The FAA's Center of Excellence for UAS Research

ASSURE

Alliance for System Safety of UAS through Research Excellence

Drexel University | Embry-Riddle Aeronautical University | Kansas State Polytechnic | The Ohio State University | UND University of North Dakota

Identify Models for Advanced Air Mobility (AAM)/Urban Air Mobility (UAM) Safe Automation

Task 2: Risk and Technology Assessments

May 15, 2024

v 1.1

NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The U.S. Government assumes no liability for the contents or use thereof. The U.S. Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report. The findings and conclusions in this report are those of the author(s) and do not necessarily represent the views of the funding agency. This document does not constitute FAA policy. Consult the FAA sponsoring organization listed on the Technical Documentation page as to its use.

LEGAL DISCLAIMER

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 Federal Aviation Administration makes 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 Federal Aviation Administration or the U.S. Department of Transportation. Neither the Federal Aviation Administration nor the U.S. Department of Transportation 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 Federal Aviation Administration and U.S. Department of Transportation shall not be liable for any claim for any loss, harm, or other damages arising from access to or use of data or information, including without limitation any direct, indirect, incidental, exemplary, special or consequential damages, even if advised of the possibility of such damages. The Federal Aviation Administration shall not be liable to anyone for any decision made or action taken, or not taken, in reliance on the information contained herein.

TECHNICAL REPORT DOCUMENTATION PAGE

1. Report No. A64 A11L UAS 98	**2. Government Accession No.**	**3. Recipient's Catalog No.**
4. Title and Subtitle Identify models for Advanced Air Mobility (AAM)/Urban Air Mobility (UAM) safe automation		**5. Report Date** May 15, 2024
		6. Performing Organization Code
7. Author(s) Steven Weber, Philip J Smith, Stephen Rice, Paul Snyder, Mark Askelson, Ellen Bass, Tim Bruner, Sean Crouse, Abhinanda Dutta, Joseph Glavin, Tom Haritos, Kurtulus Izzetoglu, Ryan Lange, Andrew Leonard, Robbie Lunnie, Matt McCrink, Katie Silas, Richard Stansbury, Sreejith Vidhyadharan		**8. Performing Organization Report No.**
9. Performing Organization Name and Address Drexel University, Embry-Riddle Aeronautical University, Kansas State University, The Ohio State University, University of North Dakota		**10. Work Unit No.**
		11. Contract or Grant No. A64
12. Sponsoring Agency Name and Address Federal Aviation Administration		**13. Type of Report and Period Covered** Final
		14. Sponsoring Agency Code 5401

15. Supplementary Notes

16. Abstract
The focus of this project is on Advanced Air Mobility (AAM) and Urban Air Mobility (UAM) operations using Uncrewed Aircraft Systems (UAS) for passenger transport and cargo delivery in urban areas. Such operations are expected to involve significant amounts of machine automation in order for operations to be profitable, including automation to enable and support management of the remotely piloted aircraft by the pilot and to help ensure safety relative to Federal Aviation Administration (FAA) policies regarding the safety continuum. This research is evaluating AAM/UAM core technology, system architecture, automation design, and system functional concepts to aid the FAA and industry standards development organizations in creating paths forward for these new operational capabilities. This document reviews qualitative and quantitative risk assessment methodologies and demonstrates their application to AAM/UAM systems, design, and operation.

Urban Air Mobility, UAM, Advanced Air Mobility, AAM, automation, system safety, standards, policy	**18. Distribution Statement** No restrictions. This document is available through the National Technical Information Service, Springfield, VA 22161. Enter any other agency mandated distribution statements. Remove NTIS statement if it does not apply.

19. Security Classification (of this report) Unclassified	**20. Security Classification (of this page)** Unclassified	**21. No. of Pages** 65	**22. Price**

Form DOT F 1700.7 (8-72) Reproduction of completed page authorized

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF ACRONYMS

AAM	Advanced Air Mobility
ADS-B	Automatic Dependent Surveillance - Broadcast
AEEC	Airlines Electronic Engineering Committee
ASN	Aviation Safety Network
ASRS	Aviation Safety Reporting System
ATC	Air Traffic Control
ATM	Air Traffic Management
BVLOS	Beyond Visual Line of Sight
CAST	Causal Analysis Using System Theory
CC	Command and Control
CFR	Code of Federal Regulations
CONOPS	Concept of Operations
DA	Decision Analysis
DAA	Detect and Avoid
DFW	Dallas Forth Worth
EASA	European Union Aviation Safety Agency
EMS	Emergency Management System
ERAU	Embry Riddle Aeronautical University
EUROCAE	European Organization for Civil Aviation Equipment
EUROCONTROL	European Organization for the Safety of Air Navigation
FAA	Federal Aviation Administration
FCP	Flight Control Processor
FDR	Flight Data Recorder
FMEA	Failure Mode and Effects Analysis
FRAM	Functional Resonance Analysis Method
FSF	Flight Safety Foundation
GCS	Ground Control System
IATA	International Air Transport Association
ICAO	International Civil Aviation Organization
ID	Influence Diagram
IOSA	IATA Operational Safety Audit
IP	Internet Protocol
IPS	Internet Protocol Suite
KSU	Kansas State University
NAS	National Airspace System
NASA	National Aeronautics and Space Administration
NORDO	No Radio
NTSB	National Traffic Safety Board
OSU	Ohio State University
PRA	Probabilistic Risk Assessment
PSU	Passenger Service Unit
RA	Risk Assessment

RNP	Required Navigation Performance
RPIC	Remote Pilot In Command
SESAR	Single European Sky ATM Research
SME	Subject Matter Expert
SRA	Safety Risk Analysis
SRMP	Safety Risk Management Policy
STAMP	System-Theoretic Accident Model and Processes
STPA	System-Theoretic Process Analysis
TDD	Time-Division Duplexing
TMF	Traffic Management Function
TFR	Temporary Flight Restriction
TRSA	Terminal Radar Service Area
UAM	Urban Air Mobility
UAS	Unmanned Aircraft Systems; also Uncrewed Aircraft Systems
UAV	Unmanned Aircraft Vehicle
UND	University of North Dakota
VAR	Vertiport Arrival Rates
VDL	VHF Data Link
VHF	Very High Frequency
VDL2	VHF Data Link Mode 2
VTOL	Vertical Takeoff and Landing

EXECUTIVE SUMMARY

This report, the second deliverable for the ASSURE A64 project, addresses risk and technology assessment in the context of Advanced Air Mobility (AAM) and Urban Air Mobility (UAM), abbreviated AAM/UAM. It builds upon the first deliverable of A64, *i.e.*, the AAM/UAM background report.

This report investigates the applicability of both qualitative and quantitative risk assessment (RA) methodologies to AAM/UAM. Qualitative and quantitative RAs are complementary in nature, each offering distinct insights not directly obtainable by the other.

Qualitative RA methodologies are beneficial to AAM/UAM on account of their ability to uncover possible hazards and risks that may not have been otherwise easily discovered. There are many such methodologies in the literature; this report reviews several of them and applies them to the context of AAM/UAM. A key insight is that application of multiple methodologies is often beneficial as different methodologies uncover different hazards and risks, and no one methodology is guaranteed of uncovering them all. This conclusion is supported by empirical studies, *e.g.*, "A recent case study comparing FMEA [Failure Modes and Effects Analysis] and STAMP [System-Theoretic Accident Model and Processes] found that STPA [System-Theoretic Process Analysis] found 27% of hazards that were missed by FMEA. However, FMEA found 30% of hazards that were missed by STPA." [Thomas, STAMP] (Note, FMEA, STAMP, and STPA are each qualitative RA methodologies reviewed in Section 2 of this report.)

Furthermore, the strategic integrated use of complementary qualitative RA methodologies offers an approach to uncover hazards not identified by either of them individually. Consequently, it is recommended that multiple (and integrated) qualitative RA methodologies be employed in the design and operation of AAM/UAM.

Quantitative RA methodologies are also important in the context of AAM/UAM. As the name implies, these methodologies are able to provide quantitative measures of risk. However, it is evident that such outputs require data as input, *e.g.*, conditional probabilities for state evolution and/or exogeneous environmental risks. This data requirement poses a challenge in the context of AAM/UAM as the relevant data is not yet widely available (at least, not publicly available), primarily due to the technology being nascent and still under active development and testing.

Nonetheless, a second key insight of this report is that quantitative RAs for AAM/UAM are both feasible and insightful for important contexts by leveraging quantitative estimates on key inputs from subject matter experts (SMEs). This report demonstrates this process in the domain of flight scheduling and strategic deconfliction; the analysis concludes that the hazard likelihood in this scenario is substantial without effective mitigations. This plausible scenario used in this illustration highlights the potential of quantitative RA methods to play an integral role in the evaluation of proposed AAM/UAM operations.

1 INTRODUCTION

The focus of this report is on qualitative and quantitative risk assessment (abbreviated as RA) methodologies in the context of Advanced Air Mobility (AAM) and Urban Air Mobility (UAM), abbreviated as AAM/UAM.

The outline of the report is as follows:

1. Section 1 (this section) gives an introduction and overview;
2. Section 2 addresses qualitative RA;
3. Section 3 addresses quantitative RA;
4. Section 4 provides a conclusion and recommendations.

This section contains three sub-sections:

1. Section 1.1 reviews the Task 1 Background Report [Rice, 2023];
2. Section 1.2 previews Section 2 on qualitative RA;
3. Section 1.3 previews Section 3 on quantitative RA.

1.1 Review of Task 1 Background Report

The report [Rice, 2023] is a background report on the literature relevant to safety automation for AAM/UAM; it is the first deliverable of the A64 project and satisfies Task 1 of the A64 project. The report summarizes technical literature and subject matter expert (SME) insights on various systems and components of AAM/UAM, namely:

1. Detect and Avoid
2. Power and Propulsion
3. Airspace and Vertiport Design
4. Flight Planning and Strategic Deconfliction
5. Communications
6. Navigation and Surveillance
7. Standards
8. Concepts of Operations
9. Command and Control
10. Human-Automation Interaction
11. System Safety

Several of these topics merit brief comment; the interested reader is referred to the report for a much more thorough and complete discussion. First, Section 4 in Task 1, entitled "Flight Planning and Strategic Deconfliction," is especially important as it is the focus of one of the four applications in Section 2.2 and is the focus of the application in Section 3.2. Second, Sections 5-10 in Task 1 are each important as they are focal points of several of the applications in Section 2 "Qualitative risk assessment." Finally, Section 11 in Task 1, entitled "System Safety," is important as it the basis from which the RA methodologies are developed and applied to AAM/UAM in Sections 2 and 3 of Task 2 (this report).

1.2 Preview of Section 2: Qualitative Risk Assessment (RA)

A comprehensive review of qualitative RA is outside the scope of this report. As mentioned in the above review of the Task 1 background report [Rice, 2023], Section 11 on system safety in that report provides a high-level overview of the relevant literature on qualitative RA.

Instead, Section 2 of this report reviews several prominent and distinct qualitative RA methodologies and applies some of them to AAM/UAM. The reviewed methodologies are (listed alphabetically):

1. Causal Analysis Using System Theory (CAST)
2. Failure Mode and Effects Analysis (FMEA)
3. Functional Resonance Analysis Method (FRAM)
4. Influence Diagrams (ID)
5. System-Theoretic Accident Model and Processes (STAMP)
6. System-Theoretic Process Analysis (STPA)

These six (6) methodologies were selected for inclusion based on three factors: *i)* their estimated scope of impact in the field of qualitative RA; *ii)* their perceived relevance to AAM/UAM; and *iii)* their distinct and complementary natures.

1.3 Preview of Section 3: Quantitative Risk Assessment (RA)

As with qualitative RA, a comprehensive review of quantitative RA is outside the scope of this report, and the interested reader is referred to Section 11 on system safety in the Task 1 background report [Rice, 2023]. In contrast with qualitative RA, however, the scope of quantitative RA reviewed in this report is significantly narrower. In particular, the primary focus is on the quantitative RA methodology known as Decision Analysis (*e.g.*, [Muenning, 2017], [Parnell, 2013], [Raiffa, 1968]), abbreviated as DA.

While quantitative RA methodologies may yield impactful insights, possibly even more impactful than those obtained by qualitative RA, they are inherently reliant upon data availability for input. As data for AAM/UAM systems is not widely available, or at least not publicly available, as is natural for a nascent technology, this scarcity limits their applicability to AAM/UAM. **That said, as Section 3 demonstrates, it is possible to leverage quantitative RA methodologies in the absence of data by *i)* considering a specific (but representative) concept of operations (CONOPS), *ii)* obtaining the required numeric inputs from a subject matter expert (SME) and iii) performing a sensitivity analysis to determine how sensitive the overall risk assessment is to the SME provided values. This informs whether SME provided values are sufficient for assessing the risk or whether other data may be required.** In particular, Section 3 applies DA to a specific AAM/UAM CONOPS focused on flight scheduling and strategic deconfliction due to uncertain adverse weather, where the specific probabilities of the relevant events have been estimated by a SME with expertise in airline meteorology.

2 QUALITATIVE RISK ASSESSMENT (RA)

This section focuses on qualitative risk assessment (RA) methodologies; Section 3 addresses quantitative RA methodologies.

As mentioned in the qualitative RA preview in Section 1.2, this report reviews six (6) prominent qualitative RA methodologies (in Section 2.1), then applies several of them to four AAM/UAM case studies (in Section 2.2).

2.1 Selective review of qualitative risk assessment (RA) methodologies

As mentioned in the qualitative RA preview in Section 1.2, the methodologies reviewed in this report are (listed alphabetically):

1. Section 2.1.1: Causal Analysis Using System Theory (CAST)
2. Section 2.1.2: Failure Mode and Effects Analysis (FMEA)
3. Section 2.1.3: Functional Resonance Analysis Method (FRAM)
4. Section 2.1.4: Influence Diagrams (ID)
5. Section 2.1.5: System-Theoretic Accident Model and Processes (STAMP)
6. Section 2.1.6: System-Theoretic Process Analysis (STPA)

These six (6) methodologies were selected for inclusion on the basis of three factors: *i)* their estimated scope of impact in the field of qualitative RA; *ii)* their perceived relevance to AAM/UAM; and *iii)* their distinct and complementary natures.

2.1.1 Causal Analysis Using System Theory (CAST)

Causal Analysis Using System Theory, abbreviated as CAST, was developed by Professor Nancy Leveson (M.I.T.) as, quoting [Leveson CAST, 2019]:

> *"a structured approach...to identify the questions that need to be asked during an accident investigation and determine why the accident occurred."*

Importantly, CAST is intended as an analysis tool looking backward after an accident has occurred, while STPA (discussed below), also developed by Professor Leveson, is intended as a proactive tool to identify and mitigate risks, *i.e.*, before accidents occur. Moreover, as discussed below, both CAST and STPA are safety analysis methods that integrate seamlessly with the STAMP framework.

A centerpiece of the philosophy of CAST is that investigators should seek to learn as much information about an accident as possible, rather than presume the existence of, and reductively search for, a singular "root cause." Professor Leveson terms this reductive approach "root cause seduction and oversimplification of causality."

The five (5) parts of a CAST analysis are shown in *Figure 1* (taken from [Leveson CAST, 2019]).

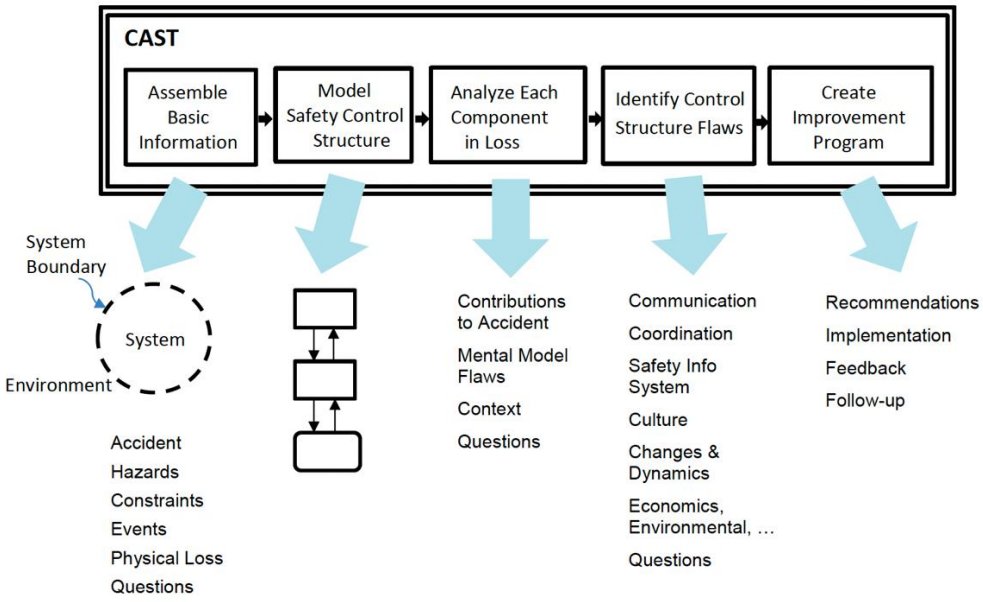

Figure 1: The five parts of a CAST analysis [Leveson CAST, 2019].

While CAST is included in the list of qualitative RA methodologies reviewed in this report on account of its importance and applicability, it is not used in this report's applications of qualitative RA to AAM/UAM on account of the fact that the authors do not have access to a specific AAM/UAM accident for analysis.

2.1.2 Failure Mode and Effects Analysis (FMEA)

Failure Mode and Effects Analysis (*e.g.*, [ASQ], [Stamatis, 2003], [Stamatis, 2015]), abbreviated as FMEA, is described by the American Society for Quality (ASQ) [ASQ] as follows:

> *"Begun in the 1940s by the U.S. military, failure modes and effects analysis (FMEA) is a step-by-step approach for identifying all possible failures in a design, a manufacturing or assembly process, or a product or service. It is a common process analysis tool."*

The general FMEA process involves many steps which are not listed here, but which are described in detail in the above references. A critical part of the process involves completing an FMEA form (table), such as the one shown in *Figure 2*, (taken from [ASQ]). As shown in the figure, the FMEA process requires enumeration of functions, identification of each function's potential failure modes, the effects of those failures, the potential causes of those failures, the process controls, the recommended actions, the responsibility for those actions and the target completion date, and the achieved results of those actions.

Function	Potential Failure Mode	Potential Effects(s) of Failure	S	Potential Cause(s) of Failure	O	Current Process Controls	D	RPN	CRIT	Recommended Action(s)	Responsibility and Target Completion Date	Action Results					
												Action Taken	S	O	D	RPN	CRIT
Dispense amount of cash requested by customer	Does not dispense cash	Customer very dissatisfied Incorrect entry to demand deposit system Discrepancy in cash balancing	8	Out of cash Machine jams Power failure during transaction	5 3 2	Internal low-cash alert Internal jam alert None	5 10 10	200 240 160	45 24 16								
	Dispenses too much cash	Bank loses money Discrepancy in cash balancing	6	Bills stuck together Denominations in wrong trays	2 3	Loading procedure (riffle ends of stack) Two-person visual verification	7 4	84 72	12 18								
	Takes too long to dispense cash	Customer somewhat annoyed	3	Heavy computer network traffic Power interruption during transaction	7 2	None None	10 10	210 60	21 6								

Figure 2: An FMEA form example, from [ASQ].

The FMEA RA methodology is employed in the analysis in Section 2.2.2 focused on flight planning & strategic deconfliction), along with ID.

2.1.3 Functional Resonance Analysis Method (FRAM)

Functional Resonance Analysis Method (*e.g.*, [Hollnagel, 2016], [Patriarca, 2020]), abbreviated as FRAM, was developed by Professor Erik Hollnagel. The following quote from [Hollnagel, 2016] helps position FRAM relative to other RA methodologies:

> *"...FRAM is a method to analyse how work activities take place either retrospectively or prospectively. This is done by analysing work activities in order to produce a model or representation of how work is done. This model can then be used for specific types of analysis, whether to determine how something went wrong, to look for possible bottlenecks or hazards, to check the feasibility of proposed solutions or interventions, or simply to understand how an activity (or a service) takes place. The FRAM is a method for modelling non-trivial socio-technical systems. It is NOT a risk assessment method and it is not an accident analysis method. Neither is a FRAM model a flow model, a network model, or a graph. But the model produced by a FRAM analysis can serve as the basis for a risk analysis, an event investigation, or for something entirely different."*

A FRAM analysis consists of the following steps, taken from [Hollnagel, 2016]:

1. *"Identify and describe essential system functions, and characterise each function using the six basic characteristics (aspects). In the first version, only use describe the aspects that are necessary or relevant. The description can always be modified later.*
2. *Check the completeness / consistency of the model.*
3. *Characterise the potential variability of the functions in the FRAM model, as well as the possible actual variability of the functions in one or more instances of the model.*

4. *Define the functional resonance based on dependencies / couplings among functions and the potential for functional variability.*
5. *Identify ways to monitor the development of resonance either to dampen variability that may lead to unwanted outcomes or to amplify variability that may lead to wanted outcomes."*

A critical part of FRAM is the specification of the six FRAM aspects (Step 1, above) to trigger a system function, as illustrated in *Figure 3*, taken from [Hollnagel, 2010].

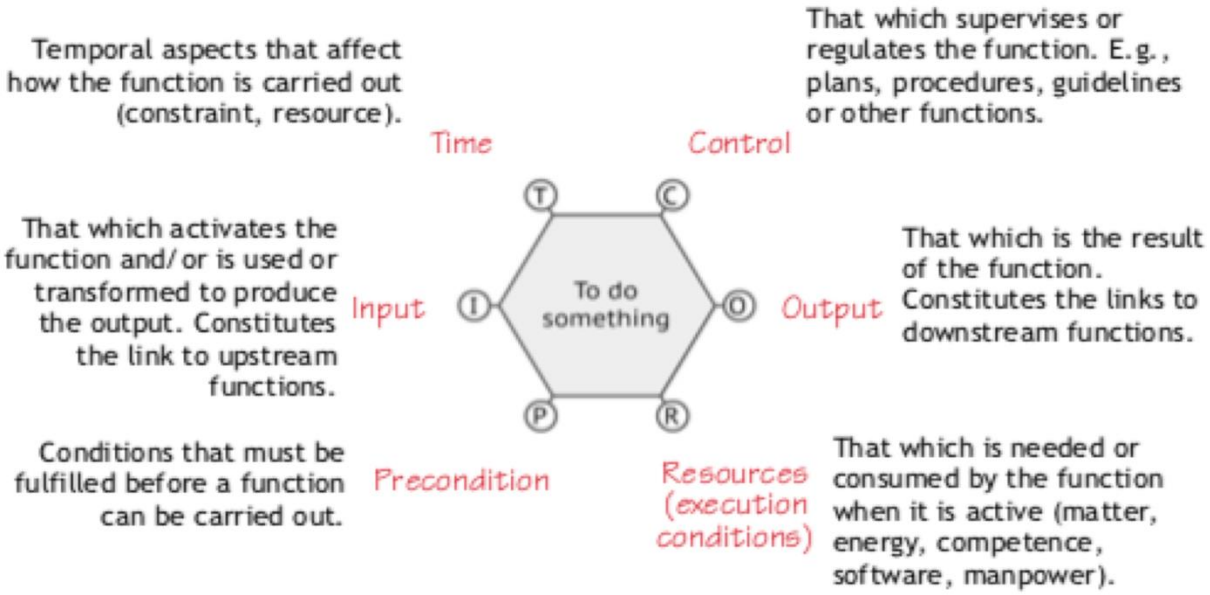

Figure 3: The six FRAM aspects of a function, from [Hollnagel, 2010].

