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

Supplement C. Task 3-3 Illustration of Application of the Risk-Based Framework

November 27, 2021

NOTICE

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

LEGAL DISCLAIMER

The information provided herein may include content supplied by third parties. Although the data and information contained herein has been produced or processed from sources believed to be reliable, the Federal Aviation Administration makes no warranty, expressed or implied, regarding the accuracy, adequacy, completeness, legality, reliability or usefulness of any information, conclusions or recommendations provided herein. Distribution of the information contained herein does not constitute an endorsement or warranty of the data or information provided herein by the Federal Aviation Administration or the U.S. Department of Transportation. Neither the Federal Aviation Administration nor the U.S. Department of Transportation shall be held liable for any improper or incorrect use of the information contained herein and assumes no responsibility for anyone's use of the information. The Federal Aviation Administration and U.S. Department of Transportation shall not be liable for any claim for any loss, harm, or other damages arising from access to or use of data or information, including without limitation any direct, indirect, incidental, exemplary, special or consequential damages, even if advised of the possibility of such damages. The Federal Aviation Administration shall not be liable to anyone for any decision made or action taken, or not taken, in reliance on the information contained herein.

TECHNICAL REPORT DOCUMENTATION PAGE

1. Report No.	**2. Government Accession No.**	**3. Recipient's Catalog No.**
4. Title and Subtitle A21 Final Report: Integrating Expanded and Non-Segregated UAS Operations into the NAS: Impact on Trends and Safety- Appendix C. Task 3-3 Illustration of Application of the Risk-Based Framework		**5. Report Date** November 27, 2021 **6. Performing Organization Code**
7. Author(s) Steven Weber, Philip J. Smith, and Ellen J. Bass		**8. Performing Organization Report No.**
9. Performing Organization Name and Address Drexel University The Ohio State University		**10. Work Unit No.** **11. Contract or Grant No.** A21
12. Sponsoring Agency Name and Address Federal Aviation Administration		**13. Type of Report and Period Covered** Final **14. Sponsoring Agency Code**
15. Supplementary Notes		
16. Abstract		
17. Key Words	**18. Distribution Statement**	

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

Form DOT F 1700.7 (8-72)

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

TABLE OF ACRONYMS

ADM	Aeronautical Decision Making
AGL	Above ground level
ASSURE	Alliance for System Safety of UAS through Research Excellence
ASTM	American Society for Testing and Materials
BVLOS	Beyond Visual Line Of Sight
C2	Command and control
CONOPS	Concept of operations
CRM	Crew Resource Management
DAA	Detect and avoid
FAA	Federal Aviation Administration
hr	Hour
kg	Kilogram
km	Kilometer
m	meter
min	Minute
NAS	National Airspace
NASEM	National Academies of Sciences, Engineering and Medicine
PIC	Pilot in command
PRA	Probabilistic Risk Assessment
sec	Second
SMS	Safety Management System
SOP	Standard Operating Procedure
SRM	Safety Risk Management
SRMP	Safety Risk Management Process
sUAS	small UAS
UA	Unmanned Aircraft
UAS	Unmanned Aircraft System
USS	UAS Service Supplier
UTM	UAS Traffic Management
VTOL	Vertical Takeoff and Landing

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."

The National Academy report also specifies that the approach to quantitative risk assessment should make use of PRAs. The development of such a framework is further 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 Unmanned Aircraft Systems, ASSURE, to conduct research to inform the safe integration of small Unmanned Aircraft Systems (sUAS) in expanded beyond visual line of sight (BVLOS) and non-segregated sUAS operations. This tasking included the objective of this report: To provide a clear and consistent process and quantitative risk-assessment framework to guide the development of applications for sUAS operations.

This report, in fulfillment of the ASSURE Project A21 Task 3-3, "Illustration of Application of the Risk-Based Framework", illustrates the refinement and application of the risk-based framework developed in the A21 Task 3-1 report, "Definition of Risk-Based Framework". This illustration of the risk-based framework focuses on the safety risks associated with flight operations with automated control of an sUAS BVLOS over people. The discussion further indicates that such a quantitative assessment based on flight operations should be considered one component of a broader Safety Risk Management Program (SRMP) and indicates the additional components required for a complete assessment of a waiver requests for an sUAS operation.

This risk-based framework incorporates a blend of statistical methods to assess safety risks associated with a proposed flight operation using sUAS. In the example presented in this report illustrating application of this framework, it is assumed that a set of relevant flight data and parachute test data has been previously collected and archived, and that the waiver applicant chooses the run the minimum required number of additional tests on his proposed sUAS model and parachute. These data are used to calculate probabilities and expected values for the three possible outcomes of interest.

Based on these data, the framework is applied to calculate the resultant expected values for the probabilities *with no parachute* for the two possible outcomes of interest. In the example that is presented, these are calculated to be:

Probability of impact on pedestrian:	0.0000311963

Probability of impact on built environment: 0.00103988

The remaining possibility, i.e., no impact, holds the balance of the probability, i.e., one minus the sum of the two impact probabilities.

Based on the use of a decision matrix described in this example analysis, these probabilities lead to the conclusion that the proposed operation is LOW risk (Minor consequence) for the built environment, but is MEDIUM risk (Major consequence) for its potential impact on pedestrians.

However, using similar computations, *if the sUAS is equipped with a parachute,* these probabilities become:

Probability of impact on pedestrian: 0.0000004812

Probability of impact on built environment: 0.0000160391

Thus, with a parachute, the operation is classified as LOW risk in terms of safety risk for both pedestrians and the built environment.

Details regarding the supporting computations are provided in this report in the context of a full description of the sample flight operation, along with a discussion of underlying assumptions.

1. INTRODUCTION

This report, in fulfillment of the ASSURE A21 project Task 3-3, "Illustration of Application of the Risk-Based Framework", illustrates the refinement and application of the risk-based framework developed in the A21 Task 3-1 report, "Definition of Risk-Based Framework". As described in FAA Orders 8000.369C "Safety Management System" (SMS, June, 2020) and 8040.4B "Safety Risk Management Policy" (SRMP, May, 2017), SMS and SRMP are the FAA's frameworks for safety and safety risk management. Accordingly, this illustration focuses on the safety risks associated with the use of flight tests to evaluate the risks associated with automated control of a sUAS beyond visual line of sight (BVLOS) over people. The discussion further indicates that such a quantitative assessment based on flight operations should be considered as one component of a broader SRM process that also considers:

- Compliance with Category 4 of RIN 2120–AK85. Operation of Small Unmanned Aircraft Systems Over People (amendment of Title 14 of the Code of Federal Regulations part 107 (14 CFR part 107), permitting the routine operation of small UAS at night or over people under certain conditions).
- Verification and validation of hardware and software supporting the safety functions integrated into the automation in order to demonstrate compliance with FAA certification requirements for automated flight control in BVLOS operations over people, including human factors design requirements. (Such certification requirements need to be further defined.)
- Documentation of an effective safety management system as an additional safety net.
- Proof of insurance.
- Continued demonstration of safe operations once a flight operation has been approved and is ongoing.

In particular, the risk-based framework is not suitable for assessing risks of hazard causes, hazard outcomes, or the impact of mitigations if the underlying probabilities associated with those same causes, outcomes, or mitigations are unknown and it is not anticipated there will be sufficient empirical data from which estimates of those probabilities may be formed. It is for this reason that the risk-based framework is viewed as one component of a broader SRM process incorporating all of the above components: risk-based frameworks are only suitable when the risk may be reliably quantified through empirical data.

The illustration is provided through a hypothetical scenario dealing with a waiver request for a sUAS concept of operation (CONOPS) involving BVLOS operations over people during daylight hours. Specifically, the framework proposed in A21 Task 3-1 is refined and applied to this scenario, with the intention of informing preparation of waiver applications as well as the FAA's waiver approval decision process.

In this illustration, the BVLOS operation of sUASs over people consists of a small (2 kg) medical package delivery via a small (10 kg) rotorcraft sUAS starting from an urban medical supply center and terminating 5 km away at an urban regional hospital. It is assumed that automation will control the sUAS for both takeoff/ascent at a departure launch pad and for descent/landing at a destination landing pad, and that the sUAS will operate autonomously BVLOS during the enroute segment.

The safety analysis focuses on the risk associated with a fully automated operation, with the assumption that there are safety nets embedded in the automation, along with the monitoring of flights by a pilot in command (PIC) who can manually activate the safety nets in the automation, and along with other procedural controls that provide an additional layer of safety beyond that quantified for the automation alone. These additional safety measures provide protection against potential brittleness of the technologies and of the PICs in their limited roles such as making pre-flight decisions regarding whether to launch flights (Smith, 2018).

The analysis presented in this report has the singular goal of illustrating the risk-based framework in a realistic scenario. It bears emphasis that, because the primary goal is illustrative, the components of the scenario to which the risk-based framework have been applied are limited in scope. As described in Section 3.1.2, "SRMP Step 2 Identified Hazards", the scenario considers four primary hazard causes and two hazard outcomes. As the primary goal is the illustration of the methodology, inclusion of additional hazard causes and hazard outcomes are not in scope.

2. SCENARIO DESCRIPTION

The scenario particulars are now described. Parameters are set with the intention of representing typical values for the envisioned task.

2.1 Scenario Parameters

The CONOPS consists of a small (2 kg) medical package delivery via a small (10 kg) rotorcraft sUAS starting from an urban medical supply center and terminating 5 km away at an urban regional hospital.

It is assumed that automation will control the sUAS for both takeoff / ascent at the departure launch pad and for descent / landing at the destination landing pad, and that the sUAS will operate autonomously BVLOS) during the enroute segment.

The CONOPS will take place over people during daylight hours and in fair weather. The sUAS and the PIC workstations have unobstructed access to satellite (GPS) signals over all points on the trajectory.

The automation will guide the vertical ascent of the sUAS to the 350-foot target altitude for flights to proceed from the supply center to the hospital. At this point, the sUAS will follow a path from the source to the destination that deviates by 30 meters around a small urban park that is heavily populated during lunch hour and during special events. Finally, the automation will guide the vertical descent of the sUAS from the 350-foot altitude down to the landing pad.

At any given time the sUAS PIC at the launch pad or landing pad who is currently responsible for providing a safety net for the automation can instruct the sUAS automation to either apply a "kill switch," put the sUAS in a hover at its current location, exit hovering and continue on its planned trajectory, instruct the sUAS to return to the launch / landing pad, or divert to the nearest preplanned landing site (the launch pad, landing pad, or one of three intermediate diversion locations).

The automation is programmed to request a transition from one of the PICs to the other when the sUAS has traveled 2.5 km (kilometers) along its route, requiring acknowledgment from the PIC receiving control. If such an acknowledgment isn't received by the time the flight reaches 3.0 km

along its route, the automation initiates a diversion to the nearest preplanned alternative landing site.

In order to minimize the risk of collision, the target altitude for deliveries from the medical supply center to the regional hospital is set at 350 feet, while the target altitude for the reverse path, from the regional hospital to the medical supply center, is set at 250 feet. These trajectories are further offset 15 m (meters) horizontally.

Table 1. Scenario specifications and parameters.

Category	Value
UAS type	Rotorcraft
UAS weight	10 kg
UAS maximum speed	65 km/hr (no wind)
Mission	Package delivery
Package weight	2 kg
Start location	Launch pad in urban area
Launch mode	Vertical from pad
Destination	Landing pad in an urban area
Landing mode	Vertical to pad
Route distance	5 km
Route duration	13-14 min
Route average speed	25 km/hr
Route altitude (A to B)	350 feet
Route altitude (B to A)	250 feet
Terrain type	Urban environment
Flight restrictions	Flight canceled or diverted if surface winds greater than 6 m/sec

The CONOPS includes three flight stages: takeoff, enroute, and landing; there is no anticipated loitering stage. The descriptions of these stages add realism to the scenario, although not all of the specifics have an effect on the calculations used in the risk-based framework.

