3.0.1, 3.0.2, 3.3.1, 3.4.1, 5.5.1,	1	RM21	Aircraft geospatial awareness systems (GPS, proximity sensors, transponder, etc.) provide position data in relation to terrain, airspace, aircraft, known enemy positions, and other obstacles that alerts the FO if safety thresholds are breached. Real-time airspace update service that can relay dynamically changing airspace/battlespace information to participating aircraft; data is pulled from high level server every X minutes to provide information to operators	ELIM	ELIM	4	3
					RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1		3	
C3.3	Aircraft must satisfy separation standards for tangible entities	H3.3	2.0.4, 2.8.3, 3.1.1,	1	RM21	Aircraft geospatial awareness systems (GPS, proximity sensors, transponder, etc.) provide position data in relation to terrain, airspace, aircraft, known enemy positions, and other obstacles that alerts the FO if safety thresholds are breached. Real-time airspace update service that can relay dynamically changing	3	4	3	3

						airspace/battlespace information to participating aircraft; data is pulled from high level server every X minutes to provide information to operators				
					RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1		3	
C3.4	Control algorithm for flight maneuvers must maintain separation standards during autonomous flight	H3.4	2.3.1,	1	RM21	Aircraft geospatial awareness systems (GPS, proximity sensors, transponder, etc.) provide position data in relation to terrain, airspace, aircraft, known enemy positions, and other obstacles that alerts the FO if safety thresholds are breached. Real-time airspace update service that can relay dynamically changing airspace/battlespace information to participating aircraft; data is pulled from high level server every X minutes to provide information to operators	3	ELIM	4	4
					RM03	Aircraft can autonomously execute specific flight maneuvers (e.g. return to base, climb/descend to specific altitudes, fly a specific straight-and-level profile, formation flight, reroute to designated airspace); maintains all structural limitations	3		4	
C4.1	Component performance must maintain safe aircraft environment	H4.1		2	RM35	Design environmental control system (ECS) that can monitor and regulate aircraft air quality and temperature to ensure proper system operation and human performance. Alerts operator of any dangerous conditions that cannot be remedied by ECS (e.g. high altitude low air density)	3	5	3	3
					RM08	Aircraft health systems monitor aircraft performance, alert FO when unsafe scenarios are approaching (e.g. engine health in danger, airframe integrity compromised, combat system malfunctions/loss of effectiveness, etc.)	2		3	
C4.2	Aircraft must be properly configured for assigned mission flight profiles	H4.2		2	RM33	Aircraft must be able to detect and validate software and hardware configuration changes and notify operator. FO must acknowledge and verify all configuration prior to operation	2	6	3	3
					RM35	Design environmental control system (ECS) that can monitor and regulate aircraft air quality and temperature to ensure proper system operation and human performance. Alerts operator of any dangerous conditions that cannot be remedied by ECS (e.g. high altitude low air density)	3		3	
					RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1		3	
C4.3	Aircraft ergonomics must be sufficient for FO health/performance	H4.3		2	RM40	Cockpit ergonomics are suitable for manned operation. Adjustable seats and flight controls that can meet the requirements for XX% of the operator population	ELIM	ELIM	4	4
					RM41	Vibration and sound dampening equipment that nullifies negative frequencies to improve aircraft performance and operator well-being	ELIM		4	
C4.4	Aircraft environment must not be susceptible to enemy action	H4.4		1	RM42	Design the immediate structure around the cockpit to be ballistically tolerant and resistant to direct-energy weapons	3	3	3	3
					RM06	Design the autonomous control system to be jam and spoof resistant	3		3	
C4.5	Environmental controller feedback must be sufficient for Operator performance	H4.5		2	RM35	Design environmental control system (ECS) that can monitor and regulate aircraft air quality and temperature to ensure proper system operation and human performance. Alerts operator of any dangerous conditions that cannot be remedied by ECS (e.g. high altitude low air density)	3	3	3	3
C5.1	Mission system operation must be sufficient in preventing collateral damage/friendly fire	H5.1	4.1.1, 4.3.1, 5.4.1,	1	RM26	Design targeting system that compiles track and target information through sensor fusion (optical, IR, radar, force tracker, etc.) to meet attack criteria	3	6	4	3
					RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1		3	
					RM36	Battle damage assessment (BDA) system that is able to detect and relay status of weapons engagement when FRWA is not able to conduct own BDA	2		3	
C5.2	Friendly assets/non-combatants must remain outside mission system envelopes during system engagement	H5.2	4.1.2, 4.3.1,	1	RM26	Design targeting system that compiles track and target information through sensor fusion (optical, IR, radar, force tracker, etc.) to meet attack criteria	3	6	3	3
					RM21	Aircraft geospatial awareness systems (GPS, proximity sensors, transponder, etc.) provide position data in relation to terrain, airspace, aircraft, known enemy positions, and other obstacles that alerts the FO if safety thresholds are breached. Real-time airspace update service that can relay dynamically changing airspace/battlespace information to participating aircraft; data is pulled from high level server every X minutes to provide information to operators	3		3	

					RM22	Aircraft must automatically send identity/position messages to friendly forces when entering a new airspace, conducting mission tasks, experiencing in-flight emergencies, etc. (e.g. BlueForce Tracker, Link-16 messages)	3		2	
					RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1		3	
					RM37	Weapons systems can inform FO of potential collateral damage/friendly fire effects based on weapon type while meeting ROE requirements	2		4	
C5.3	Mission systems must not be unintentionally operated	H5.3	4.4.1, 5.4.1,	2	RM24	Design incremental control logic that prevents unintentional activation/deactivation of mission controls, such as those associated with weapons, self-defense, and reconnaissance	ELIM	ELIM	4	4
C6.1	Mission system configuration must be appropriate for mission requirements	H6.1	4.0.2, 4.5.1, 6.0.1, 6.4.1,	2	RM33	Aircraft must be able to detect and validate software and hardware configuration changes and notify operator. FO must acknowledge and verify all configuration prior to operation	2	3	3	3
					RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1		3	
C6.2	Communication between controllers must be sufficient for mission task requirements	H6.2	3.2.1, 5.0.1, 5.6.1,	2	RM26	Design targeting system that compiles track and target information through sensor fusion (optical, IR, radar, force tracker, etc.) to meet attack criteria	3	6	3	2
					RM13	Design control logic that aids in task prioritization, detects and prevents conflicting mission commands, and provides feedback indicating which control responsibilities are under ASEC/teaming control	3		3	
					RM29	Design high assurance communications network (similar to GPS satellites) that provides multiple paths to send and receive control signals to aircraft	3		3	
					RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1		2	
					RM09	Navigation/communication system notify and request confirmation from FO when entering/leaving airspace to automatically adjust radio frequencies and transponder codes	2		3	
C6.3	Clearance must be sufficient to conduct mission	H6.3		1	RM37	Weapons systems can inform FO of potential collateral damage/friendly fire effects based on weapon type while meeting ROE requirements	2	3	3	3
					RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1		3	
C6.4	Mission tasks must not be affected by enemy action	H6.4	4.2.1, 5.1.1, 6.2.2, 6.5.1,	1	RM31	Design critical flight components to be ballistically tolerant (e.g. fuel system, rotors, control linkages, etc.)	3	6	3	2
					RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1		3	
					RM30	Design critical mission systems and computers to be hardened against EMI	3		2	
					RM23	Ensure ASEC alerts FO prior to entering hostile airspace if threat countermeasures are not engaged. System automatically activates the threat countermeasures systems if alert is not acknowledged by the FO without manual confirmation	2		3	
					RM06	Design the autonomous control system to be jam and spoof resistant	3		3	
C6.5	Mission systems must not be inadvertently operated	H6.5	4.4.1, 6.1.1, 6.4.1,	1	RM24	Design incremental control logic that prevents unintentional activation/deactivation of mission controls, such as those associated with weapons, self-defense, and reconnaissance	ELIM	ELIM	4	4
					RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1		4	
C6.6	Control authority for mission systems must be properly exchanged	H6.6	4.0.4, 4.6.1,	2	RM32	Design flight/mission control systems to ensure appropriate control authority/information exchanges between controllers that satisfy required conditions for handoff	ELIM	ELIM	4	4
					RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1		4	

