A21 Final Report: Integrating Expanded and Non-Segregated UAS Operations into the NAS: Impact on Traffic Trends and Safety

Supplement D: Task 3-1 Definition of Risk-based Framework

September 8, 2020

NOTICE

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.

Contributing Authors

The authors of this report are:

Drexel University
Steven Weber
Ellen J. Bass

The Ohio State University
Philip J. Smith

Support was provided by:

Kansas State University (Polytechnic)
Timothy Bruner
Tom Haritos

Contents

List of Figures

List of Tables

1 Executive Summary

In June 2018, the National Academies of Science, Engineering, and Medicine (NASEM), in response to a Congressional request, officially released its report *"Assessing the Risks of Integrating Unmanned Aircraft Systems (UAS) into the National Airspace System."* They found:

> *...the current FAA approaches to risk management are based on fundamentally qualitative and subjective risk analysis... The qualitative nature of the current approach leads to results that fail to be repeatable, predictable, and transparent. Evolution to an approach more reliant on applicant expertise and investment in risk analysis, modeling, and engineering assessment, as is practiced in many other areas of federal regulation, might better achieve a quantitative probabilistic risk analysis (PRA) basis for decisions... Concerns by the drone industry of overly stringent certification requirements for relatively low-risk operations place unnecessary burden on the business case and can stifle innovation.*

The National Academy report further specifies that the approach to quantitative risk assessment should make use of PRAs. The development of such a framework is also motivated by Section 345 ("Small Unmanned Aircraft Safety Standards") of Public Law 115-254.

To address this report, the Federal Aviation Administration (FAA), tasked its Center of Excellence (COE) for UAS, ASSURE, to conduct research to inform the safe integration of sUAS of expanded (beyond-visual-line-of-sight) and non-segregated UAS operations. This included the object of this report: to provide a clear and consistent process and quantitative risk-assessment framework to guide the development of applications for sUAS operations, and to provide a well-defined and consistent methodology for the FAA evaluation of these applications that incorporates consideration of both the safety risks and societal benefits. The research team developed a framework that embeds the use of PRAs into a five-step process consistent with the FAA's definition of its SMS (Safety Management System). This framework defines a process for limiting analysis to critical (high-risk) scenarios and uses thresholding to categorize quantitative risk assessments in a manner consistent with current FAA definitions of "Hazard Outcomes" and "Likelihood Definitions." Finally, this framework maps the results into the structure of the risk matrix, as defined in FAA Order 8040.6, providing a rubric that structures decision making in a manner that is consistent with long-standing FAA practice.

In addition to the framework, researchers also provide the details on the supporting mathematical and logical basis necessary to demonstrate a consistent and defensible method for evaluation of sUAS applications. Furthermore, this report describes how the approach to embedding PRAs into the evaluation process reduces complexity thereby increasing its feasibility as a tool. The next steps involve developing a case study to demonstrate this quantitative risk assessment framework application. Those results will be used to further refine the framework, as necessary.

2 List of acronyms

AC:Advisory Circular
AGL:Above ground level
AIXM:Aeronautical Information Exchange Model
AMOC:Alternative method of compliance
ASIAS:Aviation Safety Information Analysis and Sharing
ASSURE: Alliance for System Safety of UAS through Research Excellence
ATO: Air Traffic Organization
AVS: Aviation Safety
BVLOS: Beyond Visual Line Of Sight
C2: Command and control
CAR: Canadian Aviation Regulation
CDF: Cumulative distribution function
CERTAIN: City Environment for Range Testing of Autonomous Integrated Navigation
CONOPS: Concept of operations
DAA: Detect and avoid
DCP: Divert/Contingency Points
FAA: Federal Aviation Administration
FDAT: Flight Data
FFRDC: Federally Funded Research and Development Center
FIXM: Flight Information Exchange Model
FTP: Flight Termination Points
HRM: Holistic Risk Model
ISSA: In-Time System-Wide Safety Assurance
JARUS: Joint Authorities for Rulemaking on Unmanned Systems
MTBF: Mean time between failure
MTR: Military training routes
NAS: National Airspace
NASA: National Aeronautics and Space Administration
NASEM: National Academies of Sciences, Engineering and Medicine
NAVAID: Navigational Aids
ORA: Operational Risk Assessment
ORAP: Operational Risk Assessment Prototype
PCE: Polynomial chaos expansion
PMF: Probability Mass Function
PRA: Probabilistic Risk Assessment

RFI: Request for Information
RPAS: Remotely Piloted Aircraft System
RTH: Return-To-Home
RV: Random Variable
SMART: Small Aircraft Risk Technology
SMS: Safety Management System
SOP: Standard Operating Procedure
SORA: Specific Operation Risk Assessment
SRM: Safety Risk Management
SRMP: Safety Risk Management Process
STPA: Systems Theoretic Process Analysis
sUAS: small UAS
SWIM: System-Wide Information Management (SWIM)
UTM: UAS Traffic Management
UAS: Unmanned Aerial Systems
UASFM: UAS Facility Map
WIXM: Weather Information Exchange Model

3 Introduction

This report provides the details defining a quantitative framework to support risk-based decision making and waiver approvals for small unmanned aircraft systems (sUAS) that can be integrated into the FAA's Safety Management System (SMS) process. The need for the development of such a framework, and thus the motivation for this project, is driven by the National Academies of Science, Engineering, and Medicine report titled "Assessing the Risks of Integrating Unmanned Aircraft Systems" [1] which included the following recommendations to the FAA:

- Recommendation: "The FAA should expand its perspective on a quantitative risk assessment to look more holistically at the total safety risk."
- Recommendation: "The FAA should establish and publish specific guidelines for implementing a predictable, repeatable, quantitative, risk-based process for certifying UAS systems and aircraft and granting operations approval. These guidelines should interpret the Safety Risk Management Policy process described in Order 8040.4B (and in accordance with International Civil Aviation Organization Doc. 9859) in the unique context of UAS."
- Recommendation: "Where operational data are insufficient to credibly estimate likelihood and severity components of risk, the FAA should use a comparative risk analysis approach to compare proposed UAS operations to comparable existing or de minimis levels of risk."
- Recommendation: "Over the next 5 years, the FAA should evolve away from subjectivities present in portions of the Order 8040.4B process for UAS to a probabilistic risk analysis (PRA) process based on acceptable safety risk."

Accomplishing the goals set forth in these recommendations has become increasingly important given the need to progress to safe integration of expanded (beyond-visual-line-of-sight) sUAS operations and sUAS operations over people.

More specifically, this 2018 NASEM report informed Section 345 of the 2018 Congressional Reauthorization Act of 2018 [2], which directly motivated this work.

This report defines such a framework, describing a quantitative, risk-based process for granting approval of sUAS operations that makes use of PRAs. It not only provides a qualitative description of this framework, but also presents details regarding the mathematical and logical basis for this principled approach that incorporates consideration of both the safety risks and societal benefits.

This framework embeds the use of PRAs into a five-step process consistent with the FAA's definition of its SMS (Safety Management System). It further defines a process for limiting analysis to critical (high-risk) scenarios and uses thresholding to categorize quantitative risk assessments in a manner consistent with current FAA definitions of "Hazard Outcomes" and "Likelihood Definitions." Finally, this framework maps the results into the structure of the risk matrix, as defined in FAA Order 8040.6[3], providing a rubric that structures decision making in a manner that is consistent with long-standing FAA practice.

The net result is a method for producing a tractable, consistent and defensible procedure for evaluation of sUAS applications, reducing complexity in the use of PRAs and thereby increasing feasibility of completing quantitative risk assessments.

Section 4 Background and Context provides additional detail regarding the motivation for this work and the goals of this particular task.

Sections 5-9 follow the recommendations in the NASEM report and embed this quantitative risk assessment framework into the FAA's Safety Risk Management Policy Process (SRMP) Process, Order 8040.4B [4]), as informed by guidance in Order 8040.6 [3].

- **Section 5 SRMP Step 1: System Analysis.** Within this initial step, this framework makes explicit the characteristics of the proposed sUAS operation that need to be specified, including proposed mitigation (the system state). This is organized into 9 categories:
  - UAS platform and payload: properties of the sUAS platform and payload,
  - Flight readiness: requirements and process for a satisfactory pre-flight check.
  - Operator workstation: properties of the hardware and software of the workstation environment.
  - Operator training and procedures: requirements for the training of the operator and the procedures that the operator will obey.
  - Flight plan: characteristics of the flight plans for this operation.
  - C2 channel: properties of the wireless command and control (C2) channel connecting the operator and the sUAS.
  - Information acquisition, processing, and dissemination capabilities: properties of the system (e.g., sensor range, accuracy) and the environment (e.g., visibility,
  - Weather environment: proposed weather environment(s) within which the sUAS is expected to operate.
  - Airspace environment: properties of the airspace environments within which the sUAS is expected to operate.
  - Ground environment: properties of the ground environment over which flights will occur.
- **Section 6 SRMP Step 2: Identified Hazards.** Consistent with FAA practice, hazard causes and hazard outcomes are indicated. The default set of hazard causes within this framework is:
  - sUAS malfunction
  - sUAS operator error
  - C2 link failure
  - Inability to sense environment
  - Inability to control flight.

The default set of hazard outcomes is:

- Proximity to or collision with a person
- In-air proximity to or collision with a manned airborne vehicle
- Proximity to or collision with the built environment.

The framework itself allows for additional or alternative categories within these two sets. However, the categories used by a waiver applicant then provide the structure for the quantitative analysis of safety risk defined in Step 3.

More specifically, as part of Step 2, based on consideration of these categorizations from Step 2 and the system specification (Step 1), the decision making process is transformed to an evaluation of likelihoods associated with high-risk scenarios for each stage of flight that are identified by the applicant. Note that many of these may be FAA specified default scenarios to consider for certain classes of operations (such as the high-risk scenarios associated with the use of a rotorcraft to deliver medical supplies along a route that includes BVLOS operations over a dense population). Note also that, if adequately supported mitigations have been identified as part of the system state description, that makes it possible to eliminate certain otherwise high risk scenarios from further consideration when completing the PRA, thus effectively pruning the decision tree and making completion of the PRA more tractable.

- **Section 7 SRMP Step 3: Analysis of Safety Risk**. In Step 3, for each of the remaining high-risk scenarios, a PRA needs to be conducted. Details of this process are provided in Section 7.

- **Section 8 SRMP Step 4: Assessment of Safety Risk**. Step 4 involves categorization of the high risk scenarios in terms of their likelihood as computed in Step 3 using an FAA Likelihood Definitions consistent with the approach contained in FAA Order 8040.6 [3], but with category boundaries expressed relative to a certain number of flights or flight miles. It further involves using the FAA's approach of defining severity categories, again from Severity Definitions in FAA Order 8040.6 [3]. This categorization of the high-risk scenarios in terms of likelihood and severity are then combined to support decision making using a safety risk assessment matrix as defined in FAA Order 8040.6 [3].

  Note that this process thus embeds the use of PRAs within established FAA practices for safety risk assessment.

- **Section 9 SRMP Step 5: Control of Safety Risk**. This step allows for the incorporation of additional mitigations and reassessment of the safety risk due to their addition.

Section 10 Likelihood and Decision Transfer Across System States extends the framework to categorize "equivalent" system states in order to make it possible to reduce the burden on the preparation of applications when they propose an operation that is similar to already approved waiver applications in terms of all of its important characteristics.

Section 11 Conclusion and Next Steps provides conclusions and the next steps.

Appendices A-D highlight key assumptions for the application of this framework and provide a simple example outlining its application.

Appendix E provides a detailed discussion of the results of a literature review and the findings from meetings with other organizations involved in defining Appendix E also provides a discussion of the approach taken by insurance companies when evaluating requests to insure sUAS operations.

In short, this document provides the details defining a principled approach to the incorporation of PRAs into the SMS process in order to provide for quantitative risk-based decision making when evaluating proposed sUAS operations. The next steps involve developing a case study to demonstrate this quantitative risk assessment framework application and illustrate the application of the necessary details to use this framework. Those results will be used to further refine the framework, as necessary.

4 Background and context

Task 3-1 aims to address three research questions and goals:

1. How can a risk-based framework be applied for an SMS process that specifies risk-based performance standards to establish compliance with FAA rules and regulations for sUAS?
2. What is an example of the application of such a risk-based framework to another sector (non-sUAS)?
3. What is an illustration of how such a risk-based framework can be applied to the application of this framework to an example of a sUAS operation?

This report describes the developed framework to support risk-based decision making and waiver approvals for small unmanned aircraft systems (sUAS). This section of the report provides background and context, focusing on the key events and documents that informed its scope. Specifically, this section is organized as follows:

1. §4.1 *NASEM Report and Congressional Reauthorization* reviews the 2018 National Academies report on PRA for UAS integration into the NAS, and subsequent 2018 Congressional Reauthorization public law on "small unmanned aircraft safety standards".
2. §4.2 *Safety Risk Management Policy Process Order 8040.4B* reviews select components of the five-step safety risk management policy process (SRMP).
3. §4.3 *FAA Order 8040.6: SRM for UAS* reviews select components of the specialization of SRMP to UAS in Order 8040.6.
4. §4.4 *Mathematical Notation* reviews the notational conventions used in this report.

4.1 NASEM Report and Congressional Reauthorization

Task 3 of the A21 was motivated in part by a report by the National Academies, and a subsequent Congressional Reauthorization.

4.1.1 2018 NASEM Report

In 2018, the National Academies of Science, Engineering, and Medicine (NASEM) released a report entitled, "Assessing the Risks of Integrating Unmanned Aircraft Systems (UAS) into the National Airspace System" [1]. This report included eleven (11) recommendations to the FAA, including the following four, quoted here incompletely for conciseness and with emphasis added:

1. "Recommendation: The FAA should expand its perspective on a quantitative risk assessment to look more holistically at the total safety risk..."

2. "Recommendation: ... *the FAA should establish and publish specific guidelines for implementing a predictable, repeatable, quantitative, risk-based process for certifying UAS systems and aircraft and granting operations approval. These guidelines should*

interpret the Safety Risk Management Policy process described in Order 8040.4B (and in accordance with International Civil Aviation Organization Doc. 9859) in the unique context of UAS..."

3. "Recommendation: Where operational data are insufficient to credibly estimate likelihood and severity components of risk, the FAA should use a comparative risk analysis approach to compare proposed UAS operations to comparable existing or de minimis levels of risk..."

4. "Recommendation: Over the next 5 years, the FAA should evolve away from subjectivities present in portions of the Order 8040.4B process for UAS to a probabilistic risk analysis (PRA) process based on acceptable safety risk..."

The 2018 NASEM report informed Section 345 of the 2018 Congressional Reauthorization of the FAA, described next.

4.1.2 2018 Congressional Reauthorization, Section 345

The 2018 Congressional Reauthorization of the FAA [2], enacted as Public Law 115-254, includes Section 345, entitled "Small unmanned aircraft safety standards". The following are select statements from that law pertinent to Task 3-1 of Project A21, quoted here incompletely for conciseness and with emphasis added:

(a) The Administrator of the Federal Aviation Administration shall establish a process for

  (1) *accepting risk-based consensus safety standards related to the design, production, and modification of small unmanned aircraft systems;*

  (2) *authorizing the operation of small unmanned aircraft system make and model designed, produced, or modified in accordance with the consensus safety standards accepted under paragraph (1)*

  (3) *authorizing a manufacturer to self-certify a small unmanned aircraft system make or model that complies with consensus safety standards accepted under paragraph (1)*

  (4) certifying a manufacturer of small unmanned aircraft systems, or an employee of such manufacturer, that has demonstrated compliance with the consensus safety standards accepted under paragraph (1) and met any other qualifying criteria, as determined by the Administrator, to alternatively satisfy the requirements of paragraph (1)

(b) Before accepting consensus safety standards under subsection (a), the Administrator of the Federal Aviation Administration shall consider the following:

  (1) *Technologies or standards related to geographic limitations, altitude limitations, and sense and avoid capabilities.*

  (2) Using performance-based requirements.

(3) *Assessing varying levels of risk posed by different small unmanned aircraft systems and their operation and tailoring performance-based requirements to appropriately mitigate risk.*

(4) Predetermined action to maintain safety in the event that a communications link between a small unmanned aircraft and its operator is lost or compromised.

(5) Detectability and identifiability to pilots, the Federal Aviation Administration, and air traffic controllers, as appropriate.

(6) Means to prevent tampering with or modification of any system, limitation, or other safety mechanism or standard under this section or any other provision of law, including a means to identify any tampering or modification that has been made.

(7) Consensus identification standards under section 2202 of the FAA Extension, Safety, and Security Act of 2016 (Public Law 114-190; 130 Stat. 615).

(8) To the extent not considered previously by the consensus body that crafted consensus safety standards, cost-benefit and risk analyses of consensus safety standards that may be accepted pursuant to subsection (a) for newly designed small unmanned aircraft systems.

(9) Applicability of consensus safety standards to small unmanned aircraft systems that are not manufactured commercially.

(10) Any technology or standard related to small unmanned aircraft systems that promotes aviation safety.

(11) Any category of unmanned aircraft systems that should be exempt from the consensus safety standards based on risk factors.

Having reviewed select portions of Section 345 of the 2018 Congressional Reauthorization Act, the next section reviews the recommended process to develop the framework, i.e., the Safety Risk Management Process (SRMP).

4.2 FAA Order 8040.4b: Safety Risk Management Process

FAA Order 8040.4B, *Safety Risk Management Policy* (SRMP), "establishes requirements for how to conduct Safety Risk Management (SRM) in the FAA" [4]. SRM is one of four components of the FAA's Safety Management System (SMS), along with Safety Policy, Safety Assurance, and Safety Promotion. Recall, one of the recommendations from the NASEM report, described in §4.1, is that the guidelines on sUAS integration into the NAS "interpret the Safety Risk Management Policy process described in Order 8040.4B...in the unique context of UAS".

This section briefly summarizes the five steps of the SRMP process. The following are select quotes from Order 8040.4B [4], quoted incompletely for conciseness and with emphasis added:

a. *System Analysis:* "The system analysis provides information that serves as the basis for identifying and understanding hazards, as well as their causes and associated safety risk."

b. *Identify Hazards:* "A hazard is a condition that could foreseeably cause or contribute to an aircraft accident."

c. *Analyze Safety Risk:* "The safety risk associated with a hazard is the combination of the severity and the likelihood of the potential outcome(s) of the hazard. Where appropriate, existing controls are taken into account prior to safety risk determination."

d. *Assess Safety Risk:* "In this step, each hazard's associated safety risk is assessed against the risk acceptance criteria identified in the safety risk acceptance plan and plotted on a risk matrix based on the severity and likelihood of the outcome."

e. *Control Safety Risk:* "If the residual risk is not acceptable, the proposed safety risk controls are redesigned or new safety risk controls are developed as necessary and the analysis is reconducted. This is done until the proposed safety risk controls enable the safety risk acceptance criteria to be met."

The subsequent corresponding sections review of each of the five steps. Following is a section briefly summarizing the FAA's specialization of the SRMP to UAS in Order 8040.6.

4.3 FAA Order 8040.6: SRM for UAS

FAA Order 8040.6, *Unmanned Aircraft Systems Safety Risk Management Policy*, "supplements FAA Order 8040.4 Safety Risk Management Policy by establishing a methodology for conducting SRM for UAS requests to operate" [3].

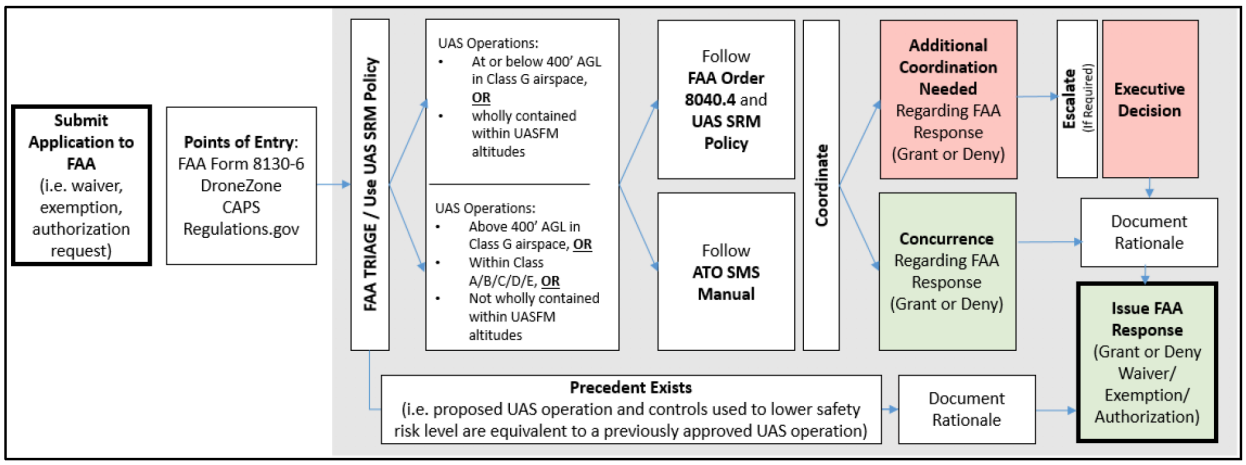

Figure 1: UAS request governance process from FAA Order 8040.6 [3] (Figure B).

Figure 1, taken from [3] (Figure B) summarizes the UAS request governance process. Two points merit comment. First, the appropriate FAA safety risk management process for evaluating a waiver application depends upon the airspace class. Second, the approval process should rely upon established precedent (previous approval and/or denial of substantively similar waiver requests).

Chapter 4 of FAA Order 8040.6, *AVS SRM for UAS Requests*, provides a twelve (12) step SRM process for UAS requests as shown on the right side of Table 1. The subsequent corresponding sections address these steps as related to the developed framework. The left

8040.4b SRMP	8040.6 SRMP
	a. Identify Safety Analyst or Team Members
a. System Analysis	b. System Analysis
b. Identify Hazards	c. Identify Hazards, Causes, and Outcomes
c. Analyze Safety Risk	d. Analyze Safety Risk
d. Assess Safety Risk	f. Assess Safety Risk
e. Control Safety Risk	e. Validity of Mitigations
	g. Additional Safety Risk Controls and Residual Safety Risk
	h. Safety Performance Monitoring and Hazard Tracking
	i. Documenting Assessments and Decisions
	j. Residual Safety Risk Acceptance
	k. Safety Risk Documentation
	l. Safety Performance Monitoring

Table 1: Steps in FAA Orders 8040.4b and 8040.6 SRMPs.

side of Table 1 highlights the FAA Order 8040.6 steps. The developed framework is described in accordance with the five-step SRMP of Order 8040.4b, where each of those five steps is informed by the corresponding step from FAA Order 8040.6.

4.4 Mathematical notation

Let $\mathbb{N}, \mathbb{Z}_+, \mathbb{Z}, \mathbb{R}_+, \mathbb{R}$ denote the positive integers, nonnegative integers, integers, nonnegative numbers, and real numbers, respectively. Sets will be denoted in script letters, e.g., $\mathcal{X}$, with set cardinalities, finite for all cases of interest, in upper case letters, e.g., $N = |\mathcal{X}|$. One exception is that the notation $[a : b]$, for $a, b \in \mathbb{Z}$, denotes the index set $\{a, \ldots, b\}$, where the most frequent usages are *i*) $[1 : N] = \{1, \ldots, N\}$, which will be abbreviated as $[N]$, and $[0 : N] = \{0, \ldots, N\}$. Vectors will be written in lower case letters, e.g., x, with $x = (x_1, \ldots, x_N)$ denoting a vector of length N. Random variables (or random vectors) are denoted by a sans-serif font, e.g., y. The Iverson bracket notation, $[P]$, for proposition P, taking value 1 (0) if P is true (false), respectively, is used; the distinction between this and the set notation $[N]$ will be clear from context.