FRAM is not explicitly used in any of the four applications in Section 2.2.

2.1.4 Influence Diagrams (ID)

Influence Diagrams (*e.g.*, [Shachter, 1986], [Howard, 2005], [Pearl, 2005]), abbreviated as ID, were developed in the 1970s out of the (quantitative) decision analysis research community. Quoting from [Howard, 2005], an influence diagram:

> *"...is at once both a formal description of the problem that can be treated by computers and a representation easily understood by people in all walks of life and degrees of technical proficiency. It thus forms a bridge between qualitative description and quantitative specification."*

As the quote makes clear, influence diagrams are at the intersection between qualitative and quantitative RA methodologies. In this paper, they are classified as qualitative methodologies, but are employed in close alignment with the quantitative methodology of decision analysis.

The ID RA methodology is employed in the analysis in Section 2.2.2 (flight planning & strategic deconfliction), along with FMEA.

2.1.5 System-Theoretic Accident Model and Processes (STAMP)

System-Theoretic Accident Model and Processes (*e.g.*, [Leveson STAMP, 2002], [Leveson STAMP, 2020], [Zhang, 2022]), abbreviated as STAMP, was developed by Professor Nancy Leveson (M.I.T.) as an accident model and process framework. Notably, it is *not* by itself intended for accident *analysis*, but is, instead, intended to serve as a "base layer" which may be profitably integrated with an accident analysis methodology, such as CAST (see above) or STPA (see below). The following quote (from [Leveson STAMP, 2002]) highlights the philosophy of STAMP:

> *"Accidents (loss events) occur when external disturbances, component failures, and/or dysfunctional interactions among system components are not adequately controlled, i.e., accidents result from inadequate control or enforcement of safety-related constraints on the development, design, and operation of the system.*
>
> *...Safety is managed by a control structure embedded in an adaptive socio-technical system. The goal of the safety control structure is to enforce safety-related constraints (1) on system development, including both the development process itself and the resulting system design, and (2) on system operation.*
>
> *In this framework, understanding why an accident occurred requires determining why the control structure was ineffective. Preventing future accidents requires designing a control structure that will enforce the necessary constraints."*

Figure 4, from [Leveson STAMP, 2020], illustrates the role of STAMP within the broader context of accident and hazard analysis.

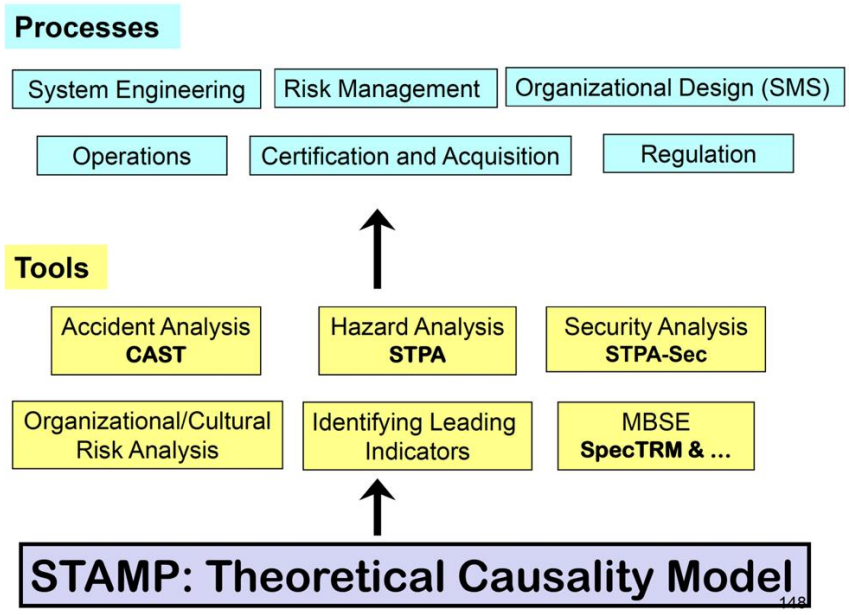

Figure 4: STAMP forms the basis for accident and hazard analysis [Leveson STAMP, 2020].

The three components of STAMP are: *i)* safety constraints, *ii)* hierarchical safety control levels, and *iii)* process control loops. In particular,

1. Safety constraints "specify those relationships between system variables that constitute the nonhazardous system states" [Leveson STAMP, 2002].

2. Hierarchical safety control levels capture the fact that "socio-technical systems can be modeled as a hierarchy of levels of organization with control processes operating at the interfaces between levels to control processes at the lower levels" [Leveson STAMP, 2002].
3. Process control loops "between the various levels of the hierarchical control structure create or do not handle dysfunctional interactions leading to violations of the safety constraints" [Leveson STAMP, 2002].

STAMP, as a basis underlying STPA, is employed in the analysis in Section 2.2.3 (Autonomous Command and Control (CC)) and Section 2.2.4 (Human-Automation Interaction and Human-Human Interaction).

2.1.6 System-Theoretic Process Analysis (STPA)

System-Theoretic Process Analysis (*e.g.*, [Leveson STPA, 2018]), abbreviated as STPA, is a hazard analysis technique created by Professor Nancy Leveson (M.I.T.). The novelty of STPA, relative to other hazard analysis techniques, is that it is (quoting from [Leveson STPA, 2018]):

> *"...based on an extended model of accident causation. In addition to component failures, STPA assumes that accidents can also be caused by unsafe interactions of system components, none of which may have failed."*

As mentioned above, *i)* STPA builds upon and integrates with the accident modeling methodology of STAMP, and *ii)* STPA is a (forward-looking, anticipatory) hazard analysis technique, while CAST, which also builds upon STAMP, is a (backward-looking, post-mortem) accident analysis technique.

Figure 5 shows the four steps of the STPA method (from [Leveson STPA, 2018]).

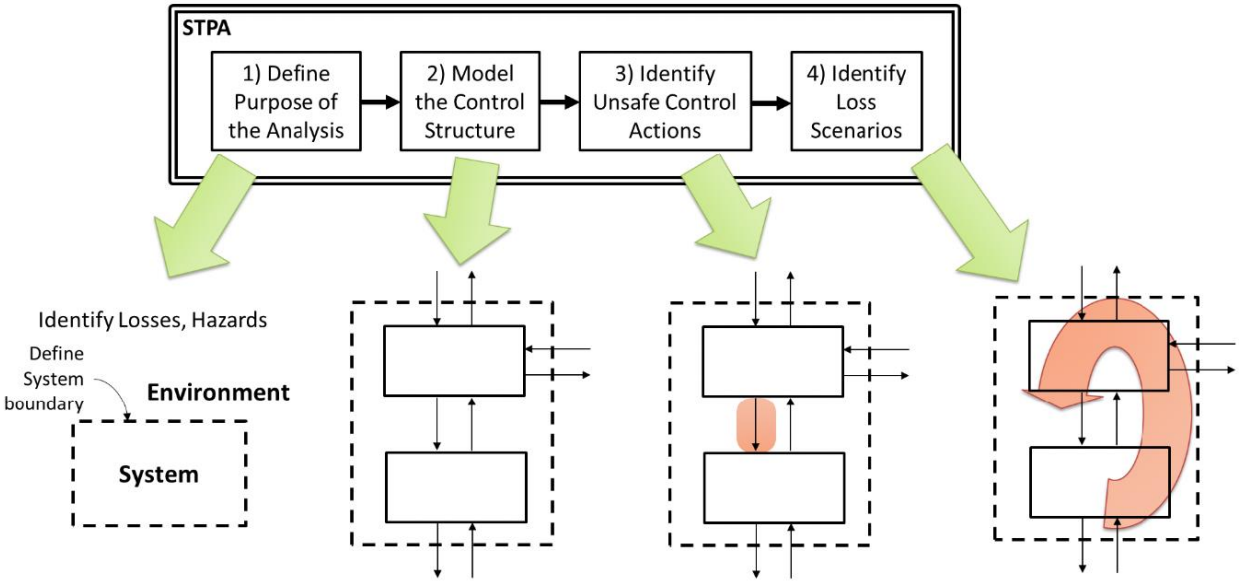

Figure 5: STPA method overview, from [Leveson STPA, 2018].

The asserted advantages of STPA, relative to other hazard analysis techniques, are its capabilities to (summarizing [Leveson STPA, 2018]):

1. Analyze very complex systems;
2. Integrate in early concept analysis;
3. Include software and human operators in the analysis;
4. Provide documentation of system functionality;
5. Integrate into system engineering processes.

STPA, building upon STAMP, is employed in the analysis in Section 2.2.3 (Autonomous command and control (CC)) and Section 2.2.4 (Human-Automation Interaction and Human-Human Interaction).

2.2 Application of Specific Qualitative RA Methodologies to AAM/UAM Systems

While Section 2.1 briefly summarizes the selected qualitative RA methodologies, this section applies them to different aspects of AAM/UAM hazard analysis. This section contains the following four sections:

1. Section 2.2.1: Detect and Avoid (DAA) Systems, Propulsion Systems, and Vertiport Operations
2. Section 2.2.2: Flight Planning & Strategic Deconfliction; Communications; Navigation & Surveillance
3. Section 2.2.3: Autonomous Command and Control (CC)
4. Section 2.2.4: Human-Automation Interaction and Human-Human Interaction

These four applications demonstrate the diverse ways qualitative RA methodologies may be applied to different aspects of AAM/UAM systems. In particular: Section 2.2.2 uses both FMEA and ID in an integrated manner, while Sections 2.2.3 and 2.2.4 use STAMP and STPA, again, in an integrated manner.

2.2.1 Detect and Avoid (DAA) Systems, Propulsion Systems, and Vertiport Operations

This first example of qualitative RA in the context of AAM/UAM focuses on three key areas of AAM/UAM design and operations, namely: *i)* detect and avoid systems, *ii)* propulsion systems, and *iii)* vertiport operations. This section contains the following sections:

1. Section 2.2.1.1: Introduction
2. Section 2.2.1.2: Scenario: Highlighting Systems Integration
3. Section 2.2.1.3: Scenario Specification
4. Section 2.2.1.4: Risk Assessment Method Used
5. Section 2.2.1.5: Results of Safety Risk Analysis (SRA)
6. Section 2.2.1.6: Dataset Development
7. Section 2.2.1.7: Benefits and Shortcomings of Risk Assessment Methodology

2.2.1.1 Introduction

To ensure a holistic approach to hazard identification, the researchers identified hazards and outcomes/harms associated with various failure scenarios and provided an analysis of the initial risk associated with each failure based on SMEs. Furthermore, researchers evaluated existing standards and used them to determine the risks associated with each failure more accurately. Lastly, the team identified current and future datasets that may further assist in providing more quantitative risk assessments. These datasets may assist researchers in further identifying gaps in standards/regulations/procedures and developing new datasets in future research.

2.2.1.2 Scenario: Highlighting Systems Integration

The scenario is built to identify the primary and subsequent failures of the related sub-systems. The scenario assumed flights took place under an established CONOPS, starting from a small rural town near an interstate system and connecting to a larger metropolitan hub where air service could continue through traditional airlines such as Delta or American Airlines.

This service entertained the model of legacy airlines supporting AAM/UAM operations by allowing customers to purchase tickets that would fly them from a small rural community to a metropolitan airport to transfer to existing airlines in a traditional airport environment. The CONOPs assumed flights originated in Class G (uncontrolled) airspace and arrived at an airport with a control tower within a Terminal Radar Service Area (TRSA). Furthermore, the scenario considered air traffic management, communication in a complex environment, and operation within existing aviation infrastructure.

The CONOPs assumed that all aircraft have some equivalent of *i)* Automatic Dependent Surveillance - Broadcast (ADS-B) in and out; *ii)* Detect and Avoid (DAA) systems that function per established consensus standards; and *iii)* automation to fly specified routes, departures, arrivals, taxiing on existing taxiways, and to fly contingency routes in case of an emergency. Predefined corridors restricted the airspace environment, and circular holding patterns around vertiports were predefined. Lastly, the flight planning required a flight operator to submit the proposed flight plan, indicating acceptable ranges for parameters, and submit proposed contingency flight plans. The software was available to evaluate the proposed flight plans. The scenario assumed Air Traffic Management (ATM) involvement and requisite training to expect the same standards for AAM/UAM vehicles as those of existing commercial aircraft. In this scenario, AAM/UAM vehicle propulsion systems met or exceeded current airworthiness standards for aircraft carrying passengers for hire.

2.2.1.3 Scenario Specification

The details and specifications of the scenario described in the previous section are as follows.

Thompson Vertiport: Located in Grand Forks County, the Thompson Vertiport is located approximately 5 miles south of Grand Forks, ND, and 2 miles east of Thompson, ND. It is 2,000 feet east of Interstate 29 at Exit 130. It has latitude 47.774230 and longitude -97.071579.

Fargo Vertiport: The Fargo Vertiport is in Cass County at the North General Aviation Ramp west of the Fargo Jet Center and east of the Arm/Disarm Pad at Hector International Airport. It is directly north of taxiway C3. It has latitude 46.930568 and longitude -96.811594.

Flight Profile Departure Procedures:
Takeoff from Thompson Vertiport.
Heading 145 degrees for 3 nm to waypoint 1 (latitude 47.73184, longitude -97.02162).
Heading 167 degrees for 49 nm to Hector International Airport.

Flight Profile Arrival Procedures:
Contact Fargo Approach 10nm north of the field.
Contact the tower before entering Class D airspace.
Use existing runways as vectors for low-level flight to taxiways.

Taxi (low-level flight) to vertiport using exiting taxiways and General Aviation ramp.
Land at Fargo Vertiport.

The aircraft can fly the Thompson to Fargo route in 25 minutes.

Altitude and Airspeed
Vertiport Operations - below 400 feet AGL.
Enroute operations - approximately 1500 – 4000 feet.
Lilliam eVTOL - max airspeed 155 mph - Thompson to Fargo route flown in 23 minutes.
Joby eVTOL - max airspeed 200 mph - Thompson to Fargo route flown in 18 minutes.
Archer Midnight eVTOL – cruise speed 150 mph, cruise altitude 2,000 feet.

2.2.1.4 Risk Assessment Method Used

In the ASSURE research project *A25: Develop Risk-Based Training and Standards for Waiver Review and Issuance* [Snyder, 2021] the team developed a prototype framework to address the consistency problem with Beyond Visual Line of Sight (BVLOS) waiver submission and review guidelines. The research team tested the results of this framework against an approved BVLOS waiver for validation purposes and conducted a tabletop exercise with key FAA stakeholders and multiple universities.

This framework created a list of key hazards associated with BVLOS waiver applications, laying a solid foundation for identifying potential failures for AAM/UAM operations. The team modified the framework from the traditional safety risk assessment requirements outlined in FAA's Order 8040.4C Safety Risk Management Policy (SRMP) [FAA 8040.4C] to meet the specific objectives of the current research project. As part of this modification, the initial risk associated with the outcome-harm noted in each column was evaluated based on the risk matrix chart for the FAAs Order 8040.6A and SMS Manual December 2022 for Air Traffic Organization (2022). While known gaps in standards exist because AAM/UAM is not yet a reality within the National Airspace System (NAS), the researchers evaluated existing standards cataloged as part of the ASSURE research project *A37: UAS Standards Tracking, Mapping, and Analysis* [Snyder, 2022] to identify existing mitigations related to each hazard and outcome/harm. This informed the SMEs on the failed system or subsystem's maturity and assisted the SME-based qualitative assessment of the risk associated with each hazard. This also provided a baseline for existing consensus standards to inform future research tasks requiring the identification of gaps in consensus standards. After identifying the initial risk associated with each identified outcome or harm, the researchers began to identify existing datasets and those needed to provide a more quantitative assessment instead of a qualitative one.

After addressing the hazards that were identified through previous research under A25 [Snyder, 2021], the researchers continued to evaluate additional hazards associated with the scenario using other resources, such as:

1. FAA Order 8040.6A "Unmanned Aircraft Systems (UAS) Safety Risk Management (SRM) Policy" [FAA 8040.6A], in particular, Appendix B of that report on "UAS Hazards, Mitigations, and Outcomes";

2. Lange, “Modeling a System of Systems for Advanced Air Mobility” in the *Journal of Air Transport Management* [Lange, 2024];
3. Arel, "Safety Management System Manual," by *Air Traffic Organization* [Arel, 2022].

These resources further refined possible fundamental failure modes within the scenario(s). Lastly, researchers assigned each hazard a category. This enabled additional sorting and analysis of the data. The team organized hazards into five categories for evaluation:

1. Technical Issue UAS (TI)
2. Human Error (HE)
3. Adverse Operating Conditions (AC)
4. Unable to See and Avoid (SA)
5. UAS Operations (OU).

Critical systems evaluated by the team were DAA, propulsion, and vertiport related.

2.2.1.5 Results of Safety Risk Analysis (SRA)

Based on the five key categories listed in the previous section, the research team identified 76 hazard conditions. For each hazard condition, subject matter experts (SMEs) identified the most credible outcome or harm. While conducting the risk assessment using the two risk matrix charts used, the risk value varied based on what risk matrix chart used. This variance further validated the need for a more objective, quantitative risk assessment method. Of the 76 hazard conditions, researchers linked 156 existing standards and procedures to the various hazard conditions and listed them as mitigations to reduce the risk associated with the outcome or harm. Many existing standards or procedures appeared for multiple entries, reflecting the importance of that standard or procedure to maintain safety and mitigate risk. It also identified the lack of existing standards or procedures related to many credible outcomes that could result from the hazards identified.

This risk assessment, in the form of a Microsoft Excel spreadsheet, accompanies this report as a supplemental document.

It was further determined that few quantitative datasets are available to identify the likelihood or probability of failures to validate subject matter experts' determinations.

2.2.1.6 Dataset Development

Within the SRA document, for each outcome or harm, the subject matter experts identify datasets, if any, that were available that might assist efforts in quantitative assessment and future probabilistic risk assessment (PRA) efforts for future tasks. In addition to the SME input, additional references were made to the following organizations as potentially able to provide datasets that might help in future quantitative risk assessments:

1. Section 2.2.1.6.1: Federal Aviation Administration (FAA)
2. Section 2.2.1.6.2: National Traffic Safety Board (NTSB)
3. Section 2.2.1.6.3: International Civil Aviation Organization (ICAO) Annex 13
4. Section 2.2.1.6.4: European Organization for the Safety of Air Navigation (EUROCONTROL)
5. Section 2.2.1.6.5: Flight Safety Foundation (FSF)
6. Section 2.2.1.6.6: Aviation Safety Network (ASN)
7. Section 2.2.1.6.7: International Air Transport Association (IATA)

These seven organizations are discussed in turn in the following sections.

2.2.1.6.1 Federal Aviation Administration (FAA)

Part 830 of the U.S. Code of Federal Regulations (CFR) is integral to the operations of the FAA and NTSB, as it sets procedures for dealing with aviation accidents and incidents. Key aspects of these procedures include immediate notifications to the NTSB for specific accidents, criteria to distinguish between accidents and incidents, and mandates for preserving crucial evidence such as aircraft wreckage, mail, cargo, and uncrewed aircraft. Additionally, guidelines are provided for reporting overdue aircraft, and the aircraft operators must submit detailed reports encompassing information about the aircraft, crew, flight, and the event itself. These regulations also needed filing a report by the pilot, detailing their perspective and operational conditions of the event. Witness statements and interviews are also collected as part of the investigative process. The analysis of data from flight recorders, weather conditions at the time of the incident, and medical or pathological information in the event of injuries or fatalities are crucial elements of the data collection. This systematic approach to gathering diverse information ensures a thorough investigation, contributing significantly to advancements in aviation safety and understanding the dynamics of aviation accidents and incidents.

The pilot's report, mandated by Part 830 of the U.S. CFR, is a comprehensive document that covers various aspects of an aviation incident or accident. It includes the pilot's identification (name, contact, license details, and flying experience), detailed aircraft information (make, model, registration, maintenance history), and specifics of the flight (flight number, type, route, departure, and destination). The report details a chronological sequence of events, weather conditions experienced, and the operational state of the aircraft (altitude, speed, configuration). It also encompasses the aircraft's performance, noting any system malfunctions, and records important communications with air traffic control. The pilot's actions and responses to the situation, execution of emergency procedures, and any resulting injuries or fatalities are also documented. Additionally, it includes the pilot's observations and any post-incident actions taken, offering valuable insights and personal viewpoints that are crucial for understanding and investigating the incident thoroughly.

2.2.1.6.2 National Traffic Safety Board (NTSB)

In aviation accident investigations, the National Transportation Safety Board (NTSB) collects a diverse range of data to ascertain the causes of the incident [NTSB, 2002], [NTSB, 2006]. This includes collecting physical evidence from the crash site, analyzing data from flight recorders like the cockpit voice and flight data recorders, and gathering operational information such as flight plans and maintenance records. They also consider meteorological data, pilot backgrounds, eyewitness testimonies, and survivability aspects of the accident. Additionally, the NTSB evaluates organizational and management practices of the involved airline, delves into human factors analysis, and reviews post-accident emergency responses. This multifaceted approach is detailed in the NTSB's *Accident Investigator's Handbook* [NTSB, 2002], which outlines their comprehensive investigation processes and methodologies. When compared to NTSB, Part 830 primarily provides the basic procedural framework for reporting and initial handling of aviation accidents and incidents. It outlines requirements for notification, classification of accidents and incidents, and preservation of evidence. NTSB's investigation approach delves deeper into the methodology of investigating an accident. It covers comprehensive data collection, detailed analysis of various factors (like human factors, organizational practices, and technical aspects),

and the development of safety recommendations. NTSB aiming to uncover the underlying causes of the accident and provides recommendations to enhance future aviation safety.

2.2.1.6.3 International Civil Aviation Organization (ICAO) Annex 13

International Civil Aviation Organization (ICAO)'s *Directive Annex 13* lays out global standards and practices for the investigation of aircraft accidents and incidents. The initial focus of the investigation is on gathering comprehensive details of the incident, including the specific circumstances of the accident, such as its date, time, and location. Investigators also collect extensive data on the aircraft involved, encompassing its type, model, registration, and maintenance history. The flight details, including the crew's composition, flight plan, cargo, passenger list, and intended route, are crucial. Additionally, the accident site is meticulously examined, with a focus on the wreckage distribution and impact marks. Weather conditions at the time and any relevant meteorological information are also gathered, alongside data from air traffic services, which include communication logs and radar tracking.