- *Takeoff:* the takeoff stage involves vertical ascent from a launch pad to the cruising altitude of 250 or 350 feet. The manufacturer specifications include a maximum ascent speed of 5 m/sec. At a nominal ascent speed of 4 m/sec, the ascent to 350 feet will take 27 seconds. To ascend to 250 feet it will take 19 seconds. The automation will control the sUAS for this flight stage.
- *Enroute:* the enroute stage involves traveling along two straight line segments at an altitude of 350 feet, with a turn in the vicinity of the urban park, thus routing it around this small

urban park that is heavily populated during lunch hour and during special events. Although the park isn't heavily populated at all times, to reduce the potential for human error in assigning a route to a given flight, the decision was made to always fly the same route around the park. Traveling at a nominal speed of 25 km/hr (well below the stated maximum sUAS speed of 65 km/hr), the sUAS will cover the 5 km distance from the launch pad to the landing pad in 12 min. The automation will control the takeoff and landing and the sUAS will operate autonomously while enroute. A significant portion of the enroute segment is beyond visual line of site.

- *Landing:* the landing stage involves vertical descent from the cruising altitude of 350 feet to the landing pad. The manufacturer specifications include a maximum descent speed of 3 m/sec. At a nominal descent speed of 3 m/sec, the descent from 350 feet will take 36 seconds. The automation will control the sUAS for this flight stage.

The total travel time of the route is therefore 27 seconds (ascent) + 12 minutes (enroute) + 36 seconds (descent), or between 13 and 14 minutes total; this is well under the manufacturer's stated maximum flight time (under the sUAS's maximum carrying capacity of a 5.5 kg load) of 25 minutes.

The risk-based framework requires the risk analyst to first identify one or more contexts of the CONOPS at which a risk-based analysis is deemed to hold value. These contexts may be tied to specific geographical locations or to specific stages of the mission. Once identified, the risk-based framework is applied at each such instance, yielding a risk score for each instance, from which the risk of the overall CONOPS may be assessed. The analysis in this scenario applies to the context of the CONOPS for which the human spatial density and the built infrastructure spatial density take prescribed values, as discussed in Section 3.1.3.6 "Analysis to Quantify the Risk of a Flight Operation with No Parachute." These spatial densities are used in the estimation of the conditional probability that the sUAS will impact a person and the built environment, respectively. It is worth emphasizing the main point: accurate assessment of the probabilities of the various hazard outcomes of the CONOPS at a particular instant requires modeling, data and measurements, and analysis that depends critically on the environment of the CONOPS at that instant.

2.2 Safety Precautions and Mitigations

Several safety precautions are in place. First, when the sUAS is within the control radius of one of the PICs, that PIC has the ability to: i) instruct the sUAS to return to the launch/ landing pad, ii) instruct the sUAS to operate in a hover mode, iii) instruct the sUAS to divert the nearest pre-planned alternate landing site, or iv) execute a kill switch that causes the sUAS to shut off all electrical and mechanical operations.

Second, for the purposes of this example, the sUAS has sensors that may trigger the kill switch if the system state is estimated to satisfy any of the prescribed kill criteria, including i) deviation beyond specified limits on planned (three-dimensional) trajectory, ii) loss of power, iii) loss of propulsion. The PIC is informed if such an event occurs.

Third, for the purposes of this example, the sUAS has sensors to detect loss of communications with either or both of the PIC workstations. If this condition is met, the sUAS makes an assessment of whether or not it may safely reach the launch pad, the landing pad, or any of the alternate sites.

The sUAS will divert to the nearest pad if such a pad is estimated to be reachable, or will initiate the kill switch if not. The PIC is informed if such an event occurs. Note that this functional requirement could not be included if the sUAS is expected to fly a route that takes it beyond the limits for the communication between the sUAS control station and the sUAS. This would place sole reliance on the automation as the safety net when flying beyond communication limits, and has implications for certification of the automation. Even when this is the case, however, the functional requirement could remain in effect when the sUAS is in the vicinity of the takeoff/landing pads.

2.3 Federal Regulations Pertinent to Scenario

As a portion of the CONOPS involves operation over people, the CONOPS is subject to RIN 2120-AK85 (Spring 2020), "Operations of Small Unmanned Aircraft Over People"[1]. In particular, the following three requirements must be satisfied:

- Category 4 eligible small unmanned aircraft must have an airworthiness certificate issued under Part 21 of FAA regulations. The aircraft must be operated in accordance with the operating limitations specified in the approved flight manual or as otherwise specified by the Administrator. The operating limitations must not prohibit operations over human beings. The aircraft must have maintenance, preventive maintenance, alterations, or inspections performed in accordance with specific requirements in the final rule.
- PIC knowledge test changes. The final rule replaces the requirement to complete an in-person recurrent test every 24 calendar months. The updated requirement is for PICs to complete online recurrent training which will include night subject areas. The online recurrent training will be offered free of charge to PICs.
- Inspection, testing, and demonstration of compliance. A PIC, owner, or person manipulating the flight controls of a small unmanned aircraft system must:
    - Have in that person's physical possession and readily accessible the remote pilot certificate with a sUAS rating and identification when exercising the privileges of that remote pilot certificate.
    - Present his or her remote pilot certificate and identification upon a request from the FAA, NTSB, TSA, or any Federal, state, or local law enforcement officer.

It should be noted that the remote PIC for this operation is limited in terms of the control functions available. As noted earlier, the PIC can only instruct the sUAS automation to either apply a "kill switch", put the sUAS in a hover at its current location, exit hovering and continue on its planned trajectory, instruct the sUAS to return to the launch / landing pad, or divert to the nearest preplanned landing site (the launch pad, landing pad, or one of three intermediate diversion locations).

It also should be noted that additional requirements for FAA certification of the sUAS may need to be specified to ensure adequate verification and validation of the software functions introduced

[1] https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202004&RIN=2120-AK85

in order to support automated control of the sUAS. This includes functional requirements dealing with the sUAS and the control workstation, as well as human factors design considerations.

3. REVIEW OF A21 TASK 3-3

Task 3-3 in the A21 research task plan (RTP) requires the following research questions be addressed:

1. What would be an informative example from the operation of sUAS to illustrate the application of the proposed risk-based framework?
2. What data are necessary to complete this example?
3. What are the results of the analyses to support this example?

3.1 Scenario Analysis

3.1.1 SRMP Step 1 System Analysis

This section applies Step 1 of the SRMP, System Analysis, to the scenario.

Definition 1: Concept of Operations (CONOPS). The concept of operations (CONOPS) for the scenario is:

- Mission: Transport package by sUAS.
- Location: The 5 km flight path
- Date and time: The proposed date is July 1, 2024 and the time is 12:00pm (noon).
- BVLOS: Yes.
- Night operations: No.
- Over people: Encompassing an urban area characterized as having a low population density as defined in MITRE (2018). This is a key assumption in the calculation of the probability of impact with a person.
- Flight path: The flight path is as described in the scenario description section.
- PIC location: sUAS PICs will be located at both the takeoff and landing locations throughout the duration of the flight.

Definition 2: Flight stages and highest risk instances. The CONOPS comprises three flight stages: takeoff, enroute, and landing; there is no anticipated loitering stage:

- Takeoff: Instant at which the sUAS takes off and instant at which the target flight altitude of 350 feet is achieved.
- Enroute: Instant at which sUAS begins lateral progress along route towards destination (at 350 feet) until instant at which sUAS begins vertical descent to landing pad.
- Landing: Instant between the sUAS reaching destination location and sUAS completing vertical descent from height of 350 feet onto landing pad.

However, as will be seen, the hazard cause distributions under consideration will not depend upon the flight stage per se. The hazard cause distribution is based on the assumption of automated control for the entire flight once the PIC specifies the trajectory, completes pre-flight checks and initiates takeoff. The hazard outcome conditional distribution will depend upon environmental factors such as a) the extent and nature of the built environment underneath the sUAS and b) the

population density underneath the sUAS. (Note that this approach is general in nature and therefore can be applied to numerous other CONOPS as well.)

Recommendation 1: System state category specification. The system state categories for the proposed scenario are:

- sUAS platform and payload: Many of these are as described in the scenario description section.
- The commercial model properties include: i) sUAS platform weight of 10 kg; ii) sUAS maximum speed of 65 km/hr.
- The payload properties include: i) maximum weight of 2 kg; ii) payload secured to sUAS by strong, thin, and light cables. If a parachute is included, it weighs 0.5 kg.
- Flight readiness: all pre-flight check status outcomes are at target / nominal levels (e.g., fuel cell charge level).
- PIC workstation: One PIC will be physically located at the launch pad and another at the landing pad. They have direct line of sight views of departures and landings and have limited views only in the vicinity of those pads while enroute.
- The use of UAS Service Supplier (USS) is a component to support the UAS operation. If there is reason to believe that the level or nature of such support is not consistent across all sites, then this would need to be considered in the definition of the equivalence class for the proposed UAS and in the necessary software verification and validation tests indicated as part of the required overall SRM process.
- The effectiveness of the software and procedures associated with UAS Traffic Management (UTM) similarly will need to be evaluated in the necessary software verification and validation tests indicated as part of the required overall SRM process.
- PIC training and procedures: The PIC has received a Remote Pilot Certificate from the FAA and is compliant with required procedures.
- Flight plan: The takeoff characteristics include a vertical ascent off the launch pad at an ascent speed of 4 m/sec (below manufacturer's specified maximum ascent speed of 5 m/sec) to the target cruising altitude of 350 feet, for an anticipated ascent duration of 27 seconds. The target speed during the horizontal travel enroute stage of the CONOPS is 25 km/hr and the route distance is 5 km, resulting in an anticipated travel time for this stage of 12 minutes. The landing characteristics include a vertical descent to the landing pad at a descent speed of 3 m/sec (consistent with the manufacturer's specified maximum descent speed of 3 m/sec), for an anticipated descent duration of 36 seconds. The total flight duration (ascent, enroute, and descent) is therefore anticipated to lie between 13 and 14 minutes.
- C2 channel: The remote controller has a maximum distance of 3.5 km. Since there is a planned transition of control from the PIC at the launch pad to the PIC at the landing pad, one of the PICs has the ability to interact with the automation at all times during the flight. The PICs and the sUAS are assumed to have clear connections to satellite (GPS) signals at all points and times on the route.
- Information acquisition, processing, and dissemination: All relevant sensors are anticipated to operate well within nominal operating ranges and to yield nominal accuracy. The

operating environment is anticipated to be favorable, with clear visibility and low electromagnetic noise.

- Weather environment: The CONOPS is assumed to include the specification that the flight will only be attempted under anticipated favorable weather environment, i.e., with maximum wind speed below the manufacturer's specified maximum wind resistance of 6 m/sec. There will be some maximum level of forecast or actual precipitation at or above which the PIC must cancel or delay the flight.
- Airspace environment: The airspace environment has been designed so the planned trajectory does not intersect any known airplane flight paths or defined helicopter routes.
- Ground environment: The ground environment underneath the 5 km route involves an urban environment.
- Available mitigations: The sUAS design includes a parachute (if the safety assessment indicates a need), a kill switch that can be initiated by the automation or the PIC, a control to initiate a diversion to a nearby site that can be initiated by the automation or the PIC, and a control that allows the PIC to initiate hovering of the sUAS at its current location and to exit hovering, continuing on its planned trajectory. Additional mitigations include Detect And Avoid (DAA) functionality, procedural safety nets involving defined use of airspace by sUASs and manned aircraft including helicopters, and the issuance of NOTAMS to inform PICs regarding the use of airspace by the sUASs.

3.1.2 SRMP Step 2 Identified Hazards

This section applies Step 2 of the SRMP, Identified Hazards, to the scenario.