5 SRMP Step 1: System Analysis

This section applies Step 1, *System Analysis*, of the SRMP to support risk-based decision making and waiver approvals for sUAS. The section is organized as follows:

1. §5.1 *Order 8040.4b SRMP Guidance on System Analysis* reviews the FAA's guidance on *System Analysis* from FAA Order 8040.4b.
2. §5.2 *Order 8040.6 SRMP Guidance on System Analysis* reviews the FAA's guidance on *System Analysis* from FAA Order 8040.6.
3. §5.3 *Recommendation: System Analysis to support risk-based decision making and waiver approvals for sUAS* applies the guidance on *System Analysis* to the problem of sUAS waiver approval.

5.1 Order 8040.4b SRMP Guidance on System Analysis

This section reviews SRMP guidance on *System Analysis*, as found in Order 8040.4b [4], where "the system analysis provides information that serves as the basis for identifying and understanding hazards, as well as their causes and associated safety risk". The SRMP breaks down *System Analysis* into six sub-steps:

(1) Define and document the scope (i.e., system boundaries) and objectives related to the system

(2) Gather the relevant available data/information regarding the issue or change to be analyzed.

(3) Develop a safety risk acceptance plan that includes evaluation against safety risk acceptance criteria, designation of authority to make the required safety risk decisions involved, and assignment of the relevant decision makers...

(4) Describe and model the system and operation in sufficient detail for the safety analysts to understand and identify the hazards that can exist in the system...

(5) Look at the system in its larger context.

(6) Consider the following in the analysis, depending on the nature and size of the system:

   (a) The function and purpose of the system
   (b) The system's operating environment
   (c) An outline of the system's processes, procedures, and performance
   (d) The personnel, equipment, and facilities necessary for the system's operation

The next section reviews the specialized guidance on system analysis for UAS from Order 8040.6.

5.2 Order 8040.6 SRMP Guidance on System Analysis

This section reviews SRMP guidance on *System Analysis*, as found in Order 8040.6 [3], defined there as comprising "the technical and operational information needed for the safety analyst or team members to verify or perform SRM". An iterative three-step feedback process between the applicant and the evaluator is described:

(1) Applicant provides the Concept of Operations (CONOPS), Operational Risk Assessment (ORA), safety case (hazard and mitigation description), operational procedures/manuals, and test documentation. The guidance states the provided information contains:

   i. The hazards identified
   ii. The potential effects of the hazards (before mitigations)
   iii. The mitigation rationale
   iv. A statement of how each mitigation is expected to reduce the severity, and likelihood of the hazard's effects
   v. The test results to validate the mitigations (if available)
   vi. The predicted residual risk (after mitigations)
   vii. The applicant's determined level of risk and rationale

(2) Evaluator conducts a System Assessment of each element of operation, including

   i. Aircraft: "equipment, size, aircraft weight, payload weight, speed, composition, configuration, software assurance, contingency features, airworthiness, camera/visual components, sensors, maintenance procedures, applicable limitations, command, control, communications (C2/C3) link, detect and avoid (DAA)"
   ii. Airman/Operator: "responsible person for waiver, part 137 agriculture operator, part 135 air carrier certificate holder,...,other crew members, experience, certification, required training, pilot's location, visual observers, safety culture, track record, procedures, contingency actions, training manuals, training curriculum, ability of pilot to intervene if autonomous flight, applicable limitations"
   iii. Airspace/Operating Environment: "class of airspace, traffic density, speed of other traffic, complexity of airspace, adjacent airspace, altitude of operations, communication with ATC, awareness of other operators, applicable limitations, types of manned aircraft the UA may encounter,..., population density, prevailing/possible weather conditions, season of operation, time of day, proximity to airports, type of operations (commercial/GA/rotorcraft) at nearby airports and in the area, terrain, structures, duration of operation, other UAS operations in the area, number of operations planned per day, applicable limitations, lateral and vertical boundaries of operating area"

(3) Evaluator issues Request for Information (RFI) to applicant when application information is incomplete or insufficient to conduct analysis.

The next section will apply the system analysis guidance from both Order 8040.4b and Order 8040.6 to the development of a PRA to support the sUAS waiver approval process.

5.3 Recommendation: System Analysis for the sUAS waiver approval process

This section applies the Order 8040.4b and Order 8040.6 SRMP guidance on *System Analysis*, reviewed in the previous section, to the development of a PRA to support the sUAS waiver

approval process.

The essence of the following observation is that a meaningful computer simulation framework for a "joint" PRA that incorporates all, or even most, of the "elements of operations" identified by Order 8040.6 is practically infeasible, for reasons listed below.

Observation 1 (Practical infeasibility of "joint" computer simulation-based PRA)**.** It is practically infeasible to develop a meaningful computer simulation framework for evaluation of proposed UAS operations in the NAS that jointly considers all, or even a significant number, of the "elements of operation" suggested in Order 8040.6. This infeasibility stems from several distinct factors:

1. *Infeasible system modeling requirement:* if a PRA is to jointly evaluate all proposed elements of operation, it is required that a corresponding holistic and comprehensive mathematical and physical model be developed that properly incorporates all such inputs and their interactions. Given that these input interactions are both large in number and highly nontrivial, the corresponding system model that realistically captures all relevant system state variables would be of an infeasible complexity.

2. *Impractical data / knowledge requirement:* even if such a system model were to be developed that would meaningfully incorporate many of the proposed elements of operation, it would still be incumbent upon the operator and/or evaluator to provide correct, or approximately correct, specifications for those elements. It is our assertion that knowledge of all such inputs is unlikely to be available, and that the obligation on the part of the operator and/or evaluator to obtain all such inputs would render the overall system to be viewed as impractical and unduly burdensome.

3. *Impossible model and output validation:* even if a comprehensive system model were to be developed, and even if all input values were to be known, it would still be required that the model, and its outputs, be validated, by comparing the model's predictions with real-world measurements. Given the outputs of a PRA analysis are to be assessments of severity and likelihood of identified hazards, validation of these outputs would require a prohibitively large and complex measurement and testing operation that again would render the entire system impractical.

In accordance with the previous observation, it is required to develop a parsimonious taxonomy describing all required and/or essential "elements of operation" pertinent in assessing the risk of a proposed sUAS flight operation. This taxonomy is captured in the proposed framework via a *system state space*, and the components of a proposed sUAS flight operation pertinent to assessing its risk are captured via a *system state vector*.

To provide the proper context for understanding these terms, however, the *concept of operations* (CONOPS) is defined first.

Definition 1 (Concept of operations (CONOPS))**.** The *concept of operations* (CONOPS) includes:

1. *Mission:* the purpose of the flight (e.g., transport packages by sUAS)
2. *Location:* the regional area where the flight will occur (e.g., East Dallas, TX)

3. *Date and time:* the date and time when the flight will occur
4. *BVLOS:* indicator of whether the sUAS will be within or beyond visual line of sight (BVLOS) of the operator
5. *Night operations:* indicator of whether or not the flight will occur at night
6. *Over people:* indicator of whether or not the sUAS will be flown over people, and if yes, the maximum anticipated spatial density of people
7. *Flight path:* the geographic flight path the flight is anticipated to follow
8. *Flight operator location:* the location of the sUAS operator during the flight

The CONOPS provides critical *summary information* about a proposed flight, but by itself it is not sufficient to enable a statistically meaningful PRA. The first step towards this goal is to recognize that flights will comprise qualitatively distinct *stages*, defined below. Moreover, a PRA analysis will need to be executed for each of a set of *highest risk instances* within each stage, and the overall decision regarding the risk of the flight will depend upon the collection of risk categories identified for each of these individual instances.

Definition 2 (Flight stages and highest risk instances)**.** The typical CONOPS will comprise some or all of the following *flight stages*: *takeoff*, *en route*, *loitering*, and *landing*. *Highest risk instances* are to be identified within each of the above stages that apply to the CONOPS where *i*) an *instance* is a particular point in time during the stage, and *ii*) an instance is *highest risk* if it estimated that the corresponding *system state* at that time (defined below) has a risk as high or higher as all other instances during the stage. If the estimation of highest risk is difficult or unreliable, then any and all instances in the stage where risk is perceived to be potentially high may be included in the evaluation set. The result of this preliminary analysis is a *set of highest risk instances* throughout the various stages of flight, each of which will be assessed for risk using the methodology described below.

The key point thus far is that a set of highest risk instances has been identified, and what remains is to establish a risk category value for each such instance. The details of the flight operation at a given instance are captured through the definitions of *system state space*, *system state category*, and *system state vector*, given below. It is of critical importance for what follows to recognize that:

1. The risk assesment of and corresponding decision for a proposed sUAS flight depends upon the collection of risk categories for the identified highest risk instances using, for example, the decision rule approach in Recommendation 10.
2. The risk category for an individual highest risk instance will be assessed using the framework that follows below, beginning with Model specification 1, where the system state captures all risk-pertinent information about the sUAS system and its environment at that instant.

Model specification 1 (System state space and system state vector)**.** Let $N_s \in \mathbb{N}$, and suppose a taxonomy is available by which all risk-relevant aspects of a proposed sUAS flight may be summarized in a *system state vector* of length N_s, denoted $x = (x_1, \ldots, x_{N_s})$, indexed by s, where the N_s components of the vector index variables / parameters deemed pertinent

in assessing its risk. Let $\mathcal{X}_s$ denote the set of possible values for category $s \in [N_s]$, and let $\mathcal{X} \equiv \mathcal{X}_1 \times \cdots \times \mathcal{X}_{N_s}$ denote the resulting *system state space*, so that if x is "well-defined" then $x \in \mathcal{X}$ (but not necessarily vice-versa).

The set $\mathcal{X}_s$ of possible values for category $s \in [N_s]$ includes a (possibly empty) subset, denoted $\bar{\mathcal{X}}_s$, termed *mitigated states*. A state is *mitigated* if it can be assessed that the risk, however it is defined, within that state is either *i*) *de minimus* or *ii*) *lowest possible* relative to all other (non-mitigated) state values within that category. Mitigated states are intended to capture *nominal* or *ideal* operating conditions as well as system state category values corresponding to the successful application of mitigation technologies, processes, or operations.

Appendix A lists all mathematical notation used in the model specification.

Recommendation 1 (System state category specification)**.** The following system state categories are proposed:

1. *sUAS platform and payload:* properties of the sUAS platform and payload, including *i*) *commerical model properties*, *ii*) *mitigations*, and *iii*) *payload properties*. Commercial model properties include sUAS platform weight and maximum speed. Mitigations include both hardware (e.g., parachute) and software (e.g., automatic return to specified location, geofencing to restrict sUAS to flight plan, and automatic parachute deployment upon hazard cause detection). Payload properties include the maximum weight and the means by which it is secured to the sUAS platform. The *mitigated states* are those in which the sUAS platform and payload properties are nominal/ideal and/or mitigation measures have been applied.
2. *Flight readiness:* pre-flight check status outcomes (e.g., fuel cell charge level). The *mitigated states* are those in which all pre-flight check status outcomes are nominal.
3. *Operator workstation:* properties of the hardware and software comprising the workstation environment, as well as properties of any mitigations specific to the workstation (e.g., guard rails around launch pad). The *mitigated states* are those in which the operator workstation properties are nominal/ideal and/or mitigation measures have been applied.
4. *Operator training and procedures:* properties of the training of the operator and the procedures the operator will obey. The *mitigated states* are those in which the operator has received all relevant traininng and obeys all recommended safety procedures.
5. *Flight plan:* properties of the sUAS anticipated flight plan (e.g., takeoff characteristics, cruising target altitude and speed, landing characterstics).
6. *C2 channel:* properties of the wireless command and control (C2) channel separating the operator and the sUAS, reasonably considered known or knowable in advance of flight (e.g., sUAS and transponder transmitter powers and receiver noise floors, and anticipated distance(s) separating the operator and the sUAS), relevant to the identified hazard causes.
7. *Information acquisition, processing, and dissemination:* properties of the system (e.g., sensor range, accuracy) and the environment (e.g., visibility, electromagnetic noise), reasonably considered known or knowable in advance of flight, that affect the ability

of the system to sense, process, and disseminate aspects of the environment relevant to the identified hazard causes.

8. *Weather environment:* properties of the weather environment external to the sUAS system (e.g., wind, precipitation) for the proposed flight, reasonably considered known or knowable in advance of flight, that affect the ability of the system to maintain its position and/or control its movement.
9. *Airspace environment:* properties of the airspace environment comprising the proposed flight (e.g., airplane flight paths, helicopter routes).
10. *Ground environment:* properties of the ground environment underlying the proposed flight (e.g., human outdoor spatial distribution, built environment characteristics).

Challenge 1 (System state category specification)**.** Two open challenges regarding the proposed system state categories in Recommendation 1 are:

1. *Category scope challenge:* to adjust this proposed list, either by adding, deleting, joining, or splitting categories, so as to best align with current and anticipated sUAS usage and practice.
2. *Category precision challenge:* to specify precisely how each category is measured, ideally by a scalar quantity, and then to quantize into an appropriate number of "value bins".
3. *Category mitigated state identification:* to identify which system state category values are mitigated and which are not.

In each of the first two challenges listed above there is a nuanced tradeoff to be judiciously managed between the twin objectives of *i*) minimizing the size of the system state space, so as to facilitate "proximity" between two system state vectors, and *ii*) increasing the "resolution" of the state space, so as to maximize the accuracy of the hazard cause likelihoods, described in the sequel.

6 SRMP Step 2: Identified Hazards

This section applies Step 2, *Hazard Identification*, of the SRMP to support risk-based decision making and waiver approvals for sUAS. The section is organized as follows:

1. §6.1 *Order 8040.4b SRMP Guidance on Hazard Identification* reviews the FAA's guidance on *Hazard Identification* from FAA Order 8040.4b.
2. §6.2 *Order 8040.6 SRMP Guidance on Hazard Identification* reviews the FAA's guidance on *Hazard Identification* from FAA Order 8040.6.
3. §6.3 *Recommendation: Hazard Identification to support risk-based decision making and waiver approvals for sUAS* applies the guidance on *Hazard Identification* to sUAS waiver approval.

6.1 Order 8040.4b SRMP Guidance on Hazard Identification

This section reviews SRMP guidance on *Hazard Identification*, as found in Order 8040.4b [4], where "a hazard is a condition that could foreseeably cause or contribute to an aircraft accident." The SRMP identifies eleven (11) hazard categories:

(1) Ambient environment (e.g., physical conditions, weather)
(2) Equipment (hardware and software)
(3) External services (e.g., contract support, electric, telephone lines)
(4) Human-machine interface
(5) Human operators
(6) Maintenance procedures
(7) Operating environment (e.g., airspace, air route design)
(8) Operational procedures
(9) Organizational culture
(10) Organizational issues
(11) Policies/rules/regulations

6.2 Order 8040.6 SRMP Guidance on Hazard Identification

This section reviews SRMP guidance on *Hazard Identification*, as found in Order 8040.6 [3]. The guidance classifies hazards by the severity of outcome:

(1) Hazards with worst credible outcomes:

   i. Collision between a UAS and a manned aircraft in the air
   ii. Collision between a UAS or its detached cargo and a person on the ground, or moving vehicle
   iii. Collision between a UAS or its detached cargo and critical infrastructure on the ground

(2) Hazards with less severe outcomes:

i. Unable to detect and avoid
ii. Human error
iii. Adverse operating conditions
iv. Technical issue with UAS
v. Deterioration of external systems supporting the UAS operation.

In addition, Appendix A of Order 8040.6 provides a list "starting point" of hazards for consideration, shown in Figure 2.

The next section will apply the hazard identification guidance from both Order 8040.4b and Order 8040.6 to support risk-based decision making and waiver approvals for sUAS.

6.3 Recommendation: Hazard Identification to support risk-based decision making and waiver approvals for sUAS

This section applies the Order 8040.4b and Order 8040.6 SRMP guidance on *Hazard Identification*, reviewed in the previous section, to support risk-based decision making and waiver approvals for sUAS. In particular, consistent with Figure 2, the framework employs both *hazard causes* and *hazard outcomes*, defined below.

Definition 3 (Hazard outcome)**.** A *hazard outcome* is any property of an sUAS operation in which the sUAS causes *i*) harm to any human, *ii*) damage to a manned airborne vehicles, or *iii*) damage to the built environment.

Definition 4 (Hazard cause)**.** A *hazard cause* is any property of an sUAS operation that is *i*) not specified in the *system state* and which *ii*) has an (potential, statistical) impact on the likelihood of one or more *hazard outcomes*.

Assumption 1 (Single hazard cause)**.** The framework assumes that multiple hazard causes will not occur within a given flight of a given sUAS, i.e., it is of course possible for multiple hazard causes to occur in practice, but the model is setup in such a way that multiple hazard causes do not occur. This is termed the *single hazard cause assumption*, and the corresponding model, given above, is termed the *single hazard cause model*.

Observation 2 (Assessment of the single hazard cause assumption)**.** The assumption is made on account of the significant simplification it enables, at the admitted expense of some loss in physical realism. Any assessment of the proposed framework should assess both these factors (benefit of model simplification and cost of reduced model accuracy). Additional commentary on the advantages and disadvantages of the single vs. multiple hazard cause models is given in Appendix B.

Model specification 2 (Hazard causes (under single hazard cause assumption))**.** Let $N_c \in \mathbb{N}$, and let the possible hazard causes associated with sUAS operation be identified with the ordered set $[0 : N_c]$ and indexed by y. In particular, $y = 0$ denotes that no hazard cause occurs.

Hazards	Hazard Definition	Causes (if applicable)	Mitigations[4]	Outcomes
Technical Issue with UAS	Malfunction of any technical component of the UAS, which causes a deviation from planned operations.	• Motor failure • Software failure • Hardware failure • Lost Link • GPS Failure • Communications failure • Flyaway • Geofence failure • Ground station failure • Battery/power failure • Avionics failure • UA leaves planned route • Failure of C2/3 change over	• Competent applicant/operator • UAS manufactured by competent or proven entity • UAS maintained by competent or proven entity • UAS developed to authority recognized design standards • C2/3 link performance appropriate • Preflight checks of UAS • Operational procedures validated • Remote crew trained and current • Safe recovery from technical issue • Methods to reduce kinetic energy • Ground population density • Emergency response plan in place • Reduce effects of ground impact • Technical containment in place and effective • Parachute or frangible aircraft	• Collision between UAS and a manned aircraft in the air • Collision between a UAS and person on ground or moving vehicle • Collision between a UAS and critical infrastructure on the ground
Deterioration of external systems supporting the UAS operation	Malfunction of any component that is not a part of the UAS but supports safe operations.	• ADS-B signal degradation • GPS signal degradation • UAS Traffic Management (UTM) failure	• Procedures are in place to handle the deterioration of external systems supporting the UAS operation • UAS is designed to manage the deterioration of external systems supporting the UAS operation • External services supporting the UAS operation are adequate to the operation	• Collision between UAS and a manned aircraft in the air • Collision between a UAS and person on ground or moving vehicle • Collision between a UAS and critical infrastructure on the ground
Human Error	A person's mistake rather than the failure of a machine, which causes a deviation from planned operations.	• Pilot errors • Maintenance Errors • Preflight Planning Errors • Mission and route planning errors • Cargo Loading Errors • Flight into unplanned weather	• Operational procedures are defined, validated, and adhered to • Remote crew trained and current and able to control abnormal situation • Multi-crew coordination • Remote crew fit to operate • Automate protection of the flight envelope from human error • Safe recovery from human error • A human factors evaluation has been performed and the human machine interaction (HMI) found appropriate to the mission. • Crew resource management practices	• Collision between UAS and a manned aircraft in the air • Collision between a UAS and person on ground or moving vehicle • Collision between a UAS and critical infrastructure on the ground
Adverse Operating Conditions	Operating into or within conditions that the UAS wasn't intended to, which causes a deviation from planned operations.	• Unforecasted weather • Reduced visibility • Climate and topography unique weather	• Operational procedures are defined, validated and adhered to • The remote crew is trained to identify critical environmental conditions and to avoid them • Environmental conditions for safe operations are defined, measurable and adhered to • UAS designed and qualified for adverse environmental conditions	• Collision between UAS and a manned aircraft in the air • Collision between a UAS and person on ground or moving vehicle • Collision between a UAS and critical infrastructure on the ground
Unable to Detect and Avoid	Beyond Visual Line of Sight (BVLOS) operations and the design of the UAS give the aircraft a limited ability to sense intruding aircraft and yield right of way as required by 14 CFR Parts §91.113 and §107.37	• Transponder failure • Communication failure between VOs • Traffic conflicts; helicopter routes/unchart ed landing surfaces • Inability to comply with 14 CFR Parts §91.113 and §107.37 • Low altitude General Aviation (GA) operations • Manned aircraft unable to see UA (due to the small size of the UA) • Pilot and crew errors • UA maneuverability (due to UA performance limitations)	• Visual Observers (VOs) (communication between pilot and observers) • Detect and avoid (DAA) system • Airspace of operation and adjacent airspace • Time of day • Operating restrictions • Restricting operations within certain boundaries or airspace volumes • Restricting operational flight time • Low altitude • ATC separation services • Traffic Alert and Collision Avoidance System (TCAS) • Proximity to structures	• Collision between UAS and a manned aircraft in the air

Figure 2: UAS Hazards, Mitigations, and Outcomes, from FAA Order 8040.6 [3] (Appendix A).

An alternative and generalized hazard cause model that removes the single cause assumption is the following *multiple hazard cause model.*

Model specification 3 (Hazard causes (under multiple hazard cause assumption))**.** Let the possible hazard causes associated with sUAS operation be described by a binary-valued *hazard cause vector* of length N_c, denoted $y = (y_1, \ldots, y_{N_c}) \in \{0,1\}^{N_c}$. By convention, $y_c = 1$ (0) if hazard cause $c \in [N_c]$ does (not) occur, respectively; it follows that the vector of N_c zeros denotes the case where no hazard cause occurs.

With acknowledgment of the guidance in FAA Order 8040.6, a preliminary list of proposed sUAS hazard causes is given below:

Recommendation 2 (Hazard cause specification)**.** The following hazard causes are proposed:

1. *sUAS malfunction:* an on-board malfunction (including software, electrical, mechanical malfunctions) compromises the proper function of the sUAS (including the sUAS's ability to sense its environment, to relay information regarding that sensed environment to the operator, to exercise sufficient flight control over its position, bearing, and direction).
2. *sUAS operator error:* the sUAS operator fails to exercise proper control (or lack thereof) of sUAS, i.e., the operator's control is inconsistent with policy, guidance,and practice, despite sufficient information about environment relayed from the sUAS and sufficient ability to operate the sUAS in such a manner.
3. *C2 link failure:* the command and control link connecting the operator and the sUAS fails on downlink (failing to relay the sensed environment to the operator) and/or uplink (failing to relay the operator's controls to the sUAS).
4. *Inability to sense environment:* the operating environment is such that there is an inability to sense critical features, even though the sUAS, the operator, and the C2 link are each functioning correctly.
5. *Inability to control flight:* the operating environment is such that there is an inability to exercise sufficient control, even though the sUAS, the operator, and the C2 link are each functioning correctly. This inability is most frequently attributable to weather (e.g., an encounter with wind gusts, convective weather, snow, sleet, or hail).

Challenge 2 (Hazard cause specification)**.** An open challenge regarding the proposed hazard causes in Recommendation 2 is to partition all likely hazard causes into categories such that *i*) most conceivable malfunctions will be readily mapped into one, and only one, of the categories, and *ii*) the hazard cause categories are *causally flat*, meaning, at least in most cases, a malfunction mapped to a given hazard cause category won't cause, or even incease the likelihood of, an additional malfunction mapped to a different hazard cause category.

Observation 3 (Tradeoff management in hazard cause specification)**.** Similar to the comment regarding the selection of system state categories, choosing the appropriate granularity of the hazard cause categories must trade off the competing objectives of reducing the complexity of the PRA (achieved by using a coarse-grained categorization) and increasing the accuracy of the PRA (achieved by using a fine-grained categorization).

Having discussed *hazard causes*, the next topic is *hazard outcomes*.