C6.7	Mission system feedback must be sufficient during flight	H6.7	3.2.1, 4.0.1, 4.0.3, 4.0.4, 4.5.1, 4.6.2, 5.6.1, 6.3.1,	2	RM26	Design targeting system that compiles track and target information through sensor fusion (optical, IR, radar, force tracker, etc.) to meet attack criteria	3	4	4	3	
					RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1				3
					RM13	Design control logic that aids in task prioritization, detects and prevents conflicting mission commands, and provides feedback indicating which control responsibilities are under ASEC/teaming control	3				4
C6.8	Environmental factors must not reduce mission system performance	H6.8	5.0.2,	2	RM38	Mission systems are able to operate in all environments; including extreme temperatures, degraded visual environments, inclement weather, and EMI	3	6	4	3	
					RM39	Performance evaluation system that can compute performance metrics and inform the FO as it relates to mission requirements; performance metrics include weapon envelopes, flight profiles, sensor capabilities, etc.	2				3
					RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1				3
C6.9	Mission tasks must be prioritized by controllers	H6.9	3.2.1, 4.0.4, 5.2.1,	2	RM13	Design control logic that aids in task prioritization, detects and prevents conflicting mission commands, and provides feedback indicating which control responsibilities are under ASEC/teaming control	ELIM	ELIM	4	4	
					RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)			4		
C6.10	Component performance must not impact mission system controller functions	H6.10	4.0.2, 4.5.1, 5.2.1, 5.3.1, 6.2.1,	2	RM14	Design redundant architecture for all critical control components to ensure proper operation (e.g. wireless signal equipment, control linkages, onboard wiring)	3	4	3	3	
					RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1				3
					RM27	Design mission systems with X seconds startup period and implement sensor feedback to alert the pilot of readiness status	3				3
C7.1	Critical information-related equipment must be able to secure critical information	H7.1	7.0.1, 7.1.4, 7.1.5, 7.1.6,	2	RM16	ASEC detects any information security faults and relays them to FO (e.g. critical information not loaded correctly, crypto keys not rolling over at correct time, attempted jamming/spoofing, etc.)	2	ELIM	2	2	
					RM14	Design redundant architecture for all critical control components to ensure proper operation (e.g. wireless signal equipment, control linkages, onboard wiring)	3				2
					RM31	Design critical flight components to be ballistically tolerant (e.g. fuel system, rotors, control linkages, etc.)	ELIM				4
C7.2	System must be able to secure critical information when FO is unable	H7.2	7.0.2, 7.1.1, 7.1.5,	1	RM16	ASEC detects any information security faults and relays them to FO (e.g. critical information not loaded correctly, crypto keys not rolling over at correct time, attempted jamming/spoofing, etc.)	2	ELIM	ELIM	1	3
					RM01	Aircraft monitors pilot health/posture/attention and automatically engages autonomous mode when FO is incapacitated/task saturated/inattentive/fixated; system can also alert and allow a remote operator to take control	ELIM			4	
					RM15	Data management system detects an emergency and purges critical information automatically (i.e. remote aircraft crash, incapacitated operator, etc.)				4	
C7.3	Communications/signals must be sufficiently encrypted to protect critical information	H7.3	7.0.1, 7.1.2,	1	RM16	ASEC detects any information security faults and relays them to FO (e.g. critical information not loaded correctly, crypto keys not rolling over at correct time, attempted jamming/spoofing, etc.)	2	ELIM	ELIM	2	2
					RM18	Require a manual input from FO to verify/confirm recommended system response for all critical information related functions	3			3	
					RM32	Design flight/mission control systems to ensure appropriate control authority/information exchanges between controllers that satisfy required conditions for handoff	ELIM			4	
					RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1			2	

C7.4	Control signal reception must be sufficient when handling critical information	H7.4	7.0.1,	1	RM16	ASEC detects any information security faults and relays them to FO (e.g. critical information not loaded correctly, crypto keys not rolling over at correct time, attempted jamming/spoofing, etc.)	2	6	3	2
					RM06	Design the autonomous control system to be jam and spoof resistant	3		3	
					RM14	Design redundant architecture for all critical control components to ensure proper operation (e.g. wireless signal equipment, control linkages, onboard wiring)	3		2	
					RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1		2	
C7.5	Critical information must be protected against enemy action	H7.5	7.0.1, 7.1.3, 7.1.4,	1	RM18	Require a manual input from FO to verify/confirm recommended system response for all critical information related functions	3	6	2	2
					RM06	Design the autonomous control system to be jam and spoof resistant	3		3	
					RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1		2	
C7.6	Critical information must not be inadvertently compromised	H7.6	7.1.6,	1	RM20	Design safety interlock to prevent inadvertent zeroization of critical information	ELIM	ELIM	4	2
					RM18	Require a manual input from FO to verify/confirm recommended system response for all critical information related functions	3		3	
					RM16	ASEC detects any information security faults and relays them to FO (e.g. critical information not loaded correctly, crypto keys not rolling over at correct time, attempted jamming/spoofing, etc.)	2		2	
					RM04	FO trained on proper preflight/flight/emergency procedures and techniques (e.g. correct checklist usage, simulator training, flight maneuvers, emergency prioritization, teaming procedures, maintenance, weapons procedures etc.)	1		2	

THE REST OF THIS PAGE LEFT INTENTIONALLY BLANK

7.3 DoD Risk Process and Application

7.3.1 Application in the DoD

The DoD engages in multiple programs that span across a massive \$1.6 trillion portfolio of defense system acquisitions that often continue to fall short of cost, schedule, and performance expectations [55]. In order to control risk within governmental projects, one approach the DoD has relied upon is its risk management guidelines defined in their latest Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs published in 2017. As a result, the DoD broadly seeks to apply risk matrices to address three key areas during risk analysis [6]:

- Estimate the likelihood the risk event will occur
- Estimate the possible consequences in terms of cost, schedule, and performance
- Determine the resulting risk level and prioritize for mitigation

Risk matrices help DoD decision makers address risk within their associated projects in a concise way. This thesis focuses its analysis on the systems safety related risks that contribute directly to performance risk at the program level and usually impact cost and schedule either directly or indirectly. Below is an example program risk matrix with expanded discussion of the identified risks for a new ram air turbine generator project [6, p. 69-73]. The same risks (in addition to others) could be discovered after analyzing the results of the STPA methodology and translating them more objectively onto the risk matrix. For example, what makes the likelihood associated with environmental temperature risk a “5” compared to the “3” ratings of the three other risks? Based on the authors’ research, a highly subjective analysis that relies on the knowledge or experience of the risk matrix developer is how ratings are typically assigned. One objective of this thesis is to inject more analysis, clarity, and objectivity into the process of risk matrix development.