Recommendation 2: Hazard cause specification. The following hazard causes are identified as relevant to the scenario:

- Loss/failure of platform power (denoted "pow"): the sUAS platform loses power due to an electrical failure;
- Loss/failure of platform propulsion (denoted "pro"): the sUAS platform loses propulsion due to an empty or failed battery or a mechanical failure;
- Loss/failure of communications (denoted "com"): the sUAS platform is unable to communicate with one or the other of the human-operated workstations at the launch and landing pads, even though the sUAS is within the nominal communication radius of the controller. For this analysis, we make the conservative assumption that the sUAS could fall to the ground, with the associated assumption that, as a safety net, the automation would divert to a diversion landing site. For other scenarios where the sUAS route extends beyond communications limits, as discussed earlier other procedures would have to be considered;
- Deviation from anticipated path (denoted "dev"): the automated controller on the sUAS fails to follow the prescribed route path. For this cause, we again make the conservative assumption that the sUAS could fall to the ground. Note that one possible cause of this could be a GPS outage.

Note that the framework allows for the addition of other hazard causes as desired. These four have been selected for the purposes of illustration.

Recommendation 3: Hazard outcome specification. Two of the three hazard outcomes identified in Recommendation 3 that are identified as relevant for the scenario consist of:

- Proximity to or collision with a person (denoted "per"): the probability of the sUAS impacting the safety of a person, either through direct or indirect contact, will be assessed as a function of the spatiotemporal density of humans at the location and time at which the sUAS falls to the ground. Indirect contact of an sUAS with a person includes an sUAS landing / crashing on a highway, thereby jeopardizing the safety of the drivers on the highway at that time. The analysis of this probability is in Section 3.1.3.6 "Analysis to Quantify the Risk of a Flight Operation with No Parachute."
- Proximity to or collision with the built environment (denoted "bui"): the probability of the sUAS colliding with a significant object in the built environment will be assessed as a function of the spatial density of such objects in the built environment along the route. It is assumed that all such collisions do not impact the safety of any person, as such an outcome is the focus of the previous "person" outcome. The analysis of this probability is in Section 3.1.3.6 "Analysis to Quantify the Risk of a Flight Operation with No Parachute."

3.1.3 SRMP Step 3 Analysis of Safety Risk

This section applies Step 3 of the SRMP, Analysis of Safety Risk, to the scenario. Note that this analysis focuses on the safety risks associated with automated control based on flight data. Additional safety nets provided by the PIC and the automation are not included in the quantitative assessment, but rather are noted as methods to further reduce risk to some unquantified extent beyond the level indicated by the quantitative risk assessment.

Note also that we assume that this quantitative assessment of safety risk based on flight data associated with the operation of the sUAS under automated control should be considered one component of a broader SRM process that also considers:

- Compliance with Category 4 of RIN 2120–AK85. Operation of Small Unmanned Aircraft Systems Over People (amendment of Title 14 of the Code of Federal Regulations part 107 (14 CFR part 107) by permitting the routine operation of sUAS at night or over people under certain conditions).
- Verification and validation of hardware and software supporting the safety functions integrated into the automation in order to demonstrate compliance with FAA certification requirements for automated flight control in BVLOS operations, including human factors design requirements. (Such certification requirements need to be further defined to meet the needs indicated in this example.)
- Documentation of an effective safety management system as an additional safety net.
- Proof of insurance.
- Continued demonstration of safe operations once a flight operation has been approved and is ongoing.

Specification of Step 3 of the SRMP to the scenario requires selection of the parameter values.

It is evident that the (unconditional) posterior distribution on the hazard outcomes is computed from the four inputs:

1. the hazard cause prior distribution parameters
2. the hazard outcome conditional prior distribution parameters
3. the hazard cause measurements / observations
4. the hazard outcome measurements / observations.

For this illustration of the framework, we describe how it can be applied to evaluate safety risk associated with the enroute portion of a flight. Similar calculations can be performed to assess the risk associated with take-off and landing.

The quantitative risk assessment framework illustrated in this report focuses on a Bayesian formulation of the decision problem as discussed in detail in the A21 Task 3-1 report, "Definition of Risk-Based Framework". Strictly speaking, that means that the prior probability distribution for hazard causes and the prior distribution for the failure of a parachute as a safety mitigation should reflect what the decision maker (the FAA) believes when making decisions about approving waiver requests for sUASs) believes about this quantity.

To make this a tractable approach, in our example formulation we assume that this decision maker estimates these prior distributions based on objective data that have been previously been collected and reported regarding:

- The flight performance of the specific model sUAS of interest for the waiver request (treating "same sUAS model" as an equivalence class).
- The performance of sUAS parachutes in general that have been designed and manufactured consistent with the sUAS parachute standard (treating "parachutes meeting this standard" as an equivalence class).

Considerations associated with this concept of an equivalence class are described below.

3.1.3.1 Use of Equivalence Classes

As noted above, in order to make this approach tractable, this framework allows a waiver applicant to make use of data provided by either a manufacturer who has produced and tested hardware or software belonging to the same equivalence class as the hardware and software to be used in the proposed operation, or data provided by other qualified sUAS PICs regarding the performance of hardware or software belonging to the same equivalence class, and who have either:

- Collected and reported appropriate test data to support of their own waiver applications.
- Collected and reported the equivalent data in actual operations.

These data must have been generated by operations using hardware and software that belong to the same equivalence class(es) as the those under consideration for a waiver. Based on *engineering judgment*, the FAA would have to define such equivalence classes, with input from appropriate industry consensus groups. The two equivalence classes used in the example documented here are i) a specific model sUAS (defined in terms all of the associated hardware and software); ii) parachutes that have met the requirements of the parachute standard for sUASs (ASTM, 2018).

This approach assumes that some organization has been authorized by the FAA to collect and provide access to flight data from manufacturers who are providing the hardware and software for sUAS, as well as from PICs who are preparing waiver requests for sUAS operations for submission to the FAA, or who have conducted actual approved flight operations. (To help motivate submission of such data by PICs, a requirement could be established indicating that, in order to access such a pooled data set for the preparation of a waiver request, an applicant must submit the collected data so that they are available for future waiver requests by other applicants.)

Note that one concern focuses on quality assurance for the data submitted. For example, if a PIC collected data at a test site that provided an area where there were no people or infrastructure that

could be affected by a failure of a sUAS or parachute, there might be a temptation to launch it without an adequate SMS process in place. To reduce this concern:

- For data on prior operations at test sites that are submitted to support the evaluation of future waiver requests:
    - The aircraft used in the tests must have documented maintenance, preventive maintenance, alterations, or inspections performed in accordance with specific requirements in the final FAA rule for sUAS flights.
    - The PIC operating the sUASs must have successfully completed the FAA Remote Pilot knowledge test.
- For data on prior actual operations that are submitted to support the evaluation of future waiver requests, a requirement for submission of such data would be documentation of the SMS process in place at the time of the data collection. Appendix A, developed by Lamb at ERAU, provides a checklist indicating documentation that could be required as part of such an SMS process. The FAA would need to determine what should be required in such a checklist for documenting the SMS process in place during tests or actual operations.
- In order to look for evidence of heterogeneity in submitted sets, a statistical test for an outlier could be conducted when a data set is submitted. However, since it would be unacceptable to reject a data set for inclusion just because it indicated significantly more failures than the numbers representative of other previously submitted data sets, the statistical test indicating a possible outlier would have to be a trigger to find an assignable cause that justified such a rejection of that data set (such as a determination that there were flights flying under conditions with excessive winds or convective weather).

3.1.3.2 Equivalence Across Environmental Conditions

Our two sample equivalence classes (same model sUAS; consistency with ASTM parachute standard) raise another question that needs to be resolved based on engineering judgment: How similar do the environmental conditions (such as winds) have to be to consider the flights used to provide data to be in the same equivalence class? For example, if 10 parachute tests are run under conditions with no winds and 10 are run with significant winds (but within the manufacturer's documentation of the expected capabilities of the parachute to function), can these be treated as belonging to the same equivalence class for the purposes of aggregating the data?

3.1.3.3 Assumptions of Independence of Flights Included in the Data

If the same specific sUAS or the same specific parachute is used to conduct a number of flight tests, should those samples be considered independent? Since a manufacturing process can produce a product that has some variability from a quality assurance perspective, this question will need to be addressed. One possible engineering decision would be that if the manufacturing and software development process meets ISO and ASTM standards to ensure the quality and safety of the product, then collection of data using the same specific sUAS or parachute multiple times can be treated as data from independent samples in the analyses.

3.1.3.4 Software/Hardware Changes

Another engineering decision involves defining what constitutes a significant change in the hardware or software associated with an sUAS or parachute used in an operation that has already received a waiver approval. At what point is a change significant enough that a new waiver application needs to be submitted and evaluated?

3.1.3.5 Minimum Additional New Tests

As a final protection to ensure that the assumptions about equivalence classes are valid, a minimum number of flights needs to be conducted by the organization submitting the waiver request (or an appropriate representative of this organization). This minimum number of flights needs to be determined by the FAA (with input from industry consensus groups) based on engineering judgment regarding the conclusions arrived at in defining equivalence classes.

These tests that are performed by the applicant need to be completed using the combination of the full set of hardware and software proposed for actual operations if the waiver is approved. In our example described earlier, we assume that, because a large number of prior flights have been incorporated into the estimation of the prior distributions (3000 operations for the sUAS itself and 1000 for prior tests of parachutes belonging to the same equivalence class), the applicant has chosen to just run the minimum required additional tests. (In this example, we assume 100 additional tests for the sUAS). Note that applicants may choose to run more than the minimum number of tests in order to tighten the confidence interval in order to try to demonstrate the necessary level of safety.

3.1.3.6 Analysis to Quantify the Risk of a Flight Operation with No Parachute

In order to estimate the hazard cause prior distribution parameters for the enroute segment of a flight, the desired level of confidence needs to be considered. We assume that the decision maker informs his beliefs regarding this prior distribution as follows:

> For the illustrated BVLOS flight operation over people, if evaluated *without the availability of a parachute as a mitigation to increase safety*, use classical statistics to find the one sided 99.99999% confidence interval for the probability of a failure during flight of this model sUAS (see JavaStat -- Binomial and Poisson Confidence Intervals (statpages.info)) based on the previously collected data.

We have selected 99.99999% for this analysis assuming the consequence level when one of the hazard causes arises is Major (see Figure 1) and that the probability of failure has to be <1 in 100,000 to be classified as a low risk. Thus, 99.99999% corresponds to the required probability of failure to be classified as low risk. (Note that this is a heuristic that we have adopted for this illustration. The FAA could develop some other rationale that results in a specifying a different required confidence level.)

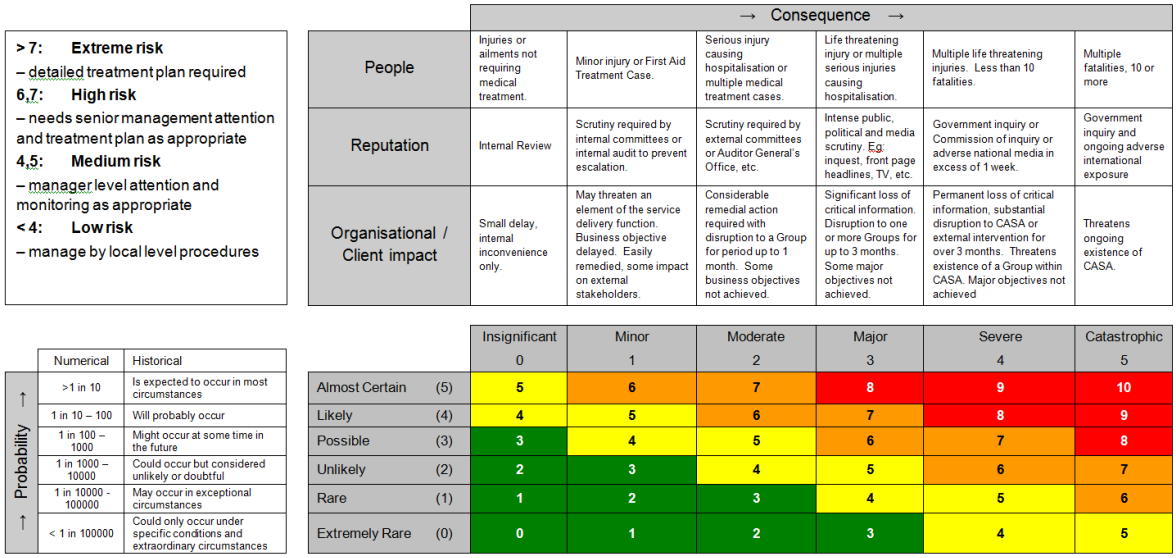

Figure 1. Decision matrix (from Pezzulo, 2009).