Assumption 2 (Single hazard outcome)**.** The framework assumes that multiple hazard outcomes will not occur within a given flight of a given sUAS, i.e., it is of course possible for multiple hazard outcomes to occur in practice, but the model is setup in such a way that multiple hazard outcomes do not occur. This is termed the *single hazard outcome assumption*, and the corresponding model, given above, is termed the *single hazard outcome model*.

Like the single hazard cause assumption in Assumption 1, the above assumption is made on account of the significant simplification it enables, at the admitted expense of some loss in physical realism. Additional commentary on the advantages and disadvantages of the single vs. multiple hazard cause models will be given below.

Model specification 4 (Hazard outcomes (under single hazard outcome assumption))**.** Let $N_o \in \mathbb{N}$, and let the possible hazard outcomes associated with sUAS operation be identified with the ordered set $[0 : N_o]$ and indexed by z. In particular, $z = 0$ denotes that no hazard outcome occurs.

An alternative and generalized hazard outcome model that removes the single hazard outcome assumption is the following *multiple hazard outcome model.*

Model specification 5 (Hazard outcomes (under multiple hazard outcome assumption))**.** Let the possible hazard outcomes associated with sUAS operation be described by a binary-valued *hazard outcome vector* of length N_o, denoted $z = (z_1, \ldots, z_{N_o}) \in \{0, 1\}^{N_o}$. By convention, $z_o = 1$ (0) if hazard outcome $o \in [N_o]$ does (not) occur, respectively; it follows that the vector of N_o zeros denotes the case where no hazard outcome occurs.

Recommendation 3 (Hazard outcome specification)**.** The following hazard outcomes are proposed:

1. *Proximity to or collision with a person:* the sUAS fails to adhere to the minimum separation distance from a person on the ground.
2. *In-air proximity to or collision with a manned airborne vehicle:* the sUAS fails to adhere to the minimum separation distance from a manned airborne vehicle (e.g., airplane, helicopter).
3. *Proximity to or collision with the built environment:* the sUAS fails to adhere to the minimum separation distance from the built environment (e.g., buildings, roads, or any space forbidden for sUAS to make contact).

Challenge 3 (Hazard outcome specification)**.** An open challenge regarding the proposed hazard outcomes in Recommendation 3 is to establish suitable values for the critical distances in the above list. The authors are in the process of consulting FAA guidance and qualified experts regarding these values.

The notion of *de minimus* risk is applied to the proposed framework in recognition of the fact that *i*) the likelihood of certain hazard causes in certain system state vectors and/or *ii*) the risk (however it may be defined) of certain hazard outcomes in certain system state vectors are sufficiently small that they may be safely excised from the model.

Model specification 6 (Hazard causes and hazard outcomes relevant to system state vector)**.** Let $Y(x) \subseteq [0 : N_c]$ (with $0 \in Y(x)$) denote the *subset of hazard causes relevant to the system state vector* x, where a cause y is irrelevant to x if the likelihood $\ell(y|x)$ is deemed to lie below a *de minimus* level. Similarly, let $Z(x) \subseteq [0 : N_o]$ (with $0 \in Z(x)$) denote the *subset of hazard outcomes relevant to the system state vector* x, where an outcome z is irrelevant to x if the risk (however it may be defined), denoted risk$(z|x)$, is deemed to lie below a *de minimus* level. Finally, let

$$N_c(x) = |Y(x)| - 1, \quad N_o(x) = |Z(x)| - 1 \tag{1}$$

denote the number of hazard causes (outcomes) relevant to system state vector x (except for the no hazard cause (outcome) 0), respectively.

Recommendation 4 (Hazard causes and hazard outcomes relevant to system state vector)**.** The identification of the hazard causes and hazard outcomes relevant to the system state vector, as described in Model Specification 6, is a critical component in the framework for the following two reasons: *i*) inclusion of hazard causes and/or hazard outcomes in the framework that are, by expert consensus, *de minimus* under the system state vector will significantly and unnecessarily increase the complexity and cost of performing the PRA, and *ii*) removing hazard causes and/or hazard outcomes from the framework that are, by expert consensus, *relevant* under the system state vector will potentially significantly decrease the validity of the PRA. The following two recommendations are put forth:

1. *Identification of relevant and de minimus causes for mitigated state vectors.* Guidance be developed by which relevant and de minimus hazard causes and hazard outcomes for common mitigated states are explicitly identified.
2. *Process for inclusion/exclusion.* A systematic decision process be developed by which hazard causes and hazard outcomes are included or excluded; this will likely include collection of expert opinion and translation into policy.

Challenge 4 (Hazard causes and hazard outcomes relevant to system state vector)**.** An open challenge regarding the proposed process for inclusion/exclusion in Recommendation 4 is to overcome the presumably high costs, measured in terms of time, effort, and dollars, to collect and systematize expert opinion.

7 SRMP Step 3: Analysis of Safety Risk

This section applies Step 3, *Safety Risk Analysis*, of the SRMP to support risk-based decision making and waiver approvals for sUAS. The section is organized as follows:

1. §7.1 *Order 8040.4b SRMP Guidance on Safety Risk Analysis* reviews the FAA's guidance on *Safety Risk Analysis* from FAA Order 8040.4b.
2. §7.2 *Order 8040.6 SRMP Guidance on Safety Risk Analysis* reviews the FAA's guidance on *Safety Risk Analysis* from FAA Order 8040.6.
3. §7.3 *Recommendation: Safety Risk Analysis to support risk-based decision making and waiver approvals for sUAS* applies the guidance on *Safety Risk Analysis* to the problem of sUAS waiver approval.

7.1 Order 8040.4b SRMP Guidance on Safety Risk Analysis

This section reviews SRMP guidance on *Safety Risk Analysis*, as found in Order 8040.4b [4], described as follows:

> The safety risk associated with a hazard is the combination of the severity and the likelihood of the potential outcome(s) of the hazard. Where appropriate, existing controls are taken into account prior to safety risk determination.

Three pertinent points of clarification are provided regarding 1) risk severity and likelihood, 2) risk analysis assumptions, and 3) risk analysis limitations:

(a) *Severity and likelihood.* "The safety risk of a hazard is the function of the severity and likelihood of the hazard's potential outcomes."

   1) *Severity* "is the potential consequence or impact of a hazard in terms of degree of loss or harm."
   2) *Likelihood* "is the estimated probability or frequency, in quantitative or qualitative terms, of the outcome(s) associated with a hazard."

(b) *Assumptions.* "In general, the SRM Team should limit assumptions as much as practical. If any assumptions are made, the assumptions and their rationale must be documented."

(c) *Limitations.* "Any known limitations of the safety risk analysis should be described. Limitations may also include the margin of error of the analysis if it can be calculated."

7.2 Order 8040.6 SRMP Guidance on Safety Risk Analysis

This section reviews SRMP guidance on *Safety Risk Analysis*, as found in Order 8040.6 [3], where the assessment of Severity and Likelihood is suggested to be determined by the following methodology:

(1) Severity:

i. What are the credible outcomes? (i.e., catastrophic, hazardous, major, minor, minimal)

ii. Why? (e.g., data, line of thought, expertise, rationale for how the safety analyst or team arrived at their determination)

iii. How do existing controls and additional mitigations change the aircraft, airman/operator, or airspace/operating environment, such that the severity is reduced?

(2) Likelihood:

i. What is the likelihood of the credible outcomes? (e.g., frequent, probable, remote, extremely remote, extremely improbable)

ii. Why? (e.g., data, line of thought, expertise, rationale for how the safety analyst or team arrived at their determination)

iii. How do mitigations change the aircraft, airman, airspace/operating environment, such that the likelihood is reduced?

The next section will apply the safety risk analysis guidance from both Order 8040.4b and Order 8040.6 to support risk-based decision making and waiver approvals for sUAS. .

7.3 Recommendation: Safety Risk Analysis to support risk-based decision making and waiver approvals for sUAS

This section applies the Order 8040.4b and Order 8040.6 SRMP guidance on *Safety Risk Analysis*, reviewed in the previous section, to support risk-based decision making and waiver approvals for sUAS.

Model specification 7 (System state, hazard cause, and hazard outcome notation)**.** Let y denote a hazard cause random variable associated with system state vector x, and let z denote a hazard outcome random variable associated with the pair (x, y).

Model specification 8 (Likelihood of hazard causes)**.** Let $\ell(y|x) = \mathbb{P}(\mathsf{y} = y|x)$ denote the *likelihood* (probability) of hazard cause value y given system state vector x. The conditional probability notation $\mathbb{P}(\mathsf{y} = y|x)$ is used as it highlights the dependence of the distribution of y upon x, but is inaccurate in that the model does not consider a distribution on system state. A more accurate notation would be $\mathbb{P}(\mathsf{y} = y; x)$, but the conditional notation is used as it facilitates more natural expressions, as will be evident in what follows.

Model specification 9 (Likelihood of hazard outcomes)**.** Let $\ell(z|x, y) = \mathbb{P}(\mathsf{z} = z|x, \mathsf{y} = y)$ denote the *conditional likelihood* of hazard outcome z under system state vector x and conditioned on the event that the hazard cause random variable y takes value y. The (unconditional) likelihood of hazard outcome vector z under system state vector x is, via the total probability theorem,

$$\ell(z|x) = \sum_{y \in [0:N_c]} \ell(z|x, y)\ell(y|x), \ z \in [0 : N_o]. \tag{2}$$

In words, the unconditional likelihood of each possible hazard outcome value z for system state vector x is the sum, over all possible hazard cause values y, of the joint probability $\ell(y, z|x) = \ell(z|x, y)\ell(y|x)$ of the pair (y, z).

Model specification 10 (Simplified likelihood of relevant hazard outcomes)**.** Under the reductions of hazard causes and hazard outcomes in Model Specification 6, the unconditional likelihood of hazard outcomes in Equation 2 of Model Specification 9 becomes:

$$\ell(z|x) = \sum_{y \in Y(x)} \ell(z|x, y)\ell(y|x), \ z \in Z(x). \tag{3}$$

Categorical probability distributions are used extensively in the model specification. In Bayesian statistics, it is standard and convenient to use a *Dirichlet distribution* for the prior distribution of a categorical random variable. By the *conjugate prior* property, incorporating observations (data) of the random variable results in an updated (posterior) distribution that is also a *Dirichlet distribution*, as explained below.

Definition 5 (Prior and posterior categorical distributions)**.** Fix $N \in \mathbb{N}$, and let the *categorical random variable* (RV) y have support $[0 : N]$. Define the N*-simplex* in $\mathbb{R}_+^{N+1}$ as:

$$\Delta_N = \{\ell = (\ell_0, \ldots, \ell_N) \in \mathbb{R}_+^{N+1} : \ell_0 + \cdots + \ell_N = 1\}. \tag{4}$$

A categorical RV y on $[0 : N]$ has a *probability mass function (PMF)*, equivalently, a likelihood distribution, given by $\ell \in \Delta_N$, with $\ell_y = \mathbb{P}(\mathsf{y} = y)$, for $y \in [0 : N]$. In the framework of *Bayesian statistics*, the likelihood ℓ is treated as random, in particular, as a random vector $\mathsf{l} \in \Delta_N$, and that random vector is given a *prior distribution*. The prior distribution on l is updated to a *posterior distribution* after observations of the categorical RV, y. As is standard within Bayesian statistics for categorical RVs, the prior distribution for l is chosen to be the *Dirichlet distribution*, with (hyper-) parameters $\alpha \in \mathbb{R}_+^{N+1}$, denoted

$$\mathsf{l} \sim \mathrm{Dir}(\alpha). \tag{5}$$

The *conjugate prior* distribution of the categorical distribution is the Dirichlet distribution; this means the posterior distribution for l, after observations, is also a Dirichlet distribution. In particular, if $v = (v_0, \ldots, v_N) \in \mathbb{Z}_+^{N+1}$ is a *count vector* recording the tally of independent and identically distributed realizations of the categorical RV y, with v_y the number of times $\mathsf{y} = y$, then the posterior distribution of l is the Dirichlet distribution with parameters $\alpha + v = (\alpha_y + v_y, y \in [0 : N])$, denoted

$$\mathsf{l}|v \sim \mathrm{Dir}(\alpha + v). \tag{6}$$

The Bayesian framework described in Model Specification 5 is adopted for the hazard cause and hazard outcome conditional likelihoods. This includes both *i*) initial estimates on likelihoods given by a prior distribution, and *ii*) updated estimates on likelihoods given by a posterior distribution. As the likelihoods are on categorical random variables, the prior distributions are Dirichlet distributions, and the corresponding posterior distributions are likewise Dirichlet distributions.

Model specification 11 (Prior distributions on hazard cause likelihoods)**.** The likelihood vector $\ell_{\mathsf{y}}(x) = (\ell(y|x), y \in Y(x)) \in \Delta_{N_c(x)}$ holds the likelihoods $\ell(y|x)$ of each hazard cause value $y \in Y(x)$ under system state vector x. Let $\bar{\alpha}(x)$ hold the (hyper-) parameters $\bar{\alpha}(x) = (\bar{\alpha}(x, y), y \in Y(x)) \in \mathbb{R}_+^{N_c(x)+1}$ of the Dirichlet prior distribution on the hazard cause likelihood categorical random variable $\mathsf{y}(x)$ for the system state vector x. The choice of $\bar{\alpha}(x)$ should reflect prior belief regarding the likelihood of each possible hazard cause under the system state vector.

Model specification 12 (Prior distributions on hazard outcome conditional likelihoods)**.** The conditional likelihood vector $\ell_{\mathsf{z}|\mathsf{y}}(x, y) = (\ell(z|x, y), z \in Z(x)) \in \Delta_{N_o(x)}$ holds the conditional likelihoods $\ell(z|x, y)$ of each hazard outcome value $z \in Z(x)$ under system state vector x and conditioned upon the hazard cause random variable taking value y. Let $\hat{\alpha}(x, y)$ hold the (hyper-) parameters $\hat{\alpha}(x, y) = (\hat{\alpha}(x, y, z), z \in Z(x)) \in \mathbb{R}_+^{N_o(x)+1}$ of the Dirichlet prior distribution on the hazard outcome conditional likelihood categorical random variable $\mathsf{z}(x, y)$ for the system state vector x conditioned on hazard cause $y \in Y(x)$. The choice of $\hat{\alpha}(x, y)$ should reflect prior belief regarding the conditional likelihood of each possible hazard outcome under the system state vector conditioned upon the hazard cause value.

Model specification 13 (Observations of hazard causes / outcomes under the system state vector)**.** Let $m(x) \in \mathbb{N}$ denote the number of times system state vector x is attempted, i.e., the number of trials / observations. The hazard cause and hazard outcome values for each trial are recorded and used to update the hazard cause likelihoods and the hazard outcome conditional likelihoods, respectively.

Model specification 14 (Posterior distributions on hazard cause likelihoods)**.** Let $\bar{v}(x)$ be the *observed hazard cause count vector*, where $\bar{v}(x) = (\bar{v}(x, y), y \in Y(x))$ is the hazard cause count vector for the $m(x)$ trials of system state vector x, i.e., $\bar{v}(x, y) \in \mathbb{Z}_+^{N_c(x)+1}$ and

$$\sum_{y \in Y(x)} \bar{v}(x, y) = m(x), \tag{7}$$

and $\bar{v}(x, y)$ is the number of the $m(x)$ trials of system state vector x that resulted in the hazard cause y. Recall, the Dirichlet prior distribution for the hazard cause likelihood under system state x has (hyper-) parameters $\bar{\alpha}(x) \in \mathbb{R}_+^{N_c(x)+1}$, and the trials discussed above result in hazard cause count vectors $\bar{v}(x) \in \mathbb{Z}_+^{N_c(x)+1}$. It follows that the posterior distribution for the hazard cause likelihood is the Dirichlet distribution with (hyper-) parameters $\bar{\alpha}(x)+\bar{v}(x)$:

$$\mathsf{l}(x)|\bar{v}(x) \sim \mathrm{Dir}(\bar{\alpha}(x) + \bar{v}(x)). \tag{8}$$

Model specification 15 (Posterior distributions on hazard outcome conditional likelihoods)**.** Let $\hat{v}(x) = (\hat{v}(x, y), y \in Y(x))$ be the *observed hazard outcome count vectors*, where $\hat{v}(x, y) = (\hat{v}(x, y, z), z \in Z(x))$ is the count vector for the trials of the system state vector x resulting in observed hazard cause y. By definition,

$$\sum_{z \in Z(x)} \hat{v}(x, y, z) = \bar{v}(x, y), \tag{9}$$

and

$$\sum_{y\in Y(x)}\sum_{z\in Z(x)}\hat{v}(x,y,z)=m(x), \tag{10}$$

and $\hat{v}(x,y,z)$ is the number of the $m(x)$ trials of system state vector x that resulted in hazard cause value y and hazard outcome value z. Recall, the Dirichlet prior distribution for the hazard outcome conditional likelihood under system state x, conditioned on hazard cause value $y \in Y(x)$, has (hyper-) parameters $\hat{\alpha}(x,y) \in \mathbb{R}_+^{N_o(x)+1}$, and the trials discussed above result in hazard outcome count vectors $\hat{v}(x,y) \in \mathbb{Z}_+^{N_o(x)+1}$. It follows that the posterior distribution for the hazard outome conditional likelihood is the Dirichlet distribution with (hyper-) parameters $\hat{\alpha}(x,y)+\hat{v}(x,y)$:

$$\mathsf{l}(x,y)|\hat{v}(x,y) \sim \mathrm{Dir}(\hat{\alpha}(x,y)+\hat{v}(x,y)). \tag{11}$$

Recommendation 5 (Prior parameter setting, data collection, and sample size)**.** It is required to set the parameters for each of the prior distributions. It is recommended that this be done using expert judgement and by mining available data sets that may shed insight into the approximate likelihood of various events of interest.

It is furthermore required to select the sample size of each data collection, and this should be done with the intention of ensuring the phenomenon of interest is observed a sufficiently large number of times with a sufficiently high probability. If a trial results in the phenomenon of interest it will be called a *hit* in what follows, and the *number of hits* is the number of times the phenomenon of interest is observed. The following guidance on the sample size of collected data is proposed:

1. *Nominal probability estimate of a hit.* A nominal estimate of the probability, say $p \in (0,1)$, of a hit is developed;
2. *Target number of hits.* The target number of hits, say $k \in \mathbb{N}$, is selected.
3. *Target probability of not reaching target hit number.* A probability, say $\epsilon \in (0,1)$, is selected, bounding the probability of not seeing the target number of hits.

With these in hand, an estimate on the required sample size is provided in Appendix C, giving the sample size, m, in terms of the three parameters, p, k, ϵ. For the special case of $k = 1$ (i.e., the target minimum number of hits is one), the resulting sample size approximation is particularly simple:

$$m = -\frac{1}{p}\log(\epsilon). \tag{12}$$

For example, with $p = 1/100$, $k = 1$, and $\epsilon = 1/10$, the required sample size to ensure less than a 10% chance of not observing at least one or more hits is $m \approx 230$.

Finally, it is observed that it is not feasible to collect data to estimate the parameters of all relevant distributions. This lack of data may slow the rate of adoption / approval for new CONOPS that differ, perhaps even only slightly, from approved CONOPS.

Challenge 5 (Prior parameter setting, data collection, and sample size)**.** Open challenges pertaining to Recommendation 5include:

1. Regarding setting of prior parameters, there is an open challenge to systematically collect and calibrate the collective wisdom of the qualified experts in aviation safety.
2. Regarding data collection and sample size, there is an open challenge to manage the associated cost, assessed in terms of time, effort, and dollars, to gather sufficient data to provide sufficiently accurate estimates of a sufficient number of the distribution parameters comprising the statistical model.

8 SRMP Step 4: Assessment of Safety Risk

This section applies Step 4, *Safety Risk Assessment*, of the SRMP to support risk-based decision making and waiver approvals for sUAS. The section is organized as follows:

1. §8.1 *Order 8040.4b SRMP Guidance on Safety Risk Assessment* reviews the FAA's guidance on *Safety Risk Assessment* from FAA Order 8040.4b.
2. §8.2 *Order 8040.6 SRMP Guidance on Safety Risk Assessment* reviews the FAA's guidance on *Safety Risk Assessment* from FAA Order 8040.6.
3. §8.3 *Recommendation: Safety Risk Assessment fo support risk-based decision making and waiver approvals for sUAS* applies the guidance on *Safety Risk Assessment* to sUAS waiver approval.

8.1 Order 8040.4b SRMP Guidance on Safety Risk Assessment

This section reviews SRMP guidance on *Safety Risk Assessment*, as found in Order 8040.4b [4], where "each hazard's associated safety risk is assessed against the risk acceptance criteria identified in the safety risk acceptance plan and plotted on a *Risk Matrix* based on the severity and likelihood of the outcome." Here, a *Risk Matrix* "provides a visual depiction of the safety risk and enables prioritization in the control of the hazards", and the *risk acceptance criteria* are the risk thresholds that determine whether the assessed risk is too high or acceptably low.

8.2 Order 8040.6 SRMP Guidance on Safety Risk Assessment

This section reviews SRMP guidance on *Safety Risk Assessment*, as found in Order 8040.6 [3]. The *Severity Level* and *Likelihood Level* form the rows and columns of the FAA's *Risk Matrix*.

The next section will apply the safety risk assessment guidance from both Order 8040.4b and Order 8040.6 to support risk-based decision making and waiver approvals for sUAS.

8.3 Recommendation: Safety Risk Assessment to support risk-based decision making and waiver approvals for sUAS

This section applies the Order 8040.4b and Order 8040.6 SRMP guidance on *Safety Risk Assessment*, reviewed in the previous section, to support risk-based decision making and waiver approvals for sUAS.

Model specification 16 (Likelihood categories)**.** Let $\mathcal{L}$ denote the *likelihood categories*, specified by a mapping, $f_L : [0,1] \to \mathcal{L}$. Thus, $L(z|x,y) = f_L(\ell(z|x,y))$ is the conditional likelihood category associated with hazard outcome value z under system state vector x, and conditioned on hazard cause value y. Likewise, $L(z|x) = f_L(\ell(z|x))$ is the (unconditional) likelihood category associated with hazard outcome value z under system state vector x.

Recommendation 6 (Likelihood categories)**.** The *likelihood categories* should be those established by FAA Order 8040.6, i.e., "frequent (A), probable (B), remote (C), extremely remote (D), extremely improbable (E)". Thus: $\mathcal{L} \equiv \{A, B, C, D, E\}$. These categories require likelihood thresholds $0 < \ell_{DE} < \ell_{CD} < \ell_{BC} < \ell_{AB} < 1$, defining the mapping $f_L : [0, 1] \to \mathcal{L}$ from likelihoods in $[0, 1]$ to likelihood categories in $\mathcal{L}$:

$$f_L(\ell) = \begin{cases} A, & \ell_{AB} < \ell \leq 1 \\ B, & \ell_{BC} < \ell \leq \ell_{AB} \\ C, & \ell_{CD} < \ell \leq \ell_{BC} \\ D, & \ell_{DE} < \ell \leq \ell_{CD} \\ E, & 0 \leq \ell \leq \ell_{DE} \end{cases} \tag{13}$$

The five likelihood categories are to be defined in terms of an anticipated number of occurrence per unit time, e.g., per year. Let $K \in \mathbb{N}$ denote an *approximate number of approved sUAS operations in the U.S. per year*. Then, under the somewhat coarse assumption that each sUAS operation is both independent and identically distributed (IID) in terms of the probability of a given risk outcome occurrence,

$$\ell_{AB} = \frac{100}{K},\ \ell_{BC} = \frac{10}{K},\ \ell_{CD} = \frac{1}{K},\ \ell_{DE} = \frac{1}{10K}. \tag{14}$$

It is recommended that these "rate-based" thresholds be replaced with suitable "rateless" thresholds, i.e., the likelihood category thresholds should be set independent of the number of approved sUAS operations per unit time.

Challenge 6 (Likelihood categories)**.** An open challenge regarding the proposed *likelihood categories* in Recommendation 6 is to determine suitable "rateless" thresholds that reflect current practice, guidance, and policy. If, instead, the current rate-based thresholds are to be maintained, then the challenge is to verify and validate that setting them using the approximate number, K, of sUAS operations per year yields an overall suitable categorization.