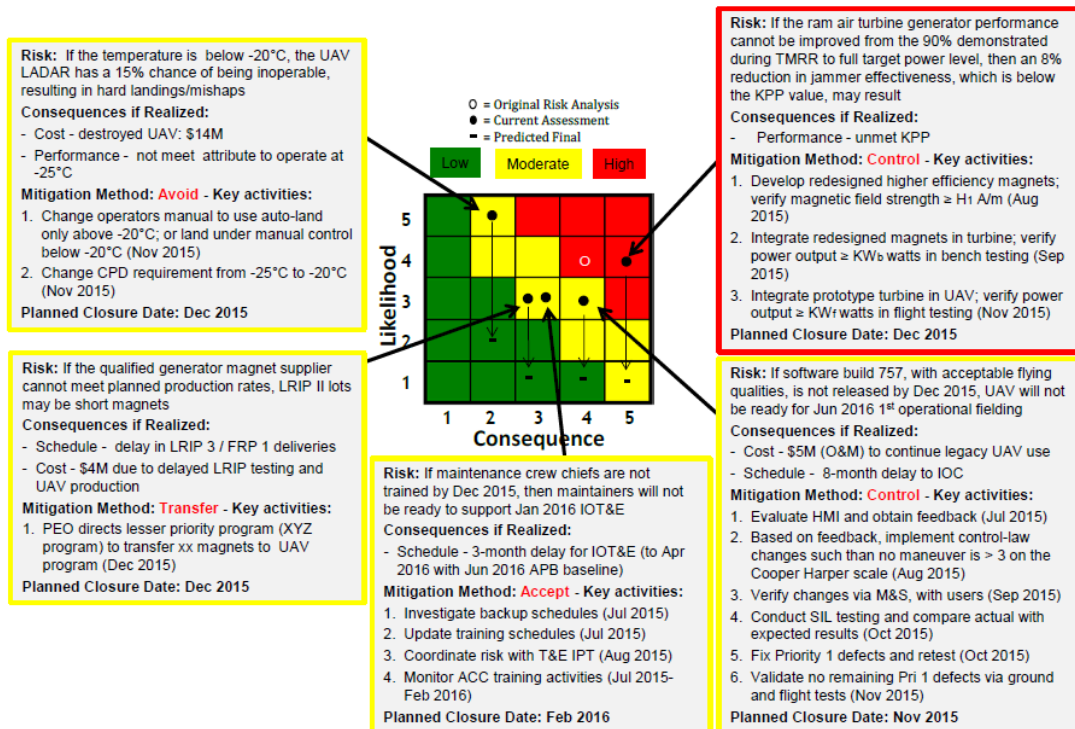


Figure 7-1: Ram Air Turbine Generator Risk Matrix Example

7.3.2 Risk Management Process

The DoD method of managing risk at the highest program level follows a five-step process. The process is applied to specific risks within a program and can be scaled as necessary within its scope. The method also

aims to determine what can go wrong and how to prevent that from happening. This approach is reviewed so readers understand how the MIL-STD-882E process fits into the DoD's overarching risk methodology.

1. Process Planning is the first step and covers the plan to mitigate individual risks within the program. It defines the administrative responsibilities, communication procedures, risk categories, and personnel training plans.
2. Risk Identification is next and simply asks the question: "What can go wrong?" This step is where planners brainstorm potential risks and their impact on the program. The goal is to delve into root causes that will guide the mitigation process.
3. Risk Analysis explores the likelihood and consequence of the identified risks. Both risk components are quantified using the scale described prior and assigned a color code (green, yellow, red) to highlight priority. Additionally, the analysis should include aggregate risk due to the individual risks of each component or phase of the program.
4. Risk Mitigation attempts to minimize or eliminate the analyzed risks associated with the program. A comprehensive plan is used to address feasibility, timing, impact, and expectations. This step is where planners decide if the risk is worth the required mitigation.
5. Risk Monitoring is required to determine the quality of the mitigation being implemented. The planners must address any emergent issues and evaluate what new mitigators may be necessary to reduce program risk further.

This five-step process is designed to be continuous with each step flowing logically into the next. The goal is for planners at each phase is to communicate freely with each other to address issues as they surface. Figure 7-2 below shows the five-step process [6].



Figure 7-2: Risk and Issue Management Process

While the DoD provides a risk process for acquisition programs, some branches utilize their own specific framework. For example, the Army's risk management process in Figure 7-3 is a similar but different five step process, which only serves as an example in this thesis to show the parallels to the process recommended by DoD and the slight differences in terminology [9]. The Army's emphasis on developing and implementing controls is like the control-focused methodology within STPA. For example, the Army's risk management process in Figure 2-6 is a similar but different five step process, which only serves as an example in this thesis to show the parallels to the process recommended by DoD and the slight differences in terminology [9]. The Army's emphasis on developing and implementing controls is like the control-focused

methodology within STPA. In this case, hazards lead to risks, instead of a risk being considered a more distinctly separate outcome.

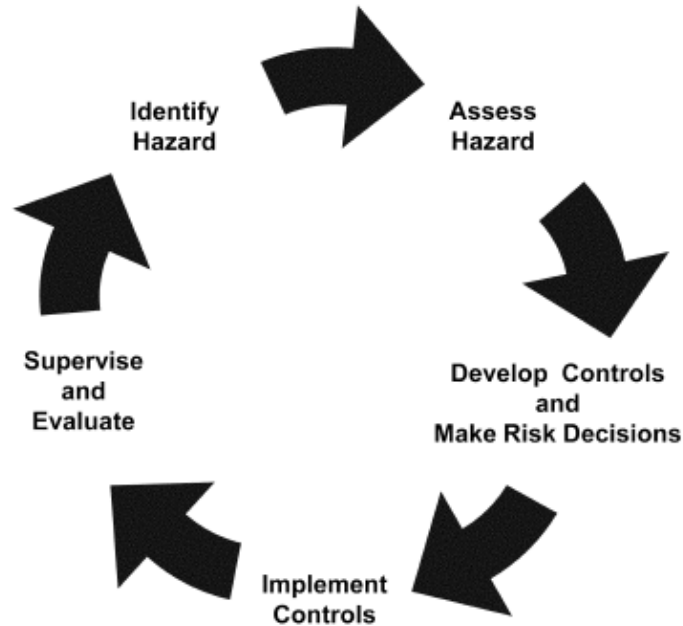


Figure 7-3: U.S. Army Risk Management Process

1. *Identify Hazard*: A hazard consists of three basic components, including a source, mechanism, and outcome, that are formed into a concise statement describing how a mishap can occur [9].
2. *Assess Hazard*: Assessment requires the assignment of a probability and severity level to the hazard to quantify the impact of the hazard. Categories of probability and severity are found in MIL-STD-882E. Probability and severity codes are combined into a matrix, generating Risk Assessment Codes (RACs).
3. *Develop Controls and Make Risk Decisions*: Once hazards are quantified and prioritized, controls are developed to mitigate remaining risk by reducing likelihood or eliminating them all together. Controls need to fit within the boundaries of the program or system and can include design selection, safety/warning devices, and/or training. Decision-making is the next part which requires an analysis of which controls are appropriate for the specific scenario.
4. *Implement Controls*: After the hazards are assessed and control decisions are made, the next steps are to determine how to fund the fix, develop an implementation action plan, and create a follow-up plan to ensure no new hazards emerge.
5. *Supervise and Evaluate*: The last step is to quality check the risk mitigation plan and determine what improvements can be made to further reduce risk or determine if any new hazards emerge and require a reassessment.

MIL-STD-882E incorporates an 8-element process more applicable to system safety related risk by including three extra steps associated with life-cycle management shown below in Figure 7-4 [11]. The DoD outlines all requirements for system safety in the MIL-STD-882E manual. Referred to as a “standard practice”, this document is the “key element of Systems Engineering (SE) that provides a standard, generic method for the identification, classification, and mitigation of hazards [11].” Other DoD instructions, specifically the DoDI 5000.02, reference MIL-STD-882E as the guideline to follow to assess system safety. The document establishes scope, supporting documents and definitions, general and detailed system safety requirements, and task sections to manage, analyze, evaluate, and verify system risk.