Further into the investigation, data from the aircraft's flight recorders, including the cockpit voice recorder and flight data recorder, are analyzed. Witness statements and interviews from those who observed the incident are crucial for providing a firsthand account. The investigation also delves into the crew's background, examining their training, experience, medical conditions, and overall performance. The performance of the aircraft itself during the flight is scrutinized using available data and simulations. Important too are the survival aspects, which look at the efficacy of safety equipment and emergency response. Additionally, an examination of the organizational and management structures of the entities involved in operating the aircraft is conducted. Human factors analysis is integral, assessing the role of human performance and potential errors. Based on these comprehensive investigations, recommendations are formulated to enhance aviation safety and prevent future incidents, ensuring the continual improvement of global aviation standards.

2.2.1.6.4 European Organization for the Safety of Air Navigation (EUROCONTROL)

The European Organization for the Safety of Air Navigation (EUROCONTROL) approach is similar to the standards set by the International Civil Aviation Organization (ICAO), ensuring consistency and effectiveness in aviation safety procedures across member states. EUROCONTROL provides a framework for the systematic reporting of aviation incidents and accidents. This involves specifying what types of events need to be reported, how they should be documented, and the timelines for reporting. The organization emphasizes the collection and analysis of data related to aviation incidents and accidents. This includes operational data, flight data, maintenance records, and witness statements, among others.

2.2.1.6.5 Flight Safety Foundation (FSF)

The Flight Safety Foundation (FSF) engages in extensive data collection and analysis to improve aviation safety [FSF AD]. This aspect of their work is crucial for identifying safety trends, risk factors, and areas for improvement in aviation FSF collects data from a variety of sources within the aviation industry. This includes incident and accident reports, flight data recorder (FDR) readings, pilot reports, air traffic control records, and maintenance logs. They also gather information from aviation regulatory bodies, airline operators, and other industry stakeholders. A significant part of their data analysis focuses on examining incidents and accidents. They look into the causes, contributing factors, and the sequence of events leading up to these occurrences. By

analyzing this data, FSF can identify common trends and areas of risk in aviation operations. FSF analyzes data to identify safety trends over time. This can include studying the frequency of certain types of incidents, the effectiveness of safety interventions, and the correlation between various factors and safety outcomes. Using this analysis, FSF develops metrics and indicators that help in assessing the safety performance of various aviation operations.

2.2.1.6.6 Aviation Safety Network (ASN)

The Aviation Safety Network (ASN) is a private initiative that plays a crucial role in the field of aviation safety by compiling and disseminating information on aviation accidents and incidents [FSF ASN]. ASN maintains an extensive and detailed database of civil aviation accidents and incidents from around the world. This database includes both major and minor incidents and is one of the most comprehensive resources of its kind available publicly. The information in the ASN database is gathered from a variety of sources. These include official aviation safety agencies, such as the NTSB and the European Union Aviation Safety Agency (EASA), news reports, aviation industry sources, and sometimes first-hand reports. This multi-source approach ensures wide coverage and varied perspectives on each incident. One of the key features of the ASN is the public accessibility of its database.

2.2.1.6.7 International Air Transport Association (IATA)

The International Air Transport Association (IATA) is known primarily as an industry trade group representing and serving airlines worldwide. IATA is deeply involved in enhancing aviation safety [IATA]. IATA collects a vast array of safety data, including incident reports from its member airlines. This data collection is a fundamental part of their efforts to monitor and analyze global aviation safety trends. IATA conducts safety audits of its member airlines through programs like the IATA Operational Safety Audit (IOSA). The IOSA program is an internationally recognized and accepted evaluation system designed to assess the operational management and control systems of an airline. The safety data collected from various sources is shared with member airlines, providing them with critical insights that can be used to enhance their operational safety. IATA's data analysis efforts help airlines identify potential risks and implement effective mitigation strategies.

2.2.1.7 Benefits and Shortcomings of Risk Assessment Methodology

The standardization roadmap created in A25 [Snyder, 2021] captures the benefits of this SRA process. This roadmap aided in identifying potential hazards requiring mitigation before any FAA approval. It also created a standardized process, allowing the FAA to add and track hazards and outcomes over time to provide the greatest availability of data to determine the probability of various types of failure. In addition to this, as the use of the UAS Aviation Safety Reporting System (ASRS) reports increases and the FAA continues to mine the data to track common failures related to UAS accidents, the hazard list can become more accurate and refined. The FAA may also require applicants to address additional hazards for future approvals. This could improve the SRA process and impact aircraft certification and approval for various AAM/UAM operations.

The shortcoming of this method is standardizing the safety assurance process. To date, the FAA still needs to provide a clear path for safety assurance for operators. Approvals gained by traditional risk assessments often get approval to fly, but they do not identify the safest way to fly or ensure continuous improvement. For example, FAA waiver approvals for BVLOS operations do not require reporting after the flight activity to verify what risk mitigation strategies worked and which did not, nor are operators required to identify what mitigation strategies had unintended consequences. This creates potential scenarios where mitigations may increase the overall risk instead of reducing the risk in the approved UAS operation, and these

conditions may go unreported. Currently, the SRA system relies heavily on subject matter experts to determine the initial risk with existing mitigations and identify the residual risk after implementing mitigations before a given operation. The fact that the same individuals flying the UAS often conduct the safety risk assessments, individuals who often do not have the proper training and may be more concerned with production than protection, may also impact results.

2.2.2 Flight Planning & Strategic Deconfliction

The second application of qualitative RA methodologies to AAM/UAM is focused on planning and strategic deconfliction. This section includes the following nine (9) sections:

1. Section 2.2.2.1: Description and Overview
2. Section 2.2.2.2: Potential Root Causes of Failures and of Potential Contributing Factors
3. Section 2.2.2.3: Interactions of the System with other Systems within Background Report Areas
4. Section 2.2.2.4: Description of the Relevant Environmental Factors for this System
5. Section 2.2.2.5: Decomposition of the System into Sub-Systems
6. Section 2.2.2.6: Description of Potential Failure Stories for the System: Scenario 1
7. Section 2.2.2.7: Description of Potential Failure Stories for the System: Scenario 2
8. Section 2.2.2.8: Integrated use of Influence Diagrams and FMEA
9. Section 2.2.2.9: Process Controls to Prevent Failure Mode

2.2.2.1 Description and Overview

The goal of the analyses presented below is to illustrate the use of two of the qualitative RA methodologies reviewed in Section 2.1, namely, influence diagrams (IDs) and failure modes and effects analysis (FMEA), in order to explore the use of these qualitative safety risk assessments in an evaluation of AAM/UAM operations. The focus of this sample analysis will be flight planning and strategic deconfliction, with attention to the impact of communications.

To perform the analyses described below, it is necessary to specify the relevant CONOPS. For this work the CONOPS is summarized below in the following eight (8) sections:

1. Section 2.2.2.1.1: Actors
2. Section 2.2.2.1.2: Missions
3. Section 2.2.2.1.3: Aircraft
4. Section 2.2.2.1.4: Airspace
5. Section 2.2.2.1.5: Airspace and Vertiport Demand
6. Section 2.2.2.1.6: Flight Planning
7. Section 2.2.2.1.7: Air Traffic Control (ATC)
8. Section 2.2.2.1.8: Communication Enablers

2.2.2.1.1 Actors

The CONOPS includes the following five (5) types of actors:

1. PSU: there is one (1) passenger service unit (PSU) for the urban area. The PSU includes a PSU manager and support staff, including a local meteorologist or some individual with the necessary meteorology expertise.
2. A traffic manager responsible for Traffic Management Functions (TMFs) for strategic deconfliction.

3. Vertiports: there are multiple (say, *M*) vertiports located in and around the metropolitan area. Each vertiport can accommodate multiple (say, *X)* aircraft and is staffed with: *i)* multiple (say, *N)* landing/departure managers, *ii)* one (1) vertiport manager, *iii)* one (1) maintenance specialist, and *iv)* one (1) communications specialist. Vertiport staff will have access to meteorology expertise as well.
4. Additional landing pads: there are multiple additional landing pads for single aircraft located in and round the metropolitan area. Each will be staffed with someone responsible for managing the operations of that specific landing pad.
5. Flight operators: there are multiple flight operators, including *i)* one (1) dispatcher/flight planner for each larger operation and *ii)* multiple remote pilots in command (RPICs) per vertiport.

2.2.2.1.2 Missions

The CONOPS missions consist of passengers and cargo delivered to and from the *M* vertiports.

2.2.2.1.3 Aircraft

The CONOPS aircraft are assumed to have the following six (6) properties and capabilities:

1. All aircraft are rotorcraft.
2. All aircraft are remotely piloted.
3. There is a single remote pilot per UAS.
4. All aircraft have some equivalent of ADSB-out and ADSB-in.
5. All aircraft have radar and vision systems to support DAA and provide RPIC situation awareness.
6. All aircraft are equipped to fly autonomously, including the capabilities to: *i)* fly planned routes (including route changes issued from the ground or autonomous changes if communications are lost while enroute); *ii)* depart and land; *iii)* support DAA; and *iv)* fly contingency routes.

2.2.2.1.4 Airspace

The CONOPS airspace has the following two (2) properties: *i)* flights are restricted to predefined corridors unless given an explicit exception; and *ii)* circular holding patterns around vertiports are predefined.

2.2.2.1.5 Airspace and Vertiport Demand

It is assumed that the CONOPS has to function in an environment where airspace and vertiport demand is high relative to capacity.

2.2.2.1.6 Flight Planning

The CONOPS flight planning sequence consists of the following five (5) steps:

1. The traffic manager responsible for TMF initiates temporary flight restrictions (TFRs).
2. The flight operator (dispatcher) submits the proposed 4D flight plan, including indication of acceptable ranges for parameters.
3. The flight operator (dispatcher) submits the proposed contingency flight plans, including indication of acceptable ranges for parameters and planned alternate sites for landing.
4. Pre-flight, the software evaluates the proposed flight plan, including contingency plans, for the traffic manager responsible for TMF, i.e., the software performs strategic deconfliction of the 4D trajectory, based on four factors: *i)* TFRs (airspace and vertiport constraints); *ii)* aircraft DAA capabilities; *iii)* the already approved flight plans; and *iv)* rules of the road.

5. Enroute, the software continuously reevaluates the 4D trajectories, vertiport availability, and the status of all enroute aircraft.

2.2.2.1.7 Air Traffic Control (ATC)

The CONOPS includes air traffic control (ATC) with FAA controller involvement under the following two (2) exceptions: *i)* the UAS enters controlled airspace as part of a planned mission; or *ii)* the UAS enters controlled airspace as a result of an off-nominal unplanned operation.

2.2.2.1.8 Communication Enablers

The CONOPS assumes primary and backup communication systems are supported and seamlessly accessed in all AAM/UAM aircraft. These communication networks might take advantage of the following three (3) technologies and protocols:

Internet protocol (IP). The principal protocol for online communications is Internet Protocol. This set of rules is foundational in how the Internet works. But, despite its widespread use throughout the world, until recently IP has played little part in communications within the aviation sector. Recently there has been a push at the international level to migrate air traffic communications to an Internet Protocol (IP)-based system, referred to generally as the Internet Protocol Suite (IPS). The drive for change came initially from ICAO but more recently has been spearheaded by the standards agencies for aviation technology, most notably the European Organization for Civil Aviation Equipment (EUROCAE) and the Airlines Electronic Engineering Committee (AEEC). Migrating to IPS is a central component of the larger scale project of modernizing air traffic management (ATM), which is being undertaken in Europe as the EU's Single European Sky ATM Research (SESAR) joint project and in the USA as the FAA's NextGen program.

Supporting IP communications, VHF Data Link mode 2 (VDL2) is a new wireless transmission mode used on aircraft for sending short messages and position data. VDL transmission operates as a single carrier half-duplex and employs time-division duplexing (TDD), where uplink and downlink typically use the same frequency, similar to modern Wi-Fi systems [Jamal, 2020]. The frequency band (25 kHz) and TDD enable robust operations in a dense urban environment.

As a backup communication system, satellite communication for AAM will be useful for offshore or remote locations, away from typical ground stations and as a backup if there is a failure of the VDL2 network. Additionally, satellites will provide a tracking mechanism for situational awareness for airspace owners for BLOS operations in dense urban environments [Duquerroy, 2021]. For this analysis, what is important is that two complementary high reliability communications networks are integrated to serve as primary and backup systems for air-to-ground and air-to-air communications [Erturk, 2020]. For the purposes of this analysis, what is important is that two complementary high reliability communications networks are integrated to serve as primary and backup systems for air-to-ground and air-to-air communications [Erturk, 2020].

2.2.2.2 Potential Root Causes of Failures and of Potential Contributing Factors

To identify potential root causes, FMEA [ASQ] was applied. *Figure 6* shows the results for strategic deconfliction. Note that potential failure modes (Column B) are specified at the level of outcomes that could, in turn, combine with other factors to result in an undesirable outcome.

Organization Ohio State University					Failure Mode and Effects Analysis								FMEA ID #
System Component Strategic Deconfliction					Design or Process Responsibility					Prepared by and their Title			
Process/Design					Team Members					FMEA Creation Date			
Process Step/Input or Design Item	Potential Failure Mode	Potential Enablers/Contributors	Potential Effect(s) of Failure	SEV	Potential Cause(s) / Mechanism(s) of Failure	OCC	Current Process Controls to Prevent Failure Mode	Current Process Controls to Detect Failure Mode	DET	RPN	Recommended Actions	Person/Org Responsible for Actions	
1. Strategic deconfliction	TFR: Overestimation of vertiport capacity	Lack of suitable alternative landing site	Inadequate estimation of vertiport capacity resulting in the need for diversion of an aircraft. If the contingency plan to handle such a diversion is inadequate, then an emergency landing may be required	9	Inaccurate weather forecast; inadequately trained and experienced PSU traffic manager and vertiport operator; lack of access to trained meteorologist	2	See Attachment X	See Attachment X	1	18	See Attachment X	PSIU, Dispatch; RPIC; Vertiport	
1. Strategic deconfliction	TFR: Underestimation of vertiport capacity		Unnecessary delays; reduced throughput		Inaccurate weather forecast; inadequately trained and experienced PSU traffic manager and vertiport operator; lack of access to trained meteorologist					**0**			
1. Strategic deconfliction	TFR: Overestimation of airepace (corridor) capacity	Lack of suitable alternative trajectory; high demand for airspace	Inadequate safety eval. of proposed 4D trajectory for a flight		Inaccurate weather forecast; inadequately trained and experienced PSU traffic manager; lack of access to trained meteorologist; brittleness of strategic deconfliction softwre								
1. Strategic deconfliction	TFR: Underestimation of airspace (corridor) capacity		Unnecessary delays; reduced throughput;		Inaccurate weather forecast; inadequately trained and experienced PSU traffic manager; lack of access to trained meteorologist; brittleness of strategic deconfliction softwre								
1. Strategic deconfliction	Inadequate evaluation of airspace restrictions	Inadequate tactical replanning	Inadequate safety eval. of proposed 4D trajectory for a flight		Inaccurate weather forecast; inadequately trained and experienced PSU traffic manager; brittleness of strategic deconfliction software								
1. Strategic deconfliction	Incorrect assumptions about obstructions		Inadequate safety eval. of proposed 4D trajectory for a flight		Inadequately trained and experienced PSU traffic manager; brittleness of strategic deconfliction software; out of date data on obstructions								
1. Strategic deconfliction	Incorrect assumptions regarding trajectories and contingency plans for other previously approved and upcoming flights	High demand for airspace and/or vertiports	Inadequate safety eval. of proposed 4D trajectory for a flight		Inadequately trained and experienced PSU traffic manager; brittleness of strategic deconfliction software								
1. Strategic deconfliction	Inadequate assumptions about performance capabilities of new flight and all other potentially interacting flights (including DAA capabilities)		Inadequate safety eval. of proposed 4D trajectory for a flight		Inadequately trained and experienced PSU traffic manager; brittleness of strategic deconfliction software; inadequate data input from flight operator regarding aircraft and automation capabilities								
1. Strategic deconfliction	1Inadequate potential trajectory conflict evaluation (DAA) algorithm	High volume and complexity in airspace usage	Inadequate safety eval. of proposed 4D trajectory for a flight		Brittleness of DAA algorithm(s); inadequate data input from flight operator regarding aircraft and automation capabilities								
1. Strategic deconfliction	Inadequate safety evaluation of proposed 4D trajectory for a flight	High volume and complexity in airspace and vertiport usage	Inadequate safety eval. of proposed 4D trajectory for a flight		Inadequately trained and experienced PSU traffic manager; brittleness of strategic deconfliction software; brittleness in DAA algorithm(s) inadequate data input from flight operator regarding aircraft and automation capabilities								

Figure 6: FMEA analysis for strategic deconfliction supporting AAM/UAM.

Figure 7: ID indicating factors that could interact to affect the safety of an AAM/UAM flight. provides an ID ([Howard, 2005], [Shachter, 1986]) indicating factors that could interact to affect the safety of a flight. It indicates that there are a number of contributing factors that could interact with the approval of a 4D trajectory and associated contingency plan for a new flight and consequently influence the level of risk.

It further indicates that there are a number of factors that could interact to affect safety, such as the actual weather encountered by this new flight while enroute, the results of the preflight inspection, the performances of the aircraft used for this flight and of other aircraft, the dissemination of TFRs by a traffic manager responsible for TMFs, and the performances of the RPIC, Dispatcher/flight planner (if any), PSU, vertiport, and ATC (if the flight enters ATC controlled airspace). It also indicates that FAA regulations and/or Community-Based Rules represent a second order factor that has an influence on things such as aircraft performance.

Figure 8 illustrates how additional detail can be added as input to the primary nodes shown in the influence diagram.

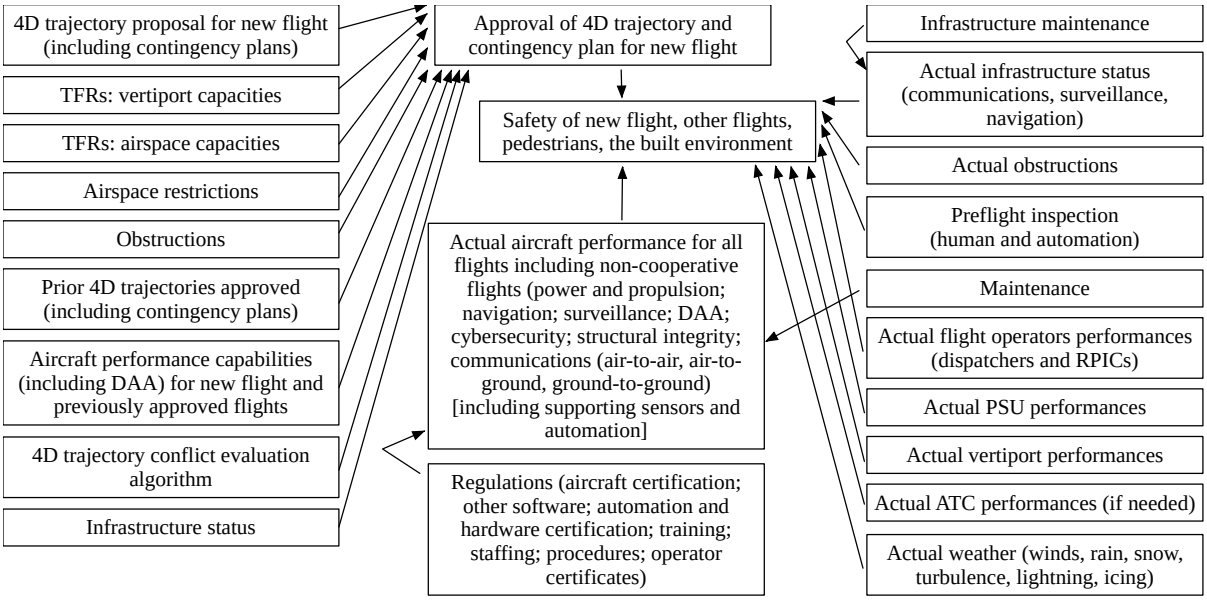

Figure 7: ID indicating factors that could interact to affect the safety of an AAM/UAM flight.

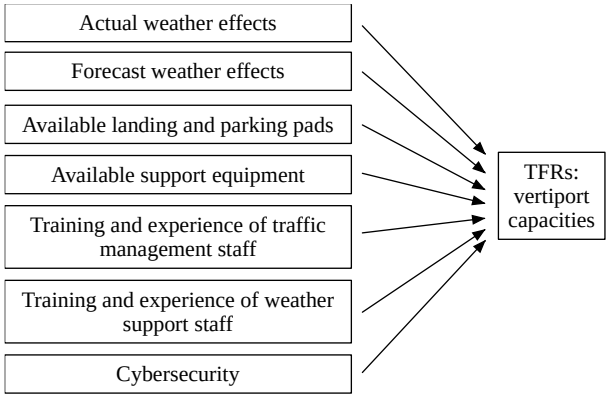

Figure 8: Factors influencing the capacity of a vertiport.

2.2.2.3 Interactions of the System with other Systems within Background Report Areas

Subsystems or products included in the A64 Task 1 background report [Rice, 2023] relevant to AAM/UAM were identified. These were used as probes for knowledge elicitation, asking: "How should the potential performance of some other subsystem or product be considered during the evaluation regarding strategic deconfliction for a proposed flight?". The process for strategic deconfliction should consider potential concerns associated with these other subsystems to evaluate the potential for an adverse outcome. All of these factors were included in the Influence Diagram (ID) in *Figure 7*. Such concerns are listed below:

1. **Detect and avoid**. This is critical to strategic deconfliction. Judgments regarding the acceptability of a given proposed 4D trajectory and its associated contingency plan have to take into consideration:

    a. The ability of the involved aircraft to detect and avoid other aircraft and flying objects (including birds) and to detect and avoid built objects and terrain.
    b. The degree of uncertainty that needs to be assumed regarding the 4D trajectories for other aircraft (due to factors such as winds or the performance capabilities of those aircraft).
2. **Power and propulsion**. The potential for the aircraft to have a partial or full loss of power and/or propulsion needs to be considered as part of the assessment of the contingency plans associated with this new proposed flight. This could include situations where the aircraft can no longer maintain its planned 4D trajectory as well as scenarios involving emergency landings. This possibility needs to be considered in developing and evaluating contingency plans.
3. **Airspace and vertiport design**. Airspace design will determine crossing points within the corridor network. Airspace design will also segregate flights based on their direction through a corridor (via altitude or lateral separation). Passing lanes will be incorporated to deal with flight flying at different speeds. Holding patterns around vertiports will provide a structured method to delay landing when necessary. Vertiports may have multiple landing pads. These structural specifications will place constraints on flight plans and DAA and will determine the buffers available to deal with off-nominal events and deviations from flight plans. These constraints need to be considered in strategic deconfliction.
4. **Communications**. Potential loss of communication by an individual aircraft, by a specific vertiport or PSU, by the traffic manager responsible for TMFs, by ATC or by the AAM/UAM communications network as a whole need to be considered. This applies to communications with the RPIC and supporting operations center, as well as communications among these other entities. Contingencies to deal with this need to be considered in strategic deconfliction.
5. **Navigation and surveillance**. Regarding navigation, the required navigation performance (RNP) capability associated with each flight is an important consideration for strategic deconfliction and interacts with the aircraft's DAA capabilities. If that aircraft capability should degrade without the knowledge of the software and the traffic manager responsible for strategic deconfliction, the potential for a loss of separation could increase. Surveillance is critical. If surveillance capabilities are degraded or lost for an individual aircraft or for a ground operator such as at a PSU or vertiport, this has major safety implications. If a more widespread loss of surveillance occurs, this is even more significant in terms of safety. Strategic deconfliction needs to consider such possibilities in evaluating a contingency plan.
6. **Standards, regulation, certification, and policy**. Strategic deconfliction needs to evaluate a given flight plan and associated contingency plans relative to the requirements based on these requirements. They must be adequately specified to ensure that compliant strategic deconfliction is safe.
7. **CONOPS and system architecture**. The assumptions regarding the CONOPS have been specified above. If this CONOPS and the supporting system architecture specified change some of the specified assumptions (such as whether or not the aircraft is controlled remotely), then assumptions about how various factors influence safety will change.
8. **Autonomous command and control**. If the aircraft is fully autonomous or enters an autonomous mode due to loss of communications, appropriate contingency plans are necessary to ensure safety and need to be evaluated as part of strategic deconfliction.
9. **Human-automation interaction and human-human interactions**. Strategic deconfliction needs to consider the potential of inappropriate human-automation or human-human

interactions. This includes all of the people potentially involved as well as the specific systems in use by each person.