Model specification 17 (Severity categories)**.** Let $\mathcal{S}$ denote a finite set of *severity categories*. Let $S = (S_z, z \in Z(x))$, with each $S_z \in \mathcal{S}$ (i.e., $S \in \mathcal{S}^{N_o(x)}$), denote a *severity category vector*, specifying the severity category of each defined hazard outcome.

Recommendation 7 (Severity categories)**.** The *severity categories* should be those established by FAA Order 8040.6, i.e., "minimal (5), minor (4), major (3), hazardous (2), catastrophic (1)". Thus: $\mathcal{S} \equiv \{5, 4, 3, 2, 1\}$.

Challenge 7 (Severity categories)**.** An open challenge regarding the proposed *severity categories* in Recommendation 7 is to determine whether these categories reflect current practice, guidance, and policy.

Model specification 18 (Safety risk assessment matrix)**.** Let $(L, S) \in \mathcal{L} \times \mathcal{S}$ denote a likelihood category and severity category pair. Let $\mathcal{A} = \{G, Y, R\}$ denote the risk matrix score values, standing for Green (low risk), Yellow (medium risk), or Red (high risk), respectively. A *safety risk assessment matrix* $U \in \mathcal{A}^{|\mathcal{L}| \times |\mathcal{S}|}$ assigns a risk score in $\mathcal{A}$ for each possible (L, S) pair in $\mathcal{L} \times \mathcal{S}$.

Recommendation 8 (Safety risk assessment matrix)**.** The safety risk assessment matrix in FAA Order 8040.6 is recommended for use in the proposed PRA.

Challenge 8 (Safety risk assessment matrix)**.** An open challenge regarding the proposed safety risk assessment matrix in Recommendation 8 is verification and validation that the safety risk level assigned to each hazard outcome likelihood category and severity category pair is consistent with current practice, guidance, and policy.

Model specification 19 (Hazard outcome risk category vector)**.** The system state x and the corresponding assessed (unconditional) likelihoods for each individual hazard outcome, denoted $\ell(x) = (\ell(z|x), z \in Z(x))$ together determine the *hazard outcome likelihood category vector* $L(x) = (L(z|x), z \in Z(x))$, for $L(z|x)$ the likelihood category for hazard outcome index z under system state x. The hazard outcome likelihood category vector $L(x)$, together with the severity category vector S, determine the *hazard outcome risk category vector*, denoted $R(x) = (R(z|x), z \in Z(x))$, where $R(z|x) = U(L(z|x), S_z)$ is the hazard outcome risk category under hazard outcome likelihood category and severity category pair $(L(z|x), S_z)$.

Recommendation 9 (Flight instance risk category decisions via hazard outcome risk category vector)**.** *Flight instance risk category decisions* may be triaged (i.e., approved, further review required, denied) on the basis of the values found in the *hazard outcome risk category vector*, defined above. Recalling that the risk matrix U takes values in the set $\mathcal{A} = \{G, Y, R\}$, the set $\bigcup_{z \in Z(x)} R_z(x)$ denotes the subset of $\mathcal{A}$ found in the vector $R(x)$. This subset may be used to triage the risk category for the flight instance:

1. $\bigcup_{z \in Z(x)} R_z(x) = \{G\}$ (i.e., all hazard outcomes have likelihood and severity pairs that map to risk level Green): flight instance risk should be deemed *low*.
2. $\bigcup_{z \in Z(x)} R_z(x) = \{G, Y\}$ (i.e., all hazard outcomes have likelihood and severity pairs that map to risk level Green or Yellow): flight instance risk should be deemed *medium*.
3. $\bigcup_{z \in Z(x)} R_z(x) \ni R$ (i.e., there is one or more hazard outcome with a likelihood and severity pair that maps to risk level Red): flight instance risk should be *high*.

Challenge 9 (Flight instance risk category decisions via hazard outcome risk category vector)**.** An open challenge regarding the above flight instance risk category decision approach is to provide suitable guidance for the situation where the flight instance risk category is *medium*. The challenge is to provide a rigorous but feasible means by which further review may be accomplished. In the absence of such guidance, the only feasible step will be to require a change to the flight plan so that the flight instance risk category is lowered to *acceptable*.

At this point the risk category assessment for a given flight instance (c.f. Definition 2) has been completed. This process is then repeated for *each* of the instances identified as *highest risk*, as described below.

Recommendation 10 (Decision on waiver request using flight instance risk categories)**.** The framework described above shall be applied to *each* instance in the set of highest risk instances identified in Definition 2. The outcome of the framework is to assign a risk category (e.g., low, medium, or high) to the instance. The overall decision for the proposed flight operation will depend upon the risk categories assigned to each instance that was evaluated. A natural triage rule is:

1. *Approve* the proposed flight operation if the risk category for each instance is low.
2. *Require further review* if not all risk categories are low but no risk category is high.
3. *Deny* the proposed flight operation if the risk category for one or more instances is high.

Challenge 10 (Decision on waiver request using flight instance risk categories)**.** An open challenge regarding the recommended decision rule on waiver requests using flight instance risk categories is for the case of *require further review*. Specifically, additional guidance is needed to specify a rigorous yet feasible mechanism in order to move to either *approve* or *deny*. If such guidance is not available, then the most likely next step is to apply mitigations, either by moving one or more system state category values to one of that category's *mitigated states*, or by applying a non-systemic mitigation, as described in §9.3.

An additional approach to the challenge listed above is to consider the *societal benefit* of the proposed flight operation, described below.

Recommendation 11 (Benefit categories)**.** The following list of societal benefit categories is proposed:

1. Indispensable societal benefit;
2. High societal benefit;
3. Medium societal benefit;
4. Low societal benefit;
5. No societal benefit.

Challenge 11 (Benefit categories)**.** An open challenge regarding the proposed benefit categories in Recommendation 11 is to establish guidance on how proposed sUAS operations should be classified. Finally, guidance is required regarding the prudent incorporation of both the benefit category of the proposed sUAS operation and the risk category assigned to the various stages of the operation.

9 SRMP Step 5: Control of Safety Risk

This section applies Step 5, *Safety Risk Control*, of the SRMP tto support risk-based decision making and waiver approvals for sUAS. The section is organized as follows:

1. §9.1 *Order 8040.4b SRMP Guidance on Safety Risk Control* reviews the FAA's guidance on *Safety Risk Control* from FAA Order 8040.4b.
2. §9.2 *Order 8040.6 SRMP Guidance on Safety Risk Control* reviews the FAA's guidance on *Safety Risk Control* from FAA Order 8040.6.
3. §9.3 *Recommendation: Safety Risk Control to support risk-based decision making and waiver approvals for sUAS* applies the guidance on *Safety Risk Control* to the problem of sUAS waiver approval.

9.1 Order 8040.4b SRMP Guidance on Safety Risk Control

This section reviews SRMP guidance on *Safety Risk Control*, as found in Order 8040.4b [4], described as follows:

> If the residual risk is not acceptable, the proposed safety risk controls are redesigned or new safety risk controls are developed as necessary and the analysis is reconducted. This is done until the proposed safety risk controls enable the safety risk acceptance criteria to be met.

9.2 Order 8040.6 SRMP Guidance on Safety Risk Control

This section reviews SRMP guidance on *Safety Risk Control*, as found in Order 8040.6 [3]. The guidance offered in Section 2-e of Chapter 4 is:

> Validity of Mitigations. The safety analyst or team must consider the validity of mitigations presented by the applicant as part of the layered approach to mitigating risk. What evidence does the FAA have that the mitigations are effective (e.g., test data, third party verification)? How are the mitigations dependent on each other? How much credit should be given for the mitigations? Is there a single point failure? This information must be included in the SRM documentation.

The next section will apply the safety risk control guidance from both Order 8040.4b and Order 8040.6 to support risk-based decision making and waiver approvals for sUAS.

9.3 Recommendation: Safety Risk Control to support risk-based decision making and waiver approvals for sUAS

This section applies the Order 8040.4b and Order 8040.6 SRMP guidance on *Safety Risk Control*, reviewed in the previous section, to support risk-based decision making and waiver approvals for sUAS.

Definition 6 (Mitigation)**.** A *mitigation* is any aspect of the proposed flight that has one of the following two properties:

1. *Systemic mitigations:* the aspect is directly captured by / reflected in the system state space definition, referred to as a *mitigated state* in Model Specification 1, and corresponds to a nominal / ideal value relative to all other possible values in the state space category.

2. *Non-systemic mitigations:* the aspect is not defined or captured within the system state space of Model Specification 1 (e.g., because the mitigation is first introduced after the sysstem state space is "canonized"), but is nonetheless capable, in one or more system state vectors, of reducing either *a*) the likelihood of a hazard cause below a *de minimus* level, or *ii*) the "risk" (however it may be defined) of a hazard outcome below a *de minimus* level.

Systemic mitigations are already incorporated into the proposed framework, while *Non-systemic mitigations* are incorporated into it in a manner made precise below.

Model specification 20 (Non-systemic mitigation set and mitigation matrices)**.** Let $N_m \in \mathbb{N}$, and suppose the set of known *non-systemic mitigations* (henceforth, the *non-systemic mitigation set*) is labeled as $[N_m]$ and indexed by $w \in [N_m]$. Let $\ell(y|w,x)$ denote the likelihood of hazard cause y under system state vector x with mitigation w applied. The $N_m \times N_c(x)$ binary matrix, termed the *mitigation to hazard cause matrix*, denoted $\bar{Q}(x) \in \{0,1\}^{N_m \times N_c(x)}$, has entries

$$\bar{Q}(x)_{w,y} = \begin{cases} 1, & \ell(y|w,x) \text{ is } \textit{de minimus} \\ 0, & \text{else} \end{cases} . \tag{15}$$

Similarly, let $\text{risk}(z|w,x)$ (however it may be defined) denote the risk associated with hazard outcome z under system state vector x with mitigation w applied. The $N_m \times N_o(x)$ binary matrix, termed the *mitigation to hazard outcome matrix*, denoted $\hat{Q}(x) \in \{0,1\}^{N_m \times N_o(x)}$, has entries

$$\hat{Q}(x)_{w,z} = \begin{cases} 1, & \text{risk}(z|w,x) \text{ is } \textit{de minimus} \\ 0, & \text{else} \end{cases} . \tag{16}$$

Finally, let $Y(w,x) \subseteq Y(x)$ denote the subset of hazard causes removed from the framework under system state vector x when mitigation w is applied, where $Y(w,x) = \{y \in Y(x) : \bar{Q}(x)_{w,y} = 1\}$. Likewise, let $Z(w,x) \subseteq Z(x)$ denote the subset of hazard outcomes removed from the framework under system state vector x when mitigation w is applied, where $Z(w,x) = \{z \in Z(x) : \hat{Q}(x)_{w,z} = 1\}$.

Model specification 21 (Reduction of hazard outcome likelihood due to mitigation)**.** Let $W \subseteq [N_m]$ denote the subset of non-systemic mitigations that have been applied. Let $Y(W,x) \subseteq Y(x)$ denote the subset of hazard causes eliminated from consideration under system state vector x due to application of mitigation set W, i.e.,

$$Y(W,x) = \bigcup_{w \in W} Y(w,x). \tag{17}$$

Let $Z(W,x) \subseteq Z(x)$ denote the subset of hazard outcomes eliminated from consideration, conditioned on hazard cause y, under system state vector x due to application of mitigation set W, i.e.,

$$Z(W,x) = \bigcup_{w \in W} Z(w,x). \tag{18}$$

The quantities $Y(W,x)$ and $Z(W,x)$ modify Equation 3 in Model Specification 10 to be

$$\ell(z|W,x) = \sum_{y \in Y(x) \setminus Y(W,x)} \ell(z|x,y)\ell(y|x), \;\; z \in Z(x) \setminus Z(W,x). \tag{19}$$

Observe that i) the list of hazard outcomes has been trimmed by removing hazards $Z(W,x)$ from consideration and ii) the likelihood of the remaining hazard outcomes has been reduced by removing hazard causes $Y(W,x)$ from consideration.

10 Likelihood and decision transfer across system states

The proposed framework, as described thus far, has focused on assessing the risk and making a decision regarding a single system state vector x, where all likelihoods ($\ell_{\mathsf{y}}(x)$) and all conditional likelihoods ($\ell_{\mathsf{z}|\mathsf{y}}(x,y)$) are obtained directly from the corresponding posterior distributions under system state vector x.

The purpose of this section is to extend the framework to enable either *i*) likelihood transfer across "equivalent" system states (§10.1) or *ii*) risk category vector decision transfer across "nearby" system states (§10.2).

10.1 Likelihood transfer across equivalent system states

The likelihoods of hazard cause y under two system state vectors (x, x'), i.e., $\ell(y|x), \ell(y|x')$, may be considered equal, provided (x, x') are "equivalent" with respect to hazard cause y, in a sense made precise below. Similarly, the conditional likelihoods $\ell(z|x,y), \ell(z|x',y)$ for system state vectors (x, x') may again be considered equal, provided (x, x') are "conditionally equivalent" with respect to hazard outcome z, conditioned on hazard cause y, again, in a sense made precise below.

Definition 7 (Set partition and element equivalence)**.** A *p_i-partition* of a finite set, say $\mathcal{S}_i$, with cardinality $n_i = |\mathcal{S}_i|$, is a collection of p_i disjoint non-empty subsets of $\mathcal{S}_i$, with $p_i \in [n_i]$, denoted $\Pi(\mathcal{S}_i) = (\mathcal{S}_i^{(1)}, \ldots, \mathcal{S}_i^{(p_i)})$. The subsets forming the partition have the property that each element $s_i \in \mathcal{S}_i$ is in exactly one of the subsets (i.e., the subsets have union $\mathcal{S}_i$ and any pair of subsets is disjoint). In what follows, two elements of $\mathcal{S}_i$, say (s_i, s_i'), are considered *equivalent* (*distinct*) with respect to the partition $\Pi(\mathcal{S}_i)$ if (s_i, s_i') are in the same (in different) subsets, respectively.

Definition 8 (Vector equivalence with respect to component partitions)**.** Let $\mathcal{S} = \mathcal{S}_1 \times \cdots \times \mathcal{S}_N$ be the Cartesian product of sets $(\mathcal{S}_1, \ldots, \mathcal{S}_N)$ with cardinalities $n_i = |\mathcal{S}_i|$, and let $s = (s_1, \ldots, s_N) \in \mathcal{S}$, where $s_i \in \mathcal{S}_i$ for each $i \in [N]$. Let $\Pi(\mathcal{S}) = (\Pi(\mathcal{S}_i), i \in [N])$ denote a collection of partitions, one for each of the component sets. Leveraging Definition 7, two vectors in $\mathcal{S}$, say (s, s'), are considered *i*) *equivalent* with respect to the collection of partitions $\Pi(\mathcal{S})$ if, for each component index $i \in [N]$, the corresponding pair of elements (s_i, s_i') are equivalent, or *ii*) *distinct* if there is one or more component index $i \in [N]$ for which the element pair (s_i, s_i') is distinct.

Model specification 22 (Hazard cause likelihood equivalence and likelihood transfer)**.** Let $X = (x^i, i \in [M])$ be a collection of M distinct system state vectors for which the likelihood of a hazard cause y is known in each case, i.e., $(\ell(y|x^i), i \in [M])$ is "known" (or estimated), and let $\Pi_y(\mathcal{X}) = (\Pi_y(\mathcal{X}_s), s \in [N_s])$ denote the collection of partitions of the different components of the state space $\mathcal{X} = \mathcal{X}_1 \times \cdots \times \mathcal{X}_{N_s}$ in Model Specification 1. The partitions are selected such that the likelihoods $\ell(y|x)$ and $\ell(y|x')$ may be treated as effectively equal for pairs of systems state vectors (x, x') equivalent in the sense of Definition 8. Given a system state vector $x \notin X$, let $X(x,y) \subseteq X$ (possibly empty) hold all system state vectors $x' \in X$ for which (x, x') are equivalent system state vectors with respect to the collection of partitions

$\Pi_y(\mathcal{X})$ (c.f. Definition 8). If $X(x, y)$ is nonempty, then the likelihood $\ell(y|x)$ is *transferred* from $\Pi(y)$ as the value $\ell(y|x')$ for any $x' \in X(x, y)$.

The above Model Specification of *hazard cause likelihood equivalence* extends, *mutatis mutandis*, in the natural way to a definition of *hazard outcome conditional likelihood equivalence*, requiring a state space partition for each hazard cause and hazard outcome pair (y, z), i.e., $\Pi_{y,z}(\mathcal{X}) = (\Pi_{y,z}(\mathcal{X}_s), s \in [N_s])$.

An important special case of the above *hazard cause likelihood equivalence* is the following *hazard cause to system state dependence matrix*. Roughly, $\bar{T}_{y,s} = 1$ corresponds to the "maximum" partition $\Pi_y(\mathcal{X}_s)$ consisting of $|\mathcal{X}_s|$ singleton sets, each holding an individual value $x_s \in \mathcal{X}_s$, while $\bar{T}_{y,s} = 0$ corresponds to the "minimum" partition $\Pi_y(\mathcal{X}_s)$ consisting of a single set, i.e., $\mathcal{X}_s$.

Model specification 23 (Hazard cause to system state dependence matrix)**.** Let $\bar{T} \in \{0, 1\}^{N_c \times N_s}$ be the $N_c \times N_s$ binary matrix where

$$\bar{T}_{y,s} = \begin{cases} 1, & y \textit{ dependent} \text{ on } s \\ 0, & y \textit{ independent} \text{ of } s \end{cases} \tag{20}$$

In particular, *independence* means the likelihood of hazard cause index y is the same for all values of the system state component index s:

$$\ell(y|(x_{\setminus s}, x_s)) = \ell(y|(x_{\setminus s}, x'_s)),\ (x_s, x'_s) \in \mathcal{X}_s^2. \tag{21}$$

Here, $x_{\setminus s}$ refers to the system state vector x, but with component index s excised, so that $(x_{\setminus s}, x_s)$ and $(x_{\setminus s}, x'_s)$ are two system state vectors with equal values in every component except for component index s.

10.2 Risk category vector decision transfer across nearby system states

The previous subsection identifies a structured means by which a collection of likelihoods for different system state vectors and a notion of likelihood equivalence allows for likelihoods for new system state vectors to be found. This subsection, in contrast, considers a collection of system state vectors approved for operation, and uses a natural notion of distance and a corresponding distance threshold in order to allow approval of system state vectors that are "nearby" to one or more system state vectors that has already been approved.

Model specification 24 (Approved system state vectors)**.** Fix $M \in \mathbb{N}$, and let $X = (x^1, \ldots, x^M)$, indexed by $i \in [M]$, denote M distinct system state vectors, i.e., $x^i \in \mathcal{X}$ for each $i \in [M]$, each one approved for sUAS operation.

Recommendation 12 (Approved system state vectors)**.** As a conservative approach, it is recommended that the only approved system state vector that is initially approved within the framework is the one for which all state category variables are in their "best possible" state, i.e., the state for which the hazard outcome likelihoods are lowest.

Challenge 12 (Approved system state vectors)**.** An open challenge regarding the proposed approved system state vector in Recommendation 12 is that it is unlikely to be sufficiently close to the system state vectors requested in practice. Identification of additional system state vectors for initial approval would hold great practical value.

Assumption 3 (System state vector distance is Hamming distance)**.** Although alternatives are certainly possible and perhaps in certain contexts will be found superior, the distance between two system state vectors, say x, x', denoted as $d(x, x')$, is measured using *Hamming distance*:

$$d(x, x') = \sum_{s \in [N_s]} [x_s \neq x'_s]. \tag{22}$$

Recall, the Iverson bracket notation $[P]$ for proposition P takes value 1 (0) if P is true (false), respectively, so $d(x, x')$ is the number of positions, indexed by $s \in [N_s]$, in which system state vectors x, x' differ (recall each set $\mathcal{X}_s$ is assumed finite), and as such $d(x, x') \in [0 : N_s]$.

Model specification 25 (Nearest neighbors and nearest neighbor distance)**.** Recall $X = (x^1, \ldots, x^M)$ holds M distinct system state vectors approved for sUAS operations. Given a proposed system state vector $x \in \mathcal{X}$ (where x need not be in X), the set of nearest neighbors and the nearest neighbor distance for x are denoted, respectively:

$$\mathrm{NN}(x, X) = \operatorname*{argmin}_{i \in [M]} d(x, x^i), \quad d_{\min}(x, X) = \min_{i \in [M]} d(x, x^i). \tag{23}$$

Recommendation 13 (Triaging waiver requests using system state distance)**.** Fix a distance threshold $\tau \in [N_s]$ and use it to define the following triage rule for waiver requests with system state vector x:

1. $d_{\min}(x, X) = 0$: zero distance from X means $x \in X$, i.e., the proposed system state vector x is equal to one of those (X) already approved for operation, so no waiver is in fact required.
2. $0 < d_{\min}(x, X) \leq \tau$: the proposed system state vector is not one of those already approved, i.e., $x \notin X$, but has a system state vector sufficiently close to one or more approved system state vectors so that a probabilistic risk assessment (PRA) may be possible. The waiver application decision will depend upon the outcome of the PRA.
3. $\tau < d_{\min}(x, X)$: the proposed system state vector is not one of those already approved, i.e., $x \notin X$, and the proposed system state vector is not sufficiently close to any approved system state vector. As such, either the waiver application is rejected, or a mitigation is identified, changing x to x', say, such that its distance from an approved system state vector is reduced below the threshold, i.e., $d_{\min}(x', X) \leq \tau$. A final option would be for the applicant to arrange for a custom comprehensive PRA of x to be conducted.

Challenge 13 (Triaging waiver requests using system state distance)**.** An open challenge regarding the proposed triaging of waiver requests using system state distance in Recommendation 13 is validation and verification that the waiver request decisions made under the proposed triage are consistent with current practice, guidance, and policy.

11 Conclusion and Next Steps

This report has applied the FAA's Safety Risk Management Process (SRMP) to develop a proposed probabilistic risk assessment (PRA) framework for evaluation of small unmanned aerial systems (sUAS) operations in the national airspace (NAS).

The primary objectives of this document are:

1. To describe a PRA-based mechanism that would facilitate the development and evaluation of waiver requests for the operation of a sUAS, and furthermore facilitate the development of a feasible method for applicants to create and evaluators to assess such proposals. It is important to note that the framework first determines whether or not a risk assessment is necessary, and only then requires additional inputs to quantify that risk.

2. To provide simplified and abstracted example scenarios that illustrate the application of the framework.

The remainder of this section reviews the model specifications, recommendations and challenges, and next steps.