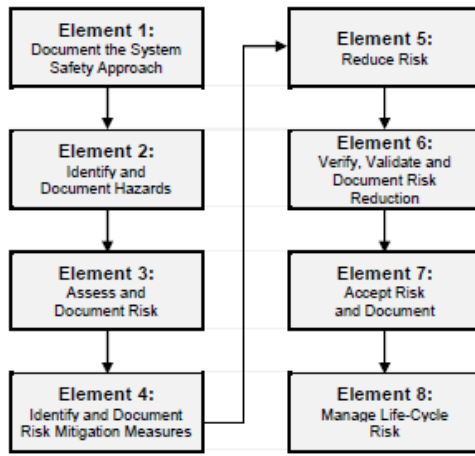


Figure 7-4: Eight Elements of the System Safety Process

MIL-STD-882E also includes the widely accepted definitions of severity and probability reviewed earlier in this chapter. Both measures of probability and severity are combined into a 4x6 risk assessment matrix (a variation from the typical 5x5). However, the overall process is nearly identical in execution and intent of managing and/or eliminating safety risk. Once severity and probability ratings are identified, the Risk Assessment Matrix (shown in Figure 7-5 below) is used to assign a Risk Assessment Code (RAC) [11]. For example, if a there is risk with severity 2 (*Critical*) and frequency of C (*Occasional*), then the RAC would be 2C (*Serious*).

RISK ASSESSMENT MATRIX				
SEVERITY \ PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

Figure 7-5: MIL-STD-882E Risk Assessment Matrix

Another interesting aspect of MIL-STD-882E is the inclusion of software control as a contributor to system safety risk because “software is generally application-specific and reliability parameters associated with it cannot be estimated in the same manner as hardware [11, p. 14-17].” In this case, there are 5 Software Control Categories from levels 1-5:

1. Autonomous (AT)
2. Semi-Autonomous (SAT)
3. Redundant Fault Tolerant (RFT)
4. Influential
5. No Safety Impact (NSI; No scientific justification for the association of these software control categories with risk).

Each of these control categories are then input into a Software Safety Criticality Matrix (SSCM, shown in Figure 7-6 below) which assigns Software Criticality Indices (SwCI), or tasks, that need to be performed to ensure confidence in the software [11]. The SwCIs are further defined by Levels of Rigor (LOR) that specify the depth of each analysis. Generally, as the system become more autonomous, more actions need to be performed to mitigate the software-related risk.

SOFTWARE SAFETY CRITICALITY MATRIX				
	SEVERITY CATEGORY			
SOFTWARE CONTROL CATEGORY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
1	SwCI 1	SwCI 1	SwCI 3	SwCI 4
2	SwCI 1	SwCI 2	SwCI 3	SwCI 4
3	SwCI 2	SwCI 3	SwCI 4	SwCI 4
4	SwCI 3	SwCI 4	SwCI 4	SwCI 4
5	SwCI 5	SwCI 5	SwCI 5	SwCI 5

SwCI	Level of Rigor Tasks
SwCI 1	Program shall perform analysis of requirements, architecture, design, and code; and conduct in-depth safety-specific testing.
SwCI 2	Program shall perform analysis of requirements, architecture, and design; and conduct in-depth safety-specific testing.
SwCI 3	Program shall perform analysis of requirements and architecture; and conduct in-depth safety-specific testing.
SwCI 4	Program shall conduct safety-specific testing.
SwCI 5	Once assessed by safety engineering as Not Safety, then no safety specific analysis or verification is required.

Figure 7-6: Software Safety Criticality Matrix

The final step is to associate the appropriate level of risk with each SwCI as shown in Figure 7-7 below [11, p. 23]. Higher risk is associated with higher SwCIs.

RELATIONSHIP BETWEEN SwCI, RISK LEVEL, LOR Tasks, AND RISK		
Software Criticality Index (SwCI)	Risk Level	Software LOR Tasks and Risk Assessment/Acceptance
SwCI 1	High	<ul style="list-style-type: none"> If SwCI 1 LOR tasks are unspecified or incomplete, the contributions to system risk will be documented as HIGH and provided to the PM for decision. The PM shall document the decision of whether to expend the resources required to implement SwCI 1 LOR tasks or prepare a formal risk assessment for acceptance of a HIGH risk.
SwCI 2	Serious	<ul style="list-style-type: none"> If SwCI 2 LOR tasks are unspecified or incomplete, the contributions to system risk will be documented as SERIOUS and provided to the PM for decision. The PM shall document the decision of whether to expend the resources required to implement SwCI 2 LOR tasks or prepare a formal risk assessment for acceptance of a SERIOUS risk.
SwCI 3	Medium	<ul style="list-style-type: none"> If SwCI 3 LOR tasks are unspecified or incomplete, the contributions to system risk will be documented as MEDIUM and provided to the PM for decision. The PM shall document the decision of whether to expend the resources required to implement SwCI 3 LOR tasks or prepare a formal risk assessment for acceptance of a MEDIUM risk.
SwCI 4	Low	<ul style="list-style-type: none"> If SwCI 4 LOR tasks are unspecified or incomplete, the contributions to system risk will be documented as LOW and provided to the PM for decision. The PM shall document the decision of whether to expend the resources required to implement SwCI 4 LOR tasks or prepare a formal risk assessment for acceptance of a LOW risk.
SwCI 5	Not Safety	<ul style="list-style-type: none"> No safety-specific analyses or testing is required.

Figure 7-7: Relationship Between Risk and SwCI

The important distinction with software-related risk is that this matrix is not identical to the typical 5x5 risk matrix. This table prescribes a series of tasks meant to mitigate risk, and highlights the consequences of negligence, instead of merely stating risk levels and their color codes. The benefit of incorporating STPA into the authors' methodology is that STPA includes risks related to software and cybersecurity in its approach, rather than treating it differently as discussed here in MIL-STD-882E.

7.3.3 Risk Assessment Process

The risk assessment process is a means to determine the risk level of a particular program or operation using qualitative and quantitative techniques. Each risk is defined by the probability and severity of it occurring and displayed in a matrix for ease of assessment and prioritization. The DoD Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs (DoD RIO) is the guiding doctrine on risk mitigation for DoD acquisitions. The DoD Standard Practice: System Safety, or MIL-STD-882E, is the document that focuses more on system-level risk analysis within specific acquisition programs and will be where this thesis focuses.

7.4 DoD Risk Documents

7.4.1 DoD Instruction 5000.02T, 5000.74, 5000.75, 5000.80, 5000.81

First Published by the DoD in 2015, the 5000.02T instructional is titled “Operation of the Defense Acquisition System” and incorporates seven total changes as of April 21, 2020 [56]. The DoDI 5000.02T has been established as a transitional document as of January 23, 2020 while the AE Office re-writes the 5000 Series of policy to apply the AAF. A more detailed table of the relationship between 5000.02T and the new policy is shown below in Table 7-1, where letters after the 5000 represent that they are currently being re-written [56].

DoDI 5000.02T, Operation of the Defense Acquisition System	Associated New Policy (Issuances with Lettered Extensions in Development)
Core Acquisition Policy (Paragraph 6, Procedures)	DoDI 5000.UG, “Major Capability Acquisition”
Enclosure 1. Acquisition Program Categories and Compliance Requirements -- Information Requirements Tables	<ul style="list-style-type: none"> • DoDI 5000.UG, “Major Capability Acquisition” • Tables “authorized by DoDI 5000.UG...” will be posted on the Adaptive Acquisition Framework website
Enclosure 2. Program Management	<ul style="list-style-type: none"> • DoDI 5000.UG, “Major Capability Acquisition” • DoDI 5010.44, “Intellectual Property,” October 16, 2019 has replaced “IP Strategy” (formerly Para 6.a.(4))
Enclosure 3. Systems Engineering	DoDI 5000.UJ, “Engineering”
<ul style="list-style-type: none"> • Enclosure 4. Developmental Test and Evaluation (DT&E) • Enclosure 5. Operational and Live Fire Test and Evaluation (OT&E and LFT&E) 	DoDI 5000.UF, “Test and Evaluation (T&E)”
Enclosure 6. Life-Cycle Sustainment	DoDI 5000.UG, “Major Capability Acquisition”
Enclosure 7. Human Systems Integration (HIS)	DoDI 5000.PR, “Human Systems Integration in Defense Acquisition”
Enclosure 8. Affordability Analysis and Investment Constraints	Replaced by direction in §807 of Public Law 114-328
Enclosure 9. Analysis of Alternatives (AoA)	Necessary information is in DoDD 5105.84 and the Defense Acquisition Guidance. Removal of this enclosure is in progress.