2.2.2.4 Description of the Relevant Environmental Factors for this System

Contingency plans need to consider the potential impact of all possible "environmental" factors. This includes factors that could affect an aircraft along its flight path or that require vectoring off the planned flight path, such as convective weather and winds, icing, birds, and obstacles introduced by the built environment. It could also include factors that impact the performance of ground personnel, such as lightning restricting activities of personnel at a vertiport or a fire, tornado or some other emergency affecting personnel at a flight operations center, a PSU, or a vertiport.

2.2.2.5 Decomposition of the System into Sub-Systems

Strategic deconfliction is a function of a TMF with global responsibilities for AAM/UAM operations within an urban area. Given the complexities of such a planning function, software support is necessary. However, given the nature of some of the contributing factors that need to be considered in such planning (such as convective weather), this software needs to provide decision support for responsible humans.

There are a number of components of the decision-making process for strategic deconfliction that need to be integrated, including:

1. Data regarding aircraft capabilities for a proposed flight, including its RNP and DAA capabilities (or compliance with some minimum requirements for all flights).
2. Software that can evaluate a proposed 4D trajectory and its associated contingency plans within the corridor network for a flight based on consideration of other already approved 4D trajectories for other flights, including manned aircraft, as well as a topographical map indicating built structures. Traffic flow restrictions (TFRs) must also be considered by this software.
3. Human input (by the traffic manager responsible for TMFs) to generate TFRs; dispatcher(s)/flight planner(s) for large flight operations; RPICs for individual flights), to develop and submit proposed 4D trajectories and contingency plans and to provide the input necessary for the software to evaluate a proposed 4D trajectory and set of contingency plans for a flight. If the number of flights and complexity of the routes within the corridor network is sufficiently complex, then the assumption is that human input is provided to the software, which then makes the assessment (but with the ability of the human to override the software by exception).

2.2.2.6 Description of Potential Failure Stories for the System: Scenario 1

Two scenarios are presented that are informed by considering the implications of the influence diagram on failure modes identified as part of the FMEA analysis for strategic deconfliction. This highlights the potential value of using the influence diagram to provide a structured method to explicitly identify factors that could interact with the failure modes identified for strategic deconfliction.

The first scenario illustrates the use of the FMEA analysis focused the reliance of strategic deconfliction on the specification of Traffic Flow Restrictions (TFRs). It highlights the interactions of several factors identified in the ID in *Figure 7*:

1. TFRs created and disseminated by the traffic manager responsible for TMFs regarding predicted vertiport and corridor capacities.
2. Decision making by the traffic manager responsible for TMFs (with automation support) to approve the contingency plan for a flight regarding alternate landing sites should arrivals the intended destination be stopped.
3. Decision making by dispatcher/flight planner and RPIC to proceed to launch the flight.
4. Aircraft performance (capacity to divert to an alternate landing site).
5. Actual weather development.
6. Actual capacities of vertiports or other landing sites.

In Scenario 1, the assumed failure mode is that the traffic manager responsible for TMFs, with support from weather forecasting software and potentially with support from a meteorology service, sets the TFRs specifying the Vertiport Arrival Rates (VARs) too high relative to uncertainty regarding the potential for convective weather to either reduce or stop arrivals at several vertiports. This is Potential Failure Mode 1.1, named "TFR: Overestimation of Vertiport Capacity," as shown in the FMEA analysis for strategic deconfliction in *Figure 6*.

As a result, when aircraft begin to arrive at the vertiports, a significant number are forced to divert. Because the TFRs set the arrival rates too high relative to this convective weather event, there are not enough alternative vertiports or other landing pads available to handle all the diverting aircraft. As a result, the emergency backup sites must be utilized to allow a number of these aircraft to land at reserve sites.

This emergency backup plan is analogous to operational planning in the military for air missions to identify precoordinated rally points for air (helicopters) and ground forces [Smith, 2021]. This requires a plan for coordination and communication among all the relevant entities. *Figure 9* indicates the nature of such coordination for potential Air Force operations. For AAM/UAM operations, this would include coordination and communication involving the RPICs for the involved aircraft, their associated dispatchers (if any), the traffic manager responsible for TMFs the PSU(s), local law enforcement and, if necessary, ATC.

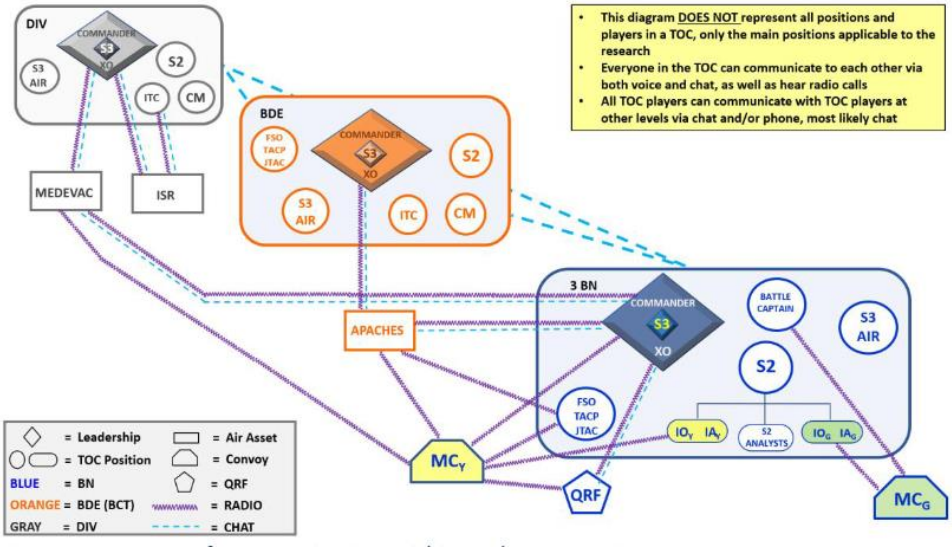

Figure 9: Coordination and communication among units for an Air Force mission.

For the military, this pre-planning further includes the identification of rally points for air (helicopter) and ground forces, such as sports fields and parks (see R1-R4 in *Figure 10*). The same could apply for the design of an AAM/UAM operation. Such rally points or emergency reserve landing areas could be considered in the design and approval of the contingency plan for a flight.

Figure 10: Pre-planned rally points as part of a contingency plan.

As long as sufficient landing areas have been identified in the AAM/UAM planning and in the specific contingency plans for the involved UASs, the end result is a safe but inefficient AAM/UAM operation. In addition, because the RPICs have control of the UASs, the traffic manager responsible for TMFs could coordinate to have aircraft land at any vertiports or landing pads that, although they are not identified as alternates in the contingency plans for aircraft, could

still be utilized for those aircraft that have sufficient energy reserves to reach them. (If a large number of aircraft require alternative landing sites, software to support the traffic manager responsible for TMFs in making such alternate airport assignments and approving the 4D trajectories to get there would be useful.)

Such coordination is viable because there is an RPIC in control of each UAV who can make the adjustments to the trajectory and landing site for the aircraft based on instructions from the traffic manager responsible for TMFs. Section 2.2.2.9 indicates the mitigations that should be employed to make sure this process is effective.

In addition, if necessary, the emergency reserve landing sites specified in the contingency plans can be used. However, if the reserve landing sites are not adequately cleared of pedestrians or objects, the operation could result in injuries or damage to property. (The likelihood of this latter possibility could be further reduced if the aircraft had vision systems to help ensure landing in a cleared area. It should also involve coordination with local law enforcement.)

This preplanning is importantly different from current FAR 121 operations, in which the dispatcher develops a contingency plan for diversion of a particular flight if there is predicted weather that could impact landing at the planned destination (for example specifying and fueling for a specific alternate airport as part of the flight release). For AAM/UAM operations, because there are fewer possible suitable sites for diversion as compared with 121 operations, approval of diversion plans for specific flights will have to be approved preflight centrally by the traffic manager responsible for TMFs.

Figure 11 provides an FMEA assessment of the risk associated with such a scenario (see the line highlighted in gray). The following notation is used in the figure:

1. SEV: How severe is the effect?
2. OCC: How frequent is the cause likely to occur?
3. DET: How probable is the detection of the mode or cause?
4. RPN: Risk Priority Number (RPN = SEV x OCC x DET)

With a Risk Priority Number (RPN) of 18, it indicates that, given the assumed CONOPS for AAM/UAM operations, there is a risk that merits investigation to determine suitable mitigations. Section 2.2.2.9 outlines such mitigations.

This analysis serves to highlight an important point. While completing such an FMEA analysis feels straightforward, assumptions are hidden within the analysis. For example, in specifying the OCC (i.e., "How frequent is the cause likely to occur?"), it feels reasonable to ask the related question: "How frequently could generation of a TFR that overestimates the capacities of vertiports lead to an emergency landing?". For this sample analysis, the thought process is that overestimation will happen occasionally and, when this happens, there is a small but not negligible likelihood that the following may occur: *i)* a diversion will be required; *ii)* the planned alternate landing sites will be unavailable; and *iii)* the emergency landing site selected by the RPIC in consultation with the traffic manager responsible for TMFs and dispatcher/flight planner might not be as safe as desired. This reasoning leads to a SEV (severity) of 9.

In short, this exercise suggests a caution regarding the completion of an FMEA: it may incorporate hidden assumptions, making the resultant numbers less than fully informative. However, if the

impact of the FMEA is to trigger a more detailed assessment of that possible failure mode in order to identify mitigation, this may appropriately lead to evaluation of mitigations.

Organization Ohio State University					**Failure Mode and Effects Analysis**							FMEA ID #
System Component Strategic Deconfliction					Design or Process Responsibility						Prepared by and their Title	
Process/Design					Team Members						FMEA Creation Date	
Process Step/Input or Design Item	Potential Failure Mode	Potential Enablers/Contributors	Potential Effect(s) of Failure	S E V	Potential Cause(s) / Mechanism(s) of Failure	O C C	Current Process Controls to Prevent Failure Mode	Current Process Controls to Detect Failure Mode	D E T	R P N	Recommended Actions	Person/Org Responsible for Actions
1. Strategic deconfliction	TFR: Overestimation of vertiport capacity	Lack of suitable alternative landing site	Inadequate estimation of vertiport capacity resulting in the need for diversion of an aircraft. If the contingency plan to handle such a diversion is inadequate, then an emergency landing may be required	9	Inaccurate weather forecast; inadequately trained and experienced traffic manager and vertiport operator; lack of access to trained meteorologist	2	See Attachment X	See Attachment X	1	18	See Attachment X	TMF; Dispatch; RPIC; Vertiport
1. Strategic deconfliction	TFR: Underestimation of vertiport capacity		Unnecessary delays; reduced throughput		Inaccurate weather forecast; inadequately trained and experienced traffic manager and vertiport operator; lack of access to trained meteorologist							
1. Strategic deconfliction	TFR: Overestimation of airepace (corridor) capacity	Lack of suitable alternative trajectory; high demand for airspace	Inadequate safety eval. of proposed 4D trajectory for a flight		Inaccurate weather forecast; inadequately trained and experienced traffic manager; lack of access to trained meteorologist; brittleness of strategic deconfliction software							
1. Strategic deconfliction	TFR: Underestimation of airspace (corridor) capacity		Unnecessary delays; reduced throughput;		Inaccurate weather forecast; inadequately trained and experienced traffic manager; lack of access to trained meteorologist; brittleness of strategic deconfliction software							
1. Strategic deconfliction	Inadequate evaluation of airspace restrictions	Inadequate tactical replanning	Inadequate safety eval. of proposed 4D trajectory for a flight		Inaccurate weather forecast; inadequately trained and experienced traffic manager; brittleness of strategic deconfliction software							
1. Strategic deconfliction	Incorrect assumptions about obstructions		Inadequate safety eval. of proposed 4D trajectory for a flight		Inadequately trained and experienced traffic manager; brittleness of strategic deconfliction software; out of date data on obstructions							
1. Strategic deconfliction	Incorrect assumptions regarding trajectories and contingency plans for other previously approved and upcoming flights	High demand for airspace and/or vertiports	Inadequate safety eval. of proposed 4D trajectory for a flight		Inadequately trained and experienced traffic manager; brittleness of strategic deconfliction software							
1. Strategic deconfliction	Inadequate assumptions about performance capabilities of new flight and all other potentially interacting flights (including DAA capabilities)		Inadequate safety eval. of proposed 4D trajectory for a flight		Inadequately trained and experienced traffic manager; brittleness of strategic deconfliction software; inadequate data input from flight operator regarding aircraft and automation capabilities							
1. Strategic deconfliction	1Inadequate potential trajectory conflict evaluation (DAA) algorithm	High volume and complexity in airspace usage	Inadequate safety eval. of proposed 4D trajectory for a flight		Brittleness of DAA algorithm(s); inadequate data input from flight operator regarding aircraft and automation capabilities							
1. Strategic deconfliction	Inadequate safety evaluation of proposed 4D trajectory for a flight	High volume and complexity in airspace and vertiport usage	Inadequate safety eval. of proposed 4D trajectory for a flight		Inadequately trained and experienced traffic manager; brittleness of strategic deconfliction software; brittleness in DAA algorithm(s) inadequate data input from flight operator regarding aircraft and automation capabilities							

Figure 11: FMEA analysis for Potential Failure Mode: TFR: Overestimation of vertiport capacity.

2.2.2.7 Description of Potential Failure Stories for the System: Scenario 2

Suppose we want to consider an extension of Scenario 1 by asking the question: "What other factors shown in the ID could interact with the occurrence of a TFR that overestimates TFR capacity?". Review of the nodes in the ID in *Figure 7* leads to the conclusion that the occurrence of this failure mode in combination with a loss of communications could result in a significant safety concern. This second scenario is driven by such a variation of Scenario 1, which was generated from the FMEA analysis focused the reliance of strategic deconfliction on the specification of TFRs (see *Figure 6*).

The additional factor added in Scenario 2 after reviewing the factors identified in the influence diagram is an interaction with another subsystem indicated in the influence diagram: communications. Namely, assume that there is a complete loss of communication for an aircraft planning to land at a vertiport that has been stopped because of convective weather. Note that a more challenging variation on this scenario would arise if several aircraft operated by a particular flight operator lost communications or if the entire AAM/UAM airspace lost communications.

In this scenario, the RPIC can no longer communicate with the UAV. Thus, the UAV must operate autonomously. Consideration of the ID in *Figure 7* indicates that a number of factors interact to determine the likelihood of such a scenario and the safety of the outcome:

1. Accuracy of the weather prediction as information to consider in determining vertiport capacities.
2. Skill of the weather forecaster and performance of supporting weather forecasting software.
3. Skill of the traffic manager and supporting software in generating TFRs for the vertiports.
4. Skill of the dispatchers and RPICs at judging the weather forecast in developing flight plans and associated contingency plans, as well as in making go/no-go decisions just prior to departure.
5. Effectiveness of the traffic manager responsible for TMFs and deconfliction software in determining TFRs as input to the strategic deconfliction decisions.
6. Effectiveness of the strategic deconfliction software.
7. Performance of RPICs, dispatchers, the traffic manager responsible for TMFs and local law enforcement in managing diversions.
8. Effectiveness of FAA or Community Based Rules (regulations) in specifying minimum energy reserves and requirements for strategic deconfliction to ensure adequate alternative landing sites (including emergency reserve sites), as well as associated procedures for making safe use of these sites.

Figure 12 shows a notional layout of an AAM/UAM system. V1-V5 are vertiports that can each serve several UAVs. The two unlabeled boxes are landing sites for single UAVs at a hospital and a business. R1-R4 are emergency reserve landing sites (at sports fields and parks). The corridors are not shown, but they connect all the landing sites.

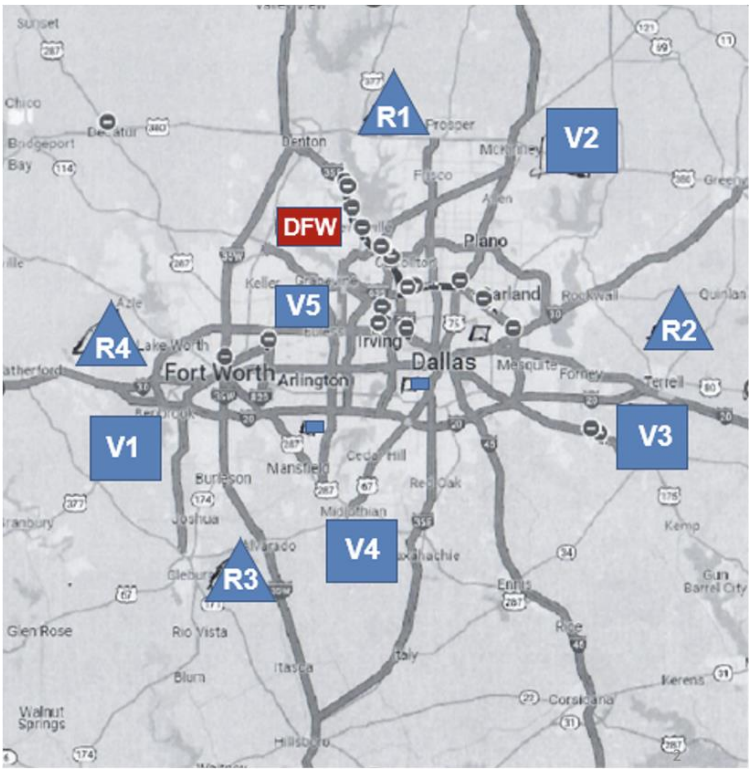

Figure 12: Notional layout of AAM/UAM system.

For Scenario 2, assume the following steps occur:

1. The weather forecast (TFM Convective Forecast) predicts sparse coverage of the entire AAM/UAM airspace (25-39%) for the next 4 hours.
2. The traffic manager responsible for TMFs for this urban area consults with a meteorologist and all of the vertiport operators and sets TFRs for each of the vertiports at 75% of maximum capacity. This assumes that any vertiport stoppages due to air mass thunderstorms may be randomly distributed across V1-V5 and R1-R3 over time.
3. A dispatcher considers the weather forecast and the TFRs and consults with a meteorologist. With concurrence of the RPIC, the dispatcher submits a proposed 4D trajectory and contingency plan for Flight XYZ, with a departure from V1 and a destination of V2. The contingency plan indicates V3 as the alternate vertiport and R1 as the planned emergency landing site if necessary. These decisions are based on the experience of the meteorologist, dispatcher and RPIC that indicates that if V2 arrivals are stopped due to convective weather, V3, V4 and R1 are unlikely to also all be impacted by storm cells at the same time. The dispatcher also sends any flight data for this aircraft necessary for the strategic deconfliction software under the control of the traffic manager responsible for TMFs to evaluate potential concerns regarding spacing relative to the DAA capabilities of all of the relevant aircraft.
4. The strategic deconfliction software used by the traffic manager responsible for TMFs evaluates the proposed 4D trajectory taking into consideration the TFRs and the already approved flights during this time period (including their proposed 4D trajectories and their contingency plans). The traffic manager responsible for TMFs is monitoring the approved trajectory and, if necessary, by exception can override the approval. In this case the trajectory

and contingency plan for Flight XYZ is approved by the software and is not overridden by the traffic manager.
5. As part of the preflight inspection, just prior to OFF, the dispatcher and RPIC evaluate the weather and conclude that the flight plan is safe.
6. The flight departs.
7. As the flight approaches V2, arrivals at V2, V3 and R1 are stopped due to thunderstorm activity.
8. Before the RPIC can coordinate with the traffic manager responsible for TMFs regarding a feasible alternative vertiport instead of V3 or V4 and send instructions to the UAV, one aircraft goes NORDO, losing both primary and secondary communications.
9. The automation takes over full control.
10. A visual signal is displayed to the aircraft as it arrives at the vicinity of V2 indicating that V2, V3 and R1 arrivals are stopped.
11. Based on this visual signal the automation diverts to the secondary alternative vertiport, V4.
12. The traffic manager responsible for TMFs coordinates with the RPICs of the other airborne aircraft to ensure that Flight XYZ has a clear route as it proceeds.
13. The automation proceeds to fly Flight XYZ to the selected landing site and it lands autonomously but safely. To enable this, the vertiport operator has coordinated with the other diversions to V4 to allow the NORDO flight to land first.

This scenario raises a number of questions that need to be addressed, including determination of whether considerations associated with factors 1-8 above will be effectively managed. It also indicates a number of questions in terms of whether Steps 1-13 above are the best design and whether each of these steps can be performed effectively. Of particular importance are the following questions:

1. Is Scenario 2 sufficiently likely to require addressing the mitigations necessary to support the steps listed above (or some alternative set of steps)?
2. How will the aircraft automation be informed regarding the stopping of landings at V2, V3 and R1? (Note: if this signal could also indicate a new diversion site in circumstances where the contingency plan is inadequate, this would add additional safety.)
3. What if the weather won't allow the NORDO aircraft to approach to V2? How is this detected and how should the aircraft automation respond?
4. How will coordination be managed by the automation if an aircraft without air-to-ground communication needs to land at one of the emergency reserve sites?
5. What should regulations specify in terms of reserve energy and the range of alternatives indicated in a contingency plan?