Model specifications. The framework includes the following model specifications ("mod. spec.", below):

1. Mod. spec. 1: System state space and system state vector
2. Mod. spec. 2: Hazard causes (under single hazard cause assumption)
3. Mod. spec. 3: Hazard causes (under multiple hazard cause assumption)
4. Mod. spec. 4: Hazard outcomes (under single hazard outcome assumption)
5. Mod. spec. 5: Hazard outcomes (under multiple hazard outcome assumption)
6. Mod. spec. 6: Hazard causes and hazard outcomes relevant to system state vector
7. Mod. spec. 7: System state, hazard cause, and hazard outcome notation
8. Mod. spec. 8: Likelihood of hazard causes
9. Mod. spec. 9: Likelihood of hazard outcomes
10. Mod. spec. 10: Simplified likelihood of relevant hazard outcomes
11. Mod. spec. 11: Prior distributions on hazard cause likelihoods
12. Mod. spec. 12: Prior distributions on hazard outcome conditional likelihoods
13. Mod. spec. 13: Observations of hazard causes / outcomes under the system state vector
14. Mod. spec. 14: Posterior distributions on hazard cause likelihoods
15. Mod. spec. 15: Posterior distributions on hazard outcome conditional likelihoods
16. Mod. spec. 16: Likelihood categories
17. Mod. spec. 17: Severity categories
18. Mod. spec. 18: Safety risk assessment matrix
19. Mod. spec. 19: Hazard outcome risk category vector

20. Mod. spec. 20: Mitigation set and mitigation matrices
21. Mod. spec. 21: Reduction of hazard outcome likelihood due to mitigation
22. Mod. spec. 22: Hazard cause likelihood equivalence and likelihood transfer
23. Mod. spec. 23: Hazard cause to system state dependence matrix
24. Mod. spec. 24: Approved system state vectors
25. Mod. spec. 25: Nearest neighbors and nearest neighbor distance

Recommendations and challenges. Several recommendations ("rec.", below) have been made for instantiation of the proposed framework, and each has been paired with a corresponding challenge ("rec.", below):

1. Rec. 1, Cha. 1: System state category specification
2. Rec. 2, Cha. 2: Hazard cause specification
3. Rec. 3, Cha. 3: Hazard outcome specification
4. Rec. 4, Cha. 4: Hazard causes and hazard outcomes relevant to system state vector
5. Rec. 5, Cha. 5: Prior parameter setting, data collection, and sample size
6. Rec. 6, Cha. 6: Likelihood categories
7. Rec. 7, Cha. 7: Severity categories
8. Rec. 8, Cha. 8: Safety risk assessment matrix
9. Rec. 9, Cha. 9: Flight instance risk category decisions via hazard outcome risk category vector
10. Rec. 10, Cha. 10: Decision on waiver request using flight instance risk categories
11. Rec. 11, Cha. 11: Benefit categories
12. Rec. 12, Cha. 12: Approved system state vectors
13. Rec. 13, Cha. 13: Triaging waiver requests using system state distance

Next steps. Each of the Challenges listed above should be thoroughly addressed. In addition, the proposed effort includes the following two next steps for assessing and illustrating the applicability of the proposed framework:

1. *Task 3-2: Demonstration and application of framework from another sector.* The goal is to demonstrate and help validate the application of this framework by reviewing the SMS framework and risk standards from another sector and, to the extent that data can be provided by the FAA or other sources, illustrate how the proposed risk assessment framework could be applied to examples from this other sector (e.g. general aviation, helicopter, passenger carrying aircraft, or dirigibles). Use this comparison to help validate results produced by this risk assessment framework.'
2. *Task 3-3: Illustration of application of the framework.* The goal of this task is to Illustrate the application of this risk-based approach using examples based on the operation of small UAS engaged in expanded and non-segregated operations. This should include illustrations involving UAS-manned aircraft interactions based on UAS data, ATC data, and be informed by findings from the UAS detection component identified in Task 1-4 of ASSURE A21.

A Appendix: Mathematical notation

Table 2 lists all the mathematical notation used in the models specification.

Symbol	Model spec.	Meaning
$\bar{\alpha}, \bar{\alpha}^i, \bar{\alpha}^i_y$	11	Dirichlet prior disbn. parameters on hazard causes
$\hat{\alpha}, \hat{\alpha}^i_y, \hat{\alpha}^i_{y,z}$	12	Dirichlet prior disbn. parameters on hazard outcomes
$\mathcal{A}$	18	risk matrix score values ($\{G, Y, R\}$)
$d(x, x')$	3	Hamming distance between state vectors x, x'
$d_{\min}(x, X)$	25	minimum distance from state x to state list X
$f_L, f_L(\ell)$	16	hazard likelihood to hazard likelihood category mapping
$\ell_{\mathsf{y}}(x), \ell(y\|x)$	8, 11	hazard cause likelihood under state vector x
$\ell(x), \ell(z\|x)$	8, 12, 19	unconditional likelihood of hazard outcome z
$\ell(z\|x, y), \ell_{\mathsf{z}\|\mathsf{y}}(x, y)$	8, 12, 19	cond. likelihood given hazard cause y of hazard outcome z
$L(x), L(z\|x, y), L(z\|x)$	16, 19	hazard outcome likelihood category
$\mathcal{L}, L$	16, 18	hazard outcome likelihood categories ($\{A, B, C, D, E\}$)
M	24	number of distinct FAA-approved system state vectors
m, m^i	13	count of number of trials for each system state index i
$N_c, N_c(x)$	2, 6	number of distinct hazard causes
N_m	20	number of distinct mitigations
$N_o, N_o(x)$	4, 6	number of distinct hazard outcomes
N_s	1	number of components in system state vector
$\mathrm{NN}(x, X)$	25	nearest neighbors of state vector x in state vector list X
$\bar{Q}(x), \hat{Q}(x)$	20	mitigation to hazard cause and hazard outcome matrices
$R(x), R(z\|x)$	19	hazard outcome risk category vector
$\mathcal{S}, S, S_z$	17, 18	hazard outcome severity categories ($\{5, 4, 3, 2, 1\}$)
$\bar{T}, \bar{T}_{y,s}$	23	hazard cause to system state category dependence matrix
τ	13	system state vector distance threshold
$U, U(L, S)$	18	safety risk assessment matrix
v	5	count vector for posterior Dirichlet distribution
$\bar{v}(x), \bar{v}(x, y)$	14	observed hazard cause counts
$\hat{v}(x, y), \hat{v}(x, y, z)$	15	observed hazard outcome counts
w, W	20, 21	mitigation value, mitigation subset
$x = (x_1, \ldots, x_{N_s})$	1	system state vector
X, x^i	24	FAA-approved system state vectors
$\mathcal{X}_s, \bar{\mathcal{X}}_s$	1	state values in category s, mitigated state values in category s
$\mathcal{X} = \mathcal{X}_1 \times \cdots \times \mathcal{X}_{N_s}$	1	system state space
y, y	1, 7	hazard cause value, random variable
$Y(x), Y(W, x)$	6, 20	relevant hazard causes and causes excised due to mitigations
z, z	4, 7	hazard outcome value, random variable
$Z(x), Z(W, x)$	6, 20	relevant hazard outcomes and outcomes excised due to mitigations

Table 2: Mathematical notation in framework

B Appendix: On single vs. multiple hazard causes

This section provides a preliminary analysis that facilitates a comparison of the single hazard cause assumption and the corresponding single and multiple hazard cause models. Under the *single hazard cause assumption* (Assumption 1), Equation 2 requires summation over $N_c + 1$ terms, one for each possible hazard cause. In contrast, under the *multiple hazard cause model*, Equation 2 would be replaced with

$$\ell(z|x) = \sum_{y \in \{0,1\}^{N_c}} \ell(z|x,y)\ell(y|x), \tag{24}$$

which is a summation over all 2^{N_c} possible hazard cause vectors y. Determining this many likelihoods may prove to be prohibitively difficult in practice. The reduction in complexity from requiring 2^{N_c} terms down to $N_c + 1$ terms is a key benefit of and rationale behind the *single hazard cause assumption*.

The following analysis on the likelihood of multiple hazard causes may be insightful. The set $\{0,1\}^{N_c}$ of 2^{N_c} hazard cause vectors y may be partitioned:

$$\{0,1\}^{N_c} = \{0\} \cup \mathcal{Y}_1 \cup \mathcal{Y}_{>1}, \tag{25}$$

where $\{0\}$ denotes the singleton set holding the vector of N_c zeros, $\mathcal{Y}_1$ holds the N_c "unit vectors", each denoted $y^{(c)}$ with a single one in position $c \in [N_c]$, and $\mathcal{Y}_{>1}$ holds the remaining $2^{N_c} - N_c - 1$ vectors that each have multiple ones. Under the *single hazard cause assumption*, the probability of the unconditional likelihood of hazard outcomes, $\ell(z|x)$, is approximated by treating the probability of the latter set as negligibly small:

$$\begin{aligned}
\ell(z|x) &= \sum_{y \in \{0,1\}^{N_c}} \ell(z|x,y)\ell(y|x) \\
&= \ell(z|x,0)\ell(0|x) + \sum_{c \in [N_c]} \ell(z|x,y^{(c)})\ell(y^{(c)}|x) + \sum_{y \in \mathcal{Y}_{>1}} \ell(z|x,y)\ell(y|x) \\
&\approx \ell(z|x,0)\ell(0|x) + \sum_{c \in [N_c]} \ell(z|x,y^{(c)})\ell(y^{(c)}|x)
\end{aligned} \tag{26}$$

In order to gain more traction on this approximation, assume for the moment that the individual hazard cause events are approximately independent, i.e.,

$$\ell(y|x) \approx \prod_{c \in [N_c]} \ell(y_c|x). \tag{27}$$

In this case, the unconditional likelihood of a hazard outcome may be approximated as

$$\ell(z|x) \approx \ell(z|x,0) \prod_{c \in [N_c]} \ell(y_c = 0|x) + \sum_{c \in [N_c]} \ell(z|x,y^{(c)})\ell(y_c = 1|x) \prod_{c' \in [N_c] \setminus c} \ell(y_{c'} = 0|x) \tag{28}$$

The following analysis is useful as a crude approximation of how the likelihood of the union of all hazard vectors with multiple causes may be bounded in terms of the likelihood of any individual hazard cause and the number of hazard causes.

Suppose $\ell(y^{(c)}|x) = \delta$ for each c, for some $\delta \in (0,1)$, and let $\bar{\delta} = 1 - \delta$. Suppose the hazard causes are independent, i.e., $\ell(y|x) = \prod_{c\in[N_c]} \ell(y_c|x)$. Then, *i*) the likelihood of 0 is $\ell(0|x) = \bar{\delta}^{N_c}$, *ii*) the likelihood of $\mathcal{Y}_1$ is $\ell(\mathcal{Y}_1|x) = \sum_{c\in[N_c]} \ell(y^{(c)}|x) = N_c\delta\bar{\delta}^{N_c-1}$, and so *iii*) the likelihood of $\mathcal{Y}_{>1}$, which for the purpose of this analysis will be considered the *error* associated with the *single hazard cause assumption*, is

$$\ell(\mathcal{Y}_{>1}|x) = g(\delta, N_c) = 1 - \bar{\delta}^{N_c} - N_c\delta\bar{\delta}^{N_c-1}. \tag{29}$$

Consider the set of (δ, N_c) pairs for which $g(\delta, N_c) < \delta$, i.e., the probability of the union of all hazard cause vectors with multiple causes is less than the (common) probability of any individual hazard. The Bernoulli inequality, $(1-d)^k \geq 1 - dk$, yields the lower bound

$$g(\delta, N_c) \geq 1 - (1 - \delta N_c) - N_c\delta(1 - \delta(N_c - 1)) = \underline{g}(\delta, N_c). \tag{30}$$

Solving $\underline{g}(\delta, N_c) = \delta$ for δ yields:

$$\underline{\delta}(N_c) = \frac{1}{N_c(N_c - 1)}. \tag{31}$$

This last result implies that, under the above assumptions, if $\delta < 1/N_c^2$ then $\ell(\mathcal{Y}_{>1}|x) < \delta$, i.e., the likelihood of the union of all hazard cause vectors with multiple causes is smaller than the likelihood of any one single hazard cause. In other words, if the hazard causes are approximately independent and have likelihoods that are small enough relative to the number of causes (here, $\delta < 1/N_c^2$), then there is a reasonably small error incurred in neglecting all hazard cause vectors with multiple causes, i.e., the *single hazard cause assumption* incurs a reasonably small level of inaccuracy. Concretely, if $\delta = 1\%$ and $N_c = 10$, i.e., if the ten hazard causes are independent and each have a 1% chance of occurrence, then there is less than 1% error incurred under the *single hazard cause assumption*.

C Appendix: Minimum sample size to observe an event

Let $p \in (0,1)$ be the probability of an event of interest, and let $m \in \mathbb{N}$ be the number of independent and identically distributed (IID) Bernoulli trials / observations, captured via IID Bernoulli random variables (RVs) $(\mathsf{x}_1, \ldots, \mathsf{x}_m)$, with $\mathsf{x}_j \sim \text{Ber}(p)$ for $j \in [m]$. The event $\{\mathsf{x}_j = 1\}$ is termed a "hit" on trial j in what follows. Let $k \in \mathbb{N}$ denote the target number of hits and let $\epsilon \in (0,1)$ be the target lowest acceptable probability that k or more hits are NOT observed in the m trials. Then, let $\bar{m} = \bar{m}(p,k,\epsilon) \in \mathbb{N}$ denote

$$\bar{m} \equiv \underset{m \in \mathbb{N}}{\text{argmin}}\, n : \mathbb{P}(\mathsf{x}_1 + \cdots + \mathsf{x}_m \leq k-1) \leq \epsilon, \tag{32}$$

i.e., $\bar{m}$ is the smallest number of trials such that the probability of observing fewer than k hits is below ϵ. Let $\text{bin}(m,p)$ denote a binomial RV with m trials and success probability p and let $\mathsf{z} \sim \text{Po}(\lambda)$ denote a Poisson RV with parameter $\lambda \in \mathbb{R}_+$. For m "large" (e.g., over 100) and p "small" (e.g., under 1/100), the *Poisson approximation* to the binomial asserts, crudely, that the binomial distribution with parameters (m,p) is approximately equal to the Poisson distribution with parameter mp, i.e., $\text{bin}(m,p) \approx \text{Po}(mp)$. Denote the cumulative distribution function (CDF) for $\mathsf{z} \sim \text{Po}(\lambda)$ as $F_{\mathsf{z}}(z;\lambda) \equiv \mathbb{P}(\mathsf{z} \leq z)$, for $z \in \mathbb{R}$. Under this approximation, (32) becomes

$$F_{\mathsf{z}}(k-1; \bar{m}p) \leq \epsilon \tag{33}$$

Consider the particular case of $k = 1$, and recall that, if $z \sim \text{Po}(\lambda)$, then $\mathbb{P}(\mathsf{z} = 0) = \text{e}^{-\lambda}$. With this in hand, (33) becomes, for $k = 1$, $\text{e}^{-\bar{m}p} \leq \epsilon$, which may be solved for $\bar{m}$ as:

$$\bar{m}(p, 1, \epsilon) = \left\lceil -\frac{1}{p} \log(\epsilon) \right\rceil. \tag{34}$$

For example, in order to ensure at most a 10% chance of not observing at least one hit of an event that occurs with probability of 1%, one would require no fewer than $\bar{m}(1/100, 1, 1/10) \approx 230$ independent trials.

D Appendix: Simple example of proposed framework

This section applies the proposed framework to a simple fabricated example scenario.

Step 1: System analysis

The CONOPS (c.f. Definition 1) will be left unspecified, to emphasize the (overall) general nature of the example. Per Definition 2, the flight stages will consist, in this example, of *takeoff*, *en route*, and *landing*. Suppose further that a single highest risk instance is identified for each of the three stages; these will be referred to as the *highest risk takeoff instance*, the *highest risk en route instance*, and the *highest risk landing instance*. Having identified these instances, it remains to apply the PRA process to each of them.

Before providing the per-instance reasoning, however, suppose for purpose of simplicity that for purpose of simplicity and illustration, it is further assumed that each of the system state categories consists of only two values: the *mitigated state*, denoted 0, and the *unmitigated state*, denoted 1. For example (c.f. Recommendation 1):

1. *sUAS platform and payload:* certified safe (0) or uncertified (1)
2. *Flight readiness:* pre-flight checks all positive (0) or one or more pre-flight check anticipated to fail (1)
3. *Operator workstation:* certified operational (0) or uncertified (1)
4. *Operator training and procedures:* trained expert (0) or operator not a trained expert (1)
5. *Flight plan:* nominal / safest possible (0) or distinct from nominal / safest possible (1)
6. *C2 channel:* high bandwidth, low latency, and low error rate (0) or anticipated to suffer low bandwidth, high latency, or high error rate (1)
7. *Information acquisition, processing, and dissemination:* anticipated operation during daylight in absence of electromagnetic interference (0) or either operating at night or in presence of interference (1)
8. *Weather environment:* anticipated no or low wind and no or low precipitation (0) or either wind or precipitation (1)
9. *Airspace environment:* anticipated no nearby unmanned or manned vehicles (0) or anticipated to intersect with established flight paths for manned vehicles (1)
10. *Ground environment:* anticipated to have no human ground presence and minimal built environment (0) or either human ground presence or a notable built environment (1)

As each system state category is assumed to be binary, it follows that $\mathcal{X}_s = \{0, 1\}$ for each $s \in [N_s]$, where (in this case) $N_s = 10$. As the system state categories do not logically preclude each other, it follows that there are $2^{N_s} = 2^{10} = 1024$ distinct system state vectors x under this simplest possible taxonomy. Furthermore, in each of these cases, i.e., in each system state category s, the *mitigated state* (the nominal/ideal) state is denoted 0 ($\bar{\mathcal{X}}_s = \{0\}$) and the non-mitigated state is denoted 1 (c.f. Model Specification 1).

Step 2: Identify hazards

Step 2 for the highest risk takeoff instance

Suppose that in the highest risk takeoff instance the operating conditions are all ideal/nominal, so that all of the system state category values are *mitigated*. The system state vector is such that all state category variables align with the least likelihood of any hazard outcomes, i.e., the zero-vector, $x^1 = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$.

Recall from Recommendation 2, the identified hazard causes are:

1. *sUAS malfunction*
2. *sUAS operator error*
3. *C2 link failure*
4. *Inability to sense environment*
5. *Inability to control flight*

and, from Recommendation 3, the three hazard outcomes are:

1. *Proximity to or collision with a person*
2. *In-air proximity to or collision with a manned airborn vehicle*
3. *Proximity to or collision with the built environment*

Finally, recall from Recommendation 4 that it is required to assess whether each hazard cause and each hazard outcome is pertinent to the current system state vector. As the system state vector specifies that *i*) the takeoff will be in a geographic region not containing any other aircraft (i.e., the airspace environment state category value is 0) and *ii*) the takeoff will be in a geographic region not containing any humans on the ground (except perhaps the operator) and not having any substantial built environment (i.e., the ground environment state category value is 0), it follows that all three hazard causes may be safely excised from the model. As no hazard outcomes remain, there is no need to conduct a PRA for this instance.

Step 2 for the highest risk en route instance

Suppose that in the highest risk en route instance the operating conditions are all again ideal/nominal, with the exception that, at the highest risk en route instance, the sUAS will be above an area that may contain humans on the ground, but for which the built environment is still negligible. The system state vector is $x^2 = (0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$. As with the highest risk takeoff instance, the fact that the airspace environment state category value is 0 precludes the possibility of the hazard outcome of in-air proximity to or collision with a manned airborn vehicle. Moreover, by the assumption that the built environment at this instant is negligible, it is also reasonable to excise the hazard outcome of proximity to or collision with the built environment. The sole hazard outcome that remains is that of proximity to or collision with a person.

Step 2 for the highest risk landing instance

Suppose that in the highest risk landing instance the operating conditions are all again ideal/nominal, with the exception that, at the highest risk landing instance, the sUAS will be in an airspace environment that may contain a manned vehicle. The system state vector is $x^3 = (0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$. By the assumption that the ground environment at this instant is negligible, it is also reasonable to excise the hazard outcome of proximity to or collision with the built environment, as well as the hazard outcome of proximity to or collision with a person. The sole hazard outcome that remains is that of proximity to or collision with a manned airborne vehicle.

Step 3: Safety risk analysis

As evident from the preceding three subsections, the PRA for the given example requires assessing *i*) the likelihood of proximity to or collision with a person in the highest risk en route instance, and *ii*) the likelihood of proximity to or collision with a manned airborne vehcile in the highest risk landing instance. The framework will be conducted on each of these two instances, separately, and the resulting risk category assigned to each instance will determine the decision for the overall flight. The discussion below applies to either of these two instances.

The components of the hazard cause Dirichlet prior distribution parameter vector $\bar{\alpha}(x)$ must be specified: one parameter for each of the relevant hazard causes, and one for the case of no hazard causes. The values of these parameters will not be estimated in this example; they should reflect the prior belief regarding the likelihood of each possible hazard cause under the current system state vector.

Also, the conditional hazard outcome Dirichlet prior distribution parameter vectors $\hat{\alpha}(x) = (\hat{\alpha}(x, y))$ must be specified, where each of the vectors $\hat{\alpha}(x, y) = (\hat{\alpha}(x, y, z))$ has one parameter for each of the pertinent hazard outcomes and one for the case of the no hazard outcome. The values of these parameters will not be estimated in this example; they should reflect the prior belief regarding the conditional likelihood of each possible hazard outcome under each possible hazard cause, for the current system state vector.

The state vector x must be tested some number of times, $m(x)$. Suppose $m(x) = 100$ tests are run, and the corresponding hazard cause (if any) and hazard outcome (if any) for each test are recorded in the following count vectors. The vector $\bar{v}(x) = (\bar{v}(x, y))$ is a count vector, summing to $m(x) = 100$, tallying the number of times each hazard outcome is observed in the $m(x) = 100$ tests. Similarly, the matrix $\hat{v}(x)$ has rows $(\hat{v}(x, y))$, records the counts of each hazard outcome z under each hazard cause y, i.e., $\hat{v}(x, y) = (\hat{v}(x, y, z))$, where $\hat{v}(x, y, z)$ counts the number of trials resulting in hazard cause y and hazard outcome z.

Having recorded all the counts, the likelihood on hazard causes under system state x, i.e., $\ell_{\mathsf{y}|x}$, is updated from its prior distribution, $\mathrm{Dir}(\bar{\alpha}(x))$, to its posterior distribution, $\mathrm{Dir}(\bar{\alpha}(x) + \bar{v}(x))$. Likewise, the conditional likelihoods on hazard outcomes under system state x for each possible hazard cause y, i.e., $\ell_{\mathsf{z}|x,y}$, are each updated from their prior conditional distribution, $\mathrm{Dir}(\hat{\alpha}(x, y))$, to the respective posterior conditional distribution, $\mathrm{Dir}(\hat{\alpha}(x, y) + \hat{v}(x, y))$.

Step 4: Assessment of safety risk

Per Recommendation 6, the *likelihood* are selected to be $\mathcal{L} \equiv \{A, B, C, D, E\}$, per Recommendation 7, the *severity categories* are selected to be $\mathcal{S} \equiv \{5, 4, 3, 2, 1\}$, and per Recommendation 8, the *safety risk assessment matrix* U is set to be that given in FAA Order 8040.6.

With the hazard cause posterior likelihoods, $\ell(y|x)$ for $y \in [0:5]$, and each of the hazard outcome posterior conditional likelihoods, $\ell(z|x,y)$ for each $z \in [0:4]$ and each $y \in [0:5]$ in hand, the hazard outcome posterior *unconditional* likelihoods, $\ell(z|x)$ for $z \in [0:4]$, may be computed using Equation 2 in Model Specification 9.

These hazard outcome posterior unconditional likelihoods are in turn used to compute hazard outcome likelihood categories, $L(z|x)$, per Model Specification 16 and Model Specification 18. The hazard outcome risk category vector $R(x) = (R(z|x), z \in [0:4])$, where $R(z|x) = U(L(z|x), S_z)$ is the risk category of hazard outcome $z \in [0:4]$ under system state x, and S_z is the corresponding risk severity level for that hazard outcome. Note, each $R(z|x) \in \mathcal{A} = \{R, Y, G\}|$, with R (red, high), Y (yellow, medium), and G (green, low) risk categories.

Next, per Recommendation 9, the system state x risk will be: *i*) *low* if the risk category for *each* hazard outcome is G (all green), *ii*) *high* if the risk category for *any* hazard outcome is R (any red), else *iii*) *medium*.

Step 5: Safety risk control

The subset W of mitigations to be applied is identified, and this in turn *i*) removes hazard causes $Y(W, x)$ from consideration and *ii*) removes hazard outcomes $Z(W, x)$ from consideration. This, in turn, allows for revised hazard outcome likelihoods for all remaining hazard outcomes to be computed, per Equation 19 in Model Specification 21. As above, these hazard outcome likelihoods are mapped into likelihood categories, creating a (possibly) revised hazard outcome risk category vector, which in turn yields a (possibly) revised hazard outcome decision.

E Appendix: Background Literature and Related Work

This appendix highlights the pertinent findings from the NASEM report that motivated this work including the concept of the three components (PRA, comparative risk analyses and the idea of insurance for low risk waiver applications) as well as the notion of considering societal benefit.