Table 7-1: Relationship Between DoDI 5000.02T and New Policy

DoDI 5000.02T serves as the primary risk management guidance within the 5000 series for Acquisitions programs, but DoDI 5000.74, 5000.75, 5000.80, and 5000.81 all provide similar (though much less detailed) supporting language towards conducting risk management.

DoDI 5000.02T policy establishes the PM as the individual “responsible for implementing effective risk management and tracking to include the identification of all known risks, key assumptions, probability of occurrence, consequences of occurrence (in terms of cost, schedule, and performance) if not mitigated, analysis of mitigation options, decisions about actions to mitigate risk, and execution of those actions [56, p. 82].” While risk matrices are not explicitly mentioned in DoDI 5000.02T, it does highlight that PMs are ultimately responsible for determining probability of occurrence and consequence of occurrence for each identified risk. Also, there are two risk management techniques that PMs must consider [56, p. 83]:

- Modeling and simulation (detailed in section 9 in Enclosure 3), to include the need for development of any new modeling and simulation tools to support a comprehensive risk management and mitigation approach.
- Independent risk assessments by outside subject matter experts.

7.4.2 Public Law 114-92, National Defense Authorization Act for FY16

The National Defense Authorization Act for FY16 approved on November 25, 2015 is statutory law that governs the military activities of the DoD, to include all acquisition related projects [57]. Section 822, paragraphs (a) and (b) require PMs to document a comprehensive approach for managing and mitigating risk (including technical, cost, and schedule risk) for all major defense acquisition programs and systems (this includes aircraft development programs as they are almost always categorized as ACAT I) [57, p. 900-902]. All aspects highlighted in the statutory law changes are reflected in DoDI 5000.02, and are discussed here to show how legislative mandates on the area of risk filter their way into DoD specific policy. The National Defense Authorization Act for FY16 approved on November 25, 2015 is statutory law that governs the military activities of the DoD, to include all acquisition related projects [57]. Section 822, paragraphs (a) and (b) require PMs to document a comprehensive approach for managing and mitigating risk (including technical, cost, and schedule risk) for all major defense acquisition programs and systems (this includes aircraft development programs as they are almost always categorized as ACAT I) [57, p. 900-902]. All aspects highlighted in the statutory law changes are reflected in DoDI 5000.02, and are discussed here to show how legislative mandates on the area of risk filter their way into DoD specific policy.

7.4.3 DoD Instruction 8510.01

First Published by the DoD in 2014, this instructional is titled “Risk Management Framework (RMF) for DoD Information Technology (IT)” and incorporates three changes since 2016 [58]. This document broadly establishes how to ensure confidentiality, integrity, and availability for all DoD IT programs, but does not once highlight or allude to the use of anything like a risk matrix. Designed to be complementary to all existing DoD acquisition management activities, the RMF focuses on a six-step process that manages information and cybersecurity risk (see Figure 7-8 below) [58]. All current and future development programs will consider the domain of cybersecurity risk, therefore understanding the related policy is important to the development of any new guidance. The use of STPA in the methodology discussed in Chapter 4 of this thesis also captures cybersecurity, in addition to traditional aspects of risk, thereby eliminating the need for separate policy or frameworks such as the RMF.

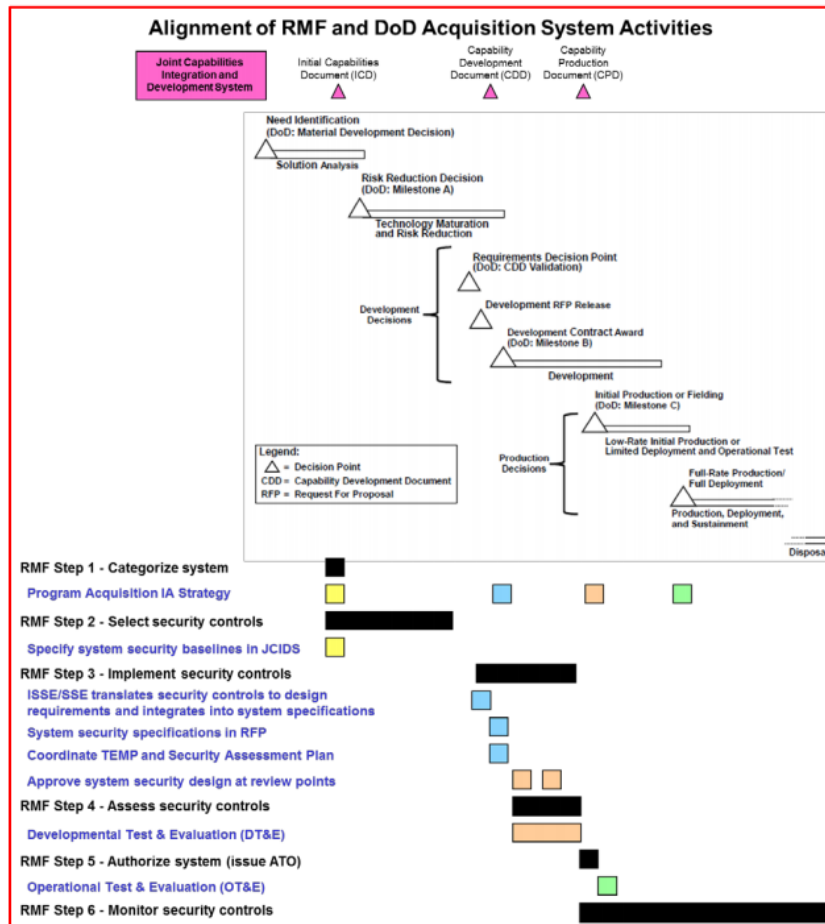


Figure 7-8: RMF and the Defense Acquisition Management System

7.4.4 NIST Special Publication 800-37

The National Institute of Standards and Technology (NIST) is an organization within the U.S. Department of Commerce that has published a Risk Management Framework for Information Systems and Organizations. This publication provides a seven-step process (see Figure 7-9 below) for risk management specifically applied more towards managing security and privacy risks risk to organizational operations, assets,

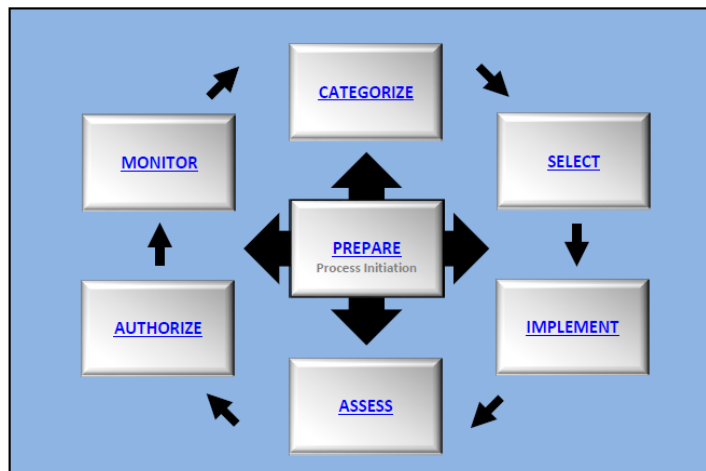


Figure 7-9: NIST 800-37 RMF

individuals, other organizations, and the Nation [59, p. 9]. This document is not mandatory policy but serves as a best practice for organizations to follow.

NIST 800-37 does not specifically mention the risk matrix as a tool for visualizing/managing risk, but rather focuses on describing the risk management process. In other words, very little in the form of concrete tools to assess, measure, visualize, and control risk are discussed. Because STPA is a formal methodology that can be used to address all types of systems, to include those surrounding privacy and security, the process introduced in this thesis can fully support more thorough risk assessment and requirements definition described by the NIST 800-37.