Note that, methodologically, these two scenarios suggest that a thorough SRA should employ standard SRA methods, as described earlier, and then be supplemented with a test plan for evaluating a specified set of critical scenarios. The generation of these scenarios could be enhanced through the use of an ID to provide a shared visual representation for use by SMEs to consider possible critical interactions more completely among factors that could result in a significant safety risk. This is analogous to the requirement to use Critical Task Analysis Reports for guidance in the design and evaluation of FAA software (see page B-7 of [FAA HFEQ]).

2.2.2.8 Integrated Use of IDs and FMEA

The above discussion indicates how IDs can be used to provide a structured method to identify potential interactions among the different factors that influence the safety of an AAM/UAM operation. There are two assumptions that merit discussion:

1. Section 2.2.2.8.1: Assumption #1: The ID can Facilitate Collaboration by Multiple SMEs.
2. Section 2.2.2.8.2: Assumption #2: The ID can be used to Systematically Identify Factors that Interact to Affect Safety.

2.2.2.8.1 Assumption #1: The ID can Facilitate Collaboration by Multiple SMEs

The first assumption is that such a shared visual representation can more effectively support collaboration by multiple SMEs to produce a more complete and accurate representation indicating the risk factors and the interactions that need to be considered in completing an SRA. Essentially, the methodology is to work with SMEs to generate the ID, and includes the following factors:

1. A draft ID is prepared by a single SME or a focus group with several SMEs collaborating. For this project, this draft diagram was produced by SMEs at The Ohio State University (OSU).
2. This draft is sent to other SMEs with an appropriate range of expertise to address the following questions, which were sent along with the draft ID to SMEs at the University of North Dakota (UND), Kansas State University (KSU), and Embry-Riddle Aeronautic University (ERAU):
    a. Question 1: Should any high-level nodes be added, deleted, relabeled, or broken up into more than one separate node to produce an updated ID? The STAMP analyses produced by ERAU suggested that an additional "regulation" node be added, including regulation of aircraft certification, other software, automation and hardware certification or approval; training; staffing; procedures; approval of operators' certificates].
    b. Question 2: Should subcategories be produced showing underlying factors influencing one or more of the high-level nodes in the updated ID. Figure 8 shows an initial draft for one of the nodes.

First, regarding actual vertiport performances, the factors identified in the initial draft by OSU SMEs included: *i)* actual weather; *ii)* forecast weather; *iii)* available landing and parking pads; *iv)* available staff; *v)* training and experience of traffic management staff; *vi)* training and experience of weather support staff; and *vii)* cybersecurity. The additional factors identified by UND SMEs include: *i)* the capability of vertipads to meet aircraft requirements (*i.e.*, compliance with standards such as required size of concrete and the load-bearing capability of the pad); *ii)* night operations capabilities; *iii)* wake turbulence and ability to adapt for landing; and *iv)* automation support.

Second, regarding actual flight operator performance, the factors identified in the initial draft by OSU SMEs included: *i)* staffing levels; and *ii)* procedures. The additional factors identified by ERAU, KSU, and UND SMEs included: *i)* training and experience of flight operator staff (RPICs, dispatchers and meteorologists); and *ii)* automation support.

Third, regarding detect and avoid (DAA), the factors identified in initial draft by OSU SMEs included: *i)* staffing levels; *ii)* procedures; *iii)* cybersecurity; and *iv)* separation requirements. The additional factors identified by ERAU, KSU, and UND SMEs included: *i)* training and experience of flight operator staff (RPICs, dispatchers and meteorologists); *ii)* presence of wildlife (such as birds or other items not ‘seen’ by DAA system); *iii)* hardware performance; *iv)* software

performance; *v)* weather impacts on DAA performance (fog and clouds); *vi)* presence of low altitude obstacles that may impact maneuvers (i.e., buildings and powerlines restrict where you can move).

Fourth, regarding power and propulsion, the factors identified by ERAU, KSU, and UND SMEs included: *i)* reliability of propulsion system; *ii)* control system failures impacting effectiveness; *iii)* redundancy of propulsion systems; *iv)* icing effect on propulsion systems; *v)* maintenance; *vi)* qualifications to repair various propulsion systems.

Note that the above analysis is for illustration purposes only. A more complete analysis would require the participation of a greater range of SMEs.

2.2.2.8.2 Assumption #2: The ID can be used to Systematically Identify Factors that Affect Safety

The second assumption is that the updated ID can be used to systematically ask the question: What factors could interact to affect safety? This can be accomplished by selecting one of the failure modes identified by the FMEA and reviewing each of the nodes and sub-hazards identified in the influence diagram, asking the question: Could this factor shown in the ID have an impact on the likelihood of occurrence of a failure mode or the severity of its consequences? If so, it may need to be incorporated into the critical scenarios included in the test plan for scenario-based safety assessment.

The two scenarios described earlier illustrate this very clearly, with the identification of a number of factors identified in the ID that could affect the impact of the failure mode "TFR: Overestimation of Vertiport Capacity" on safety. An extreme example in terms of a system design challenge was the interaction in Scenario 2 of an overestimation of vertiport capacity (due to an unexpected stopping of arrivals due to weather at the intended destination and two of the landing sites that were planned as contingencies for a flight) with a loss of communication by a UAV planning to land at that vertiport, resulting in a significant increase in risk.

2.2.2.9 Process Controls to Prevent Failure Mode

The traffic manager responsible for TMFs is responsible for developing a TFR indicating the predicted capacity for a vertiport for some time period based in part on weather forecasts. The dispatcher and RPIC are responsible to consider this when deciding whether to launch a flight. If the failure mode arises, the RPIC can coordinate with the traffic manager responsible for TMFs to determine the landing site to use for a diversion due to the closure of a vertiport.

Recommended Actions: a much more integrated process for coordination needs to be defined and supported by automation -

1. Preflight, the flight operator needs to submit its contingency plan for diversions.
2. Preflight, the strategic deconfliction automation used by the traffic manager responsible for TMFs needs to consider the contingency plans for all of the proposed and active flights and determine whether sufficient capacity has been reserved to ensure safe diversion landing sites for all aircraft.
3. The traffic manager responsible for TMFs, dispatchers/flight planners, RPICs, ATC and local law enforcement need to be trained on a procedure to manage a flight that needs to divert.
4. The automation needs to support the traffic manager responsible for TMFs in determining safe diversion sites for aircraft that cannot land at their planned vertiports and in ensuring that the 4D trajectory for diversions are conflict free.

2.2.3 Autonomous Command and Control (CC)

The third application of qualitative RA to AAM/UAM applies the STPA hazard analysis framework (Section 2.1) to the autonomous command and control (CC) system in an AAM/UAM setting. This section contains the following sections:

1. Section 2.2.3.1: System Analysis
2. Section 2.2.3.2: Identifying Constraints
3. Section 2.2.3.3: Hierarchical Safety Control Structure
4. Section 2.2.3.4: Accident Analysis

2.2.3.1 System Analysis

The intention of system analysis is to understand the system as a whole, including all components, interactions, and functions, with a focus on its structure and behavior. *Figure 13* shows a block diagram illustrating the interactions between the different components in the normal operation of autonomous CC. The Flight Control Processor (FCP) will receive data from the Communication modules from the Ground Control Systems (GCS). That data will then be analyzed and processed via the FCP and passed to the Emergency Management System (EMS) to adjust the movement of the UAV.

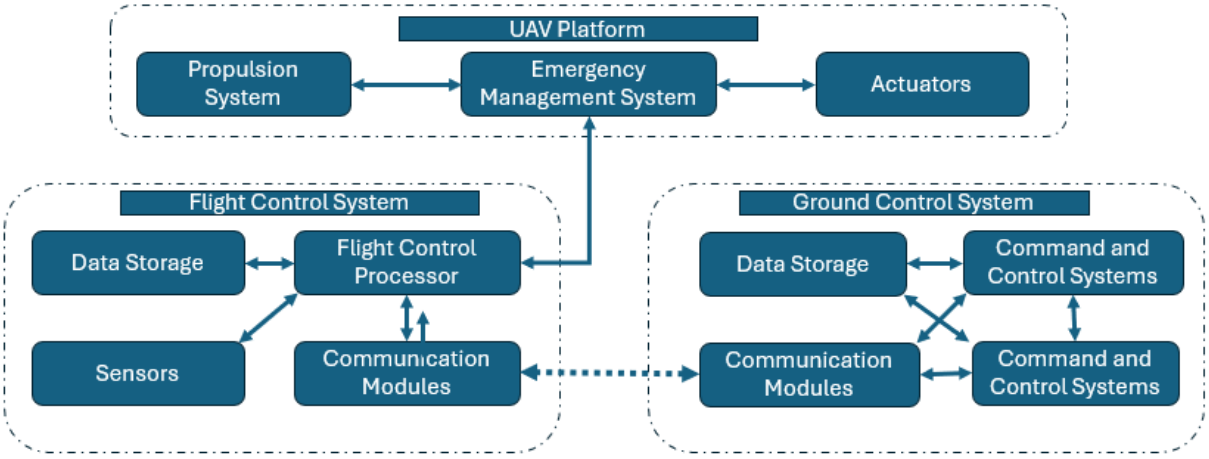

Figure 13: STPA applied to command and control (CC): system components and interactions.

2.2.3.2 Identifying Constraints

The next step is determining the necessary safety constraints for the system to operate without leading to an accident. These are rules or conditions to maintain safety. The constraints were identified through the following five (5) step process:

1. *Step 1: Root Causes* - List potential root causes of failures and potential contributing factors.
2. *Step 2: System Interactions* - Describe the system's interactions with other systems.
3. *Step 3: Environmental Factors* - Describe relevant environmental factors for this system.
4. *Step 4: Subsystems* - Decompose the system into sub-systems.
5. *Step 5: Failure Scenarios* - Describe potential failure stories (scenarios) for the system.

2.2.3.2.1 Step 1: Root Causes

Three primary safety constraints have been identified for autonomous CC:

1. In case of primary channel failure, The AAM/UAM system must maintain a continuous and secure communication link with ATC, with automatic failover to backup channels.
2. All critical components of the AAM/UAM system must have operational redundancy to ensure continuous functionality under failure conditions.
3. The system must perform real-time operational monitoring with automated diagnostics to detect and alert deviations from standard operating parameters.

2.2.3.2.2 Step 2: System Interactions

Autonomous CC interacts with and relies upon network reliability constraints in the following three (3) ways:

1. The communication network must maintain at least two independent communication channels to ensure redundancy.
2. Network protocols must dynamically adjust based on real-time data analysis to safely optimize performance and reliability.
3. In case of primary channel failure, the communication system must automatically switch to a backup channel within a predefined time frame.

The likelihood of the system operating within the safety constraints will be improved through the use of the following three (3) best practices:

1. Use data analytics to predict and address potential network failures before they occur. By analyzing trends and patterns in network performance data, maintenance can be scheduled proactively, reducing the risk of unexpected failures.
2. Implement real-time monitoring systems to detect and respond to network issues instantly. This allows for immediate corrective actions, minimizing the impact of any network disruptions.
3. Incorporate multiple layers of security within the communication networks to protect against cyber threats, ensuring that the data used for safety protocols is available, secure, and reliable.

In addition, designing the AAM/UAM system with the following three (3) trajectory control and deconfliction constraints will also improve the likelihood of operating under safety constraints:

1. The system must continuously monitor and adjust flight trajectories to avoid conflicts, with a minimum separation distance maintained at all times.
2. Conflict detection algorithms must identify potential trajectory conflicts and initiate resolution procedures automatically and in real time.
3. Trajectory adjustments in response to detected conflicts must be executed within a specific time frame to ensure timely deconfliction.

2.2.3.2.3 Step 3: Environmental Factors

The following two (2) environmental factors directly impact the safe operation of autonomous CC:

1. Signal strength and reliability.
2. Weather conditions.

Regarding signal strength and reliability, the following three (3) best practices will mitigate the impact of low or unreliable signal strength on the safe operation of the autonomous CC system:

1. Implement protocols for regular testing and validation of signal strength and quality.
2. Ensure multiple communication channels to provide backup in case of failure.
3. Establish protocols to identify and mitigate potential sources of signal interference.

Regarding weather conditions, the following three (3) best practices will mitigate the impact of inclement or uncertain weather on the safe operation of the autonomous CC system:

1. Integrate advanced weather monitoring sensors and systems for real-time updates.
2. Develop protocols for adaptive responses to changing weather conditions, including automatic route adjustments.
3. Implement procedures for handling severe weather scenarios, including system shutdowns or rerouting to safe locations.

2.2.3.2.4 Step 4: Subsystems

There are two relevant subsystems for autonomous CC:

1. Communication channel encryption: All communication within the autonomous CC system must utilize robust encryption protocols to prevent unauthorized access, which are regularly updated to address emerging security threats.
2. Redundant communication channels: The system must maintain multiple independent communication channels to guarantee connectivity at all times, even if one channel fails.

2.2.3.2.5 Step 5: Failure Scenarios

Two failure scenarios of autonomous CC have been identified as examples:

1. Failure due to communications loss and/or delay.
2. Failure due to cyber-attack.

The first failure scenario will occur under the following two situations:

1. First, there is either i) a lack of timely response over the communications channel or ii) inappropriate maneuvers in response to communication loss.
2. Second, there is an overreliance on automated systems without adequate fail-safes for communication breakdowns.

To reduce the likelihood and/or severity of the first failure scenario, it is recommended that the following components and procedures be included in the design:

1. In case of communication loss, the AAM/UAM system must initiate an immediate response protocol to manage the vehicle, avoiding inappropriate maneuvers safely.
2. The AAM/UAM system must maintain multiple, independent communication channels to ensure continuous connectivity, even if one channel fails.

The first failure scenario will occur under the following two situations:

1. First, there is a failure to detect and respond to the cyber-intrusion in a timely manner;
2. Second, either incorrect or malicious commands are being followed by the AAM/UAM vehicles due to the system being compromised.

To reduce the likelihood and/or severity of the second failure scenario, it is recommended that the following components and procedures be included in the design:

1. The autonomous CC system must incorporate advanced cyber-intrusion detection mechanisms that continuously monitor for and immediately flag any unauthorized access or anomalies;
2. AAM/UAM vehicles must be equipped with an autonomous fail-safe operational mode that activates in case of compromised CC system control, ensuring safe operation or landing.

2.2.3.3 Hierarchical Safety Control Structure

The block diagram in *Figure 13* has been redesigned to include redundant backup communication systems, onboard CC systems, a cyber-intrusion detection system, and an automated fail-safe landing system, as shown in *Figure 14*.

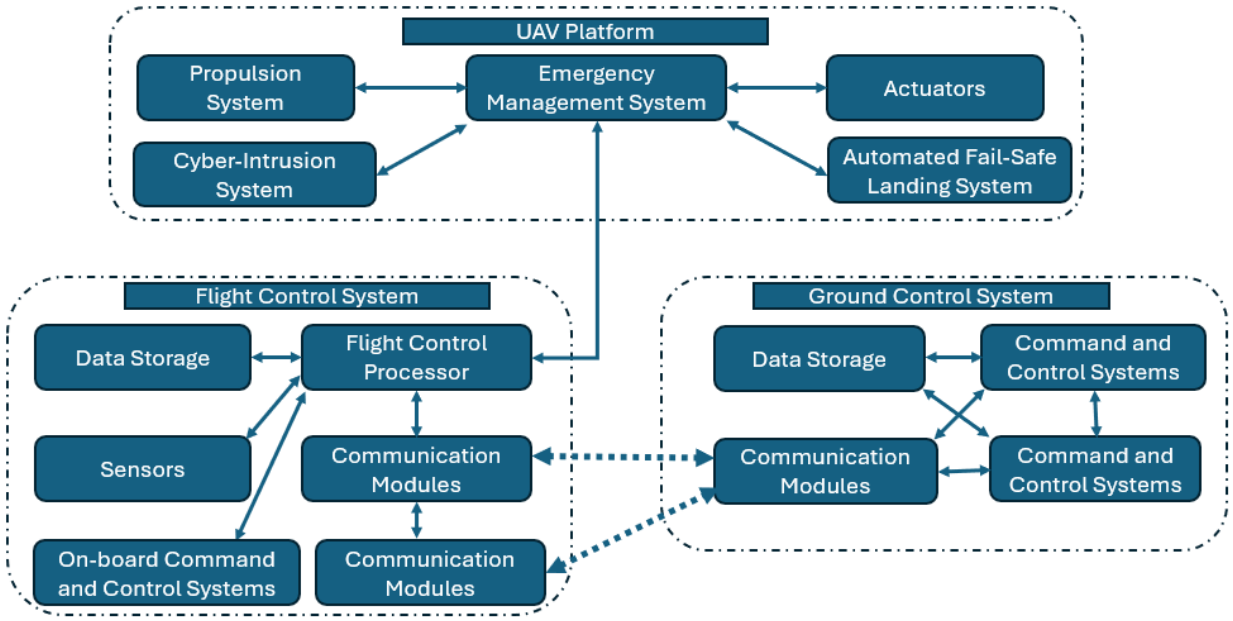

Figure 14: STPA applied to command and control (CC): augmented system diagram.

2.2.3.4 Accident Analysis

The first failure scenario involved a communication failure where the communication channels between AAM/UAM vehicles and ground control systems experience a malfunction or total failure, leading to a possible airspace conflict. To mitigate the risk of a communication failure, redundant communication models were implemented into the AAM/UAM flight control system to ensure constant communication with ground control stations. Additionally, an on-board CC system should be implemented into the onboard flight control system to provide real-time automated command and control given a ground communication fault. These two systems should mitigate the risks associated with the first failure scenario.

The second failure scenario involved a cyber-attack where the CC systems are compromised due to a malicious cyber intrusion. Two new mitigations were put into the block diagram to prevent cyber-attacks on the AAM/UAM. The first is a cyber-intrusion system that detects cyber anomalous behaviors and sends alerts to the pilot in command and flight controllers. The second system would be an automated fail-safe landing system for an AAM/UAM compromise. The automated system would take over all craft functions and land it at the nearest, safe location to prevent malicious behaviors toward the AAM/UAM.

2.2.4 Human-Automation Interaction and Human-Human Interaction

The fourth and final application of qualitative RA to AAM/UAM applies the STPA hazard analysis framework (Section 2.1) to human-automation and human-human interaction in an AAM/UAM setting. This section contains the following sections:

1. Section 2.2.3.1: System Analysis
2. Section 2.2.3.2: Identifying Constraints
3. Section 2.2.3.3: Hierarchical Safety Control Structure
4. Section 2.2.3.4: Accident Analysis

2.2.4.1 System Analysis

The intention of system analysis is to understand the system as a whole, including all components, interactions, and functions, with a focus on its structure and behavior. *Figure 15* shows a block diagram illustrating human-automation interactions in the normal operation of an AAM/UAM system. Conceptually, the automation portion of human-automation interaction can be broken down into a control system, navigation system, and human interface with the control system. The human operator at the ground control will interact with the command-and-control system. The communication modules will then relay the data to the UAV platform. In the event of a communications malfunction (and possible additional non-normal events), the human passenger could have an interface on the UAV platform for the human-automation interaction with the control system for manual control. Naturally, there is difficulty in designing this interface for non-expert human passengers to maximize the likelihood of a low-severity outcome.

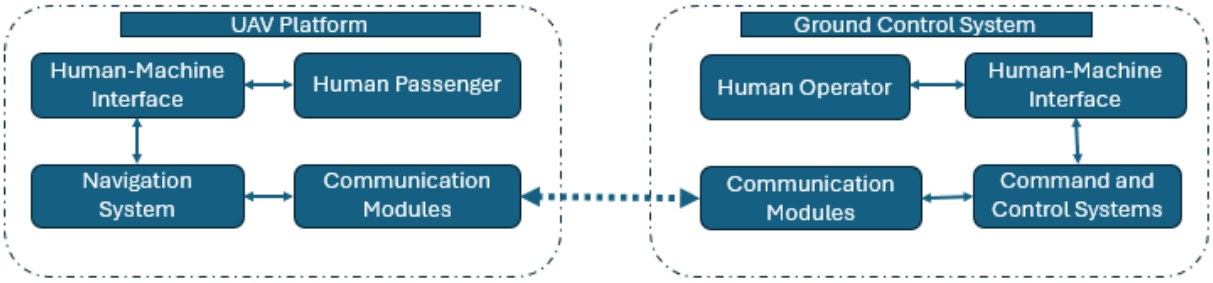

Figure 15: STPA applied to human automation: system components and interactions.

2.2.4.2 Identifying Constraints

The next step is determining the necessary safety constraints for the system to operate without leading to an accident. These are rules or conditions to maintain safety. The constraints were identified through the following five (5) step process:

1. *Step 1: Root Causes* - List potential root causes of failures and potential contributing factors;
2. *Step 2: System Interactions* - Describe the interactions of the system with other systems;
3. *Step 3: Environmental Factors* - Describe relevant environmental factors for this system;
4. *Step 4: Subsystems* - Decompose the system into sub-systems;
5. *Step 5: Failure Scenarios* - Describe potential failure stories (scenarios) for the system.

2.2.4.2.1 Step 1: Root Causes

Four primary safety constraints have been identified:

1. Systems must be designed to facilitate intuitive and efficient interaction between the human operator and the automation, enabling seamless transitions between automated and manual control.
2. Autonomous systems must provide operators with clear and understandable feedback regarding their decision-making processes and current operational status to support informed human oversight.

3. Operators of semi-autonomous systems must receive comprehensive training and regular skill updates to manage and intervene in automated operations effectively.
4. Systems must support effective communication and collaboration among human operators in control centers, facilitating coordinated responses to emergencies or system failures.

2.2.4.2.2 Step 2: System Interactions

Four safety constraints specific to the interaction have been identified.

1. The AAM/UAM system must provide comprehensive fail-safes and override capabilities that allow human pilots to take immediate and full manual control in case of automation failure or unforeseen circumstances.
2. The AAM/UAM system must incorporate advanced collision avoidance and situational awareness technologies to assist human passengers and ensure safe operation during manual control.
3. The AAM/UAM system must maintain continuous, transparent communication with human supervisors, alerting them to system status and potential issues and allowing for timely human intervention when needed.
4. The AAM/UAM system must implement stringent cybersecurity measures to protect against hacking, unauthorized access, and other cyber threats at all automation levels.

2.2.4.2.3 Step 3: Environmental Factors

The following two (2) environmental factors directly impact the safe operation of human-automation interaction:

1. Emergencies and critical weather conditions.
2. Unique and/or distinct geographical features.

Regarding the environmental factor of emergencies and critical weather conditions, the following safety protocol for human interaction with autonomous systems is recommended:

1. Emergency Override Systems: Ensure that human operators can quickly and effectively take control of the autonomous system in an emergency.
2. Advanced Weather Prediction and Response Systems: Integrate advanced weather prediction technologies to anticipate and respond to critical weather conditions.
3. Training in Emergency Procedures: Provide comprehensive training to human operators in handling emergencies and operating in critical weather conditions.
4. User Interface Design for Emergency Situations: Design user interfaces that present critical information and options during emergencies, allowing quick and informed decision-making.