This appendix overviews the current SMS process with a focus on Safety Risk Management. It highlights the anticipated challenges in successfully applying a risk-based PRA methodology to the six SRM steps.

It further characterizes current approaches based on fundamentally qualitative and subjective risk analysis and associated weaknesses. It reviews the Joint Authorities for Rulemaking on Unmanned Systems (JARUS) Specific Operation Risk Assessment (SORA) and highlights its subjective approach requiring extensive subject matter expertise and lack of repeatability.

It addresses related projects supported by the FAA including MITRE's Operational Risk Assessment Prototype that seeks to provide a quantitative risk assessment model that the FAA can use to streamline the waiver approval process, to support regulatory development, and to facilitate safety risk analysis. It addresses parallel efforts by Transport Canada and Periculum Labs Inc. which is developing a PRA methodology for scenario-based risk assessment for BVLOS with UAS,

To support the insurance component of the framework, the appendix presents the current approach and self-assessment of insurance companies re UAS insurance.

It ends with a review of relevant PRA related literature.

E.1 Introduction

In support of Task 3-1 of Project A21, this appendix summarizes the current state with respect to risk frameworks as well as relevant probabilistic risk assessment research. These findings will support the development of a framework that defines a process for making risk-based decisions that applies across the varying levels of risk associated with the operation of different small UAS and considers performance-based requirements to mitigate risk.

E.2 Safety Management System

E.2.1 Overview

Within the FAA, SMS is the formal, top-down, organization-wide approach to managing safety risk and assuring the effectiveness of safety risk controls [5] [6]. It includes systematic procedures, practices, and policies for the management of safety risk. The four main components of an SMS are [5]:

1. Safety policy,
2. Safety risk management,
3. Safety assurance, and
4. Safety promotion

The FAA will only approve waivers for UAS flight operations that can be conducted with an Acceptable Level of Safety, as determined in part through the information in Advisory Circular (AC) 120-92B [7]. This document provides guidance on how the SMS may be developed to achieve the safety performance objectives outlined by an organization. The AC makes clear that there is no single SMS design that the FAA expects each air carrier to develop as it should work for its unique operation. The methods mentioned in the AC are not the only means of compliance. This philosophy is important to consider.

E.2.1.1 Safety policy FAA Order 8000.369C Safety Management Systems [5] describes that safety policy is the FAA's documented commitment to safety, which defines safety objectives and the accountabilities and responsibilities of its employees in regard to safety management. Elements include:

1. safety policy, requirements, methods, and processes used to achieve the desired safety outcomes,
2. management commitment and safety accountabilities,
3. key safety personnel,
4. emergency preparedness and response, and
5. SMS documentation and records

E.2.1.2 Safety risk management Safety risk management (SRM) provides for initial and continuing identification of hazards and the analysis and assessment of safety risk. FAA Order 8040.4B Safety Risk Management Policy [4] establishes processes used to analyze, assess, mitigate, and accept safety risk. The process is briefly described here and in more detail below.

1. System analysis through establishing an understanding of significant system design and performance factors, human interface, processes, and activities to the level necessary to identify hazards. When describing and analyzing the system, it is important to do the following:
   (a) Define and document the scope (i.e., system boundaries) and objectives related to the system.
   (b) Gather relevant data
   (c) Develop a safety risk acceptance plan
   (d) Describe and model the system and operation in sufficient detail for the safety analysts to understand and identify the hazards that can exist in the system, as well as their sources and possible outcomes
   (e) Address the effects on the interfaces or other systems
   (f) Address the effects of the broader system (such as operating environment, system's processes and procedures, and personnel, equipment, and facilities)
2. Identify and document hazards that have the potential to affect safety risk in sufficient detail to determine the associated safety risk

3. Determine and analyze the safety risk, currently through severity and likelihood of potential effects associated with the identified hazards.
4. Assess safety risk currently by comparing the safety risk of each identified hazard's effect to established safety performance targets and/or hazard ranks based on risk. The objective is to determine the acceptability of the safety risk of each hazard.
5. Control safety risk through design and implementation of safety risk control(s) for hazards with associated unacceptable risk.
6. Track identified hazards and monitor implemented safety risk controls/mitigations to ensure that they achieve their intended objectives. Tracking and monitoring are described in a monitoring plan and are primarily accomplished through Safety Assurance functions.

E.2.1.3 Safety assurance Safety assurance ensures that the risk mitigations put in place by SRM continue to be effective in a dynamic operational environment. It provides confidence that an organization meets or exceeds safety requirements by applying system safety concepts and quality management processes. It involves:

1. Data/information acquisition
2. Data/information analysis
3. System assessment
4. Corrective action
5. Management reviews of SMS effectiveness, assessments of the need for changes, and implementation of changes to the SMS to achieve continuous improvement

E.2.1.4 Safety promotion Safety promotion is a combination of training and communication of safety information to support the implementation and operation of an SMS in an organization. It involves: and quality management processes. It involves:

1. competencies and training, and
2. communications and awareness including promoting a positive safety culture.

E.2.2 Safety Risk Management details

SRM is the second component of SMS. With respect to SRM, the objective is to provide information regarding hazards, safety risks, and safety risk controls to decision makers to support addressing safety risks in the NAS [4]. A thorough understanding of the safety risk components requires an examination of the factors that increase or decrease the likelihood of system events (e.g., errors or failures) that can result in unwanted outcomes (e.g., accidents or incidents).

The governing orders are dependent on the line of business and related context. For example, the FAA's Office of Aviation Safety (AVS) is responsible for using FAA Order 8040.4, Safety Risk Management Policy Requirements, if operation occurs at or below UAS Facility Map (UASFM) altitudes, wholly within UASFM altitudes, or at or below 400 feet above ground level (AGL) in Class G airspace.

The FAA's Air Traffic Organization (ATO) is responsible for determining the altitude values that populate the UASFM and applying SRM in accordance with the ATO SMS Manual [8] for any request for UAS operation that occurs above 400 feet AGL in Class G airspace, or within Class A/B/C/D/E airspace not wholly contained within UASFM altitudes (e.g., transitioning UAS), or when the provision of air traffic services during UAS operations are altered or required.

The FAA's Unmanned Aircraft Systems Safety Risk Management Policy Order 8040.6 [3] establishes the methods by which the FAA manages applicants' requests to operate UAS and how the Office of Aviation Safety (AVS) performs SRM in accordance with FAA Order 8040.4 for UAS requests for appropriate action to operate (e.g., waivers, exemptions, authorizations). It includes a template for documenting the steps of SRM. FAA Order 8040.6 supplements FAA Order 8040.4 by establishing a methodology for conducting SRM for UAS requests. It establishes a baseline with common hazards and mitigations. When the safety risk associated with a proposed operation is compared to a previous analysis and is not known, the request is considered a change to the NAS because the FAA has not granted the request previously. In this case the request must undergo SRM.

The following subsections provide more detail about each step of AVS's UAS SRM process.

E.2.2.1 Identify Safety Analyst or Team Members The first activity is **Identify Safety Analyst or Team Members**. The safety analyst or team reviews the application package and other available information to determine the expected level of safety risk.

E.2.2.2 System Analysis The second activity in the process is **System Analysis**. The applicant provides the technical and operational information needed for the safety analyst or team members to verify or perform SRM with three subactivities:

1. The applicant provides a Concept of Operations (CONOPS) description of operational scenarios/environment, Operational Risk Assessment (ORA), the safety case, which includes a description of each hazard and mitigation, operational procedures/manuals, and test documentation. The applicants' submission should contain:

   (a) hazards identified,
   (b) potential effects of the hazards (before mitigations),
   (c) mitigation rationale,
   (d) statement of how each mitigation is expected to reduce the severity, and likelihood of the hazard's effects,
   (e) test results to validate the mitigations (if available),
   (f) predicted residual risk (after mitigations),
   (g) applicant's determined level of risk and rationale.

2. The safety analyst or team reviews the CONOPS, ORA, and/or safety case, or other risk assessment tool to ensure completeness and accuracy. Additional hazards may be identified by SRM analysts or the team. The safety analyst or the team documents the system assessment with information pertaining to the aircraft, operator, and the environment,

3. The applicant may be asked for more information.

With respect to the safety case, FAA Order 8900.1 CHG 625 [9] identifies the contents of the safety case as follows:

1. Description of the environment
2. Criteria for categorizing hazards (e.g., severity and likelihood)
3. A detailed airworthiness description of the affected items associated with the proposed alternative method of compliance (AMOC), which includes, as a minimum:
   (a) For all aircraft operators:
      i. Capabilities of the aircraft;
      ii. Flight data (FDAT);
      iii. Accident data;
      iv. Emergency procedures;
      v. Pilot/crew roles and responsibilities.
   (b) For public aircraft operators only: a statement of airworthiness
   (c) For civil UAS operators only:
      i. Certification status of components and systems, or statement of airworthiness for public aircraft
      ii. Reliability data
      iii. Redundant systems
      iv. Failure modes and effects, including system response to loss of control link;
      v. An airworthiness determination.

The format of the Safety Case is as follows [9]:

1. Executive summary: This should include the list of the hazards with associated risk level (high/medium/low) and corresponding initial and predicted residual risk. It should include a high-level system description, a summary of how the safety case was developed, and what process/method was used to move through the risk assessment process.
2. Introduction: This should include the rationale for the initiative with the scope of the proposed AMOC
3. Current System/System Baseline: This should include the current system or existing procedures and the corresponding (operational) system states and delineate unique challenges associated with its unique situation.
4. Proposed Change: The descriptions of the proposed change/procedure should be explained including identifying which safety parameters are involved.
5. Safety Risk Management (SRM) Planning and Impacted Organization: This should describe the SRM participants, SRM panel, and milestones. It should assign tasks and responsibilities. For organizations that the change impacts, it should describe the method used for collaboration between those organizations during the identification, mitigation, tracking, and monitoring of hazards associated with the change.

6. Assumptions: Assumptions should be defined.
7. Phase 1 System Description: System/procedure, its operational environment, the people involved/affected by the change/procedure, and the equipment required to accommodate the proposal must be provided.
8. Phase 2 Identified Hazards: The SRM Panel identifies hazards as a collaborative effort. The tool(s) and technique(s) used to identify hazards should be specified and discussed. The identified hazards are documented as well as their corresponding causes, the corresponding system states considered, and the consequent potential outcome. System states with less severe outcomes should not be ignored.
9. Phase 3 Risk Analysis and Phase 4 Risks Assessed: The process used to analyze the risks associated with the identified hazards must be provided including specification of what type of data was used to determine the likelihood of risk occurrence (e.g., quantitative or qualitative), as well as the sources of the data. A risk matrix should provide an illustration of the predicted initial/current risk(s) associated with the identified hazards.
10. Phase 5 Treatment of Risks/Mitigation of Hazards: If the existing controls and mitigations do not acceptably mitigate the hazards, then additional recommended safety requirements should be identified. An explanation of how the recommended safety requirements are expected to reduce the initial/current risk to an acceptable predicted residual risk level should be included. Low-risk hazards may still warrant recommended safety requirements.
11. Tracking and Monitoring of Hazards: Once the proposal has been approved and implemented, tracking of hazards and verification of the effectiveness of mitigation controls throughout the life cycle of the system or change are required. Also, the methodology for this tracking and monitoring should be outlined.

FAA Order 8900.1 CHG 625 also highlights [9] that the applicant must submit contingency plans that address emergency recovery or flight termination of the aircraft (in the event of unrecoverable system failure). Emergency recovery or flight termination of the unmanned aircraft (UA) in the event of unrecoverable system failure is required and per operation the following are necessary:

1. Lost Link Points (LLP),
2. Divert/Contingency Points (DCP),
3. Flight Termination Points (FTP)

Risk mitigation plans are required to mitigate the risk of collision with other aircraft and the risk posed to persons and property on the ground for above. Consideration includes airspace constructs, and avoiding published airways, military training routes (MTR), Navigational Aids (NAVAID), and congested areas. The use of a chase aircraft is preferred when the UAS is operated outside of Restricted or Warning Areas.

E.2.2.3 Identify Hazards, and Causes The third activity in the process is **Identify Hazards, and Causes**. During this step, the SRM analyst or team must identify hazards,

causes, and outcomes. A hazard is a condition that could foreseeably cause or contribute to an aircraft accident. With respect to UAS, the worst possible outcomes are:

1. Collision between a UAS and a manned aircraft in the air
2. Collision between a UAS or its detached cargo and a person on the ground, or moving vehicle
3. Collision between a UAS or its detached cargo and critical infrastructure on the ground

Other possible hazards involve:

1. Unable to detect and avoid
2. Human error
3. Adverse operating conditions
4. Technical issue with UAS
5. Deterioration of external systems supporting the UAS operation

Appendix A of FAA Order 8040.6 includes some common hazards. See Figure 2 for example hazards, hazards definitions, causes if applicable, mitigations and outcomes related to UAS.

Appendix A (Risk Assessment Tools) of Advisory Circular AC107-2 [10] also discusses hazard identification. The AC states:

> Hazards in the sUAS and its operating environment must be identified, documented, and controlled. The analysis process used to define hazards needs to consider all components of the system, based on the equipment being used and the environment it is being operated in. The key question to ask during analysis of the sUAS and its operation is, "what if?" sUAS remote PICs are expected to exercise due diligence in identifying significant and reasonably foreseeable hazards related to their operations.

E.2.2.4 Analyze Safety Risk The fourth activity in the process is **Analyze Safety Risk**. During this step, the safety analyst or team must determine the initial risk levels expected with the proposed UAS operation. The initial risk (low, medium, high) is based upon the proposed operation including applicant controls and existing controls. The initial risk level is used to determine the level of AVS management that may accept risk. The safety analyst or team's rationale for how the determination was made is just as important as the severity and/or likelihood determination itself. The severity and likelihood definitions and risk matrix are used to better define the safety impact of the proposed UAS operation.

The risk is currently determined by severity and likelihood. Severity is the potential consequence or impact of a hazard in terms of degree of loss or harm.

Questions to consider include:

1. What are the credible outcomes (i.e., catastrophic, hazardous, major, minor, minimal)?
2. Why (e.g., data, line of thought, expertise, rationale for how the safety analyst or team arrived at the determination)?

3. How do existing controls and additional mitigations change the aircraft, airman/operator, or airspace/operating environment, such that the severity is reduced?

Likelihood is the estimated probability or frequency, in quantitative or qualitative terms, of the outcome(s) associated with a hazard. Questions to consider include:

1. What is the likelihood of the credible outcomes? (e.g., frequent, probable, remote, extremely remote, extremely improbable)
2. Why? (e.g., data, line of thought, expertise, rationale for how the safety analyst or team arrived at their determination)

Severity of Consequences			**Likelihood of Occurrence**		
Severity Level	Definition	Value	Likelihood Level	Definition	Value
Catastrophic	Equipment destroyed, multiple deaths.	5	Frequent	Likely to occur many times	5
Hazardous	Large reduction in safety margins, physical distress, or a workload such that crewmembers cannot be relied upon to perform their tasks accurately or completely. Serious injury or death. Major equipment damage.	4	Occasional	Likely to occur sometimes	4
Major	Significant reduction in safety margins, reduction in the ability of crewmembers to cope with adverse operating conditions as a result of an increase in workload, or as result of conditions impairing their efficiency. Serious incident. Injury to persons.	3	Remote	Unlikely, but possible to occur	3
Minor	Nuisance. Operating limitations. Use of emergency procedures. Minor incident.	2	Improbable	Very unlikely to occur	2
Negligible	Little consequence.	1	Extremely Improbable	Almost inconceivable that the event will occur	1

Figure 3: AC 107-2 Sample Severity and Likelihood Criteria [10]

3. How do mitigations change the aircraft, airman, airspace/operating environment, such that the likelihood is reduced?

Appendix A (Risk Assessment Tools) of Advisory Circular AC107-2 [10] discusses risk analysis and assessment. Note that the philosophy as stated in Appendix A is to "reduce risk to as low as practicable regardless of whether or not the assessment shows that it can be accepted as is". The AC states:

> The risk assessment should use a conventional breakdown of risk by its two components: likelihood of occurrence and severity.

Advisory Circular AC107-2 uses a different set of terms for severity and likelihood criteria in the example as compared to FAA Orders 8040.4B and 8040.6 (see Figure 3).

According to AC 107-2 [10], in the development of risk assessment criteria, sUAS remote PICs are expected to develop risk acceptance procedures, including acceptance criteria and designation of authority and responsibility for risk management decision making. The AC describes three notional risk acceptability levels: unacceptable, acceptable, and acceptable with mitigation. When combinations of severity and likelihood cause risk to fall into the unacceptable level, further work would be required to design an intervention to eliminate that associated hazard or to control the factors that lead to higher risk likelihood or severity. The combinations may suggest that the risk may be accepted without further action. The risk assessment can find that the risk may be accepted under defined conditions of mitigation. The risk matrix example in Appendix A of AC107-2 (see Figure 4) also shows that the terms differ from those in FAA Orders 8040.4B and 8040.6.

The Advisory Circular [10] makes the point that other tools can be used for operational risk assessments as long as "all potential hazards and risks are identified and appropriate ac-

Risk Likelihood		**Risk Severity**				
		Catastrophic A	Hazardous B	Major C	Minor D	Negligible E
Frequent	5	5A	5B	5C	5D	5E
Occasional	4	4A	4B	4C	4D	4E
Remote	3	3A	3B	3C	3D	3E
Improbable	2	2A	2B	2C	2D	2E
Extremely Improbable	1	1A	1B	1C	1D	1E

Note: The direction of higher/lower and more/less scales on a matrix is at the discretion of the remote PIC.

Figure 4: AC 107-2 Safety Risk Matrix Example [10]

tions are taken to reduce the risk to persons and property not associated with the operations" (see Section A.5.2 of [10]).

E.2.2.5 Validity of Mitigations The fifth activity in the process is **Validity of Mitigations**. Questions to consider include:

1. What evidence does the FAA have that the mitigations are effective (e.g., test data, third party verification)?
2. How are the mitigations dependent on each other? How much credit should be given for the mitigations?
3. Is there a single point failure?

The first question may be challenging to answer due to context as evidence may exist for specific instances that may not be exactly the same from one situation to the next. Knowing how to generalize across cases would be helpful. The second question highlights issues associated with interdependency. There may be information for individual mitigations but not about the coupling of them.

E.2.2.6 Assess Safety Risk The sixth activity in the process is **Assess Safety Risk**. One tool is the risk matrix that provides a visual depiction of the safety risk and enables prioritization in the control of the hazards. As mentioned, other methods can be used. Regardless, it is important to document the rationale of how the severity and likelihood was determined as well as the comparison of the level against the risk acceptance criteria [10].

E.2.2.7 Additional Safety Risk Controls and Residual Safety Risk The seventh activity in the process is **Additional Safety Risk Controls and Residual Safety Risk**. The safety analyst or team assesses the need for additional controls (i.e, conditions and limitations in exemptions and special provisions in waivers) to reduce the risk of the operation to an acceptable level.

E.2.2.8 Safety Performance Monitoring and Hazard Tracking The eighth activity in the process is **Safety Performance Monitoring and Hazard Tracking**. When the safety risk assessment is complete, tracking and monitoring are required in accordance with FAA Order 8040.4 [4] for medium and high residual risk levels.

E.2.2.9 Documenting Assessments and Decisions The ninth activity in the process is **Documenting Assessments and Decisions**. The safety analyst or team documents the safety risk assessment.

E.2.2.10 Residual Safety Risk Acceptance The tenth activity in the process is **Residual Safety Risk Acceptance**. Accepting risk is a management decision.

E.2.2.11 Safety Risk Documentation The eleventh activity in the process is **Safety Risk Documentation**. Once SRM is completed, the information must be documented in accordance with FAA Order 8040.4 [4].

E.2.2.12 Safety Performance Monitoring The twelfth activity in the process is **Safety Performance Monitoring**. Per the monitoring plan, safety performance monitoring is conducted to verify the risk assessment and the safety controls.

E.2.3 Relevance to Project A21 Task 3-1

SRM is the component of SMS most relevant to the probabilistic risk assessment (PRA) of A21 Task 3-1. The six-step SRM process summarized in §E.2.1.2 is the proper framework for assessing the risk of UAS integration into the NAS, although there appear to be significant challenges at several of these steps. The list below describes high-level anticipated challenges in successfully applying the six SRM steps described in §E.2.1.2.

1. System analysis challenge: identifying the "boundary" (what is included and what is not), the "components" (how is the system subdivided), and "parameters" (how to formally describe these components) of the system.

2. Identify hazards challenge: articulating the risks to safety, including for example from the physical environment, technology, and people.

3. Determine safety risk challenge: modeling how to numerically assess the probability distributions of the various adverse outcomes and quantifying their "cost"

4. Determine safety performance targets challenge: establishing target risk tolerances and expected cost thresholds consistent with FAA and other government standards pertaining to policy to ensure public safety

5. Control safety risk challenge: identifying, modeling, and quantifying the impact of all possible mitigations and scenario restrictions and assumptions that may reduce the associated risk and cost of the concept of operations

6. Track hazards and monitor challenge: establish feasible and scalable mechanisms for continuous operational and environmental monitoring and controls, so that accurate risk assessment may be performed on regular basis.

E.3 National Academies (NASEM) 2018 Report

Directed by the Congress and sponsored by the FAA, the National Academies of Sciences, Engineering and Medicine (NASEM) published a report titled "Assessing the Risks of Integrating Unmanned Aircraft Systems (UAS) into the National Airspace System"[1]. This report in part motivated Project A21 Task 3.

The NASEM 2018 [1] study focused on questions including:

- What are the benefits and limitations of these alternative risk assessment methods? How do these alternative methods compare to probabilistic risk analysis methods as well as severity and probability metrics traditionally used by the FAA for manned aircraft?

- What state-of-the-art assessment methods are currently in use by industry, academia, other agencies of the U.S. government, or other international civil aviation authorities that could benefit the FAA?
- What are the key advancements or goals for performance-based expanded UAS operations in the National Airspace System that can reasonably be achieved through the application of the recommended risk assessment methods in the short term (1-5 years), mid-term (5-10 years), and longer term (10-20 years)?
- What are the key challenges or barriers that must be overcome to implement the recommended risk assessment methods in order to attain these key goals?

The report concluded that the public is likely to accept risk for small UAS operations similar to the context of levels of *de minimis* risk for other levels of societal activities. It articulates that *de minimis* risk is useful in establishing safety standards for small UAS operations. Current FAA probabilistic risk analysis methodologies do not take societal safety-related benefits into account. The idea is that UAS operations can increase safety with respect to societal need (such as keeping human workers away from hazardous areas) and thus such societal benefit should be considered as part of analyses. Also the FAA can delegate to the UAS industry the responsibility for quantitative risk assessment activities for UAS operations or it could require the UAS industry to obtain insurance for UAS operations in lieu of having a separate risk analysis.

As a snapshot, the 2018 NASEM report [1] highlighted:

- Consider broader societal benefits in addition to risk when conducting safety assessment.
- Do not simply treat UAS risk in the same manner as the single probability assessed when evaluating risk of manned aircraft operations: consider risk as a multivariate measure.
- Performance requirements for UAS should be commensurate with risk and backed by performance-based standards.
- Consider new institutional mechanisms for conducting, or delegating, risk analysis.

The following provides relevant details from the report.

E.3.1 Guiding principles and assumptions

In the 2018 report [1], guiding principles and assumptions are laid out that are relevant to this work:

- Rules, regulations, and restrictions for UAS operations should be commensurate with the risk posed by the specific operation.
- Potential safety risks of UAS operations primarily include collisions with other aircraft and injury to people on the ground.
- UAS operations can reduce safety risks of operations by replacing activities that put people at risk.
- The regulatory framework and practices established by other countries can inform the process of integration of UAS into the NAS.