7.4.5 Air Force Program Risk Management

The Air Force is represented within the OASD by the Assistant Secretary of the Air Force for Acquisition, Technology, and Logistics. As the CAE for the branch, this individual oversees all acquisition activities with a total annual budget of \$60 billion across 550 acquisition programs [60]. The primary policy document used by the Air Force is Air Force Instruction (AFI) 63-101/20-101 on Integrated Life Cycle Management. Paragraph 4.6 of this document directs specific risk management requirements, chiefly that “the PM shall use the likelihood criteria, consequence criteria, and 5x5 risk matrix provided in Attachment 3 (of this AFI).” This document directs specific risk management requirements, chiefly that “the PM shall use the likelihood criteria, consequence criteria, and 5x5 risk matrix provided in Attachment 3 (of this AFI) [61, p. 37-41].” The risk matrix in this AFI similarly mirrors the figures shown in Section 2.2.

Additionally, Air Force Pamphlet (AFPAM) 63-128, covers Life Cycle Risk Management (LCRM) in great detail throughout Chapter 12. Section 12.2.4.6 mandates use of the same 5x5 risk matrix to assist decision makers with understanding programmatic risks, which is based on the DoD RIO [6]. The following table from AFPAM 63-128 explains the standard consequence with respect to performance, which is where significant system safety risks are categorized. This document is complementary to AFI 63-101 and provides additional guidance and recommendations to implementing life cycle management. AFPAM 63-128 mandates use of the same 5x5 risk matrix to assist decision makers with understanding programmatic risks, which is based on the DoD RIO [7, p. 96]. Table 7-2 below taken from AFPAM 63-128 explains the standard consequence with respect to performance, which is where significant system safety risks are categorized [7, p. 96].

Level	Standard AF Consequence Criteria - Performance
1	Minimal consequence to technical performance or supportability but no overall impact to the program success. A successful outcome is not dependent on this issue; the technical performance goals or technical design margins will still be met.
2	Minor reduction in technical performance or supportability, can be tolerated with little impact on program success. Technical performance will be below the goal or technical design margins will be reduced, but within acceptable limits.
3	Moderate shortfall in technical performance or supportability with limited impact on program success. Technical performance will be below the goal, but approaching unacceptable limits; or, technical design margins are significantly reduced and jeopardize achieving the system performance threshold values.
4	Significant degradation in technical performance or major shortfall in supportability with a moderate impact on program success. Technical performance is unacceptably below the goal; or, no technical design margins available and system performance will be below threshold values.
5	Severe degradation in technical performance or supportability, will jeopardize program success; or will cause one of the triggers listed below (Note 1)
Note 1: Any root cause that, when evaluated by the cross-functional team, has a likelihood of generating one of the following consequences is rated at Consequence Level 5 in Performance:	

Table 7-2: Standard AF Consequence Criteria for Performance

7.4.6 Army Program Risk Management

The Army is represented within the OASD by the Assistant Secretary of the Army for Acquisition, Logistics, and Technology (ASA(ALT)). As the CAE for the Army, he is the highest MDA for this branch and has the principal responsibility for all acquisitions and logistics related matters [62]. The ASAALT maintains oversight of 14 distinct PEOs and Joint PEOs. This organizational hierarchy relies upon branch-specific policy to manage risk.

Risk management within the Army is governed by three primary documents. DA PAM 385-16 is titled “System Safety Management Guide” and serves as the primary governing risk management document in terms of ESOH related risks [9]. The risk management process outlined is the same and states that “hazard risk, probability, and severity will be categorized according to MIL-STD-882E [9, p. 13]. DA-PAM 385-16 lends flexibility to programs to deviate from the MIL-STD matrix to develop one tailored to its specific needs per AR 70-1.

AR 70-1 is titled “Army Acquisition Policy” and is the Army’s subordinate policy to DoDI 5000.01 and 5000.02 on all research, development, and acquisition related activities [63]. AR 70-1 makes no mention of risk matrices or approval processes for alternative use cases. Rather, the document appears to have a circular loop of referencing another set of policies that then reference itself. For example, in *Para 4-10 e* on System Safety Management, two vague statements on risk are written followed by “refer to DoDI 5000.02, enclosure 3, DoDI 5000.69, AR 385-10, and DA PAM 385-16 [63].

Further guidance on how to specifically address programmatic related risks is not provided within AR 70-1 as it would seem to defer to higher DoD policy, such as the DoD RIO. While AR 385-30 titled “Risk Management” does include detailed discussion and use of risk matrices in Chapter 3, this document focuses on addressing operational risks once a system is fielded and is not directly applicable to the study of new development programs [64].

The discrepancy in risk assessment only highlights the subjective and imprecise nature of likelihood/probability assignment within DoD risk matrix development. The problem with lack of granularity in likelihood assignment and the overall flawed aspect of attempting to assign probability to risk events that have never been studied before (in complex new system development) is further compounded by differing definitions/ranges for probability within established Army vs. DoD policy.

7.4.7 Navy Program Risk Management

Within OASD, the Navy is represented by the Assistant Secretary of the Navy, Research Development, and Acquisition (ASN RDA) who oversees the System Command (SYSCOM) Commanders and PEOs [65]. The governing document for naval program risk management is the Naval SYSCOM Risk Management Policy Manual which established rules and responsibilities for all SYSCOMs and PEOs in Naval acquisition [66]. There are six SYSCOMs and 14 PEOs [66].

Each SYSCOM is responsible for full life-cycle support for military hardware and software, including research, development, procurement, testing, repair, and logistics support [67], while the PEOs are responsible for their respective programs. While the manual defines risk, management, and tracking procedures, it also highlights the importance of residual risk and the appropriate approval authorities. Residual risk is defined as the risk remaining after mitigating factors are implemented to manage the original risk [66, p. 4]. Each SYSCOM is responsible for full life-cycle support for military hardware and software, including research, development, procurement, testing, repair, and logistics support [66], while the PEOs are responsible for their respective programs.

SYSCOMs

MCSC	Marine Corps Systems
NAVAIR	Naval Air Systems
NAVFAC	Naval Facilities Engineering
NAVSEA	Naval Sea Systems
NAVSUP	Naval Supply Systems
NAVWAR	Naval Information Warfare Systems

PEOs

Aircraft Carriers
ASW, Assault, and Special Mission Programs
C4I
Enterprise Information Systems
Integrated Warfare
Joint Strike Fighter
Land Systems
Ships
Space
Space Systems
Strike Weapons and Unmanned Aviation
Submarines
Tactical Air Programs
Unmanned and Small Combatants

Table 7-3: U.S. Navy SYSCOMs and PEOs

The manual also includes a risk matrix, waterfall chart, and briefing procedures that standardize how to present program risk for all SYSCOMs and PEOs. Additionally, it provides a NAVAIR-specific risk matrix tailored for aircraft hazards. Each risk frequency is defined by mishaps/flight hour interval while severity is defined in terms of cost and injury. Flight hour intervals are divided into five categories and severity is divided into four as shown in Table 7-4 and Figure 7-10 [66, p. 21].