Regarding the environmental factor of unique and/or distinct geographical features, the following safety protocol for human interaction with autonomous systems is recommended:

1. Incorporate detailed geographical data into the system to assist operators in understanding the unique challenges of different locations.
2. Develop protocols that allow operators to customize their decision-making processes based on local conditions and requirements.
3. Provide specialized training for operators in managing AAM/UAM systems in different geographical locations, focusing on unique challenges and requirements.

2.2.4.2.4 Step 4: Subsystems

There are two relevant subsystems for human-automation interaction:

1. Control and navigation system.

2. Non-normal condition response system.

Regarding the control and navigation system, the following safety constraints on the design are recommended:

1. The control system must be designed with redundancy to ensure continuous operation even in the event of a component failure. It must incorporate real-time diagnostic capabilities to detect and address faults promptly.
2. The navigation system must integrate multimodal sensors (e.g., GPS, radar, and lidar) to ensure accurate positioning and routing and must be capable of functioning under various environmental conditions, including those that may disrupt standard GPS signals.
3. The human-interface system must be intuitively designed to facilitate easy and effective interaction between the operator and the system, providing clear, concise, and timely information to support decision-making, especially in emergency situations.

Regarding the non-normal condition response system, the following safety constraints on the design are recommended:

1. In the event of a non-normal condition, the system must allow human operators to quickly and efficiently take control, overriding automated functions if necessary.
2. The system must provide comprehensive and understandable information to the human operator regarding the nature of the non-normal condition and the status of automated functions, facilitating informed decision-making.
3. Human operators must be thoroughly trained to handle non-normal conditions, including simulations of various scenarios, to ensure preparedness for real-world emergencies.
4. The system must be resilient to a range of non-normal conditions, including cyber-attacks, system malfunctions, and environmental challenges, and must have protocols in place to safely manage these situations with or without human intervention.

2.2.4.2.5 Step 5: Failure Scenarios

Four failures scenarios of human-automation interaction have been identified:

1. Communication issues.
2. Weather, environment, and geography neglect.
3. Vulnerability to GPS/ADS-B jamming and spoofing.
4. Autopilot mismanagement in aviation.

First, semi-autonomous operations are vulnerable to failure when communication channel considerations are not incorporated sufficiently well into the navigation and traffic systems. In order to reduce the likelihood and/or severity of the first failure scenario, it is recommended that the system have multiple, independent communication channels to ensure continuous and reliable connectivity, enabling manual override at all times.

Second, semi-autonomous operations are vulnerable to failure when weather, environment, and geography are not adequately incorporated into navigation and traffic systems. In order to reduce the likelihood and/or severity of the second failure scenario, it is recommended that navigation and traffic alerting systems integrate real-time environmental and geographical data to adjust operational parameters accordingly.

Third, semi-autonomous operations are vulnerable to failure when there is over-reliance on Global Positioning System (GPS) and ADS-B without the benefit of a backup navigation system; this is

because of the vulnerability of GPS and ADS-B to jamming and spoofing. To reduce the likelihood and/or severity of the third failure scenario, it is recommended that navigation systems be designed to include countermeasures against GPS/ADS-B jamming and spoofing, ensuring alternative navigation capabilities.

Fourth, semi-autonomous operations are vulnerable to failure when incorrect input in autopilot altitude settings occurs. To reduce the likelihood and/or severity of the fourth failure scenario, it is recommended that pilots receive comprehensive training on autopilot systems and adhere to strict verification procedures for all autopilot settings.

2.2.4.3 Hierarchical Safety Control Structure

The block diagram in *Figure 15* has been redesigned to include redundant backup communication systems, onboard CC systems, a cyber-intrusion detection system, and an automated fail-safe landing system, as shown in *Figure 16*.

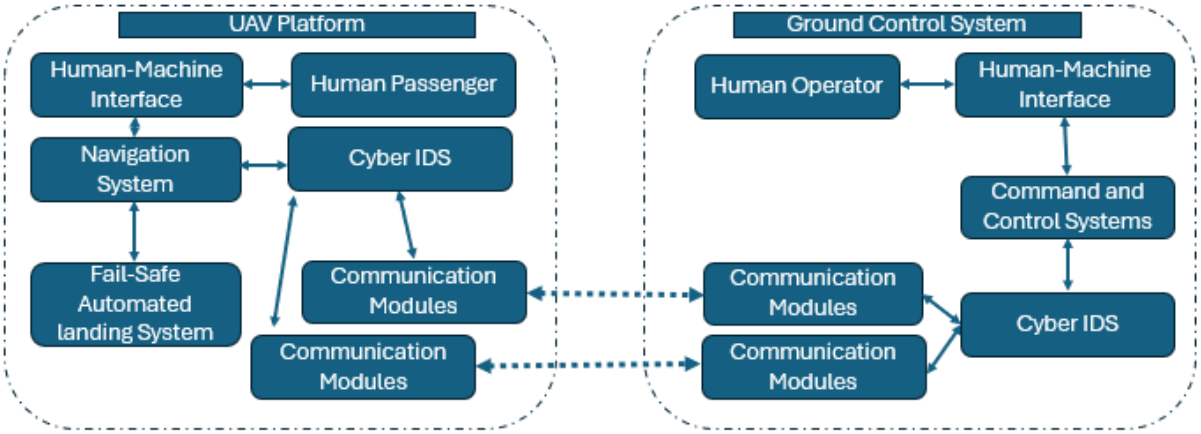

Figure 16: STPA applied to human automation: augmented system diagram.

2.2.4.4 Accident Analysis

One of the human-interaction failure scenarios outlined autopilot mismanagement, where the PIC activates the autopilot system but inadvertently selects an incorrect altitude setting. Training and communication constraints were identified to mitigate the risk of autopilot mismanagement. This training should facilitate effective communication and collaboration among PICs at operation centers. In addition, redundant checks from a primary and secondary operator could be implemented to ensure all settings are correct for each flight. The additional training should mitigate the risks associated with this failure scenario. The automation could also monitor for an implausible or unusual altitude setting.

Another of the human-interaction scenarios highlighted pilots misinterpreting instructions. Like the previous scenario, training programs should be implemented to mitigate this risk. The fail-safe automated landing system has also been added to the block diagram to autonomously land the UAV platform if it operates in non-normal conditions. The additional training and automated system should mitigate the risk of this failure scenario.

3 QUANTITATIVE RISK ASSESSMENT (RA)

While Section 2 addressed qualitative RA methodologies, this section focuses on quantitative RA methodologies. As mentioned in the quantitative RA preview in Section 1.3, this report *i)* reviews one specific quantitative RA methodology known as Decision Analysis in Section 3.1 and *ii)* applies it to the specific AAM/UAM concept of operations (CONOPS) in Section 3.2.

3.1 Selective Review of Quantitative Risk Assessment (RA) Methodologies

Decision Analysis, (*e.g.*, [Muenning, 2017], [Parnell, 2013], [Raiffa, 1968]), abbreviated as DA, is a well-established technique in which the sequence of uncertain outcomes leading to an event of interest is laid out as a tree (*i.e.*, a mathematical graph without loops), typically from a starting state or condition on the left (the root of the tree) and ending in any one of the possible end states or conditions on the right (the leaves of the tree). All vertices (including the root) except for the leaves represent an uncertain event in that one of multiple states will result, due to either the evolution of the system state or due to a relevant environmental factor.

This tree, as described thus far, effectively enumerates possible final states that may plausibly result from the initial state. But this enumeration is only the first part of the decision tree; the critical second part is to enumerate the conditional probabilities at each decision vertex. More precisely, for any such vertex, say v, hereafter called the parent, it will a set of child vertices, say $(v_1,...,v_k)$, and the directed edges, say $(e_1,...,e_k)$, connecting the parent with its children will be labeled with the conditional probability of the state evolving from the parent to each child. These labels, *say* $(l_1,...,l_k)$, are nonnegative numbers that sum to one (*1*), i.e., the labels represent a (conditional) probability distribution for the evolution of the system conditioned on being at the parent.

For any leaf (end state), the (conditional) probability of ending on that leaf is obtained by multiplying the (conditional) probabilities on the edges forming the (unique) path from the root to the leaf. Naturally, adding up the (conditional) probabilities of all possible leaves yields one, so that the collection of edge (conditional) probabilities in the tree induce a probability distribution on the leaves. It is often the case that the leaves may be aggregated, say into desirable vs. undesirable events, and the probability of a desirable vs. undesirable end state is obtained by summing the (conditional) probabilities over the leaves in each event.

The advantage of a decision tree is its specification of all possible end states and (more importantly) the probability distribution on those states, but this advantage is only possible due to the (often, in practice, large) number of edge (conditional) probabilities needed to specify the tree. This specification requirement is the primary disadvantage of decision trees because knowledge, or even a feasible means of estimation, of these (conditional) probabilities is unavailable.

A critical design aspect of decision trees is parsimony, in the sense of the goal of any model is to provide sufficient level of detail to capture the dynamics of interest, but any additional detail should be cut. In the context of decision trees, this parsimony is reflected in the choice of all possible children for each parent vertex. That is, in practice, the enumeration of all possible next states that might result from a parent vertex depends critically on what types of system dynamics and exogeneous factors are considered sufficiently plausible for inclusion in the model.

In the specific application of decision trees for safety, the issue of parsimony is particularly fraught on account that the intention of the model is to capture, or even uncover, hazardous states that may

give rise to accidents. That is, a parsimonious safety model may be self-defeating in that if attention is only given to normal operations, then all non-normal states that might result in an accident are omitted. On the other hand, a non-parsimonious model, say an extravagant model, may be impractical on account of the difficulty in estimating (conditional) probabilities of rare events.

3.2 Application of Specific Quantitative RA Methodologies to AAM/UAM Systems

This section extends Section 2.2.2 which leveraged two qualitative RA methodologies (ID and FMEA) in the context of flight planning and strategic deconfliction of AAM/UAM. In particular, it applies decision trees (DT) to a scenario, denoted Scenario 3 and described below, which is a variation of Scenario 1 as described in Section 2.2.2. This section includes the following sections:

1. Section 3.2.1: Scenario 3 Specification
2. Section 3.2.2: Scenario-Based Evaluation of Risks
3. Section 3.2.3: Incorporation of Subjective Probabilities into a DT
4. Section 3.2.4: Mitigations to Reduce Risk
5. Section 3.2.5: Further Consideration of Scenario 2

3.2.1 Scenario 3 Specification

Recall, the largest source of uncertainty regarding the likelihood of a significant safety risk in Scenario 1 is the adequacy of the weather forecast and the translation of such a forecast into TFRs. On the plus side, the timeframes for such forecasts for UAM operations are much shorter than those involved in traditional FAR Part 121, 135 and 91 operations. On the challenging side, the sensors and weather prediction models are currently much more limited for AAM/UAM operations than they are for higher altitude flights.

Scenario 3 was developed during knowledge elicitation with a meteorologist with over 19 years of experience with aviation weather forecasting for an airline. *Figure 17* provides the outline of the scenario presented to this SME. The Vs are vertiports; the Rs are pre-planned emergency landing sites such as parks; and the unlabeled blue boxes are landing pads for individual aircraft at urban sites such as hospitals or businesses.

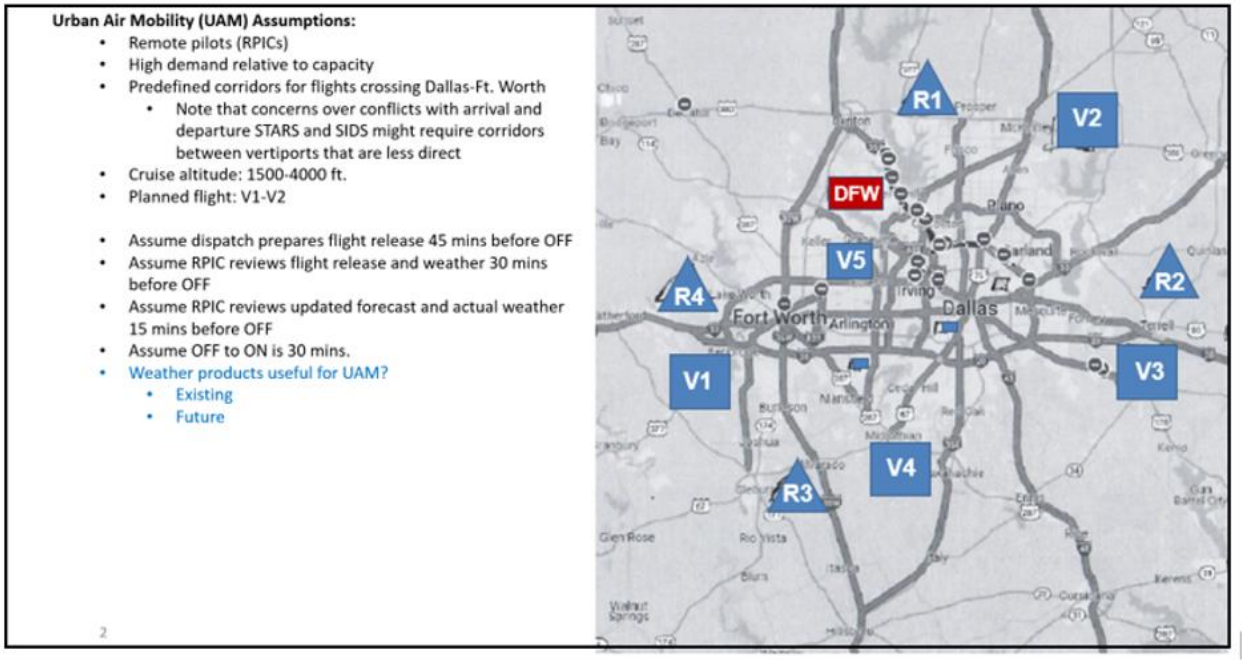

Figure 17: Description of Scenario 3.

As part of the presentation of this slide, the SME was asked about relevant weather information and provided the following input:

1. *"You would need sensors that provide information on a number of variables, such as winds, ceilings, visibility, temperature, barometric pressure, radar and lightning detection. This includes actual and forecast weather."*
2. *"Since this is a small area, you would need sensors that provide adequate data."*
3. *"The meteorologist would want high resolution weather models to provide forecasts for short time frames, and the ability to manually input parameters when necessary."*

Figure 18 indicates the flight corridors and provides an example from a military operations order of pre-planned emergency landing sites. It also indicates that the focus of Scenario 3 involves a flight from V1-V2 at 2100Z in July.

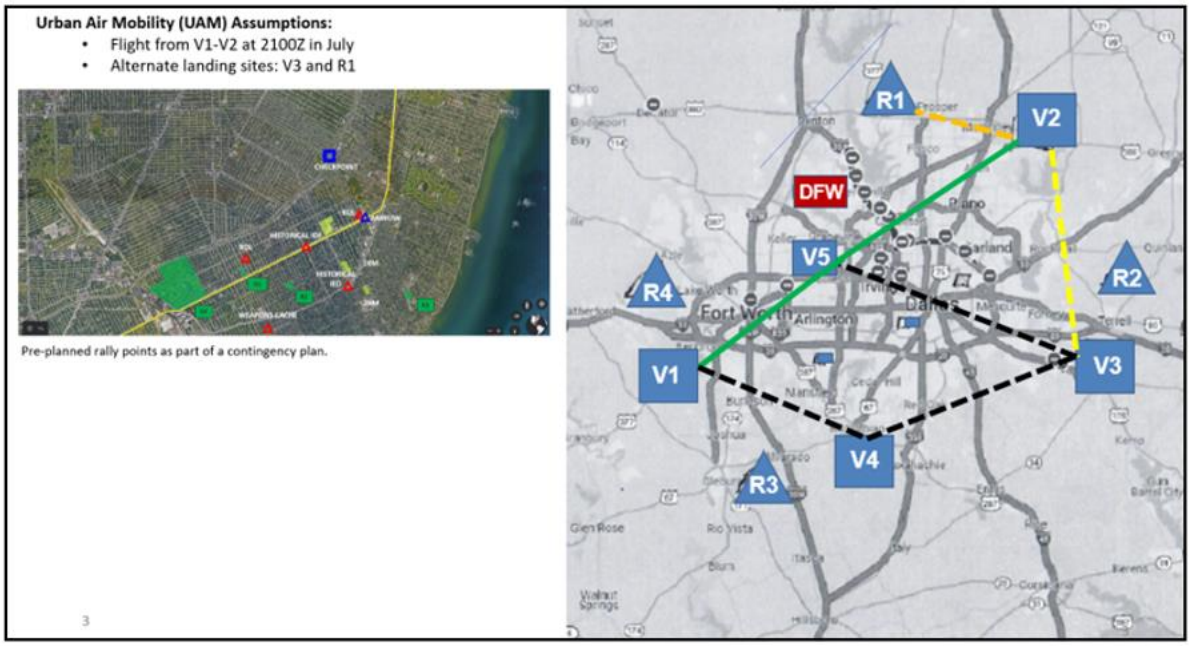

Figure 18: Flight corridors for Scenario 3.

It should be noted that, although this corridor design was used for the purposes of discussion, the SME indicated there could be significant issues with these corridors crossing arrival and departure gates. This could necessitate a different layout for the corridors along with a possible need at times for coordination with ATC.

The SME indicated that the details of the scenario are very important (such as location, time of day, time of year and specifics of the weather forecast). For example, he indicated that if the scenario were at 23Z, the likelihood of a thunderstorm developing and closing V2 would be much lower than at 2100Z.

This has major implications for SRAs: *aggregation of probabilities over large time frames, locations and conditions are not very informative relative to evaluating the safety risks involved with a particular AAM/UAM operation*.

To create an example, the meteorologist suggested showing a frontal system or trough over Denton, TX moving southwest at 40 kts (see *Figure 19*):

1. *"If a frontal system was coming through over Denton, or even a trough, then I can time it out and plan. With this example, it is likely it will close landing sites at some points."*
2. *"If it's moving at 40 kts., the pilot should usually be fine to depart from V1 and land at V2."*

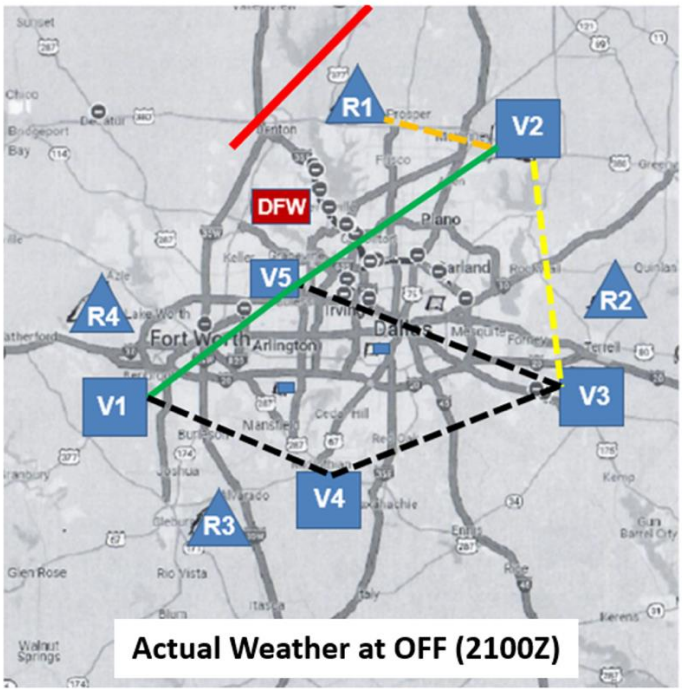

Figure 19: Scenario 3 with a frontal system or trough over Denton at 2100Z.

As illustrated earlier, the use of FMEA includes a structured process for subjective estimation of the likelihood and severity of the outcomes associated with the different failure modes that have been identified [ASQ].

As an extension of this method, DTs (as described in Section 3.1 and as discussed in [Muenning, 2017], [Parnell, 2013], [Raiffa, 1968]) could be used for specific critical scenarios to support a quantitative analysis for a safety risk assessment.

3.2.2 Scenario-Based Evaluation of Risks

The fundamental concept illustrated here is that, to support effective evaluation of the risk associated with a proposed UAM operations, a test plan should be developed that specifies a representative set of concrete scenarios that covers all of the importantly different *classes* of situations that need to be safely handled by a proposed operation. In this test set, each such class is defined generically and then illustrated by a concrete exemplar to help the evaluators more fully effectively assess risks and potential mitigations.

It should be noted that a number of the scenarios in this test set likely apply to UAM operations for any urban area. The test set therefore does not need to be re-developed from scratch when a proposal for operations at a new UAM site is considered. There will likely be a few additional classes of scenarios that need to be added to capture unique considerations associated with any given urban area, but this generalization of the test set across different UAM sites helps make this approach more feasible.

For the example below, the generic class focuses on ensuring safe UAM operations for scenarios where a frontal system is impacting the capacity of vertiports. To help in the evaluation of the safety of a proposed operation in such a scenario, a concrete illustration using a flight in the Dallas-Fort Worth (DFW) area is developed.

The fundamental hypothesis is that such a scenario-based evaluation of risks based on consideration of the risks and potential mitigations associated with concrete scenarios will help the evaluators of a proposed UAM operation to more fully and accurately complete their assessment.

The process illustrated below involves several steps:

1. Use the results of an FMEA analysis to identify a critical failure mode as a starting point. Then use an influence diagram to identify the factors that need to be incorporated into an illustrative scenario that captures the important interactions and cascading of actions, events and environmental conditions interacting with that failure mode and impacting the associated risk.
2. Define the scope of the class of scenarios that this scenario is intended to represent. For this example, the failure mode used is the development of a TFR that overestimates the capacity of vertiports. The particular cause discussed in this scenario is the development of a convective weather system.
3. Specify the details of a concrete, illustrative scenario to characterize this class of scenarios.
4. Develop a DT that captures the important decisions and events characterizing this scenario, as well as the outcomes.
5. Estimate the probabilities associated with chance nodes in this decision tree. To provide a sensitivity analysis, this could include estimates of confidence intervals for these probabilities instead of just point estimates. These estimates could be based on subjective probabilities provided by SMEs or historical data if available.
6. Estimate the probability of occurrence of the possible outcomes associated with this specific scenario.

The evaluator can then use this analysis to inform an assessment of the risk associated with this particular scenario and of the broader class of scenarios that it represents. This includes:

1. Characterize the severity of the potential consequences associated with each path through the DT, using a decision matrix such as the one shown in *Figure 20*.
2. Consider the estimated probabilities of the different paths and the severity of the associated consequences to produce an assessment of the risk associated with each path though the DT.

If certain paths are judged to have excessive risk, specify the mitigations necessary to reduce that risk to an acceptable level so that a proposed flight operation can be approved.

This process does not attempt to fully quantify risk. Rather it is intended to improve the judgment of an evaluator by providing a structured framework indicating contributing factors along with quantification of the likelihood of certain outcomes in order to support an evaluation.