E.3.2 Pertinent findings

Several findings in the report are relevant to this work:

- Better measures for assessing UAS risk could be considered: Can we make UAS "as safe as other background risks that people experience daily"? And how can the concept of *de minimis* risk inform the process of assessing acceptable levels of risk posed by UAS? For example, the FAA does not ground airplanes because birds fly in the airspace, although birds can and do bring down aircraft.
- Drones have and will continue to be used to carry out missions of measurable economic and safety benefit to society (e.g., inspection of critical infrastructure that pose tangible danger to human inspectors, humanitarian delivery of medicines and other lifesaving cargo to rural areas or areas hard to reach by other transportation means, emergency response, search and rescue, and agricultural sensing, leading to reduction in use of pesticides, water, and other chemicals). These benefits to society may outweigh any risks added to the NAS by their operations.
- Systems with high levels of autonomy have the potential to improve the operational safety of UAS. However, existing verification, validation, and certification processes cannot ensure that highly autonomous systems that are adaptive or nondeterministic can satisfy safety standards for commercial aircraft. For this reason, highly autonomous systems are not currently allowed for commercial UAS flying within the NAS. Opportunities to increase the safety of UAS operations through increased autonomy are being missed due to a lack of accepted risk assessment methods.
- Given the substantial variety of types of UAS and related operations, risk characterization should include multivariate measures with co-variates such as the mission type, characteristics of the vehicle (e.g., weight) and other environment variables.
- Concerns related to the teaming of humans and machines can be reflected in the risk analysis methods applied to UAS. There are no broad-brush statements that can be reliably made about the role of the human and machine technologies within UAS. Instead, those design variables that determine system sensitivity to likely machine failures, and to foreseeable inadvertent slips and mistakes by humans, can be accounted for within each system. Further, this risk analysis, by examining how the human-machine team interacts, can better capture how the UAS will detect and resolve hazards that arise within the team. This risk analysis would also determine the extent to which humans and machine technologies are able to coordinate to resolve hazards arising in the broader operational environment outside the UAS.
- Accepting risk is far easier when the risk is well quantified by relevant empirical data. Uncertain risk does not equate to high risk, however. By accepting the uncertain risk associated with a new technology, with reasonable mitigations, one can obtain the data needed to better quantify that risk. As the uncertainty diminishes, one can remove or augment the mitigations as appropriate.
- Additional empirical data are needed to support probabilistic risk analyses for UAS collision modeling.

- Processes and plans for the collection, retention, analysis, and protection of UAS operational and risk related data are currently under development by the Unmanned Aircraft Safety Team (UAST).
- Integration of sensors and analytics present an opportunity for the FAA to learn and test new models for better data collection and analysis with the aim of improving overall safety.
- When computational models are being used, model prediction uncertainties are not always being calculated and no distinction is being made to distinguish between uncertainties due to lack of knowledge and those due to natural variability of the data.
- The current FAA Order 8040 [4] approach to risk management is based on fundamentally qualitative and subjective risk analysis. The Specific Operations Risk Assessment (SORA) approach of the Joint Authorities for Rulemaking of Unmanned Systems (JARUS) is conceptually the same [11]. These subjective approaches require a depth and breadth of subject matter expertise for the approval process that is not universally available. The qualitative nature of the current approach might lead to results that fail to be repeatable, predictable, and transparent. Evolution to an approach more reliant on applicant expertise and investment in risk analysis, modeling, and engineering assessment, as is practiced in many other areas of federal regulation, might better achieve a quantitative PRA basis for decisions. The FAA's UAS risk assessment process documentation, including Order 8040.4B and Part 107.200, is inconsistent, lacks specific numeric guidance, and does not provide sufficient guidance for proponents. Some organizations outside of the FAA such as MITRE, NASA and Transport Canada have moved forward to help to fill these gaps.

E.3.3 Relevance to Project A21 Task 3-1

This subsection highlights some recommendations that demonstrate the need to consider quantitative risk assessment and other strategies.

1. Where operational data are insufficient to credibly estimate likelihood and severity components of risk, the FAA should use a comparative risk analysis approach to compare proposed UAS operations to comparable existing or *de minimis* levels of risk. The FAA should research and publish applicable quantitative levels of acceptable risk in comparison to other societal activities that pose *de minimis* risk to people. Risk level and risk mitigation strategies should consider not only aircraft collisions but also third-party risks (e.g., to people on the ground).
2. The FAA should evolve to a probabilistic risk analysis (PRA) process based on acceptable safety risk. The FAA should consider relying on the applicant to provide a PRA demonstrating the achieved level of safety, as is common in other regulatory sectors.
    (a) The FAA should screen applicant PRAs by comparison to existing or *de minimis* levels of risk. The FAA needs to research applicable quantitative levels of acceptable risk in comparison to other societal activities in establishing a level of *de minimis* risk for aviation.

(b) These acceptable levels of risk need to include risk to people on the ground and risk of collisions with a manned aircraft, particularly with regard to collision with a large commercial transport.

(c) In evaluating applicant-generated PRA, the FAA should value the importance of risk mitigation opportunities and their potential for simplifying the analysis of risk.

(d) In situations where the risk is low enough, the FAA should encourage applicants to obtain insurance for UAS operations in lieu of having a separate risk analysis.

3. The FAA should identify classes of operations where the level of additional risk is expected to be so low that it is appropriate to base approval of those operations on requiring insurance in lieu of having a separate risk analysis.
4. In coordination with other domestic and international agencies, the FAA should pursue a planned research program in PRA, including the aspect of comparative risk, so that FAA personnel can interpret or apply PRA for proposed technology innovations.

E.4 Probabilistic Structural Risk Assessment and Risk Management for Small Airplanes

Probabilistic fatigue evaluation of general aviation aircraft is vital to provide important insight into the severity or criticality of a potential structural issue. In FAA report AA-AR-11-14-2017 entitled "Probabilistic Structural Risk Assessment and Risk Management for Small Airplanes" [12], a probabilistic risk assessment methodology is developed for risk assessment and risk management of structural-fatigue-failure issues. Because of significant airplane-to-airplane and flight-to-flight variations, probability density functions of the critical variables were investigated and developed. The methodology developed is incorporated into the SMART (Small Aircraft Risk Technology) software, which has been developed under FAA support. Moreover, the methodology and software were demonstrated on two different structural risk-assessment examples.

E.5 Operational Risk Assessment Prototype

MITRE is a federally funded research and development center (FFRDC) supporting scientific research and analysis, development and acquisition, and systems engineering and integration. MITRE also has an independent research program that explores new and expanded uses of technologies to solve sponsors' problems.

Ellen Bass, Phil Smith, and Steven Weber jointly interviewed Jeff Breunig, Michelle Duquette, Norm Fenlason, Mike Girbert, Michael Noe, Tyler Smith, and Shereef Sayed of MITRE about the Operational Risk Assessment Prototype (ORAP) and related work.

The MITRE group described that AFS had discussed the development of a tool to support processing sUAS waivers (0-400 ft). MITRE started reviewing the JARUS SORA documentation but it is very qualitative in nature. Thus MITRE has embarked on developing the Operational Risk Assessment Prototype (ORAP). The goal of ORAP is to provide a quantitative risk assessment model that the FAA can use to streamline the waiver approval process, to support regulatory development, and to facilitate safety risk analysis. The current focus

is on ground collision but the plan is to focus on air collision in the future. In MITRE's work, they assume that the operator is trained, proficient, law-abiding, and aware of device limitations.

The risk assessment model accounts for different types of sUAS vehicles and operational missions. It leverages MITRE's sUAS Airworthiness Assessment Tool (sAAT) which quantifies the risk of fatality to third-party people on the ground from sUAS operations by combining characteristics of the intended vehicle type with the planned operations [13].

The MITRE approach uses simulation in order to develop sUAS risk models. The likelihood of fatal injuries to third parties is calculated as:

$$L_{\text{OOC}} \times L_{\text{Struck|OOC}} \times L_{\text{Fatal|Struck}} = L_{\text{Fatal}}, \tag{35}$$

where

L_{OOC}: Likelihood of having sUAS operation out-of-control

$L_{\text{Struck|OOC}}$: Likelihood of person or aircraft struck by the out-of-control sUAS

$L_{\text{Fatal|Struck}}$: Likelihood that, if struck, the result is fatal

L_{Fatal}: Likelihood of fatal injuries to 3rd parties.

Data are required to parameterize the model. The likelihood of having sUAS operation out-of-control is a function of vehicle reliability, component reliability, operator error, mission duration and visibility. The likelihood of person or aircraft struck by the UAS is a function of aircraft density, vehicle trajectory, population density type, pedestrian behavior, and vehicle weight and size. The likelihood that if struck, the result is fatal, is a function of velocity, height, mass and frangibility.

As of the interview, MITRE had modeled nine missions profiles. Examples include sparse areas such as for an agricultural application, contained areas such as real estate photography, linear area such as waterfront advertising, public events such as a parade, network operations such as small cargo delivery, and a dynamic area such as a police chase. Mission characteristics address factors such as density of people/pedestrians, mission area size, and the number of launches and landings (e.g., for package delivery).

MITRE has been focusing on different operational characteristics: beyond visual line of sight (BVLOS), daytime/night time, flight duration, and operating altitude. Another set of parameters involve vehicle characteristics such as size, weight, type (rotorcraft, fixed wing), endurance, payload, reliability (mean time between failure (MTBF)) and maximum speed. They also address mitigations. The model accounts for vehicle failures and models three types of falls (spiral, glide, and drop).

Vehicle reliability profile data are critical for risk assessment but may be difficult to estimate from data or model. MTBF may best be considered as the responsibility of the manufacturer.

Time of day makes a difference with respect to whether people are home and whether when they are home, if they are outside. Sheltering models can be helpful to address sheltering factors, the fraction of time that people are outside. MITRE therefore differentiates

people density, the number of people exposed to the sUAS operation as opposed to *population density* based on where people sleep.

Quantitative risk modeling can be complex and many elements are difficult to appropriately incorporate such as weather conditions.

Once risk is established, the idea is how to measure risk reduction through mitigating those risks. It is difficult to quantify hazard mitigations including reliability (e.g. parachutes, detect and avoid (DAA), and geofencing).

E.5.1 Data sets and analyses to consider

The data mentioned above would need to be available to parameterize the models. Datasets that might be helpful for this work include:

1. Population density from the U.S. census and the related tools for using census data
2. Vehicles by weight categories in the marketplace (AUVSI maintains a database of commercially available sUAS): dimension, performance
3. FAA certificate of authorization (backend developed by MITRE)

With respect to population density, Oak Ridge National Laboratory's LandScan™ has global population density estimates at the one square km resolution. The US census data are more up to date and precise. For example, a particular operator may avoid populated sides of highways as an example and census data can support such analyses.

Open-source building datasets could be very useful to distinguish between residential and commercial buildings. Zoning laws are different by county and it might be useful to explore Microsoft building extrusions.

Research has focused on the use of satellite data for estimating building heights which may be useful for estimating the number of people in a building (see for example [14]).

Social media data are becoming a ubiquitous data source. They have been used in the airline industry to determine which flights to cancel or delay. Sentiment analysis [15] is the process of computationally identifying and categorizing opinions expressed in a piece of text. Such data may be useful near schools and other areas to address where people are and their attitudes about events such as UAS flight.

While having each individual data source would be helpful, there can be interactions that are complicated to address. For example, parachutes reduce impact energy but may also increase the area where a vehicle lands. With respect to mitigations, parachute drop tests are needed.

E.6 Joint Authorities for Rulemaking on Unmanned Systems Specific Operation Risk Assessment

The purpose of Joint Authorities for Rulemaking on Unmanned Systems (JARUS) is to recommend technical, safety and operational requirements for the safe operation of the UAS. JARUS's guidance material aims to facilitate writing requirements and to avoid duplicate efforts across the members. Relevant references include [11, 16, 17, 18, 19, 20, 21].

JARUS's Working Group (WG 6) focuses on SRM. The Specific Operation Risk Assessment (SORA) is the JARUS WG-6 consensus vision on how to safely create, evaluate and conduct UAS operations [11, 20]. The SORA proposes a methodology for risk assessment primarily required to support the application for an authorization to operate an UAS within the specification category. The 2017 SORA document [11] focuses on the assessment of ground and air risk and mentions that a risk assessment of critical infrastructure should also be performed.

The SORA introduces a Holistic Risk Model (HRM) to support the assessment of risks involved in the operation of an UAS. The HRM provides a generic framework to identify the hazards, threats and the relevant harm and threat barriers applicable to any UAS operation through five steps:

1. Harm identification is the identification of the harms for which the risk needs to be assessed.

2. Hazard identification is the identification of the hazards related to the UAS operation that may lead to the retained harm. Its three categories of harm (fatal injuries to third parties on the ground, fatal injuries to third parties in the air (catastrophic mid-air collision with manned aircraft), and damage to critical infrastructure are similar to the worst cases mentioned in the **Identify Hazards, and Causes** step of [3].

3. Identification of generic threats is the identification of the issues that can cause the hazard to occur if not kept under control. Its five generic categories of threats (technical issue with the UAS, human error, aircraft on collision course, adverse operating conditions, and deterioration of external systems supporting the UAS operation) are similar to the other possible hazards of the **Identify Hazards, and Causes** step of [3].

4. Harm barrier identification is the identification of the mitigations applicable to a specific harm for a defined hazard. Harm barriers affect the likelihood that, once it occurs, the hazard can cause the harm and/or the severity of the consequences of the hazard with respect to the harm. This is similar to part of the **Analyze Safety Risk** and **Validity of Mitigations** steps of [3].

5. Threat barrier identification is the identification of the mitigations applicable to a specific threat for a defined hazard. Threat barriers affect the likelihood that a threat can cause the hazard. This is also similar to part of the **Analyze Safety Risk** and **Validity of Mitigations** steps of [3].

As with the approach in [3], the SORA approach to risk assessment uses the combination of the frequency (probability) of an occurrence and its associated level of severity. With respect to parameters, the SORA mentions three:

1. fatal injuries to third parties on ground,

2. fatal injuries to third parties in the air, and

3. damage to critical infrastructure.

The 2017 version of the document has no recommended values but rather provides "a conceptual reference for the introduction of qualitative levels for the specific category" ([11] p. 22).

The document mentions several caveats. It highlights that quantitative risks expressed in the form of probability and severity are not consistent with qualitative approaches made by each individual in perception of risk. It also mentions evaluating the uncertainties of the risk model in order to decide how detailed of an analysis to conduct. It raises the point that quantitative assessment of risk is subject to scenario completeness uncertainties and modeling uncertainties in addition to parameter value uncertainties. Thus the document highlights that "the likelihood estimation should be preferably of qualitative nature" ([11] p. 20).

The SORA document presents a fourteen step process for risk assessment. As mentioned in [1] it is a subjective approach requiring extensive subject matter expertise and may fail to be repeatable, predictable, and transparent.

[22] describes that SORA provides a qualitative level of confidence that a given UAS operation remains safely controlled, identifyies a number of inconsistencies in risk identification and assessment, and discusses plausible strategies to close the associated gaps. The approach encoded the semantics of risk modification using Bayesian networks. Bayesian networks support a flexible probabilistic framework that affords efficient algorithms for reasoning under uncertainty, considering discrete and continuous random variables. Another key advantage is the specification of prior probabilities for the risk model parameters when there is insufficient information, and to update the priors, e.g., using operational data.

E.7 Relevant work from Canada: Transport Canada

Remotely Piloted Aircraft System (RPAS Traffic Management) (similar to UTM) Action Team is a joint government/industry effort, co-chaired by Transport Canada and NAV-Canada, defining the way-ahead for RTM/UTM in Canada. They have developed a national roadmap, and the framework for a trials program, which has led to the need for policies and mechanisms to share data, conduct analyses, and share results. These trials are more broadly within the context of proving BVLOS operations and informing the regulatory process.

Draft Advisory Circular [23] 903-001 was issued in July 2019. It provides information and guidance to manufacturers and operators intending to develop or operate a RPAS for operations in accordance with the requirements of Part IX, Subpart 3 of the Canadian Aviation Regulations (CARs). The draft describes an operational risk assessment (ORA) method based on the JARUS SORA process [11]. AECs 7 and 8 do not apply to Canadian airspace and there are other minor differences.

The draft AC includes some sources of uncertainty that can be useful for sensitivity analysis. It includes the concept of an operational volume that includes flight geography, the contingency volume, and a 1-to-1 ground risk buffer. Flight geography is the area or path where the RPA is intended to be flown for the specific operation with positioning errors. The contributors to positioning error include the following:

1. Path definition error refers to the difference between the intended path through the environment (laterally and vertically) and the defined path (i.e., what the pilot or

autopilot is actually trying to follow). Path definition errors may result from:

(a) Map projection differences

(b) Earth reference model differences

(c) Altitude considerations (e.g., if the operation is planned to occur in an area with rolling terrain, the 3D path either needs to adjust altitude to follow the terrain, or set a consistent altitude such that the aircraft remains below 400 ft AGL at the lowest terrain elevation that will be overflown)

2. Flight technical error refers to the accuracy with which the reported aircraft position and altitude are controlled relative to the defined path. This error is dependent on:

   (a) The means of control and its associated performance (e.g., manual control vs. autopilot).

   (b) The means of determining the difference between the reported position and the defined path. For a pilot, the ability to follow a 3D path is highly dependent on the way the path and path deviation data are displayed

3. Navigation solution (lateral) and altimetry system (vertical) accuracy must be considered to determine the potential difference between the reported position and the actual position of the aircraft.

4. Any latencies in the C2 link(s), navigation solution computation, or altimetry system may add to the total system error depending on the system architecture.

The contingency volume is intended to provide a buffer area beyond the flight geography to allow time and space for contingency procedures to be enacted. Contingency procedures are put in place to support recovery from undesirable states that, if not addressed, could lead to unsafe situations. If an automatic Return-To-Home (RTH) function is used as part of any contingency procedures (e.g. for loss of C2 link), the design of this function should be considered in the definition of the contingency volume. If automatic landing at present position or a specified alternate location is included as part of any contingency procedures, the area surrounding the landing location should be addressed as part of the contingency volume if it may be outside of the flight geography. If a manual control takeover by the pilot in command (PIC) (or a secondary pilot) is included as a contingency procedure to address departures from the planned flight path/area, the contingency volume needs to provide sufficient time and space to allow the pilot to recognize the deviation from the planned path, execute the manual control takeover procedure, and maneuver the aircraft back to the planned flight path/area.

The ground risk buffer is added based on the expectation that some mechanism of flight termination may be included as part of the emergency procedure if the aircraft exceeds the contingency volume. Thus, some ground area outside of the contingency volume needs to be considered as part of the ground risk determination. The '1-to-1' concept means that the buffer is defined, at minimum, as a horizontal distance equal to the aircraft's planned maximum altitude above ground level (AGL).

The JARUS SORA process [11] includes requirements for an assessment of adjacent areas and airspace to determine what hazards may exist in the event of a loss of control of the operation resulting in a fly away. The document leaves it up to the judgment of the operator and the certifying authority to determine what constitutes adjacent areas and adjacent airspace. A conservative approach to identifying adjacent areas/airspace would be to consider the maximum performance of the RPA and identify any locations attainable by the RPA under worst-case flyaway conditions. The definition of adjacent areas and airspace involves determining the time required to perform the emergency procedures related to an aircraft flyaway and using this time to establish practical limits on what locations the aircraft could reach before risk mitigations can be applied. The intent is to provide a reasonable safety buffer around the operational volume that gives the operator time to implement emergency procedures before the RPA reaches higher risk locations.

Unmanned Systems Canada (USC) is the national industry association representing entrepreneurs, businesses, students academia, industry, and government organizations working in the aerial, ground and marine remotely-piloted and unmanned vehicle systems sector. To aid in approving Transport Canada for BVLOS operations, Periculum Labs of Ottawa engaged with USC on a quantitative risk assessment platform. The model was already developed (Sandia Labs/NASA) and was repurposed specifically to gain approvals. The model has also been promoted as a means for C-UAS requirements to be assessed for risk reduction (cost/benefit). This solution may inform Task 3.

On March 5 2020, Ellen Bass, Steven Weber, and Phil Smith met with Mark Aruja, Chair Emeritus of USC, and Stephen Eisenhawer, the Chief Scientist at Periculum Labs Inc. Stephen presented Periculum Labs' "Scenario-based Risk Assessment for Beyond Visual Line of Sight Operations with Unmanned Aerial Systems." A particular mission can be performed in a variety of ways that are referred to as mission scenarios. For each mission scenario, there are several off-normal sequences that can generate a loss. In Periculum Labs' approach, the total risk for a mission scenario is obtained by an aggregation across all of the off-normal sequences in which a consequence of concern is identified. These off-normal sequences are referred to as risk scenarios.

When probabilistic risk analysis is employed, the likelihood of this consequence for a risk scenario is expressed as a probability. Total risk is dominated in many systems by one or a few risk scenarios. Therefore, it is important that a risk assessment identifies the main risk scenarios and that the risk metric is computed in a manner that is defensible and traceable.

An explicit requirement for using a risk-based approach to the regulation of commercial UAS operations is the concept of risk acceptance. Risk acceptance is understood to require the establishment of a threshold level of risk. The threshold risk is based on reference to one or multiple comparable risks. A systematic approach to setting a value for the threshold risk includes setting qualitative safety goals, converting these goals to quantitative safety objectives, and then deriving one or more operational safety limits that will be collectively sufficient to achieve the safety objective.

E.8 In-Time System-Wide Safety Assurance

NASA researchers are conducting research in enhanced safety methods. In NASA Langley's Research Directorate, the Safety-Critical Avionics Systems Branch conducts research into

new methodologies and tools for designing, verifying, validating, and assuring high confidence software-intensive systems to improve safety, reliability, and capacity in mission- or life-critical aero-space systems. In an exemplar paper [24] the authors consider the Functional Hazard Assessment (FHA) and Systems Theoretic Process Analysis (STPA) techniques for hazard assessment and evaluate whether they can be used in a complementary fashion for regulatory approval purposes. They perform an FHA and an STPA on an electric vertical takeoff and landing (eVTOL) vehicle undergoing an urban air mobility (UAM) passenger carrying reference scenario and present excerpts of this analysis. However, this document focuses more specifically on research that supports the SMS approach.

The 2018 NASEM report [25] focuses on "in-time" aviation safety management. The National Aeronautics and Space Administration (NASA) has been developing new concepts and technologies as part of "In-Time System-Wide Safety Assurance (ISSA)". The NASA technical report TM-2020-220440 [26] delineates a framework for applying ISSA capabilities in the context of risk monitoring, assessment, and mitigation for sUAS, specifically within the context of low-altitude flights near and in urban areas.

Prior work by NASA has identified safety-critical risks for such flights, including:

- flight outside of approved airspace
- unsafe proximity to air traffic
- people on the ground, or property
- critical system failures (including loss of link, loss or degraded positioning system performance, loss of power, and engine failure)
- loss-of-control due to envelope excursion or flight control system failure
- severe weather encounters (including wind gusts)
- security-related risks (cyber or physical)
- human factors-related risks

NASA Technical Report 220440-2020 [26] covers the architecture of the proposed risk management system, which is cast within the ISSA and In-time Safety Assurance Management System (IASMS) system architectures. A list of 16 "guiding principles and overarching traits" is provided, and these principles are consistent with the architecture of existing information sharing networks in use by the FAA, including UAS Traffic Management (UTM) concept, the Aviation Safety Information Analysis and Sharing (ASIAS) platform, and the System-Wide Information Management (SWIM) service. Information exchange architecture and messaging protocol primitives are discussed, and the onboard functions available through the CoreFlight system are outlined.

Section 3 of [26] discusses the information requirements of the proposed system. Information is divided into sixteen (16) classes, including:

1. Aircraft State
2. Geo-spatial Constraints
3. Weather (MET)
4. Population Density
5. Link Performance

6. Nav Performance
7. Power Health
8. Engine/Motor Health
9. Aerodynamic Model
10. Airspace Conformance
11. Air Traffic
12. ANSP Infrastructure
13. Human Performance
14. Safety Reports
15. Flight Plan
16. Configuration Settings

These sixteen information sources are fed into ten distinct models:

1. Aircraft aerodynamic model
2. Geo-spatial feature model (including terrain and obstacles)
3. Weather forecast model
4. Population density model
5. Link performance model
6. GNC system performance model (incl. Nav Quality model)
7. Battery performance model
8. Engine performance model
9. Power estimation model
10. Mean time between failure (MTBF) models (for critical components)

Data quality requirements for the sixteen data sources, and the ten models in which they are fed, are specified in RTCA DO-200B, "Standards for Processing Aeronautical Data" [27].