To decide whether a parachute is necessary, the outcome posterior probabilities, Probability(sUAS experiences one of the 4 hazard causes and falls toward the ground AND the sUAS falls within a two meter X two meter area containing a person) and Probability(sUAS experiences one of the 4 hazard causes and falls toward the ground AND the sUAS hits a significant object in the built environment), both need to be calculated.

The model for person impact is kept as simple as possible, for purpose of illustration of the overall statistical method. Namely, a person impact either occurs or it does not, and there is no incorporation of the number of persons impacted or the severity of the injuries sustained as a function of the kinetic energy of the sUAS and its angle of impact. These considerations, while important, are outside the scope of this report.

Estimating Parameters for Prior Distribution of 4 Hazard Causes for the Enroute Segment. As discussed above:

- Assuming no parachute, use classical statistics to find the (one sided) 99.99999% confidence interval for the probability of a failure during flight of this model sUAS
- As an illustration, in our example we assume that of the 3,100 previously recorded flights of 5 km or greater, there were 0 failures during launch, enroute flight and landing. Given these data, the one-sided 99.99999% confidence interval for the probability of a failure is 0 to $f = 0.005199385694027315$.

This confidence interval has been derived using the method in Appendix B.

Prior Distribution on Hazard Causes. The decision maker decides that this result best informs his belief about the prior distribution and translates it to:

Dirichlet prior distribution on hazard causes = [*1-f, f/4, f/4, f/4, f/4*], for *f* given above.

Here, the five numbers denote the prior distribution weights on the "null-cause" (no hazard, listed first), and the four "non-null" hazard causes ("pow", "pro", "com", and "dev" listed in " Recommendation 2: Hazard cause specification" of SRMP Step 2). See Appendix B for additional details on this calculation and those that follow.

Prior Distribution on Hazard Outcomes. For our example, we estimate the probability that a person will be impacted if the sUAS falls to the ground to be 0.006. (The justification for this estimated probability that a person will be impacted if the sUAS falls to the ground is described in the next subsection.)

Estimation of Probability That a Person will be Impacted if the sUAS Falls to the Ground. For this example, we use the approach discussed in MITRE (2018). We estimate the probability that the sUAS falls within a two meter X two meter area containing a person based on an assumption that the trajectory flies over an urban area with low pedestrian density (4050 people per square mile as indicated in Figure 2). One square mile is 2,589,988 square meters, so the probability of a sUAS falling on a pedestrian is estimated as the ratio of occupied space (4,050 people each consuming 4 square meters) over total space (2,589,988 square meters):

4050 *4/2,589,988=0.006

	Category	Median (ppl/mi²)	% Contiguous US Land Area	% US Population
Rural	Low	0	95.78	10.5
	Medium	600	2.04	12.4
	High	1,733	0.98	16.1
Urban	Low	4,050	1.15	29.3
	Medium	17,169	0.051	19.2
	High	85,160	0.0017	7.5
Open Air Assembly	Low	1,219,882*	N/A	4.4
	Medium	1,904,935*	N/A	0.7
	High	2,589,990*	N/A	0

*not median, but chosen people density value

Figure 2. Estimation of pedestrian density (from MITRE, 2018).

Alternatively, a more detailed characterization of pedestrian density could be developed considering that subset of the trajectory flying over a busy highway with fast moving traffic during certain times of the day as a worst case. In addition, the assumption of occupied space is "worst-case" in the sense that it assumes each person to occupy a disjoint 2m x 2m square, when, in actuality, a more refined model would incorporate the spatial correlations of human locations in an outdoor environment. Such a model refinement is outside the scope of this report.

It is also worth noting that the U.S. Census has identified population density in an urban U.S. environment to be 2,534 per square mile[2]. This urban density is lower than the 4,050 per square mile used above, making this analysis more conservative.

Collision with the Built Environment. We further simply assume for the purposes of illustration that the probability of proximity to or collision with a significant object in the built environment if the sUAS falls to the ground is 0.200[3] and that the associated consequence is MINOR (see Figure *1*). Such objects could include streetlights, awnings, buildings, and parked cars.

Hazard Outcome Conditional Prior Distribution. From the above calculations, it is estimated that the probability of hitting a person is 0.006 based on the analysis above, the probability of hitting the built environment is 0.200, and the probability of hitting neither is 0.794. Note that, for the purposes of this example, we have arbitrarily assigned the value of 0.200. The probability to use for a real example would have to be dome derived from some data source. This yields the following hazard outcome conditional prior distribution:

|1 0.794 0.794 0.794 0.794|

|0 0.200 0.200 0.200 0.200|

|0 0.006 0.006 0.006 0.006|

This matrix has dimensions 3 x 4, where the rows correspond to hazard outcomes and the columns correspond to hazard causes. The first row is the "null outcome" (no hazard outcome), the second row is the "built environment" hazard outcome, and the third row is the "pedestrian" hazard outcome. The first column is the "null cause" (no hazard cause), and the remaining four columns are the four "non-null" hazard causes ("pow", "pro", "com", and "dev"). Each column sums to one and is the conditional distribution on the hazard outcomes conditioned on the column's hazard cause.

For purpose of illustration and simplicity, the model assumes that the conditional probabilities for the hazard outcomes are the same for all non-null hazard causes. In other words, what matters in this model is simply whether or not there is a non-null hazard cause, and it is not essential to know, under this assumption, the exact nature of the hazard cause. In many cases this assumption will be entirely reasonable, i.e., the probability of a particular hazard outcome is well captured by simply knowing something is wrong and the additional information of what exactly is wrong does not add substantial accuracy to that probability. In some cases, the assumption will not hold, as some specific hazard outcomes will have conditional probabilities that vary significantly with the exact hazard cause.

Hazard Cause Measurements. It is assumed that the waiver applicant conducts 100 trials and that all of these trials result in a null hazard cause.

---

[2] https://www.census.gov/programs-surveys/geography/guidance/geo-areas/urban-rural/ua-facts.html

[3] The total area includes total land area and total water area. The total land area includes the total developed area and the total undeveloped area. The total developed area includes streets, residential areas, commercial areas, industrial areas, railroad, parks, public and semi-public property and other areas. For a sUAS to collide with property or people, it must land in the developed area where built infrastructure exists.

As before, these five numbers correspond to the hazard causes: the "null cause" (no hazard cause), and the four "non-null" hazard causes ("pow", "pro", "com", and "dev"). These measurements are combined with the hazard cause prior distribution weights to yield the posterior distribution parameters on hazard causes.

Outcome Posterior Probabilities. These data are used to calculate posterior probabilities and expected values for the three possible hazard outcomes. The resulting values for the posterior probabilities *with no parachute* are:

Probability of impact on pedestrian:	0.0000311963
Probability of impact on built environment:	0.00103988

The above (unconditional) posterior distribution on hazard outcomes is computed from the posterior hazard cause distribution parameters and the posterior hazard outcome conditional distribution parameters using the total probability theorem, as detailed in the appendices.

3.1.4 SRMP Step 4 Assessment of Safety Risk

This section applies Step 4 of the SRMP, Assessment of Safety Risk, to the scenario. We illustrate it based on the calculations above that assume automated control of the sUAS once it is launched, with no parachute as a mitigation.

Model specification 19: Hazard outcome risk category vector (Defined in the A21 Task 3-1 report, "Definition of Risk-Based Framework"): Risk categories are assigned to the two distinct hazard outcomes under consideration in this scenario:

- Proximity to or collision with a person (denoted "per") is assigned Consequence Category 4: MAJOR.
- Proximity to or collision with a significant object in the built environment (denoted "bui") is assigned Consequence Category 2: MINOR.

Recommendation 9: Flight instance risk category decisions via hazard outcome risk category vector (Defined in the A21 Task 3-1 report, "Definition of Risk-Based Framework" and using the Risk Decision Matrix shown in Figure *1*:

- The Risk Categories in the "MINOR" consequence column range from "High Risk" down to "Low Risk", as the Risk Probability varies from "Almost Certain" to "Extremely Rare".
- The Risk Categories in the "MAJOR" consequence column range from "Extreme Risk" down to "Low Risk", as the Risk Probability varies from "Almost Certain" to "Extremely Rare".

To categorize the safety of this operation based on flight operations without the use of a parachute as a mitigation:

- The expected value for the posterior probability of impacting a person with a Major consequence is estimated to be greater than 1 in 100,000 (0.0000311963). This indicates the need for an additional mitigation such as a parachute or increased data collection in order to potentially demonstrate confidence in a lower posterior probability (if the data continue to indicate a very low frequency of occurrences for the hazard causes).
- The posterior probability of impacting a significant object in the built environment with a Minor consequence is less than 1 in 10,000 (0.00103988). This indicates that, in terms of

the safety risk impacting the build environment, there is no need for an additional mitigation such as a parachute or increased data collection in order to potentially demonstrate confidence in a lower posterior probability (if the data continue to indicate a very low frequency of occurrences for the hazard causes) relative to the thresholds indicated in the decision table. However, the outcome noted above that the posterior probability of impacting a person with a Major consequence is estimated to be greater than 1 in 100,000 would dominate the decision, requiring an additional mitigation such as a parachute or increased data collection.

The conclusion is that, without the use of a parachute as a mitigation, the CONOPS has an overall Medium risk, making it necessary to further assess the safety risk if a parachute is provided as a mitigation. This is done in the next section.

3.1.5 SRMP Step 5 Control of Safety Risk

This section applies Step 5 of the SRMP, Control of Safety Risk, to the scenario.

First, it should again be noted that the quantitative risk assessment framework illustrated in this report focuses on one dimension of an overall risk assessment process. It focuses on the safety risks based on flight observations to evaluate the risks associated with automated control of the sUAS.

Based on the risk assessment associated with automated operation of the sUAS with no parachute as illustrated above, the results indicate that, in order to achieve categorization as a low risk, this proposed operation would need some mitigation such as the use of a parachute. Below we provide a high-level discussion of the assessment of whether such a mitigation is sufficient given the available data assumed for our example. This analysis is described in detail in Appendices B and C.

First, the consequence needs to be specified. Since the event of interest is the case when one or more of the hazard causes identified earlier occurs and when the parachute fails, we use the same consequence category as in the previous analysis: MAJOR.

In the interest of illustrating the risk-based methodology, it is assumed that a parachute deployment is binary: it either succeeds or it fails. Moreover, if it succeeds then it is assumed that there is no possibility of a hazard outcome, i.e., the kinetic energy of the sUAS under a successful parachute deployment is sufficiently low so as to minimize the possibility of injury to a person or damage to the built environment. Moreover, if it fails then it fails entirely and the failed parachute has subsequently no impact on the resulting calculations of likelihood and severity. A more refined model would potentially increase the set of possible outcomes for a parachute deployment and model the resulting kinetic energy of each one, as well as model the role of the kinetic energy on the severity of impact. These extensions are outside the scope of this report but would be allowed within this framework.