>7: Extreme risk
– detailed treatment plan required
6,7: High risk
– needs senior management attention and treatment plan as appropriate
4,5: Medium risk
– manager level attention and monitoring as appropriate
<4: Low risk
– manage by local level procedures

	→ Consequence →					
People	Injuries or ailments not requiring medical treatment.	Minor injury or First Aid Treatment Case.	Serious injury causing hospitalisation or multiple medical treatment cases.	Life threatening injury or multiple serious injuries causing hospitalisation.	Multiple life threatening injuries. Less than 10 fatalities.	Multiple fatalities, 10 or more
Reputation	Internal Review	Scrutiny required by internal committees or internal audit to prevent escalation.	Scrutiny required by external committees or Auditor General's Office, etc.	Intense public, political and media scrutiny. Eg: inquest, front page headlines, TV, etc.	Government inquiry or Commission of inquiry or adverse national media in excess of 1 week.	Government inquiry and ongoing adverse international exposure
Organisational / Client impact	Small delay, internal inconvenience only.	May threaten an element of the service delivery function. Business objective delayed. Easily remedied, some impact on external stakeholders.	Considerable remedial action required with disruption to a Group for period up to 1 month. Some business objectives not achieved.	Significant loss of critical information. Disruption to one or more Groups for up to 3 months. Some major objectives not achieved.	Permanent loss of critical information, substantial disruption to CASA or external intervention for over 3 months. Threatens existence of a Group within CASA. Major objectives not achieved	Threatens ongoing existence of CASA.

Probability ↑	Numerical	Historical
	>1 in 10	Is expected to occur in most circumstances
	1 in 10 – 100	Will probably occur
	1 in 100 – 1000	Might occur at some time in the future
	1 in 1000 – 10000	Could occur but considered unlikely or doubtful
	1 in 10000 - 100000	May occur in exceptional circumstances
↑	< 1 in 100000	Could only occur under specific conditions and extraordinary circumstances

		Insignificant 0	Minor 1	Moderate 2	Major 3	Severe 4	Catastrophic 5
Almost Certain	(5)	5	6	7	8	9	10
Likely	(4)	4	5	6	7	8	9
Possible	(3)	3	4	5	6	7	8
Unlikely	(2)	2	3	4	5	6	7
Rare	(1)	1	2	3	4	5	6
Extremely Rare	(0)	0	1	2	3	4	5

Figure 20: Sample decision matrix from ASSURE A21 Final Report [Smith, 2022].

3.2.3 Incorporation of Subjective Probabilities into a DT

For quantitative support of a risk assessment, the combination of FMEA analyses and IDs can help to generate and describe critical scenarios such as Scenario 3 above (See *Figure 19*). For each such scenario, a decision tree can then be developed to assess risk.

Figure 21 shows an illustrative decision tree for Scenario 3. For the purposes of this sample analysis, it is assumed that the traffic manager responsible for TMFs consults with a meteorologist and decides to assign a TFR restricting each of the vertiports and emergency reserve areas to 75% of their full capacity in order to ensure the availability of landing slots if diversions are necessary. It is further assumed that, during the pre-flight evaluation just prior to OFF, the RPIC decides that the weather is favorable and the flight departs.

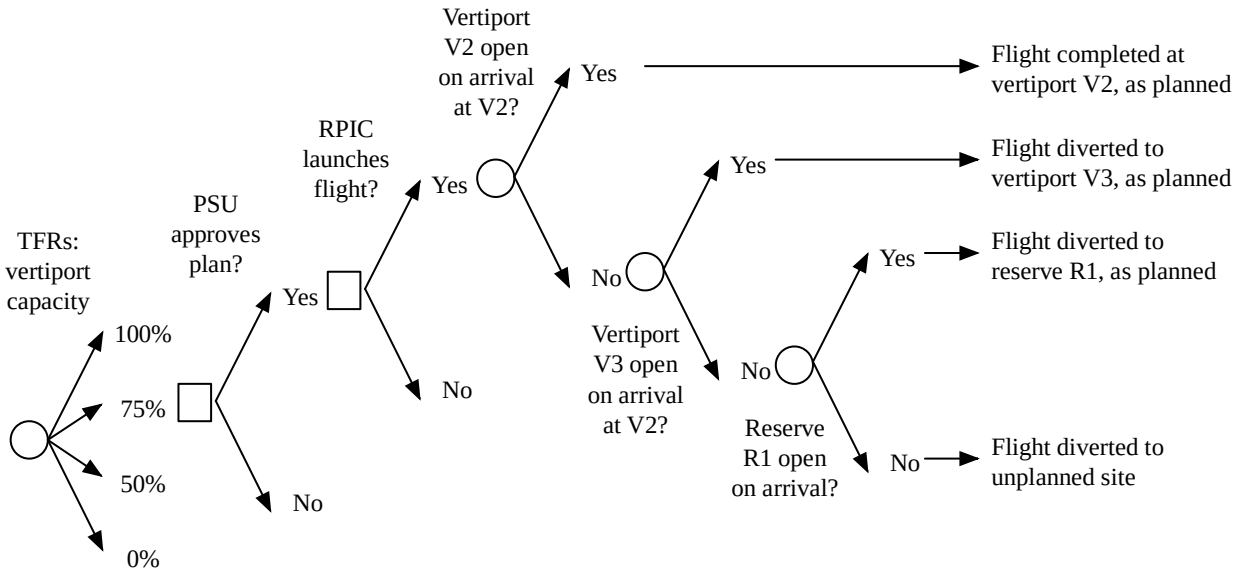

Figure 21: Decision tree for Scenario 3.

The DT in *Figure 21* indicates that there are three major decisions that are made in this scenario: *i)* creating TFRs (which don't have to be the same for all of the vertiports and could also be focused on corridor airspace segments); *ii)* approval of the proposed flight plan and associated contingency plan by the traffic manager responsible for TMFs based on consideration of all of the flights relevant to this timeframe; and *iii)* a final decision by the RPIC to proceed with the flight shortly before departure). There are also three chance nodes associated with the impact of the actual weather development on the availability of V2, V3, and R1 for landing this flight.

Figure 22 shows the subjective probability estimates relevant to this DT provided by the expert meteorologist. *Figure 23* then shows the aggregation of these event probabilities to estimate the probability of different scenario variations (paths) associated with the decision tree.

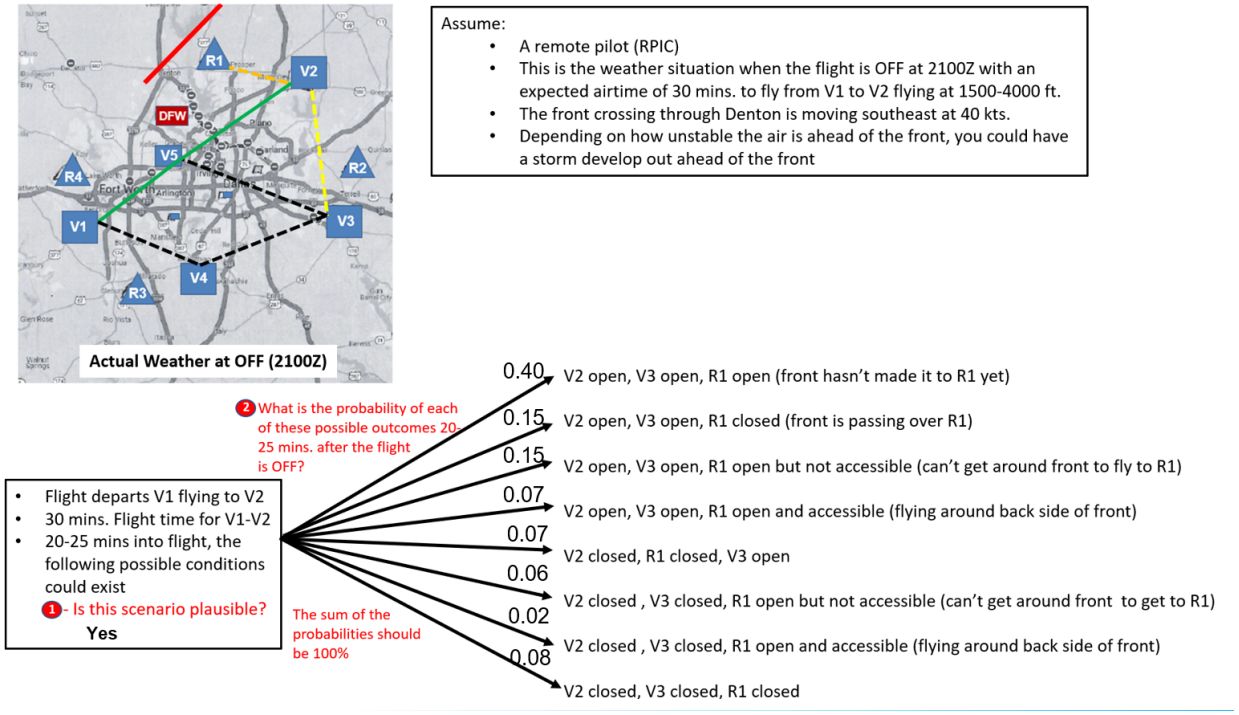

Figure 22: Subjective probability estimates provided by meteorologist.

Other input from meteorologist included:

1. *"You're going to have to think about whether some of these routes could be crossing through arrival or departure lanes for DFW."*
2. *"Here are my answers to your questions, but please remember that there are so many variables that could affect these answers."*
3. *"This is a very realistic scenario."*
4. *"If possible, the dispatcher should probably have planned and fueled to have V5 and maybe even V4 available as feasible alternates, and made R1 the least desirable alternate. But that begins to add extra fuel requirements. And they'll also be required to have a certain amount of reserve fuel in addition to having enough to make it to all of these alternates."*
5. *"You'd like to have the meteorologist monitoring and in close contact with the dispatcher."*
6. *"The by the traffic manager responsible for TMFs needs access to meteorology expertise as well."*

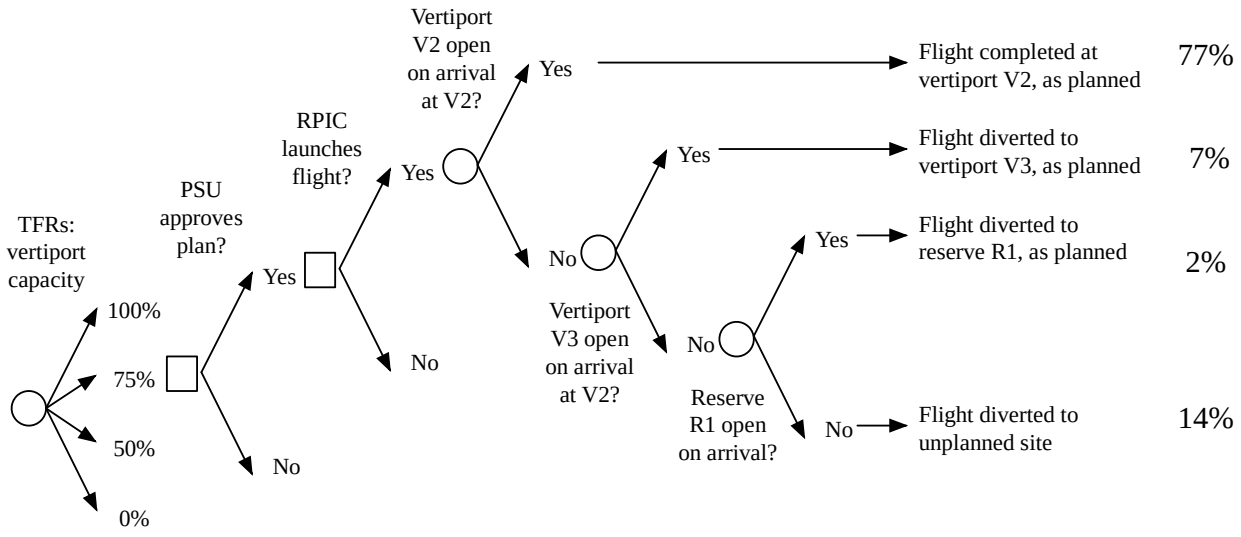

Figure 23: Decision tree for Scenario 3 with probabilities on each leaf.

As additional input, the meteorologist (who has had a great deal of experience observing the decision making of airline dispatchers and pilots in Part 121 operations) provided estimates of the probability of a pilot deciding to proceed with the flight in this scenario (see *Figure 24*).

- Assume that the schedule places time pressure on the pilot to depart when making the go/no-go decision.
- What is the probability that the remote pilot will decide to depart as scheduled at 2100 with the actual weather as shown on the previous slide?
  - If the remote pilot is well trained and experienced and is supported by a dispatcher and meteorologist at an operations center? **0.85**
  - If the remote pilot is relatively new without dispatch support, and is part of a small fleet of aircraft that relies on the general information provided by a meteorology service? **0.15**

Figure 24: Estimates of the probability of a pilot making a decision to proceed with the flight.

Reviewing this scenario, an evaluator could conclude that:

1. This is a plausible, likely scenario for the proposed urban area. This conclusion might be further supported by analysis of historical weather data or further input from expert meteorologists.
2. Without additional specified mitigations, if this scenario occurs, the performance of the flight described in this example is not sufficiently safe. If launched, it is likely (with an estimated conditional probability of 14%) that, given this scenario, the flight will have to attempt an emergency landing at an unplanned site (such as a sports park or on a highway), with the potential for minor or moderate consequences (injury to passengers or pedestrians and a negative impact on the perception of the safety of such flight operations, having an major impact on the achievement of business objectives).
3. Without additional specified mitigations, performance of the proposed operation is categorized as high risk. Thus, without additional specified mitigations, the proposed flight operation should not be approved based on this scenario.

In summary, the Scenario Based Evaluation process described above defines a six (6) step process. For each scenario in the test set:

1. Judge whether in the proposed urban area a given scenario from the test set is likely.

2. Determine the possible outcomes (paths in the DT) if this scenario occurs in the proposed urban area.
3. Estimate the probability of each outcome (paths in the DT) in the proposed urban area, conditional on the occurrence of this scenario.
4. Characterize the consequences associated with each outcome (path in the DT) in the proposed urban area.
5. Categorize the risk associated with this scenario using a risk matrix like the one shown in *Figure 20* based on the (conditional) probabilities of the different outcomes (paths in the DT) and the associated consequences.
6. If any one of the scenarios in the test set that is judged to be likely in the proposed urban area has an assigned risk based on the matrix in *Figure 20* that is established as high or extreme, then the proposed flight operation should be rejected unless sufficient mitigations are added as part of the proposed flight operation and documented in the request for approval.

In this example, the conditional probability of the path in the DT with arrivals to V2, V3 and R1 stopped has been estimated as almost certain (14%) for this scenario. If that outcome occurs, the consequence can be categorized as potentially minor or moderate as the contingency plan indicated that V2, V3 and R1 were the only available planned alternates for this flight. Using the decision matrix shown in *Figure 20*, performance in this scenario would be categorized as high risk. The requested approval of this flight operation would therefore be rejected unless mitigations were introduced and documented in a revised request for approval.

3.2.4 Mitigations to Reduce Risk

The following five (5) mitigations will reduce risk and increase approval of the proposed flight operation:

1. Section 3.2.4.1: Ensure Defined Procedures and Adequate Training;
2. Section 3.2.4.2: Pre-Flight Evaluation of Contingency Plans by the Traffic Manager Responsible for TMFs;
3. Section 3.2.4.3: Flight Operator Pre-Flight Contingency Planning;
4. Section 3.2.4.4: Real-Time Traffic Management;
5. Section 3.2.4.5: Broad Mitigations.

3.2.4.1 *Ensure Defined Procedures and Adequate Training*

The first mitigation is to require defined procedures and adequate training of all the involved personnel to ensure effective coordination and communication among them if an ad hoc emergency landing or a landing at one of the designed emergency landing sites is necessary (keeping in mind the possibility that this could involve coordination to land more than just this one UAV at a particular site).

3.2.4.2 *Pre-Flight Evaluation of Contingency Plans by the Traffic Manager Responsible for TMFs*

The second mitigation is pre-flight evaluation of the contingency plan for each proposed flight by the traffic manager responsible for the TMF relative to the already approved plans for other flights to ensure that there are enough landing slots available at the available vertiports to deal with potential off-nominal weather scenarios that result in diversions.

This assessment could be made easier if the number of potential landing slots constructed at the vertiports is large relative to possible demand. If demand is expected to be high relative to capacity, however, the flight operator would need to demonstrate that there will be a qualified traffic

manager responsible for the TMF and for evaluating each flight who will, with automation support, determine whether the proposed 4D trajectory and associated contingency plan for alternative landing sites for a given flight is feasible given the already approved plans for other flights. Note that this approval would likely be an automatic assessment (using the TFRs) and approval/disapproval for each proposed flight by the technology based on constraints specified by the traffic manager.

To support this function of the traffic manager responsible for the TMF, that individual would be responsible for the specification of TFRs defining ground delay programs to limit the number of slots at each vertiport planned to be filled by approved flights if there are no diversions. This information would need to be disseminated to the flight operators to inform their flight planning. (Ground stops for arrivals at a given vertiport could also be used for more tactical traffic flow management.)

To evaluate proposed flight plans, the traffic manager would then have to provide the supporting automation with input specifying the possible scenarios that need to be accommodated. For example, based on an ensemble weather forecast, for Scenario 3 the traffic manager might specify that the set of approved 4D trajectories and contingency plans for Scenario 3 has to be viable if landings at V2, V3 and R1 are stopped from 2120-2230Z. This type of judgment would require the expertise of a meteorologist (or a traffic manager with sufficient meteorology training). And this information would have to be disseminated to the flight operators as well in order to inform their flight planning.

The automation could then consider the active TFRs to determine whether a particular proposed flight plan and its associated contingency plan should be approved (with oversight by the traffic manager responsible for the TMF). (If the flight operator submitted a range of acceptable arrival times along with a preference for a flight's estimated time of arrival, then the automation could use this flexibility in its consideration for approval of the proposed flight plan.)

The need to conduct such contingency planning implies a requirement to demonstrate adequate staffing and training of traffic managers responsible for the TMF and meteorologists, as well as for the design of procedures and supporting automation.

The implication is that, for a proposed flight operation to be approved, the above mitigations would have to be demonstrated as part of the proposal.

3.2.4.3 *Flight Operator Pre-Flight Contingency Planning*

A further implication of this scenario is that, in order to get approval for the proposed flight operation, the dispatcher/flight planner (which for smaller operations could be the RPIC) would be trained and capable of using this information from the traffic manager responsible for the TMF to generate a proposed 4D trajectory and contingency plan specifying feasible alternative landing sites for each flight. Note that such pre-flight planning would likely occur 45-60 minutes before planned OFF and would require automation support.

In the example presented for Scenario 3 above, the specified contingency plan indicated that V3 and R1 were the only alternates that this flight could use. If the traffic manager responsible for the TMF has indicated that contingency plans must deal with the possibility that V2, V3 and R1 could all be closed from 2120-2230Z, then this submitted flight plan with its contingency plan would be rejected by the traffic manager responsible for the TMF. As long as it has been specified that the

traffic manager responsible for the TMF has the responsibility and capability to make such a judgment, the proposal by the flight operator could be approved as this check by the traffic manager responsible for the TMF would provide the necessary safeguard when the flight operator submitted a proposed flight plan that was not acceptable from a system safety perspective.

Given this process, the flight operator could consider the information from the traffic manager responsible for the TMF when developing the contingency plan for the flight in Scenario 3 and either:

1. Submit as contingencies V3, V5 and R1 if the aircraft could be fueled to use those sites as alternates (but could not divert to V4), as the traffic manager responsible for the TMF has not indicated that V5 might be stopped for arrivals in this scenario. This would then be a viable contingency plan that the traffic manager responsible for the TMF could approve if there weren't too many other diversions to V5 relative to its capacity with a 75% reduction in arrivals due to the ground delay program.
2. Submit a flight plan that indicated an estimated time of departure at 2230Z, indicating V3 and R1 as the alternates because it could not be fueled to divert to V5.

3.2.4.4 *Real-Time Traffic Management*

The fourth mitigation, i.e., real-time traffic management, involves the following:

1. Shortly before the estimated time of departure, the process submitted for approval would have to indicate that a qualified RPIC (potentially with input from a qualified meteorologist) would review the current weather and make the final go/no go decision based on the weather development shortly before departure.
2. The submission would also need to indicate that, as the flight proceeded, the RPIC and meteorologist would monitor the weather to see if an early diversion decision should be made. In Scenario 3, for instance, the meteorologist might inform the RPIC of the need to divert to V5 15 minutes into the flight. Because of the limited availability of landing slots, however, this would need to be coordinated with the traffic manager responsible for the TMF (with supporting software). (The comment of the meteorology SME who was consulted was that the RPIC would want to have the meteorologist "looking over his shoulder" during this flight.)
3. The submission for approval of this flight operation would further have to indicate that if, as an example, the traffic manager responsible for the TMF (with input from his supporting meteorologist and the V2 and V3 vertiport managers) stopped arrivals into V2 and V3 20-25 minutes into the flight discussed in Scenario 3, the traffic manager responsible for the TMF (with automation support) would have to consider the approved contingency plans for all of the flights filed to arrive at V2 and V3 in this time period and assign and communicate diversion airports to the RPICs of the airborne aircraft based on consideration of the number of available slots at V4 and V5. A ground stop would also have to be initiated for flights filed to arrive at V2 and V3 if they had not yet departed.
4. The automation used for traffic flow management (with oversight by the traffic manager responsible for the TMF) is assumed to have responsibility for approving the 4D trajectory for a flight. The trajectories for the diversions would need to be checked in real time as part of the assignment of diversion vertiports to particular flights, or the structure of the corridor airspace would have to be designed appropriately, with separate lanes for each direction along a corridor and ideally with passing lanes and/or reliance on DAA for safe separation. Note that this

includes an assumption that, in the real-time planning of the diversions, flights have sufficiently conflict free 4D trajectories to their diversion vertiports and have been planned to arrive at different times for landing at their vertiports, or that automation is capable of sequencing flights for landing as they arrive at the diversion vertiports.

Note that this latter mitigation (Point 4) may be the most challenging mitigation to implement and would require careful thought regarding the necessary ground-based support automation (for the traffic manager responsible for the TMF and staff at vertiports) and/or necessary on-board support automation.

3.2.4.5 *Broad Mitigations*

Finally, in terms of the challenges of defining an acceptably safe process to support Scenario 3, there are some broad mitigations that could be considered:

1. Ensure that the available vertiports have a landing capacity that is significantly higher than the potential demand in off-nominal scenarios so that contingency planning is much easier.
2. Limit operations to short flight durations to reduce the need to plan for unexpected weather.
3. Design corridors with unidirectional lanes that allow passing.
4. Require a pilot on-board for flights to reduce the potential consequences associated with emergency landings for missions with potentially high consequences (such as flights with passengers on-board or flights over areas with a high density of pedestrians).

In summary, the discussion above illustrates the benefit of evaluating the approval of a proposed flight operation based on consideration of concrete scenarios, as this helps the evaluator by increasing the perspicuity of important considerations.