Section 4 of [26] covers uncertainty management (UM), where uncertainty is identified as having two key components: aleatoric (statistical) and epistemic (systematic). Uncertainty quantification (UQ) is proposed to be addressed by the polynomial chaos expansion (PCE) method, an alternative to Monte-Carlo.

Section 5 of [26] integrates the framework with existing FAA information *exchange models and protocols*, including:

- Aeronautical Information Exchange Model (AIXM),
- Weather Information Exchange Model (WIXM), and
- Flight Information Exchange Model (FIXM).

Section 6 of [26] describes the supporting tests run to validate the framework, including both simulation-based tests (at NASA Ames Research Center) and flight-based tests (at NASA Langley Research Center using the City Environment for Range Testing of Autonomous Integrated Navigation (CERTAIN) platform). Section 7 of [26] briefly covers related industry developments and Section 8 gives a summary and plan for updates. The report closes with appendices detailing the analyses completed.

E.8.1 Summary of the discussion with the authors

Ellen Bass and Steven Weber spoke with several of the authors of [26, 28, 29, 30] on May 27, 2020, including Steven Young, Ersin Ancel, and Natasha Neogi. The discussion providing context and motivation for [26], and additional information pertaining to ongoing and anticipated efforts. The authors shared that the report is a milestone in a larger multi-year project. The report addresses part of NASA's strategic plan, focused on in-time safety assurance, as opposed to relying exclusively on traditional design-based verification and validation. The authors also shared that the 2018 NASEM report [25] served as a catalyst for their investigations.

Assessing third party casualty risk (e.g., civilians in urban spaces injured by sUAS malfunction) is key motivation behind the effort, with a primary goal of the framework to enable an interested party to file a flight plan, receive risk values for different types of malfunctions, and then apply appropriate mitigations to the flight plan to reduce the risks to acceptably low tolerances.

The availability, suitability, and reliability of the data to make the required risk assessments was discussed, with a focus on population density. The authors described a data source relying upon cell phone signals that offers "live" population counts at the spatial granularity of 10 meters by 10 meters, updated hourly. The authors described that the intention of the framework is to enable the models to provide coarse-grained first-order approximations to relevant flight risks, so as to improve pre-flight risk mitigation, with the understanding that an in-flight system would then be able to better apply mitigations to deal with unexpected deviations from the pre-flight model.

The role of the proposed polynomial chaos expansion (PCE) and its merits relative to the more traditional Monte Carlo paradigm were discussed. These merits include the capability of developing table lookups for risk assessment, suitable for real-time access.

The failure, information, and model taxonomies were discussed, and the authors emphasized that existing ASIAS and SWIM networks share a large amount of data, including most of the information sources anticipated to be useful for the sUAS risk models.

The authors shared that two motivations behind the research were *i*) to ask, conceptually, what data sources would be useful in real-time risk assessment and how would they be used, and *ii*) is it in fact feasible to get and share that data. The sixteen data sources listed in the report are the sources deemed useful, the ten models listed in the report notionally express how the data would be used, and the section on information sharing protocols makes clear that in fact much of these data are already being shared using the ASIAS and SWIM protocols.

The authors commented upon the role of mitigations in risk assessment. For example, a parachute on a sUAS changes the trajectory as well as the impact force. They commented on the distinctions between traditional FAA risk assessment for large aircraft and whether it applies wholesale to risk assessment for sUAS as the impacts are so different.

E.8.2 Relevance to Project A21 Task 3-1

The NASA ISSA framework addresses pre-flight, in-flight, and post-flight risk assessment and mitigation and thus is more comprehensive in its approach to modeling, assessing, and

mitigating risk than is required for a pre-flight waiver. In addition the real-time aspect of NASA's ISSA is out of scope for Project A21. However, the report [26] provides insights into failure modes, information sources, environmental models, information sharing architecture and protocols, and risk quantification and management. Several types of model reductions and simplifications are possible such as:

- Focus on pre-flight, as opposed to pre-, during, and post-flight risk assessment
- Focus on information available pre-flight, as opposed to information that would be available in flight through information exchange systems such as ASIAS and SWIM
- Focus on *de minimus* risk assessment, i.e., seek to answer whether various flight risks are above or below a threshold, as opposed to accurate estimation of the flight risks themselves.

Together, it is anticipated that these reductions in scope of effort will enable significant simplifications in the model complexity and significant reductions in the required information/inputs to those models.

Simplification aside, the NASA ISSA framework may benefit development of system state and operating environment models. The few concrete models developed in the appendices of the report demonstrate there is extensive work required to develop, test, and integrate these models for the purpose of holistic risk assessment.

E.9 Relevant findings from the UAS Insurance Industry

Some in the UAS industry are looking to insurance industry to be the driving force and ultimate arbiter of the various risk management initiatives currently in development. To meet demand, insurers must set parameters, create standard and quantifiable risk factors, and determine how to allocate and mitigate risks. [31]. Coverage issues surround the unmanned vehicle, its component parts and associated equipment, first party coverage, and liability coverage. For manufacturers of units and component parts, issues arise related to liability for alleged defective design, manufacturing, or failure to warn, as well as strict liability, negligence and breach of warranty. Cyber and cargo coverage may be needed for different types applications.

Common questions that come up regarding UAV insurance include:

1. Do I need insurance for my drone?
2. How much does UAS insurance cost?
3. Do I need to be approved by the FAA to obtain UAS insurance?
4. What would commercial UAV insurance cover?

While commercial airline and general aviation accidents are hard to predict using even the most sophisticated modeling tools, insurers at least have a good sense of the premium they need to charge to cover the likely loss activity in any given year. However, with commercial UASs, there are less data upon which to make similar predictions. Most models of UAVs have not existed long enough for insurers to acquire an understanding of the particular

features that could influence the likelihood of an accident or system failure. Another hurdle to address is the wide range of experience that operators have when they start in the UAS business. Insurance is a "for profit" industry where the byproduct of profitability is safety. Insurance is profitable for one of two reasons; loss ratios are below 70% (underwriting profit) or stock markets and other investment vehicles are returning profits in excess of losses through the investment of unearned premium (investment profit). Without profitability, insurance will either exit the business or adjust underwriting and raising premiums. If there is an underwriting profit, then that is generally the direct result of safe operations or a booming economy.

One primary risk management tool for UAVs that insurers will be looking at is training. Without effective training in the hazards involved, UAV operators will never be able to operate at optimal safely. Training for all levels of UAS operation is becoming widely available, from an online course to custom training for team of operators. Some insurance providers already require operators to undertake some type of formal training. Expect training to ultimately become mandatory by insurers.

Another issue related to safety training is the quality of the operating manual and after-sales support. Currently, it varies enormously. Important information, such as the relative battery deterioration in cold weather, is missing from many instruction manuals.

Safety documents such as pre-flight checklists, logbooks and a Standard Operating Procedure (SOP) are established components of manned aviation at all levels. Important technical issues include:

1. Interaction between the operator and observer
2. Weather and environmental issues
3. Maintaining a safe distance from the UAS
4. Ensuring airworthiness of the aircraft
5. Pre-flight and post-flight checks

The responsibility will fall on the operator to inspect prior to each flight to ensure the vehicle is in a suitable condition for safe operation.

E.9.1 Discussion with Transport Risk Management, Inc.

Terry Miller of Transport Risk Management described in an interview that using the company's underwriting criteria and premium levels, the company is profitable and safe with a 9% to 12% loss ratio. While the underwriting process and algorithms are confidential and proprietary, the company has developed an underwriting process and insurance product that is economically affordable to consumers and profitable to insurers. Mr. Miller suggested that the FAA might consider choosing underwriters who have a loss ratio (below 40%) and requiring that operators be insured through them. If they are declined or deemed uninsurable by those underwriters, then that would be an excellent indication that the operator is viewed as unprofitable to insurers which translates to being unsafe.

The company's insurance application sheds some light on the factors under consideration. Data required for an application include:

1. Is applicant individual, partnership, corporation or other?
2. Will the aircraft be operated under an exemption (and what type)?
3. Has the applicant been involved in accidents, incidents or claims in the last five years?
4. Has insurance ever been canceled or not renewed?
5. Will the aircraft be operated by a third party?
6. What is the aircraft year, make and model, wingspan, length, maximum weight, and payload weight?
7. What flight controller is employed?
8. What is the base station and transmitter year, make and model, and related specifications?
9. What is the payload year, make and model, and specifications (type and use): sensor, downlink and gimbal?
10. How many annual hours will each UAV be operated?
11. What is the maximum endurance (flight duration)?
12. What is the UAV maximum speed?
13. What are the primary means of control: line of sight or computer guided?
14. Does the UAS have autoland or return to home?
15. Is the powerplant gas or electric or other?
16. Can the UAS deploy/drop payload or other items?
17. What is the anticipated mission: sales, demo, aerial photo, public safety, other? Describe all anticipated use.
18. What experience does each operator have in hours flying types of equipment?
19. How is aircraft maintenance provided?
20. Where will the UAS be operated?
21. What type of ground school has each operator had?
22. What type of build log is maintained?
23. What type of flight log is maintained? Does the aircraft have an iOSD? Does the aircraft have a remotely recordable flight log?
24. Will the UAS be operated over water? How often?

25. Will the UAS be operated indoors? How often?
26. Will the UAS be rented to a third party?
27. What formal safety program is in place?
28. What procedures are in place?

E.10 Relevant findings from the PRA literature

This section provides a brief review of papers not already discussed herein from the technical literature deemed relevant to the framework to be developed for Project A21 Task 3-1.

E.10.1 Risk modeling techniques

E.10.1.1 Bayesian techniques Reece Clothier, Rodney Walker and colleagues [32, 33] have focused on analyzing safety risks associated with the operation of unmanned aircraft in the civil airspace system and over inhabited areas. They note the challenges associated with quantifying the specification of high-level safety criteria, the identification, analysis and evaluation of the risks, and the effectiveness of available technical and operational mitigation strategies. With respect to modeling risk for hazards on the ground, they consider hazardous events given that the risk (to human life or property).

$$Pr(HE) = Pr(HE \mid UFCE \times Pr(UFCE) \tag{36}$$

Where:

Pr(HE) = Probability of a Hazardous Event (HE)

Pr(HE |UFCE) = Probability of a HE given an Unrecoverable Flight-Critical Event (UFCE). This is the conditional probability that an undesired descent constitutes a hazardous event.

Pr(UFCE) = Probability of a UFCE occurs at a particular point in space and time. This is indicative of the undesired descent rate.

For UAS, the conditional probability is a function of the number of people and property exposed on the ground which is specific to the operating environment and not just the UAS system.

For UAS operations over inhabited areas, Equation 36 can be re-written as:

$$Pr(HE) = Pr(C \mid I) \times Pr(I \mid UFCE) \times Pr(UFCE) \tag{37}$$

Where:

Pr(C |I) = Conditional probability of a Casualty (C) given an Impact in an inhabited area (I), that is the conditional probability that certain magnitudes of consequence are observed given a mishap for a particular impact location and time

Pr(I |UFCE) = Conditional probability of an Impact in an inhabited area (I) given an Unrecoverable Flight-Critical Event (UFCE).

Pr(UFCE), is the characterization of the likelihood that at a particular point in time and space and under certain conditions (operational and environmental) the UAS experiences an unrecoverable flight critical event.

Modeling the probability of a flight critical failure occurring at a given point in space and time is a complex task. More difficult to model will be those failures which are related to human factors, failures due to latent errors (particularly in software or mission planning), and those due to procedural (e.g. maintenance and operational) or environmental factors (e.g. hazardous weather conditions).

Determining the likelihood that an impact occurs in an inhabited area is also complex as it depends on factors such as kinematics, initial conditions, performance of the platform, environmental factors, level of operator and autonomous control, whether mitigation strategies are employed, and terrain.

Finally there is a need to determine the likelihood of observing a certain magnitudes of consequences as a result of a mishap at a given point in space and time. This is primarily a function of the impact mode, distribution of the value at risk (e.g. people) and the ability of the airborne platform to impart damage to the object at risk (e.g. kinetic energy).

Challenges include uncertainty in the model. Aleatory uncertainty stems from the lack of available data. Epistemic uncertainty arises from a lack of knowledge in the event or system being modeled. The latter can only be reduced with operational experience and presents the greatest challenge to the risk modeling task.

E.10.1.2 Event tree methods In [34] the authors present a framework that can link UAS reliability and physical characteristics to the effects on the bystander population. The study proposes using a Target Level of Safety approach and an event tree format, populated with data from existing studies that share characteristics of UAS crashes to enable casualty prediction for UAS operations.

E.10.1.3 Risk maps In [35] the authors propose the use of risk maps to define the risk associated to accidents with unmanned aircraft. It is a two-dimensional location-based map that quantifies the risk to the population on ground of flight operations over a specified area. The risk map is generated through a probabilistic approach and combines several layers, including population density, sheltering factor, no-fly zones, and obstacles. Each element of the risk map has associated a risk value that quantifies the risk of flying over a specific location. Risk values are defined by a risk assessment process using different uncontrolled descent events, drone parameters, environmental characteristics, as well as uncertainties on parameters. The risk map is able to quantify the risk of large areas, such as urban environments, and allows for easy identification of high and low-risk locations. The map is a tool for informed decision making, and our results report some examples of risk map with different aircraft in a realistic urban environment.

E.10.1.4 Societal costs and benefits In [36] the authors describe that decisions based on risk analysis require some form of risk acceptance criteria. The objective of this paper

is to outline an approach by which societal risk acceptance criteria may be established, albeit in a different domain (maritime). The idea is to make it possible to discriminate between ship types representing different risks and importance to society. The societal risk acceptance criteria are calibrated against occupational fatality rates, and transportation fatality rate for scheduled air traffic worldwide. Examples are given for some different ship types. It should be noted that many other criteria would be needed in the decision process, like e.g. individual risks, criteria based on cost effectiveness, and criteria for environmental consequences. Normally a decision would have to be based on acceptance by all these criteria. Only one specific method to arrive at societal risk criteria is dealt with herein.

E.10.1.5 De minimis risk management strategy [37] describes that a de minimis risk management strategy sets a threshold so that risks below the specified level are defined as trivial and exempted from further consideration. The intended purpose is to help avoid inappropriate and wasteful concern with insignificant low-level risks. In most instances a de minimis strategy is likely to have beneficial or innocuous effects, but under certain circumstances large differences may develop between nominal and actual de minimis levels. The potential for such discrepancies illustrates why de minimis (and all other risk management) strategies should be evaluated on the basis of the portfolio of risks that would accumulate from applying such strategies over time, rather than on the apparent reasonableness of any single instance of application.

E.10.2 Fast-time simulation

Modeling of unmanned aircraft system traffic will require simulation options. One exemplar is described in [38]. The Flexible engine for Fast-time evaluation of Flight environments (Fe3) provides the capability of statistically analyzing high-density, high-fidelity, and low-altitude traffic without conducting infeasible and cost-prohibitive flight tests that involve a large volume of aerial vehicles. With this simulation capability, stakeholders can study the impacts of critical factors, define requirements, policies, and protocols needed to support a safe yet efficient traffic system, assess operational risks, and optimize flight schedules. [38] provides an introduction to this simulation tool including its architecture and various models involved. Its performance and applications in high density air traffic operations are also presented.

References

[1] "FAA Order 8040.6 - Unmanned Aircraft Systems Safety Risk Management Policy," 2019. https://www.faa.gov/regulations_policies/orders_notices/index.cfm/go/document.information/documentID/1036752.

[2] "FAA Advisory Circular: Small Unmanned Aircraft Systems (sUAS)," Tech. Rep. AC 107-2, U.S Department of Transportation (DOT) Federal Aviation Administration (FAA), June 2016.

[3] "Assessing the Risks of Integrating Unmanned Aircraft Systems (UAS) into the National Airspace System," tech. rep., The National Academies of Sciences, Engineering, and Medicine (NASEM), Washington, DC, 2018.

[4] U.S. Congress, "FAA Reauthorization Act of 2018," 2018. https://www.congress.gov/bill/115th-congress/house-bill/302/.

[5] "FAA Order 8040.4B - Safety Risk Management Policy," 2017. https://www.faa.gov/regulations_policies/orders_notices/index.cfm/go/document.current/documentNumber/8040.4.

[6] "FAA Order 8000.369C - Safety Management Systems," 2020. https://www.faa.gov/documentLibrary/media/Order/Order_8000.369C.pdf.

[7] "FAA Order 8900.1 Chg 615- Flight Standards Information Management System, Volume 17 Safety Management System," 2019. http://fsims.faa.gov/wdocs/8900.1/v17safetymanagementsystem/chapter03/17_003_003.htm.

[8] "FAA Advisory Circular 120-92B - Safety Management Systems for Aviation Service Providers," 2015. https://www.faa.gov/regulations_policies/advisory_circulars/index.cfm/go/document.information/documentid/1026670.

[9] "Air Traffic Organization Safety Management System Manual," 2015. https://www.faa.gov/air_traffic/publications/media/ATO-SMS-Manual.pdf.

[10] "FAA Order 8900.1 Chg 625- Flight Standards Information Management System, Volume 16 Unmanned Aircraft Systems," 2018. http://fsims.faa.gov/PICDetail.aspx?docId=8900.1,Vol.16,Ch4,Sec8.

[11] "Specific Operations Risk Assessment (SORA), JAR-DEL-WG6-D.04," 2017. http://jarus-rpas.org/sites/jarus-rpas.org/files/jar_doc_06_jarus_sora_v1.0.pdf.

[12] H. Millwater, J. Ocampo, G. Singh, H. Smith, and E. Meyer, "Probabilistic structural risk assessment and risk management for small airplanes," Tech. Rep. DOT-FAA-AR-11-14, U.S Department of Transportation (DOT) Federal Aviation Administration (FAA), November 2017.

[13] J. Breunig, J. Forman, S. Sayed, L. Audenaerd, A. Branch, and M. Hadjimichael, "Modeling risk-based approach for small unmanned aircraft systems," Tech. Rep. 18-1364, The Mitre Corporation, 2018.

[14] K. Steinnocher, A. D. Bono, B. Chatenoux, D. Tiede, and L. Wendt, "Estimating urban population patterns from stereo-satellite imagery," *European Journal of Remote Sensing*, vol. 52, no. sup2, pp. 12–25, 2019.

[15] R. Feldman, "Techniques and applications for sentiment analysis," *Communications of the ACM*, vol. 56, no. 4, pp. 82–89, 2013.

[16] "JARUS CS-UAS: Recommendations for Certification Specification for Unmanned Aircraft Systems," Tech. Rep. JARUS-DEL-WG3-CS-UAS-D.04, Joint Authorities for Rulemaking of Unmanned Systems (JARUS), September 2019.

[17] "JARUS Glossary," Tech. Rep. JAR-DEL-Glossary-D.4, Joint Authorities for Rulemaking of Unmanned Systems (JARUS), July 2018.

[18] "JARUS OPS A and B: Recommendations for Unmanned Aircraft Systems (UAS) Category A and Category B Operations," Tech. Rep. JAR-DEL-WG2-D.04, Joint Authorities for Rulemaking of Unmanned Systems (JARUS), July 2019.

[19] "JARUS Recommendation for Remote Pilot Competency (RPC) for UAS Operations in Category A (Open) and Category B (Specific)," Tech. Rep. JAR-DEL-WG1-D.04, Joint Authorities for Rulemaking of Unmanned Systems (JARUS), August 2019.

[20] "JARUS Guidelines on Specific Operations Risk Assessment (SORA)," Tech. Rep. JAR-DEL-WG6-D.04, Joint Authorities for Rulemaking of Unmanned Systems (JARUS), January 2019. `http://jarus-rpas.org/sites/jarus-rpas.org/files/jar_doc_06_jarus_sora_v2.0.pdf`.

[21] "JARUS Guidelines on SORA (JARUS-STS-01) Standard Scenarios for Aerial Work Operations," Tech. Rep. JAR-DEL-WG6-D.04, Joint Authorities for Rulemaking of Unmanned Systems (JARUS), November 2019. `http://jarus-rpas.org/sites/jarus-rpas.org/files/jar_doc_6_sora_sts_01_edition1.1.pdf`.

[22] E. Denney, G. Pai, and M. Johnson, "Towards a rigorous basis for specific operations risk assessment of UAS," in *IEEE/AIAA Digital Avionics Systems Conference (DASC)*, (London, UK), September 2018.

[23] "Remotely piloted aircraft systems operational risk assessment," Tech. Rep. AC 903-001-X, Transport Canada, 2019.

[24] M. S. Graydon and N. A. Neogi, "Guidance for designing safety into urban air mobility: Hazard analysis techniques," in *AIAA SciTech Forum*, (Orlando, FL), January 2020.

[25] "In-Time Aviation Safety Management Challenges and Research for an Evolving Aviation System," tech. rep., The National Academies of Sciences, Engineering, and Medicine (NASEM), Washington, DC, 2018.

[26] Steven Young et al., "Architecture and information requirements to assess and predict flight safety risks during highly autonomous urban flight operations," Tech. Rep. NASA/TM–2020-220440, National Aeronautics and Space Administration (NASA) Langley Research Center, January 2020.

[27] RTCA, "DO-200B Standards for Processing Aeronautical Data," tech. rep., RTCA, June 2015.

[28] E. Ancel, F. M. Capriston, and J. V. Foster, "Real-time risk assessment framework for unmanned aircraft system (UAS) traffic management (UTM)," in *Proceedings of the AIAA Aviation Technology, Integration, and Operations Conference*, (Denver, CO), June 2017.

[29] L. C. Barr, R. L. Newman, E. Ancel, C. M. Belcastro, J. V. Foster, J. K. Evans, and D. H. Klyde, "Preliminary risk assessment for small unmanned aircraft systems," in *Proceedings of the AIAA Aviation Technology, Integration, and Operations Conference*, (Denver, CO), June 2017.

[30] E. Ancel, F. M. Capristan, J. V. Foster, and R. C. Condotta, "In-time non-participant casualty risk assessment to support onboard decision making for autonomous unmanned aircraft," in *Proceedings of the AIAA Aviation Technology, Integration, and Operations Conference*, (Dallas, TX), June 2019.

[31] S. Stuart and D. A. Smith, "Insurance issues related to unmanned aerial systems," *In-House Defense Quarterly*, pp. 58–65, Spring 2015.

[32] R. Clothier, R. Walker, N. Fulton, and D. Campbell, "A casualty risk analysis for unmanned aerial system (UAS) operations over inhabited areas," in *Proceedings of the Australasian Unmanned Air Vehicles Conference*, Melbourne, Australia: Springer, March 2007.

[33] R. Clothier and R. Walker, "The safety risk management of unmanned aircraft systems," in *Handbook of Unmanned Aerial Vehicles*, Dordrecht, Netherlands: Springer Science + Business Media, 2013.

[34] R. Melnyk, D. Schrage, V. Volovoi, and H. Jimenez, "A third-party casualty risk model for unmanned aircraft system operations," *Reliability Engineering and System Safety*, vol. 124, pp. 105–116, 2014.

[35] S. Primatesta, A. Rizzo, and A. la Cour-Harbo, "Ground risk map for unmanned aircraft in urban environments," *Springer Journal of Intelligent and Robotic Systems*, May 2019.

[36] R. Skjong and M. Eknes, "Economic activity and societal risk acceptance," 2001.

[37] J. Mumpower, "An analysis of the de minimis strategy for risk management," *Risk Analysis*, vol. 6, no. 4, pp. 437–446, 1986.

[38] M. X. J. Rios, J. Silva, A. Ishihara, and Z. Zhu, "Fe3: An evaluation tool for low-altitude air traffic operations," in *AIAA Aviation Technology, Integration, and Operations Conference (AVIATION)*, (Atlanta, GA), June 2018.