Frequency	Category	Mishap/ Flight Hour	Severity	Class	Damage	Injury
Frequent	A	>100/100K	Catastrophic	A	>\$1M	Fatal; Permanent Total Disability
Probable	B	10-00/100K	Critical	B	\$200K-\$1M	Permanent Partial Disability; >3 personnel hospitalized
Occasional	C	1.0-9.9/100K	Marginal	C	\$20K-\$200K	>1 workday lost
Remote	D	0.1-0.99/100K	Negligible	D	<\$20K	<1 workday lost
Improbable	E	<0.1/100K				

Table 7-4: Navy Risk Management Frequency and Severity Categories

NAVAIR SYSTEM SAFETY RISK MATRIX

HAZARD CATEGORIZATION		SEVERITY			
		CATASTROPHIC (1)	CRITICAL (2)	MARGINAL (3)	NEGLECTIBLE (4)
FREQUENCY	FREQUENT (A) = or > 100/100K flt hrs	1	3	7	13
	PROBABLE (B) 10-99/100K flt hrs	2	5	9	16
	OCCASIONAL (C) 1.0-9.9/100K flt hrs	4	6	11	18
	REMOTE (D) 0.1-0.99/100K flt hrs	8	10	14	19
	IMPROBABLE (E) = or < 0.1/100K flt hrs	12	15	17	20

UNACCEPTABLE

ASN/CNO / CMC/CFFC*
Acceptance
1-5 HIGH SAFETY RISK

**ACCEPTABLE
WITH REVIEW**

PM/TYCOM N43/WING CDR* Acceptance
11-17 MEDIUM SAFETY RISK

UNDESIRABLE

PEO/CFFC N43/TYCOM*
Acceptance
6-10 SERIOUS SAFETY RISK

**ACCEPTABLE
WITHOUT REVIEW**

PM/RMB Acceptance
18-20 LOW SAFETY RISK

* Fleet Acceptance for aircraft that have achieved IOC

Severity is the worst credible consequence of a hazard in terms of degree of injury, property damage or effect on mission defined below:

- Catastrophic** - Class A (damage > \$1M / fatality / permanent total disability)
- Critical** - Class B (\$200K < damage < \$1M / permanent partial disability / hospitalization of 3 or more personnel)
- Marginal** - Class C (\$20K < damage < \$200K / injury results in 1 or more lost workdays)
- Negligible** - All other injury/damage less than Class C

Probability of occurrence for discrete events may replace Frequency based upon the chart below:

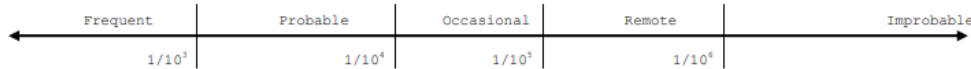


Figure 7-10: NAVAIR System Safety Risk Matrix

For NAVAIR system risk, a numerical value (like RAC from MIL-STD-882E) is assigned after determining frequency and severity and is used to determine risk level based on a four-level scale for approval authority, who ultimately decides to whether to accept the risk. An example risk acceptance table is shown below in Table 7-5.

Risk Level	RAC	Approval Authority
Unacceptable	1-5	ASN/CNO/CMC/CFFC
Undesirable	6-10	PEO/CFFC N43/TYCOM
Acceptable w/ Review	11-17	PM/TYCOM N43/WING CDR
Acceptable w/o Review	18-20	PM/RMB

Table 7-5: Risk Acceptance Table

8 REFERENCES

- [1] N. Leveson and J. Thomas, *STPA Handbook*. Cambridge, MA, USA, 2018. [Online]. https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf
- [2] “Emergent Behavior - Tool/Concept/Definition,” *Thwink*. <https://www.thwink.org/sustain/glossary/EmergentBehavior.htm> (accessed Feb. 02, 2021).
- [3] “Risk matrix literature review,” Risk Management Ltd, New Zealand, 2016. [Online]. Available: 882.
- [4] D. E. Hussey, “Portfolio analysis: Practical experience with the Directional Policy Matrix,” *Long Range Plann.*, vol. 11, no. 4, pp. 2–8, Aug. 1978, doi: 10.1016/0024-6301(78)90001-8.
- [5] D. A. Moore, “The use of a ranking matrix and recommendation prioritization system for process hazard analysis studies,” *Process Saf. Prog.*, vol. 16, no. 2, pp. 83–85, 1997, doi: 10.1002/prs.680160208.
- [6] Department of Defense, “DoD Risk, Issue, and Opportunity Management Guide.” DoD RIO, Washington, D.C., USA, 2017, Accessed: Feb. 01, 2021. [Online]. Available: <https://acqnotes.com/wp-content/uploads/2017/07/DoD-Risk-Issue-and-Opportunity-Management-Guide-Jan-2017.pdf>.
- [7] Department of the Air Force, “Integrated Life Cycle Management.” AF PAM 63-128, Washington, D.C., USA, 2014, Accessed: Jul. 07, 2020. [Online]. Available: https://static.e-publishing.af.mil/production/1/saf_aq/publication/afpam63-128/afpam63-128.pdf.
- [8] N. Leveson, “Improving the Standard Risk Matrix: Part 1,” Cambridge, MA, USA, Feb. 2019, p. 14, [Online]. Available: <http://sunnyday.mit.edu/Risk-Matrix.pdf>.
- [9] Department of the Army, “System Safety Management Guide.” DA PAM 385-16, Washington, D.C., USA, 2013, [Online]. Available: https://armypubs.army.mil/ebooks/DR_pubs/DR_a/pdf/web/p385_16.pdf.
- [10] “DoD Risk, Issue, and Opportunity Management Guide,” p. 96.
- [11] Department of Defense, “System Safety.” MIL-STD 882E, Washington, D.C., USA, 2012, [Online]. Available: <https://www.dau.edu/cop/armyesoh/DAU%20Sponsored%20Documents/MIL-STD-882E.pdf>.
- [12] Defense Acquisition University, “DAU News - How to Write a Good Risk Statement.” <https://www.dau.edu/library/defense-atl/blog/How-to-Write-a-Good-Risk-Statement> (accessed Jun. 29, 2020).
- [13] Alex Boydston, “Risk Management Interview,” Jun. 12, 2020.
- [14] Amy Alexander, “Risk Management Interview,” Jun. 24, 2020.

- [15] Claude Vance, “Risk Management Interview,” Jun. 18, 2020.
- [16] COL James Wilson, “Risk Management Interview,” Jun. 03, 2020.
- [17] Drake Mailes, “Risk Management Interview,” Jun. 22, 2020.
- [18] Edward Stanhouse, “Risk Management Interview,” Jun. 09, 2020.
- [19] Frank Kendall, “Risk Management Interview,” Jun. 09, 2020.
- [20] Jenn Ahearn, “Risk Management Interview,” Jul. 09, 2020.
- [21] Jennifer Gould, “Risk Management Interview,” Jun. 12, 2020.
- [22] LTC Dan Visosky, “Risk Management Interview,” Jun. 01, 2020.
- [23] MAJ Christopher Carson, “Risk Management Interview,” Jun. 02, 2020.
- [24] MAJ Hunter Gray, “Risk Management Interview,” Jun. 01, 2020.
- [25] MAJ Joe Robinson, “Risk Management Interview,” Jun. 03, 2020.
- [26] MAJ Sara Summers, “Risk Management Interview,” Jun. 16, 2020.
- [27] Meghan Ruddick, “Risk Management Interview,” Jun. 01, 2020.
- [28] Michael Beasley, “Risk Management Interview,” Jun. 11, 2020.
- [29] Michael Fitzgerald, “Risk Management Interview,” Jun. 10, 2020.
- [30] Paul Iguanti, “Risk Management Interview,” Jul. 29, 2020.
- [31] Ryan Petit, “Risk Management Interview,” Jun. 25, 2020.
- [32] Scott Hardiman, “Risk Management Interview,” Jun. 10, 2020.
- [33] Tim Watt, “Risk Management Interview,” Jun. 22, 2020.
- [34] Tom Chiang, “Risk Management Interview,” Jun. 10, 2020.
- [35] Tom Toner, “Risk Management Interview,” Jun. 04, 2020.
- [36] J. Talbot, “What’s right with risk matrices?,” *juliantalbot*, Jul. 09, 2017.
<https://www.juliantalbot.com/post/2018/07/31/whats-right-with-risk-matrices> (accessed Feb. 01, 2021).
- [37] “Utility Helicopter Project Office Risk Management Plan.” Department of Defense.