Because we are using MAJOR as the consequence level, the required confidence level will be left the same as in the previous analysis, 99.99999%. If we assume that there have previously been 1,045 parachute tests with 0 failures, using the upper bound on the confidence interval of 0.015424014977497298, the calculations described in Appendix B provide the following results:

	No Parachute	With Parachute
Probability of impact on pedestrian:	0.0000311963	0.0000004812
Probability of impact on built environment:	0.00103988	0.0000160391

Repeating SRMP Step 4, Assessment of Safety Risk, but now assuming a parachute, the risk assessment for the enroute segment of the flight in terms of an impact on a pedestrian is now LOW, as the Consequence category remains Major but the estimate of the posterior probability of an impact on a pedestrian is Extremely Rare (0.0000004812). Similarly, assuming a parachute, the risk assessment for the enroute segment of the flight in terms of an impact on the built environment remains LOW, as the Consequence category is remains Minor and the estimate of the posterior probability of an impact on the built environment is Rare (0.0000160391).

Finally, note that, for the takeoff and landing segments *for this rotorcraft operation,* we assume a Minor consequence if the takeoff and landing portions of the flight are approximately vertical (VTOL) and that the areas underneath these segments of the trajectories are protected in order to ensure that no person or significant object is standing underneath the sUAS as it takes off and lands. The computations are analogous, using the same previous and additional data sets as were used for the analysis of the enroute segment. Because the Consequence category is Minor, even without a parachute the safety risk would be categorized as LOW.

One caveat, however, is that the calculations for the risks associated with an operation with a parachute are based on certain simplifying assumptions that provide conservative estimates of the posterior probabilities for this example analysis. These assumptions merit additional research in order to more exactly guide the decision process for all scenarios.

3.1.6 SRMP Step 6 Process Monitoring

We have added a sixth step in addition to the five defined in the A21 Task 3-1 report, "Definition of Risk-Based Framework". This sixth step is based on the recognition that certain assumptions have been made in conducting the analyses defined in the previous steps (such as the definition of equivalence classes).

Step 6 essentially focuses on collecting data from actual approved operations, looking for evidence that a safety risk exists in spite of the rigor of the approval process. Step 6 of the specifies that data will be collected and evaluated in order to monitor for the following types of events:

- Unapproved entry of an sUAS into departure or arrival airspace.
- Failure of an sUAS to conform to LAANC approval for an sUAS.
- Failure of an sUAS to avoid -
    - Close proximity to another sUAS.
    - Close proximity to a manned aircraft.
- Collision of an sUAS with:
    - Another sUAS.
    - A manned aircraft.

The FAA repository documenting reportable accidents would be another relevant data source.

Such data may be used to evaluate the operation of a particular sUAS operation. Within this framework, however, the focus is on the use of the data to evaluate the adequacy of assumptions

and conclusions within an application of the framework in case they need to be refined. For example, if incident report data from actual operations provides evidence that not all parachutes conforming to the ASTM standard are equally effective, then it might be necessary to reconsider the equivalence class for parachute safety as defined in the sample analysis presented in the Task 3-3 report regarding parachute safety.

As a concrete example, consider the following analyses using Aeroscope data for sUAS in conjunction with ADSB-data for manned aircraft in the vicinity of DFW (provided by ERAU). First, as Figure 3 illustrates, Aeroscope data can be used to identify the locations of sUAS in a given airspace region. In the future, the requirement for Remote ID while an sUAS is in flight will make it possible to further associate registration information with a specific sUAS.

Second, as Figures 4-5 illustrate that, in terms concerns regarding the proximity of sUAS and manned aircraft, such data can be used to ask questions such as: Is there objective data indicating that, with a frequency higher than that expected based on assumptions made regarding the approval of that type of sUAS operation, sUAS are demonstrating:

- Unapproved entry of an sUAS into departure or arrival airspace?
- Failure of an sUAS to avoid close proximity to a manned aircraft?

Figure 4 indicates a case where there was no correlation between a sighting report and sUAS activity as indicated by Aeroscope data (keeping in mind that the Aeroscope only detects DJI sUAS, which represent about 72% of the market). Figure 5 indicates a case where there was UAS activity at 0.60 NM S of DFW between RWY 36R and RWY35L approach corridors and also that there was a correlation between a sighting by ATC and the location of an sUAS (correlated reported activity, no factor to ASH5981 departure; UAS detected at 390' AGL). Figure 6 indicates another case where there was a correlation between an sUAS sighting and an sUAS location.

If such events are occurring at a higher than predicted frequency, then that should motivate investigation into the underlying causes, which in turn could indicate a need to refine the framework itself, to investigate the quality of the data provided in sUAS waiver requests, or to assess the rules applied to allow sUAV operations more generally.

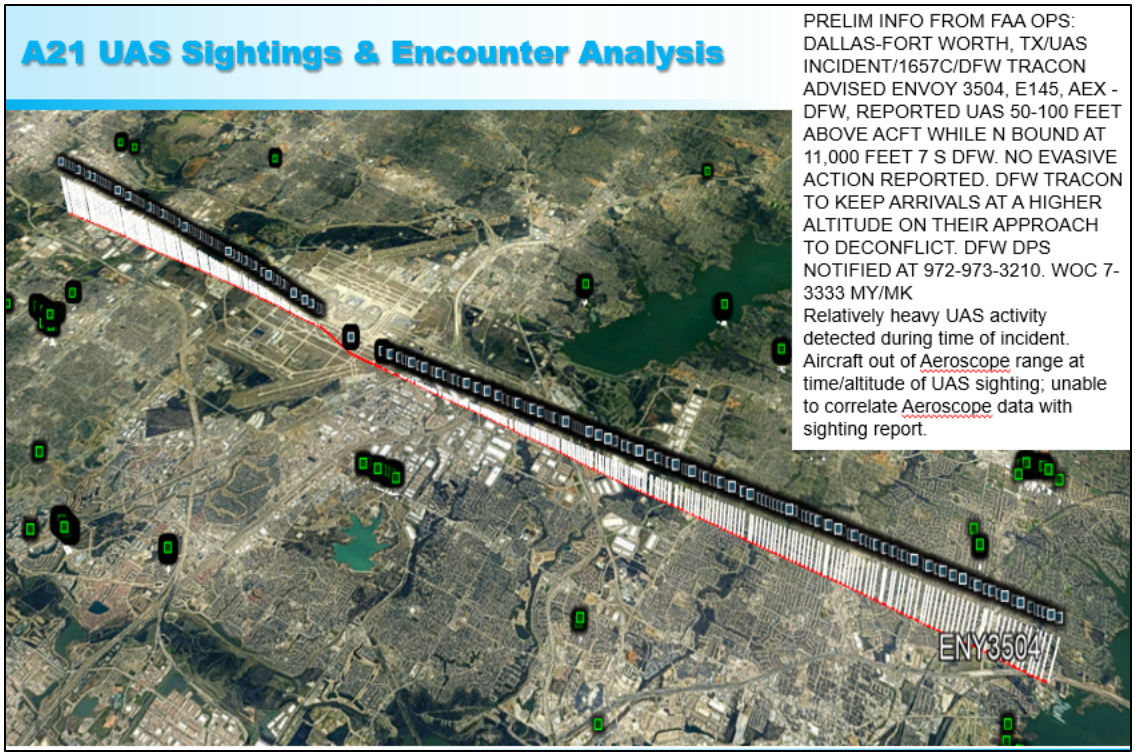

Figure 3. sUAS (green boxes) detection using Aeroscope data illustrating data available regarding the locations of sUAS in the airspace at a given point in time

N998GB 20200628 2350Z

- PRELIM INFO FROM FAA OPS: DALLAS, TX/UAS INCIDENT/1753C/DALLAS TRACON ADVISED N998GB, CESSNA C560, REPORTED A QUADCOPTER FLEW RIGHT OVER TOP OF THEM WHILE W BOUND AT 2,500 FEET 3 S ADDISON ARPT, DALLAS, TX. NO EVASIVE ACTION TAKEN. DPS NOTIFIED AT 972-973-3210. WOC 7-3333 PM/MY
- Nearest UAS (MavicPro) 1.1 NM from aircraft trajectory at 98 ft AGL; highly unlikely UAS flew overhead aircraft as reported

Figure 4. Illustration of data available to evaluate the location of an sUAS relative to a named aircraft (sUAS is shown as green box)

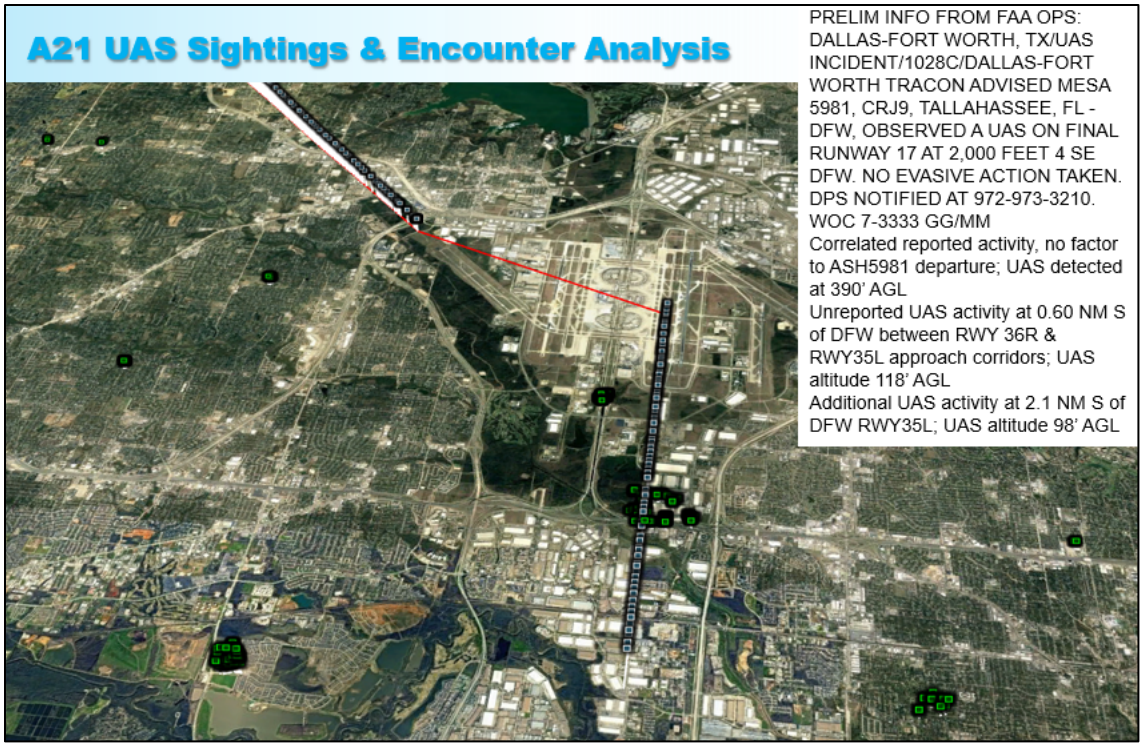

Figure 5. Illustration of data indicating sUAS activity in the vicinity of approach airspace for DFW and a correlation between an ATC sighting report of an sUAV and a manned aircraft (sUAS are shown as green boxes)

Figure 6. Additional illustration of data available to evaluate the location of an sUAS relative to a sighting report for a manned aircraft (sUAS is shown as green box)

Note that those analyses that require access to sUAS trajectory data can't be applied across the entire NAS, as they require access to Aeroscope data or the equivalent and are not universally available. However, since the goal in this context is to monitor for certain types of events in order to assess the adequacy of the framework and its assumptions or to assess the quality of the data submitted in waiver requests, any such data that is available is useful.