3.2.5 Further Consideration of Scenario 2

Scenario 2 added an additional factor: loss of air-ground communication as a flight approaches its destination in a scenario where convective weather stops arrivals to one or more vertiports. To evaluate the extent to which this scenario needs to be considered in determining the approval of a proposed flight operation two questions arise. First, how likely is this to occur? Is loss of communication going to be rare enough that it can simply be ignored? Second, if it does arise, what mitigations are necessary to make it safe?

The likelihood of a loss of communication depends strongly on the details regarding the design of the communication capabilities, including backup systems. That capability is likely to improve significantly by the time remotely piloted UAM vehicles become routine, so a thorough analysis was not attempted.

However, an expert in aviation communications was asked to provide a qualitative assessment of the likelihood of a communication outage for a single aircraft in order to emphasize the importance of looking at interacting factors such as a closure of vertiports simultaneously with a loss of air-ground communication using the envisioned communication network as describe earlier in the CONOPS for Scenarios 1-3. The response of the SME to the following questions is provided below.

Question: Assume loss of air-ground communication by a single remotely piloted UAM aircraft. How could this communications system fail? How likely are such failures?

1. Mechanical failure such as an antenna. SME response: *"Low likelihood. There are well-tested products available that could be used for UAM application. The newly integrated systems may have a slightly higher risk associated with failure while operational limits are being pushed in dense environments."*
2. Software failure/bug. SME response: "*Moderate likelihood. Software failures are less likely than bugs. However, due to constant software updates, some systems can be more vulnerable to operational errors (e.g., an operator uploading source code without robust testing causing the failure). As the new UAM networks begin to converge into the NAS, constant software updates may be required based on demands, which could increase the likelihood of this failure.*"
3. Cyberattack? SME response: "*Moderate to high likelihood. As UAM becomes increasingly integrated into the NAS, it will create more and more attack vectors. This could increase the likelihood of advanced persistent threat actors targeting the systems. The actors could aim for espionage, data theft, or system disruptions.*"
4. Other? SME response: "*The other points of failure would revolve around environmental concerns. First, Weather conditions could disrupt communications. This would be a low to moderate likelihood, but very dependent on the geographical location. Second, solar flares could disrupt satellite communications. This would be a low to moderate likelihood based on the solar maximum.*"

These qualitative estimates suggest that a scenario involving the closure of a vertiport along with a loss of air-ground communication needs to be addressed in the evaluation of a proposed flight operation. One mitigation is obviously to improve the design of the hardware and software to reduce the likelihood of such a communications failure relative to these estimates. However, this input from the SME suggests that additional mitigations need to be in place assuming this kind of scenario could arise.

4 CONCLUSION AND RECOMMENDATIONS

This report has addressed the use of both qualitative (Section 2) and quantitative (Section 3) RA methods to many aspects of AAM/UAM design and operations.

The discussion of qualitative RA in Section 2 included both an overview of methods (Section 2.1) and an application of those methods to AAM/UAM (Section 2.2). The overview of methods in Section 2.1 consisted of an overview of six (6) prominent and applicable qualitative RA methods (CAST, FMEA, FRAM, ID, STAMP, and STPA). The application of those methods to AAM/UAM in Section 2.2 presented four applications of various methods to AAM/UAM design and operations, namely: *i)* DAA systems, propulsion systems, and vertiport operations; *ii)* flight planning and strategic deconfliction; *iii)* autonomous CC; and *iv)* human-automation interaction and human-human interaction.

The discussion of quantitative RA in Section 3 included both an overview of the DA method (Section 3.1) and an application of the DA method to AAM/UAM (Section 3.2). The overview of the DA method in Section 3.1 highlighted the method's strengths (detailed and thorough description of system state) and weaknesses (calculation or estimation of every single conditional probability), as well as the critical and difficult problem of model parsimony in safety models. The application of the DA method to AAM/UAM in Section 3.2 demonstrated that these methods can be profitably applied by estimating the conditional probabilities using a SME, and the analysis

uncovered the important fact that the risk of accident in the considered flight planning and strategic deconfliction scenario is substantive. The clear implication is that such methodologies should play an integral role in AAM/UAM design and operations.

These results provided guidance in developing a proposal for an approach to integrate multiple safety risk assessment methods in the assessment of proposed AAM/UAM operations. The need for this is emphasized by findings reported by [Thomas, STAMP]: "A recent case study comparing FMEA and STAMP found that STPA found 27% of hazards that were missed by FMEA. However, FMEA found 30% of hazards that were missed by STPA."

The following seven (7) steps for the integrated use of qualitative and quantitative RA methodologies in AAM/UAM design and operations follow from the analysis in Sections 2 and 3:

1. Step 1. Apply a qualitative risk assessment method to evaluate a proposed AAM/UAM operation in order to identify key hazards and associated risks. The qualitative SRA framework illustrated in Section 2.2.1, which is a refinement of the traditional safety risk assessment requirements outlined in FAA's Order 8040.4C Safety Risk Management Policy (SRMP) [FAA 8040.4C] is very suitable for such an initial step in this proposed integrated approach. (As discussed in Section 2.2.1, the illustration of this method to evaluate DAA systems, propulsion systems and vertiport systems for a sample flight operation identified 76 plausible hazard conditions, which are documented in the attached spreadsheet.) Alternatively, for this first step, FMEA could be applied to identify all of the potential failure modes for a proposed flight operation instead of this SRA framework, as this method similarly produces a list of hazard conditions.
2. Step 2. Screen the set of identified hazard conditions or failure modes to eliminate from further consideration those hazard conditions for which a sufficient mitigation has been specified to prevent that hazard condition from arising in the proposed flight operation.
3. Step 3. As illustrated in Section 2.2.2.2, develop an influence diagram (ID) to make explicit the factors that could interact to determine the safety risk associated with the proposed AAM/UAM flight operation. This ID can be used as a shared visual representation to work with the necessary range of SMEs to identify all of these factors. Identification of the factors to include in this influence diagram could be further informed by a STAMP analysis.
4. Step 4. For each of the remaining plausible hazard conditions identified in Step 1, determine whether a combination of the factors identified in the ID could interact with that hazard condition to result in a cascade of events, actions, and environmental conditions to create a scenario that could result in a significant consequence (ranging from minor to catastrophic) as defined in *Figure 20*. (If the consequence is deemed to be insignificant, still ensure that any necessary procedures are in place to deal with the hazard condition.) The result of this step is a test set including the range of scenarios necessary to fully evaluate a proposed flight operation.
5. Step 5. Sketch a decision tree for each such scenario associated with a given hazard condition that could result in a significant consequence to make explicit the potential sequence of events, actions, and environmental conditions.
6. Step 6. Using SME input or historical data, estimate the conditional probability of each possible outcome (path in the decision tree) given that the defining hazard condition arises.

7. Step 7. Determine whether sufficient mitigations have been specified in the proposed flight operation to sufficiently reduce the likelihood of a possible outcome (path in the decision tree) or reduce the potential consequences associated with a given scenario as specified by the decision matrix shown in *Figure 20*. If not, reject the proposed flight operation.

In summary, it is recommended that an integrated set of RA methodologies should be considered in risk analysis of AAM/UAM systems. Integrated RA methodologies facilitate comprehensive hazard analysis, which is crucial for these highly complex systems. The justification for this recommendation is that *i)* AAM/UAM systems are highly complex and *ii)* the potential severity of AAM/UAM accidents is high. The complexity of AAM/UAM systems is self-evident; this complexity is underscored by the many integral and integrated systems comprising AAM/UAM operations, as outlined in the A64 Task 1 background report [Rice, 2023]. RA methodologies are designed specifically to facilitate hazard analysis of complex systems, and they have proven to be essential in other systems with similar (or greater) complexity and similar (or greater) likelihood and/or severity of hazards and accidents [Luther, 2023].

While the scenarios and analysis in this report are merely representative and nowhere near comprehensive, they together highlight several facts. First, the scope of RA methodologies is quite wide, spanning both quantitative and qualitative, and encompassing widely varying approaches within each of these two groups. Second, the scope of AAM/UAM subsystems and operations to which RA methodologies may be applied is likewise quite wide, spanning communications, command and control, detect and avoid, strategic deconfliction, and many others. The implication is that the application of an integrated set of RA methodologies is well-aligned with the needs of AAM/UAM risk analysis, which is, by its nature, a diverse and challenging problem.

More specifically, AAM/UAM risk analyses should include: *i)* multiple complementary qualitative RA methodologies employed in an integrated manner, and *ii)* qualitative and quantitative RA methodologies employed in an integrated manner. The justification for this recommendation comes from the effective and insightful methodological integrations found in this report. First, as shown in Section 2.2.2 on flight planning and strategic deconfliction, the two qualitative RA methodologies of ID and FMEA can be effectively integrated to yield a robust hazard analysis richer than either methodology would yield individually. Second, as shown in Section 3.2 on the application of quantitative RA methodologies to AAM/UAM systems, the qualitative analysis from Section 2.2.2 is effectively leveraged in setting up the quantitative analysis of the flight planning and strategic deconfliction scenario. The insight is that the structured thinking about problem domain, system decomposition, hazard identification, and subsystem interdependencies, which form an essential component of qualitative RA methodologies, is an essential precursor to the effective use of the quantitative RA methodologies. Briefly, the qualitative RA methodologies help frame the hazard analysis questions, and the quantitative RA methodologies help assemble the calculations involved in obtaining numerical answers to those questions.

To support these RAs, a test set of detailed and representative AAM/UAM scenarios should be developed and used within the context of qualitative RA methodologies. Note that this test set potentially applies to all AAM/UAM sites, thus leveraging the work to produce it. The justification for this recommendation is found in the useful applications of insightful and feasible AAM/UAM scenarios in both Section 2.2 (applications of qualitative RA methodologies) and Section 3.2

(applications of quantitative RA methodologies). The necessity for scenario-based RA is self-evident: the varied environmental operating conditions that are possible and likely for anticipated AAM/UAM CONOPS are incredibly large --- far too large to even be "enumerated," much less individually analyzed in detail. The recommended approach to address this discrepancy between problem scope and solution feasibility is to carefully develop a suite of scenarios and apply qualitative and quantitative RA methodologies to each. The handful of scenarios discussed in this report is a useful illustration of this approach.

To support such risk assessments, it is recommended that a robust data collection framework be established, sharing it among stakeholders, including manufacturers, operators, and regulatory bodies. Effective RA methodologies rely heavily on accurate and comprehensive data. Since AAM/UAM is an emerging technology with limited public data, fostering collaboration and data sharing can enhance the precision of RA models. A framework similar to the Aviation Information Sharing and Analysis Center (Aviation ISAC), which gathers industry information on cyber-attacks, should be developed for AAM/UAM. This AAM/UAM-specific framework would focus on collecting data related to operational performance, incident reports, maintenance records, and environmental factors. Such a system would enable real-time data sharing and analysis, leading to more accurate risk assessments and timely identification of emerging risks. This collaborative approach would also facilitate the development of industry-wide best practices and improve the overall safety and reliability of AAM/UAM operations.

And to further improve effectiveness in conducting such RAs standardized procedures should be developed for conducting qualitative and quantitative RA across UAM/AAM operations. Standardizing RA procedures will ensure consistency and reliability in safety assessments across the AAM/UAM industry. A standardized format for RA would enable the FAA to effectively manage and approve industry partners, streamline the certification process, and facilitate the comparison of safety practices. These standardized procedures should be comprehensive, covering all aspects of AAM/UAM operations, from design and manufacturing to daily operations and maintenance. The FAA can ensure that all stakeholders adhere to the same high safety standards by providing clear guidelines and requirements. This will improve safety outcomes and foster greater trust and collaboration within the industry.

An additional recommendation is to take advantage of the scenario-based approach described above to implement scenario-based training programs for all AAM/UAM operations personnel, specifically focusing on non-normal operations. Scenario-based training programs are essential for preparing personnel to handle real-world operations, particularly under non-normal conditions. These training programs should be designed to simulate various scenarios AAM/UAM operators might encounter, including emergency situations, system failures, and adverse weather conditions. By incorporating human factor-based evidence, these programs can help identify and mitigate risks associated with human performance and interaction with automated systems. Training scenarios should be regularly updated based on operational data and emerging threats, ensuring personnel are always prepared for the latest challenges. This approach will enhance the readiness and resilience of AAM/UAM operations, leading to improved safety and efficiency.

Finally, industry safety standards for UAM/AAM should be established through stakeholder collaboration, guided by the results of RAs as described above. Developing specific safety standards tailored to the UAM/AAM industry is crucial for enhancing safety, facilitating

regulatory compliance, and improving technology implementation. These standards should be created with industry stakeholders, including manufacturers, operators, regulatory bodies, and research institutions. The standards should address the unique challenges and risks associated with AAM/UAM operations, such as urban airspace management, vertiport operations, and integration with existing air traffic control systems when flights enter controlled airspace. By setting clear and consistent safety standards, the industry can ensure that all AAM/UAM operations are conducted safely and efficiently. These standards will also help guide developing and deploying new technologies, ensuring they meet the highest safety and performance criteria.

5 REFERENCES

[Arel, 2022]
Arel, T.L.
"Safety Management System Manual"
Air Traffic Organization
2022
https://www.faa.gov/air_traffic/publications/media/ATO-SMS-Manual.pdf

[ASQ]
American Society for Quality (ASQ)
"Failure mode and effects analysis (FMEA)"
https://asq.org/quality-resources/fmea

[Duquerroy, 2021]
Duquerroy, L., and Dow, R.M.
"Space for Urban Air Mobility Webinar" (Slides)
European Space Agency
https://business.esa.int/sites/business/files/Urban Air Mobility - Webinar slides 10.02.2021.pdf

[Ertürk, 2020]
Cenk Ertürk, M., Hosseini, N., Jamal, H., Şahin, A., Matolak, D. and Haque, J.
"Requirements And Technologies Towards UAM: Communication, Navigation, And Surveillance"
Integrated Communications Navigation and Surveillance Conference (ICNS)
Herndon, VA
pp. 2C2: 1-15
2020
https://doi.org/10.1109/ICNS50378.2020.9223003

[FAA 8040.4C]
Federal Aviation Administration (FAA)
Order 8040.4C: Safety Risk Management Policy (SRMP)
2023
https://www.faa.gov/documentLibrary/media/Order/FAA_Order_8040.4C.pdf

[FAA 8040.6A]
Federal Aviation Administration (FAA)
Order 8040.6A - Unmanned Aircraft Systems (UAS) Safety Risk Management (SRM) Policy
2023
https://www.faa.gov/documentLibrary/media/Order/Order_8040.6A.pdf

[FAA HFEQ]
Federal Aviation Administration (FAA)
Standard Practice: Human Factors Engineering Requirements
HF-STD-004a

September, 2016
https://hf.tc.faa.gov/publications/2016-09-human-factors-engineering-requirements/HF-STD-004A.pdf

[FAA UAM 2023]
Federal Aviation Administration (FAA)
"Urban Air Mobility (UAM) Concept of Operations, Version 2.0"
April, 2023
https://www.faa.gov/sites/faa.gov/files/Urban Air Mobility %28UAM%29 Concept of Operations 2.0_0.pdf

[FSF AD]
Flight Safety Foundation
"Accident Data"
https://flightsafety.org/category/accident-data/

[FSF ASN]
Flight Safety Foundation
"Aviation Safety Network"
https://aviation-safety.net/database/

[Hollnagel, 2010]
Hollnagel, E.
"The functional resonance analysis method"
2010
https://functionalresonance.com/onewebmedia/FRAM 101 ds 0.1.pdf

[Hollnagel, 2016]
Hollnagel, E.
"The functional resonance analysis method"
2016
https://functionalresonance.com/

[Howard, 2005]
Howard, R. and Matheson, J.
"Influence diagrams"
Decision Analysis
vol. 2, no. 3, pp. 127-143
September, 2005
https://doi.org/10.1287/deca.1050.0020

[IATA]
International Air Transport Association (IATA)
https://www.iata.org/

[Jamal, 2020]

Jamal, H. and Matolak, D.W.
"Advanced Physical-Layer Technologies in VHF Data Link Communications"
Proceedings of the AIAA/IEEE Digital Avionics Systems Conference (DASC)
San Antonio, TX
October, 2020
https://doi.org/10.1109/DASC50938.2020.9256527

[Lange, 2024]
Lange, R., Rice, S., Wallace, R.J., Winter, S.R., Vasquez, M.N., and Woods, S.
"Modeling a System of Systems for Advanced Air Mobility Operations"
Journal of Air Transport Management
2024 (DRAFT)

[Leveson STAMP, 2002]
Leveson, N.G.
"System Safety Engineering: Back To The Future"
Department of Aeronautics and Astronautics, Massachusetts Institute of Technology (M.I.T.)
2002
http://sunnyday.mit.edu/book2.pdf

[Leveson STPA, 2018]
Leveson, N.G. and Thomas, J.
STPA Handbook
2018
http://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

[Leveson CAST, 2019]
Leveson, N.G.
CAST Handbook: How to Learn More from Incidents and Accidents
2019
http://psas.scripts.mit.edu/home/get_file4.php?name=CAST_handbook.pdf

[Leveson STAMP, 2020]
Leveson, N.G.
"Introduction to STAMP: Part 1" (Slides)
2020
http://psas.scripts.mit.edu/home/wp-content/uploads/2020/07/STAMP-Tutorial.pdf

[Luther, 2023]
Luther, B., Gunawan, I., and Nguyen, N.
"Identifying effective risk management frameworks for complex socio-technical systems"
Safety Science (Elsevier)
vol. 158, pp. 105989
2023
https://doi.org/10.1016/j.ssci.2022.105989

[Muenning, 2017]
Muenning, P.
"Decision Analytic Modeling"
International Encyclopedia of Public Health (Second Edition)
pp. 211-216
2017
https://doi.org/10.1016/B978-0-12-803678-5.00099-0

[NTSB, 2002]
National Transportation Safety Board (NTSB)
"Aviation Investigation Manual: Major Team Investigations (and Appendices)"
November, 2002
https://www.ntsb.gov/about/Documents/MajorInvestigationsManual.pdf
https://www.ntsb.gov/about/Documents/MajorInvestigationsManualApp.pdf

[NTSB, 2006]
National Transportation Safety Board (NTSB)
"2006 Annual Report to Congress"
Report # NTSB/SPC-07/01
January, 2007
https://www.ntsb.gov/about/Documents/SPC0701.pdf

[Parnell, 2013]
Parnell, G.S., Bresnick, T., Tani, S.N., and Johnson, E.R.
Handbook of decision analysis
John Wiley & Sons
2013
https://onlinelibrary.wiley.com/doi/book/10.1002/9781118515853

[Patriarca, 2020]
Patriarca, R. *et al.*
"Framing the FRAM: A literature review on the functional resonance analysis method"
Safety Science, vol. 129, 104827
September, 2020
https://doi.org/10.1016/j.ssci.2020.104827

[Pearl, 2005]
Pearl, J.
"Influence diagrams -- historical and personal perspectives"
Journal of Decision Analysis
vol. 2, no. 4, pp. 232--234
December, 2005
https://doi.org/10.1287/deca.1050.0055

[Raiffa, 1968]
Raiffa, H.

Decision Analysis: Introductory Lectures on Choices Under Uncertainty
Addison-Wesley
1968

[Rice, 2023]
Rice, S. *et al.*
"A64: Task 1: Background Report for Identify Models for Advanced Air Mobility (AAM)/Urban Air Mobility (UAM) Safe Automation"
FAA ASSURE
2023
https://www.assureuas.org/projects/identify-models-for-advanced-air-mobility-aam-urban-air-mobility-uam-safe-automation/

[Shachter, 1986]
Shachter, R.
"Evaluating influence diagrams"
Operations Research
vol. 34, no. 6, pp. 871-882
1986
https://doi.org/10.1287/opre.34.6.871

[Smith, 2021]
Smith, P.J. and Spencer, A.
"Design Concepts to Support Distributed Work: Human-Automation Interaction in The Shared Control of Unmanned Aerial Vehicles - Final Report,"
The Ohio State University, CSEL-2021-4
2021
https://www.researchgate.net/publication/358576336_DESIGN_CONCEPTS_TO_SUPPORT_DISTRIBUTED_WORK_HUMAN-AUTOMATION_INTERACTION_IN_THE_SHARED_CONTROL_OF_UNMANNED_AERIAL_VEHICLES_Final_Report

[Smith, 2022]
Smith, P.J. et al.
"A21: Integrating Expanded And Non-Segregated UAS Operations Into The NAS: Impact On Traffic Trends And Safety: Final Report"
https://www.assureuas.org/wp-content/uploads/2021/06/A21-Final-Report.pdf

[Snyder, 2021]
Snyder *et al.*
“A25: Develop Risk-Based Training and Standards for Waiver Review and Issuance”
FAA ASSURE
2021
https://www.assureuas.org/projects/low-altitude-risk-assessment-roadmap/

[Stamatis, 2003]

Stamatis, D.H.
Failure Mode and Effect Analysis: FMEA from Theory to Execution, Second Edition
American Society for Quality (ASQ), Quality Press
https://asq.org/quality-press/display-item?item=H1188

[Stamatis, 2015]
Stamatis, D.H.
The ASQ Pocket Guide to Failure Mode and Effect Analysis (FMEA)
American Society for Quality (ASQ), Quality Press
2015
https://asq.org/quality-press/display-item?item=E1468

[Stansbury, 2022]
Stansbury, R. *et al.*
"A37: UAS Standards Tracking, Mapping, and Analysis"
FAA ASSURE
2022
https://www.assureuas.org/projects/standard-tracking-mapping-analysis/

[Sulaman, 2019]
Sulaman, S.M. et al.
"Comparison of the FMEA and STPA safety analysis methods–a case study"
Journal of Software Quality, vol. 27, pp. 349--387
2019
https://doi.org/10.1007/s11219-017-9396-0

[Thomas, 2013]
Thomas, J.
"Basic STPA Tutorial"
2013
http://psas.scripts.mit.edu/home/wp-content/uploads/2013/04/Basic_STPA_Tutorial1.pdf

[Thomas, 2016]
Thomas, J.
"Intro to Systems Theoretic Process Analysis (STPA)"
2016
http://psas.scripts.mit.edu/home/wp-content/uploads/2016/01/Systems-Theoretic-Process-Analysis-STPA-John-Thomas.pdf

[Thomas, STAMP]
Thomas, S.
"An introduction to STAMP"
Functional Safety Engineer
https://functionalsafetyengineer.com/introduction-to-stamp/

[U.S. Army, 2015]

U.S. Army
Accident Investigators Handbook
2015
https://safety.army.mil/Portals/0/Documents/REPORTINGANDINVESTIGATION/REPORTINGANDINVESTIGATIONHOME/Standard/Accident_Investigators_Handbook.pdf

[Zhang, 2022]
Zhang, Y. *et al.*
"Systems theoretic accident model and process (STAMP): A literature review
Elsevier Safety Science
vol. 152, pp. 105596
November, 2021
https://doi.org/10.1016/j.ssci.2021.105596