- [38] S. Hargreaves, "The battery that grounded Boeing," *CNNMoney*, Jan. 17, 2013. <https://money.cnn.com/2013/01/17/technology/boeing-battery/index.html> (accessed Jul. 30, 2020).
- [39] SC&H Group, "Risk and Control Matrix: A Powerful Tool to Understand and...", *SC&H Group*, Jul. 02, 2019. <https://www.schgroup.com/resource/blog-post/risk-and-control-matrix-a-powerful-tool-to-understand-and-optimize-your-organizations-risk-profile/> (accessed Feb. 02, 2021).
- [40] Federal Aviation Administration, "System Safety Handbook Chapter 3: Principles of System Safety." Washington, D.C., USA, Dec. 30, 2000, Accessed: Feb. 02, 2021. [Online]. Available: https://www.faa.gov/regulations_policies/handbooks_manuals/aviation/risk_management/ss_handbook/media/chap3_1200.pdf.
- [41] T. English, "Understanding Coaxial Rotor Helicopter Design," *Interesting Engineering*, Feb. 02, 2020. <https://interestingengineering.com/the-perfect-helicopter-understanding-coaxial-rotor-design> (accessed Oct. 07, 2020).
- [42] Gyrodyne, "Coaxial Benefits," *Gyrodyne Helicopters*, 2013. http://www.gyrodynehelicopters.com/coaxial_benefits.htm (accessed Oct. 07, 2020).
- [43] Cobham, "Cobham Mission Systems, Air-to-Air Refuelling, Aircraft Fuel Tanks," *Cobham Mission Systems*, Apr. 16, 2020. <https://www.cobhammissionsystems.com/air-to-air-refuelling/aircraft-fuel-tanks/> (accessed Oct. 07, 2020).
- [44] S. Hariram, P. Philipp, and D. Dummeyer, "AERO - Fire Protection: Engines and Auxiliary Power Units," *Boeing*, 2010. https://www.boeing.com/commercial/aeromagazine/articles/2010_q4/3/ (accessed Feb. 02, 2021).
- [45] Henley Honda, "Understanding Honda's Blind Spot Information System," *Henley Honda*, Apr. 14, 2019. <https://www.henleyhonda.com/2019/04/14/understanding-honda-blind-spot-information-system/> (accessed Sep. 16, 2020).
- [46] J. Beltz Snyder, "Toyota patents an A-pillar you can see through," *Autoblog*, Aug. 22, 2017. <https://www.autoblog.com/2017/08/22/toyota-patents-car-a-pillar-you-can-see-through/> (accessed Feb. 02, 2021).
- [47] K. Bell, "Toyota patent shows device that can make car pillars transparent," *Motor Authority*, Aug. 17, 2017. https://www.motorauthority.com/news/1112013_the-advantages-of-the-mercedes-benz-48-volt-system (accessed Feb. 02, 2021).
- [48] "Boeing 787-8 Dreamliner: Operating Manual and Checklists," *FlightGear wiki*, Jul. 04, 2015. http://wiki.flightgear.org/Boeing_787-8_Dreamliner:_Operating_Manual_and_Checklists (accessed Oct. 26, 2020).

- [49] S. Shappell, "Human Error and Commercial Aviation Accidents: A Comprehensive, Fine-Grained Analysis Using HFACS." Federal Aviation Administration, Jul. 2006, Accessed: Oct. 26, 2020. [Online]. Available: https://www.faa.gov/data_research/research/med_humanfacs/oamtechreports/2000s/media/200618.pdf.
- [50] MiliSource, *State-of-the-art Helicopter Simulator: UH-60 Black Hawk Aircrew Trainer*. 2017.
- [51] "“BAT’ Trainer Modernizes Helicopter Simulator Flying,” *U.S. DEPARTMENT OF DEFENSE*. <https://www.defense.gov/Explore/News/Article/Article/1157888/bat-trainer-modernizes-helicopter-simulator-flying/> (accessed Oct. 26, 2020).
- [52] M. Stipek, "Stock Photo - Adrenaline walking trail at the edge of steep cliff in Birg, near village of Murren, Switzerland," *123RF*. https://www.123rf.com/photo_117634939_adrenaline-walking-trail-at-the-edge-of-steep-cliff-in-birg-near-village-of-murren-switzerland.html (accessed Jan. 25, 2021).
- [53] H. Yahia and E. Fawzy, "Range Extender System for Electric Vehicles." Valeo, Mar. 2013, Accessed: Feb. 02, 2021. [Online]. Available: https://psas.scripts.mit.edu/home/wp-content/uploads/2013/04/02_Yahia_STAMP-STPA-case-study-on-Electric-vehicle-range-extender.pdf.
- [54] R. Cabosky, "A Human Factors Study on Vehicle Automation," M.S. Thesis, Dept. of Aeronautics and Astronautics, Massachusetts Institute of Technology, Cambridge, MA, USA, 2020.
- [55] Government Accountability Office, "U.S. Government Accountability Office (U.S. GAO)." <https://www.gao.gov> (accessed Jun. 05, 2020).
- [56] Department of Defense, "Operation of the Defense Acquisition Management System." DoD Instruction 5000.02T, Washington, D.C., USA, 2020, [Online]. Available: <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500002Tp.pdf?ver=2020-09-15-152849-783>.
- [57] 114th Congress, "National Defense Authorization Act for Fiscal Year 2016." PL 114-92, Washington, D.C., USA, 2016, Accessed: Jun. 18, 2020. [Online]. Available: <https://www.govinfo.gov/content/pkg/PLAW-114publ92/html/PLAW-114publ92.htm>.
- [58] Department of Defense, "Risk Management Framework for DoD Information Technology." DoD Instruction 8510.01, Washington, D.C., USA, 2020, Accessed: Feb. 02, 2021. [Online]. Available: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf?ver=qEE2HGN_HE4Blu7161t1TQ%3D%3D.
- [59] National Institute of Standards and Technology, "Risk management framework for information systems and organizations:: a system life cycle approach for security and privacy." NIST SP 800-37, 2018, doi: 10.6028/NIST.SP.800-37r2.

- [60] US Air Force, “Dr. Will Roper Bibliography.” <https://www.af.mil/About-Us/Biographies/Display/Article/1467795/dr-will-roper/> (accessed Feb. 02, 2021).
- [61] Department of the Air Force, “Integrated Life Cycle Management.” AFI 63-101/20-101, Washington, D.C., USA, 2020, [Online]. Available: https://static.e-publishing.af.mil/production/1/saf_aq/publication/afi63-101_20-101/afi63-101_20-101.pdf.
- [62] “About Us, OASA(ALT) Leadership,” *Assistant Secretary of the Army Acquisition, Logistics & Technology*. <https://www.asaalt.army.mil/About-Us/OASA-ALT-Leadership/> (accessed Jun. 24, 2020).
- [63] D. J. Reimer and J. B. Hudson, “AR 70-1 Research, Development, and Acquisition. Army Acquisition Policy.,” Defense Technical Information Center, Fort Belvoir, VA, Jan. 1998. doi: 10.21236/ADA343448.
- [64] Department of the Army, “Safety Risk Management.” DA PAM 385-30, Washington, D.C., USA, 2014, Accessed: Jul. 11, 2020. [Online]. Available: https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/p385_30.pdf.
- [65] “ASN(RDA) Overall Structure,” *Assistant Secretary of the Navy for Research, Development, and Acquisition*. <https://www.secnav.navy.mil/rda/Pages/ASNRDAOrgChart.aspx> (accessed Feb. 02, 2021).
- [66] Department of the Navy, “Naval SYSCOM Risk Management Policy.” NAVAIRINST 5000.21B, Washington, D.C., USA, 2008, Accessed: Feb. 01, 2021. [Online]. Available: <https://www.dau.edu/cop/risk/DAU%20Sponsored%20Documents/NAVSYSCOM%20RM%20Manual.pdf>.
- [67] “United States Navy Systems Commands,” *Wikipedia*. Dec. 28, 2020, Accessed: Feb. 01, 2021. [Online]. Available: https://en.wikipedia.org/w/index.php?title=United_States_Navy_systems_commands&oldid=996839589.