Finally, regarding the question of what data is sufficiently reliable to use as the basis for evaluation of the framework, preliminary analyses indicate that the objective data based on the correlation of Aeroscope and ADSB-out data raise questions about the validity of many sighting reports. (This issue will be addressed in greater detail in a future ASSURE report.) A preliminary study by ERAU to assess the validity of sUAS sighting reports at DFW by comparing aircraft telemetry against sUAS detection telemetry provided the following results:

- 288 sUAS sightings reports occurring at DFW from Jan '18-Dec '20 were evaluated
    - 65 cases were removed as they were outside of sUAS detection sampling timeframe.
    - 104 cases were removed as they were outside of sUAS sampling range (~13.5 miles from DFW max)
    - 72 cases removed; inadequate data available for assessment
- 47 total case studies evaluated; 2018 (4); 2019 (17); 2020 (26)
- General Findings
    - *Only 4 cases (8.5%) able to be positively correlated to detected sUAS activity; no cases presented a threat to reporting aircraft due to altitude or lateral separation.*
    - No noted sUAS in position described by sighting report (48.9%).
    - Sighting occurred outside Aeroscope range (29.8%).
    - Inadequate ADS-B data to make determination (6.4%).
    - Inadequate Aeroscope data available.
    - Incorrect time correlation between Aeroscope/ADS-B data (2.1%).
    - Uncorrelated sUAS activity that was not factor relative to aircraft trajectory (2.1%).

Such results suggest the value of using Aeroscope data in combination with ADS-B data (along with other data sources such as FAA accident reports) rather than sightings data in order to monitor for evidence that there are concerns with the application of the framework or to inform the approval certain types of sUAS operations more generally. (Note that such analyses could be applied more broadly to identify instances of concern regardless of whether there was any associated sighting report.)

3.1.6.1 SRMP Step 6. Process Monitoring – Summary. Step 6 is included in the overall framework to emphasize the point that assumptions regarding such things as the definition of equivalence classes need to be validated over time in order to refine the application of the proposed framework. Data are available for this purpose and should be collected and evaluated relative to the goal of this step in the proposed SRMP framework.

3.2 Additional Considerations

3.2.1 Bayesian Framework vs. Classical Statistics

Classical statistics have been incorporated into the calculations in this example analysis in a limited role (calculating a confidence interval for the probability of an sUAS failure given previously available data and calculating the confidence interval for the probability of a parachute failure

given previously available data). These confidence intervals have been used to inform the prior distribution on hazard causes. However, the framework is primarily based on Bayesian statistics.

As a way to produce converging evidence on the validity of the estimates of the posterior probabilities, it would be useful to look at the estimates based solely on the use of classical statistics. This approach could also offer a complementary framework for quantifying the safety risks associated with a given proposed sUAS flight operation.

A quick analysis using classical statistics, which merits further consideration to refine the methods and provide converging evidence, provides the following approximate comparison of results:

With No Parachute

Probability of impact on pedestrian (sUAS hitting pedestrian without benefit of parachute) =
Classical Statistics: 0.00001

Bayesian Framework: 0.00003

With Parachute

Probability of impact on pedestrian (sUAS hitting pedestrian without benefit of parachute) =
Classical Statistics: 0.0000005

Bayesian Framework: 0.0000005

3.2.2 Data Collection – Additional Factors to Consider

The example discussed earlier illustrated a framework for quantitative risk assessment for sUASs focusing on the use of flight operations (data from test sites or actual operations) to evaluate the risk associated with the following hazard causes: i) deviation beyond specified limits on the planned (three-dimensional) trajectory, ii) loss of power, iii) loss of propulsion, or iv) loss of communications (C2 link) with either or both of the PIC workstations. The set of potential hazard causes to consider could be expanded as desired within this framework.

For the flight operation used in this example operation, the PIC has proposed a flight distance of 5 km. Therefore, to test the enroute portion of the proposed operation, the flights used to estimate the prior distribution on hazard cause likelihoods needs to be restricted to prior flights (at test sites or in actual operations) of 5 km or longer. A method to include flights as data that have flown distances other than 5 km could potentially be developed by considering the sum of the distances flown by the set of test flights.

To estimate the prior distribution on hazard cause likelihoods for the enroute stage, each such flight is coded as a 0 if there is no failure associated with any of the hazard causes or a 1 if one or more of the hazard causes occurs. The prior distribution on hazard causes for takeoffs and landings would be coded similarly (0 or 1), except that the requirement for an included flight to have an enroute portion of 5 km is removed.

Deviation beyond specified limits on the planned (three-dimensional) trajectory is similarly coded as a 0 or 1 based on whether or not a flight exceeds the specified limits for conformance to the 3D trajectory at any point in its flight during the takeoff, enroute or landing stages (trajectory conformance). The conformance limit is set based on data regarding the 3D control accuracy of the sUAS and the accuracy of the GPS signal. (To make use of available FAA performance

statistics, we assume the observed altitude and horizontal position for a flight is measured using GPS values.) For our analysis, we assume that the PIC has proposed a conformance limit of 10 meters laterally and 15 meters vertically (above and below) to separate the flight vertically from the highest obstacle on the ground, as well as to separate it vertically from any of the PIC's sUASs traveling in opposite directions and from helicopter operations.

We further assume for the purposes of illustration, that the absolute value for the maximum lateral deviations observed on the 3100 flights considered in the waiver request analysis had a range of 0.1-2.0 meters. And we assume that the absolute value for the maximum vertical deviations observed for the 3100 flights considered in the waiver request analysis had a range 0.5-2.6 meters.

FAA statistics indicate the 99.99999 % confidence limit for accuracy of altitude estimates provided by GPS signals is approximately 8 meters (see Figure 7). Even if we assume that the GPS signals were off by the 99.99999% confidence limit of 8 meters, this leads to coding conformance for altitude for all 3100 flights as a 0 (meaning that all of the flights had a maximum absolute altitude deviation less that the proposed conformance limit for altitude of 15 meters), as with this assumption all of the flights had absolute deviations less than 8 meters + 2.6 meters.

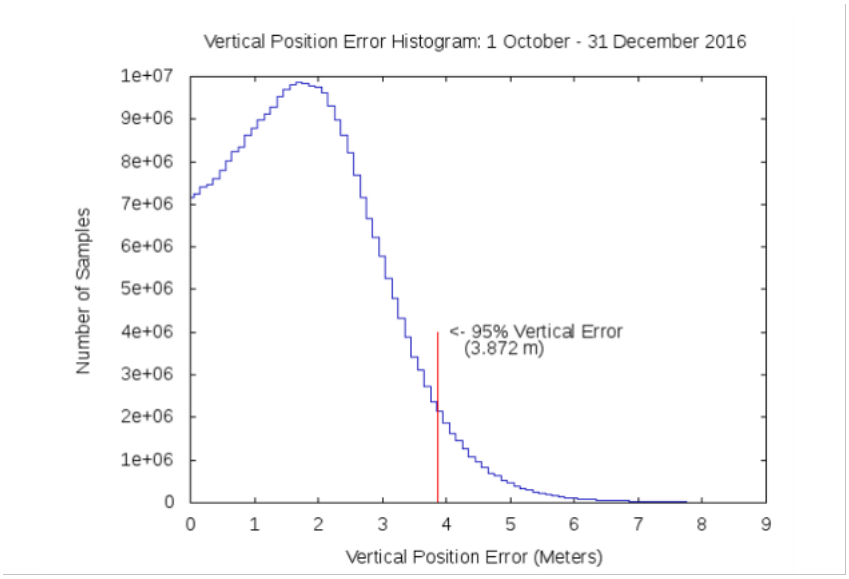

Figure 7. Vertical position error (meters) (from page 22 of https://www.nstb.tc.faa.gov/reports/PAN96_0117.pdf.

FAA statistics further indicate that the 99.99999% confidence limit for accuracy of lateral (horizontal) location estimates provided by GPS signals is approximately 7 meters (see Figures 8-9). Even if we assume that the GPS signals were off by the 99.99999% confidence limit of 8 meters, this leads to coding conformance for the absolute horizontal deviation for all 3100 flights as a 0 (meaning that all of the flights had a maximum absolute horizontal deviation less that the proposed conformance limit for horizontal position of 10 meters), as with this assumption all of the flights had deviations less than 7 meters + 1.2 meters.

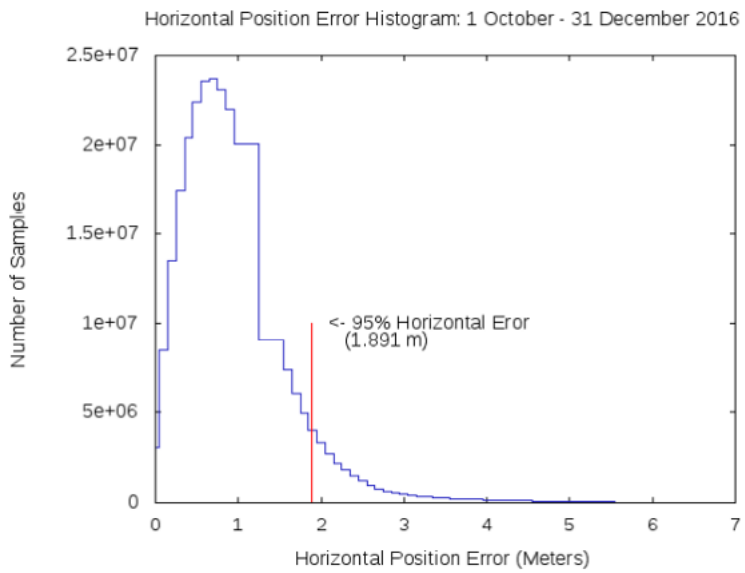

Figure 8. Horizontal position error (meters) (from page 22 of https://www.nstb.tc.faa.gov/reports/PAN96_0117.pdf.

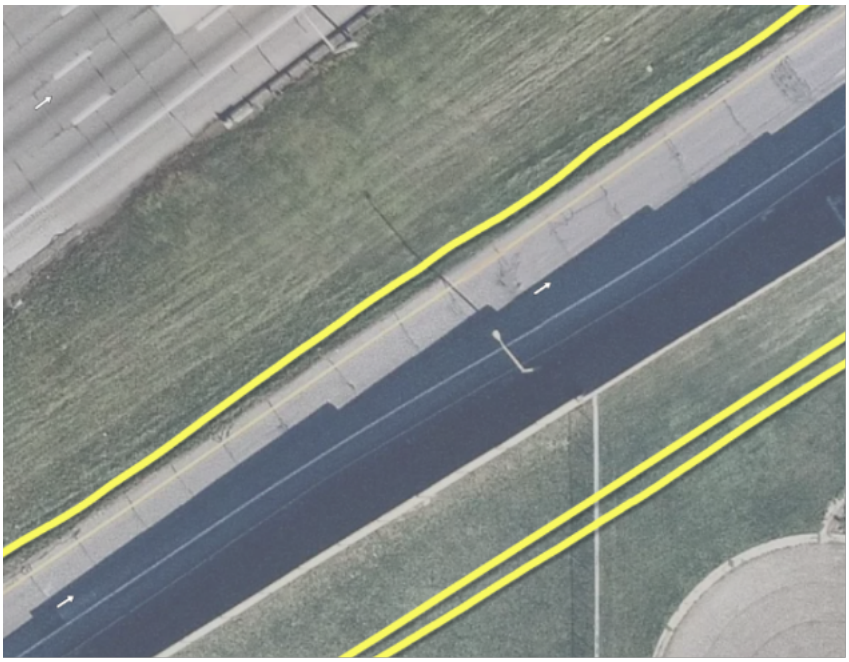

Figure 9. Sample display of actual flight trajectories.

The same approach applies for estimating the prior distribution on failure of the parachute. Each test result is coded as a 0 if the parachute functions properly or a 1 if it fails. In our example analysis we assume that there are data for 1000 from prior tests of parachutes in the same equivalence class. For illustrative purposes, the example analysis assumes all parachute tests were successful.

3.2.3 Software V&V Requirements

The framework for risk assessment presented earlier focuses on an approach utilizing flight data to assess risk in a quantitative manner. However, there are additional safety-critical hardware and software evaluations that need to be completed to fully evaluate the risks associated with the use of a particular sUAS. These evaluations fall into the category of hardware and software verification and validation requirements and, as such, require documentation of an appropriate software architecture that minimizes dependencies across safety-related functions in order to avoid a combinatorial explosion of possible interactions, as well as an appropriate set of simulation and bench tests. They also include evaluation of computer-human interactions in terms of functionality and interface design from a human factors perspective for the full range of relevant use cases, helping to ensure that the PIC can effectively fulfill his role as a safety net.

We assume these required evaluations are specified as part of the definition of the waiver approval process for the sUAS and therefore are complementary requirements to accompany the quantitative risk assessment as defined by our framework that is based on flight operations. One approach would be for the FAA to specify and conduct an approval process to ensure adequacy of the verification and validation process for a specified list of required automated safety nets or, if the UAS will be close enough for direct of remote observation by the PIC(s) of its route and status, a specified list of the required manual safety nets. Another approach would be for the FAA to specify the required automated and/or manual safety nets and to indicate that an approval request must include documentation that the requirements defined in a specific standard for ensuring software dependability have been met. An example might be ASTM F3201-16 (Standard Practice for Ensuring Dependability of Software Used in Unmanned Aircraft Systems (UAS)).

Note that, as a third approach, since FAA certification is currently limited to Part 135 operations (FAA 2020), if the FAA does not choose to require documentation regarding the adequacy of the required automation and/or manual safety nets based on some form of validation and verification, then this aspect of waiver approval would have to be based on the assumption that flight data has been collected that demonstrates sufficiently high reliability of the sUAS and any associated mitigation such as a parachute, and is therefore considered satisfactory for approval without requiring additional documentation demonstrating additional verification and validation of the automated and/or manual safety nets.

Note also that the validation and verification of the software could potentially be based on simulations and bench tests that include evaluation of the triggers and responses to all of the safety nets embedded in the software. This includes testing the sensors that trigger and activation of the kill switch if the system state is estimated to satisfy any of the prescribed kill criteria, including i) deviation beyond specified limits on planned (three-dimensional) trajectory, ii) loss of power, iii) loss of propulsion, as well as evaluation of the triggers and displays for the associated alerts to the PIC.

It also includes testing of the transfer of control between the two PICs and the functioning of the sensors that detect loss of communications (C2 link) with the controlling PIC workstation, as well as testing the response of the automation when this condition is met. This response involves making an assessment of whether or not the sUAS can safely reach the launch pad, the landing pad, or any of the alternate sites and diverting to the nearest pad if such a pad is estimated to be reachable, or initiating the kill switch if not. Note again that this functional requirement focused

on manual safety nets could not be included if the sUAS is expected to fly a route that takes it beyond the limits for the communication between the sUAS control station and the sUAS. In that case, sole reliance would have to be placed on the automation as the safety net when flying beyond communication limits and has implications for required verification and validation of the automation. Even when this is the case, however, the functional requirement for manual interventions could remain in effect when the sUAS is in the vicinity of the takeoff/landing pads.

Finally, we assume the verification and validation process specifies any architectural requirements for the software as well as necessary software verification and validation assessments in order to evaluate Detect And Avoid (DAA) software if such a capability is required for sUAS by the FAA, as the software to support DAA will be much more complex than for other safety nets.

In short, the assumption is that, for a waiver request for such a BVLOS flight operation over people, in order for a sUAS waiver request to be approved, such FAA requirements for verification and validation of the automation and/or manual safety nets need to be successfully met, in addition to successfully meeting the decision criteria specified by the assessment framework illustrated in this report that is based on flight tests. In addition, the FAA may specify additional criteria that must be met for waiver approval, such as the documentation of an adequate SMS process (see Appendix A.)

3.2.4 Mitigations and Safety Nets

The framework illustrated in the example described earlier evaluates the safety of the proposed operation based on performance when operating under the control of the sUAS automation alone, and with the added mitigation of a parachute. However, in that example the automation also has built-in monitoring functions that can be triggered in response to: i) deviation beyond specified limits on the planned (three-dimensional) trajectory, ii) loss of power, iii) loss of propulsion, iv) loss of communications (C2 link) with either or both of the PIC workstations. (Additional triggers could be added beyond those included in this example, such as detection of a sensor or actuator failure.) These automated safety functions represent a safety net reducing risk beyond that calculated based on flight data.

The sUAS PICs provide a further, proactive safety net based on their responsibility to evaluate weather conditions (actual and forecast winds, convective weather and icing conditions), perform pre-flight checks, act as visual observers during takeoff and landing and, as necessary, to cancel a flight. And, either in response to an alert from the automation or on his own initiative, the sUAS PIC can instruct the automation to kill the power and electrical systems or direct the sUAS to hover or divert. Thus, the ability of the PIC to intervene represents an additional safety net over and above the quantified level of risk based on flight tests associated with operation by the automation alone. And, beyond just the definition and training of the PIC regarding his responsibilities, the SMS process overall provides a safety net with its requirement for systematic procedures, practices, and policies to manage safety risk.

Other proposed procedural safety nets also increase safety. First, by operating sUASs from the supply center to the hospital at 350 feet AGL and sUASs from the hospital to the supply center at 250 feet AGL with a 15 m horizontal offset, the risk of a head on collision by the sUASs flying for this flight operation is managed.

Second, since the sUASs plan to fly within narrow 3D corridors below 400 feet, they are below the normal enroute altitudes flown by helicopters and, for this proposed operation, are not in the vicinity of any airports. To deal with the takeoff and landing of helicopters: i) the landing/departure pads for the sUASs could be sited at a distance from any landing/departure pads for helicopters; ii) landing and takeoff patterns for helicopters for arrivals and departures of helicopters from established landing/departure pads (at the hospital, for instance) could be defined such that they do not cross the 3D corridors used by the sUASs; iii) NOTAMs could be published informing all relevant traffic of the location of the 3D corridors used by the sUASs. Note that if there are larger-than-small VTOL vehicles temporarily operating on an ad hoc basis below 400 feet, such exceptions would have to be managed by reliance on DAA safety nets.

Third, the operation described earlier conservatively defines the routes for the 3D corridors for the sUASs such that they are a safe distance from the area where there could at times be a dense collection of people (the urban park) and provides pre-planned alternative landing sites as contingencies.

Finally, if the protections provided by the software and the PIC should fail and a fly-away does occur, contingency plans should provide procedures under which the PIC contacts ATC for assistance to help ensure that other manned aircraft are not in jeopardy.

3.2.5 After-the Fact Reactive Measures

After-the-fact performance analyses provide an additional safety net to help protect against an inadequate definition of an equivalence class, and indeed more broadly to protect against the possibility that the data used for the risk assessment were not sufficiently representative of actual performance within that equivalence class (noisy data). This protection is reactive, however, as it relies on the analysis of reported incidents and accidents and on the analysis of flight data after flights have been completed.

3.2.6 Specification of the Decision Matrix

The decision matrix shown in Figure 1 was used for illustrative purposes to indicate how probabilities can be combined with consequences in order to evaluate the level of risk associated with a proposed flight operation. The FAA would need to determine the final definition of the categories illustrated in this matrix and assign risk categories.

As a comparison, as a benchmark to consider in defining these risk categories, in 2016 there were approximately 108 accidents out of 5,942,584 general aviation flights, with 29 fatalities[4].

3.2.7 Criteria for Classification as a De Minimus Risk Operation with Insurance Requirements

Keeping in mind that the decision matrix above is meant to be illustrative only, none of the columns in the table above are green (LOW risk) for all categories of probability. With this in mind, one approach to defining conditions under which an operation does not require a waiver approval for

[4] See https://download.aopa.org/hr/Report_on_General_Aviation_Trends.pdf and https://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=21274.

a BVLOS operations over people would be to specify that the consequence has to be categorized as Insignificant or Minor while also meeting the following conditions:

- Either:
    - The FAA has certified the hardware and software for the sUAS and any intended mitigations (such as a parachute), including the support provided by USS contractors, based on new certification requirements for sUAS software verification and validation to assure safety during operations controlled by the automation.
    - Data that has been collected that indicates the high reliability of the sUAS and any associated mitigation such as a parachute is considered sufficient for approval; or
    - Each waiver approval has to provide documentation indicating sufficient validation and verification of required safety nets.
- Documentation of an SMS process consistent with FAA requirements. (See Appendix A for an example of possible components of such a process.)
    - This process must include documented maintenance, preventive maintenance, alterations, or inspections performed in accordance with specific requirements in the final FAA rule for sUAS flights.
    - The PIC operating the sUASs must have successfully completed the FAA Remote Pilot knowledge test.
- Insurance coverage.
- Documentation available upon inspection that the quantitative framework for risk assessment based on flight operations illustrated earlier has been applied and has resulted in classification of the operation in terms of LOW risk with Minor or Insignificant consequence as defined in the decision matrix.

Note that this process requires that the FAA provide a clear definition of how an operation should be classified in terms of the consequence categories in the decision matrix.

4. CONCLUSION

The example detailed in this report provides a concrete illustration of the refinement and application of the risk-based framework developed in the A21 Task 3-1 report, "Definition of Risk-Based Framework". This example focuses on the use of flight tests to evaluate the safety risks associated with automated control of an sUAS that flies BVLOS over people.

The safety analysis focuses on the risk associated with a fully automated operation, with the assumption that the safety nets embedded in the automation, along with the ability of the PICs to manually activate these safety nets within the automation, and along with other procedural controls, provide an additional layer of safety beyond that provided by the automation alone as protection against potential brittleness of the technologies and of the PICs in their limited roles (Smith, 2018).

The risk-based framework that is illustrated incorporates a blend of classical and Bayesian statistics. Several key requirements are included and are illustrated using a concrete example of a proposed sUAS operation. In order to reduce the burden of data collection for any one waiver applicant, one requirement this framework describes is the designation of an authoritative source to collect, store and disseminate the results of previous flight operations for specific models of

sUASs, and for an equivalence class consisting of parachutes that meet the requirements of the ASTM standard for sUAS parachutes (or some equivalent standard that is acceptable to the FAA). This authoritative source is charged with collecting data on previous flight tests or actual operations using a particular sUAS model, as well as data on previous tests of sUAS parachutes.

The concept of data pooling and the definition of equivalence classes are two important aspects of this framework. The use of classical statistics to calculate confidence intervals and use them to inform prior distributions for the probabilities of hazard causes and outcomes is another.

A Bayesian framework is then used to guide calculations that consider these prior distributions, along with additional data collected by the sUAS waiver applicant. These calculations provide estimates of the expected values for posterior probabilities that can be used to guide decision making.

These posterior probabilities can be calculated for a sUAS with or without a parachute. They can then be used for an assessment of safety risk based on the data regarding flight performance and parachute performance. The posterior probabilities to support decision making as illustrated in this example when assuming the sUAS has a parachute are:

Probability of impact on pedestrian:	0.0000004812
Probability of impact on built environment:	0.0000160391

Using these estimates of the posterior probabilities as input for consideration within a Decision Matrix (see Figure 1) leads to the following conclusion to help guide decision making in this example:

> With a parachute, the operation is classified as LOW risk in terms of safety risk for both pedestrians and the built environment.

The example notes, however, that while this framework provides a methodology for a quantitative risk-based safety assessment based on objective data regarding sUAS flight performance and parachute performance, there are other components of the decision making broader SRM process that also need to be considered:

- Compliance with Category 4 of RIN 2120–AK85. Operation of Small Unmanned Aircraft Systems Over People (amendment of Title 14 of the Code of Federal Regulations part 107 (14 CFR part 107) by permitting the routine operation of sUAS at night or over people under certain conditions).
- Verification and validation of hardware and software supporting the safety functions integrated into the automation in order to demonstrate compliance with FAA certification requirements for automated flight control in BVLOS operations over people, including human factors design requirements. (Such certification requirements need to be further defined.)
- Documentation of an effective safety management system as an additional safety net.
- Proof of insurance.
- Continued demonstration of safe operations once a flight operation has been approved and is ongoing.

4.1 Future Research Needs

The Bayesian analysis based on the use of Dirichlet probability distributions when a parachute is included makes certain assumptions that, in this example, lead to conservative estimates. These assumptions need to be further evaluated in order to improve the accuracy and generality of the estimation process. In addition, the informativeness of the final results would benefit from calculation of confidence intervals for the output of the calculations (probability of impact on pedestrians and probability of impact on the built environment).

In addition, while the decision matrix used in this example supports a concrete illustration of the application of this risk-based decision process, the categorizations used for Probability and for Consequences may or may not be appropriate for decisions focused on sUAS operations. Thus, while the use of the decision matrix is an important part of the framework, the definition of the categories within that matrix merit investigation.

Additional research needs to address:

- Understanding the advantages and disadvantages of using of a Bayesian framework vs. using a framework based on classical statistics (or using both to provide converging evidence).
- Defining a methodology based on classical decision analysis for evaluating the trade-offs between the costs and benefits associated with a proposed sUAS operation.
- Determining how to calculate the number of samples (both the number of flight tests and the number parachute tests) that the waiver applicant should collect in order to achieve a desired level of statistical power.
- Defining the data that should be collected and the statistics that should be calculated in order to monitor the actual flight performances of approved operations (data analytics) as a reactive safety net to determine that operation by a particular PIC needs to be suspended, that the certification of a particular set of hardware and/or software needs to be suspended, or that some aspect of the approval framework illustrated earlier needs to be revised. This latter response could involve modifying the framework itself, or it could involve reassessing the quality of the data used for approval of a particular operation or collection of operations.
- Determining reasonable assumptions for defining equivalence classes, considering the significance of such factors as winds, UAS speed, GPS reliability and the verification and validation of USS service reliability.
- Designing an effective and easy to use dashboard to inform decision makers regarding the results of the reactive data analyses described in the bullet above.
- Defining a methodology for combining data from flights traveling different enroute distances.
- Developing more sophisticated ways to estimate the probability of the impact of a falling sUAS on pedestrians and on the built environment.
- Defining a test for homogeneity of the data from different PICs in order to detect outliers.
- Describing the process if there are no prior data.
- Providing a “cookbook” description of how an applicant can easily apply this quantitative analysis of safety risk based on flight operations and parachute tests, perhaps in the form

of a website that supports incorporation of this quantitative framework for risk assessment into the development of a waiver request.

Finally, it should be noted that a possible variation on this example would be one where:

- An sUAS manufacturer has done the work to gather the necessary data (from the pooled data source providing data on previous flights and from additional flight tests).
- This manufacturer has completed the necessary computations to specify the data-driven estimation of the probability that this specific sUAS model could experience one of the 4 hazard causes and fall toward the ground.
- The manufacturer has packaged these results for inclusion in a waiver request prepared by a flight operations organization.

The manufacturer could similarly pre-package the results of an analysis of data based a parachute tests when the parachute is used in association with a specific sUAS model.

5. ACKNOWLEDGEMENTS

We appreciate the support from Ryan Wallace and Tracy Lamb (Embry Riddle Aeronautical University) in providing an analysis of Aeroscope and ADS-B data and in producing the information in Appendix A on Safety Management Systems, as well as input from Mark Askelson (University of North Dakota), regarding the accuracy of GPS.

6. REFERENCES

Ahn, J., & Chang, D. (2016). Fuzzy-based HAZOP study for process industry [Hazards Effects Management Process (HEMP) Risk Assessment Matrix]. Journal of hazardous materials, 317, 303-311.

ASTM (2018). ASTM F3322-18, Standard Specification for Small Unmanned Aircraft System (sUAS) Parachutes, ASTM International, West Conshohocken, PA, 2018, www.astm.org

FAA (2017). https://www.nstb.tc.faa.gov/reports/PAN96_0117.pdf#page=22

MITRE (2018). (https://www.mitre.org/sites/default/files/publications/pr-18-1364-modeling-risk-based-approach-for-small-uas.pdf).

National Academies of Sciences, Engineering, and Medicine (NASEM) (2018). Assessing the Risks of Integrating Unmanned Aircraft Systems (UAS) into the National Airspace System, National Academies Press.

Smith, P. J. (2018). Making brittle technologies useful. In P.J Smith and R.L. Hoffman (eds). Cognitive Systems Engineering: The Future for a Changing World. Boca Raton, FL: CRC Press, 181-208.
https://www.researchgate.net/publication/346405624_Making_Brittle_Technologies_Useful

FAA Order 800.369C, "Safety Management System", June 24, 2020.
https://www.faa.gov/regulations_policies/orders_notices/index.cfm/go/document.current/documentNumber/8000.369

FAA Order 8040.4B Safety Risk Management Policy, May 2, 2017.
https://www.faa.gov/documentLibrary/media/Order/FAA_Order_8040.4B.pdf

APPENDIX A.

PROBABILISTIC RISK MANAGEMENT THROUGH SMALL UAS SMS FRAMEWORKS: AN OPERATIONAL ASSESSMENT CHECKLIST

Tracy Lamb

Embry Riddle Aeronautical University

Predictive risk management as part of a proactive safety culture is one of the most challenging concepts for operators of small commercial UAS to master (AUVSI, 2019; Lamb, 2019; 2021). Primarily, safety relies upon a complex web of latent factors that are 'unseen' within the organization and operation, making them difficult to identify and measure (Reason, 2016). Safety is often judged by what does not happen, as much as what does happen (Levenson, 2015; Stoop & Dekker, 2012); the invisible causes of safety threats hold the key to probabilistic risk management, often referred to as *leading indicators* (Lamb, 2021; Levenson, 2015; Silver, 2012). A small commercial UAS operator's most powerful tool to track the many observable factors contributing to safety performance is the Safety Management System (ICAO, 2018; Lamb, 2019, 2021; Stolzer et al., 2015). However, an operator of sUAS may not be familiar with industry or regulator's guidance on SMS, or how to apply those concepts to their operations. The international Civil Aviation Organization has captured the relevant and practical information from years of SMS development for these UAS operators and presented this in a simplified UAS Toolkit which can be accessed on the website (ICAO, 2021). The toolkit is designed to assist UAS pilots, and the organizations they operate for; therefore, this a high-level operational checklist is designed to support SMS for operators of small commercial UAS irrespective of the size the of the UAS operation[i].

Safety is described by the International Civil Aviation Organization as "A systematic approach to managing safety, including the necessary organizational structures, accountabilities, responsibilities, policies, and procedures" (ICAO, 2018, p viii). The FAA national policy on SMS states that Safety Management System consists of four foundational pillars; Policy, Risk Management, Safety Promotion, and Safety Assurance (FAA, 2021; FAA, 2016). Although all pillars of the SMS are interdependent, small commercial UAS operators are required by best practices and regulations in some countries to commit to each of the pillars' activities to have a workable SMS. This checklist framework for SMS has been developed from industry and government subject matter experts during the AUVSI Trusted Operator Program initiative to assist operators in developing their own compliance with SMS guidelines, industry best practices, and standards. The Commercial Unmanned Aircraft Systems SMS Checklist

This checklist has been adapted from over 300 industry standards, and government SMS guidance to provide and support commercial UAS operations in predictive and proactive risk assessment and encourage a proactive safety culture (AUVSI, 2019; Helmreich et al., 1999). The checklist elements have been developed from International Organization for Standardization, 2009. ISO 31000:2009(E), the FAA SMS guidance, and the ICAO quality, safety, and risk management standards and best practices (FAA, 2021; 2015, 2016; ICAO, 2008, 2009, 2013, 2018). Like within the business aviation field, industry associations and standards bodies continue to contribute valuable safety standards, tools, and programs to UAS safety. One of these initiatives includes the Trusted Operator Program™ (TOP), which was developed by the Association for Unmanned

Vehicle Systems international along with 192 industry and government experts to incorporate FAA guidance in addition to over 300 industry standards and best practices for small commercial UAS (AUVSI, 2019).

This checklist framework is an internal operation assessment guide to assist commercial UAS operators in identifying recommendations and deficiencies relevant to ICAO Safety Management Systems guidance, industry standards and best practice, and FAA voluntary SMS elements, including essential aspects of risk management, including how to best equip the operator for emergency preparedness, and the requirements to support BVLOS and operations over people(Alexander, 2015; AUVSI, 2019; Brady, 2003; FAA, 2021; 2015; FAA, 2016; FAA, 2020; Renner, 2001).

This checklist is an internal operations assessment guide to assist commercial UAS operators in identifying recommendations and deficiencies relevant to ICAO Safety Management Systems guidance, industry standards and best practice, and FAA voluntary SMS elements, risk management and emergency preparedness.

UAS OPERATOR DETAILS	
Company / Operator:	
Operation location/mission:	
Contact person:	
Contact details:	
KEY / MANAGEMENT PERSONNEL	
Accountable Manager	
Chief Pilot / Controller	
Safety Manager	
Maintenance Controller	
Deputy Chief Pilot /Controller	
Safety Officer	
REMOTE PILOTED AIRCRAFT(RPA) STATISTICS	
UAS Fleet No. & Type	
Major UAS Accidents Last 5 Years	
Major OH&S Incidents Last 5 Years	
INSURANCE PROVISION	
Third Party/Combined/Liability Insurance coverage	

1. Safety Management System

POLICY & STRUCTURE		ORGANISATION & ACCOUNTABILITIES	
Policy Statement		Designated UAS Aviation Safety Officer/Manager	
Formal Safety Management System		Safety Team / Committee Structure	
Objectives and Strategies		Defined UAS Accountabilities and Responsibilities	
Safety Plan/Targets		UAS Aviation Safety Training	
Documented SMS (Manual)		Maintenance Management Involvement	
Culture and Awareness			
SAFETY MANAGEMENT PLAN		**REVIEW PROCESS**	
Regular Meetings		Safety performance monitored	
Dissemination & closeout		Internal Safety Audit Program	
Confidential Reporting Mechanism		Safety Database (Manual or Electronic)	
Incident/Accident Reporting Process		Case by case risk assessment process	
Incident Reporting and Follow-up		Management Review (Accountable Manager involvement)	
Safety Event Trend Monitoring		Follow Up Process	
Remedial Action Plan		Alignment with ICAO UASMOS	
Risk Assessment Process			
ACCIDENT / INCIDENTS REPORTING		**RECORDS**	
Regulatory Body Involvement (CAA,CASA, FAA, HKCAD)		Occurrence Reports Reviewed	
Defined responsibilities		Review of accidents/incidents in last 5 years	
Requirement to report accidents/ incidents		All Accidents/Incidents adequately recorded	
Safety Management / Officer Involvement		Review and follow-up	
ERP – Regularly exercised and reviewed		Use of database	
Trend analysis			
RECOMMENDATIONS			
DEFICIENCIES			

2. Flight Operations Quality Assurance

UAS ORGANISATION			
Operations QA Policy		Reporting chain/function	
Part of QA Department		No conflicts of interest	
Responsible Manager		Ops QA Manual/Procedures Defined	
CONTROL SYSTEM			
Audits by Head Office		Audits to Plan & Recorded	
Internal Audit Plan		Findings Recorded	
Internal Audit Plan Schedule		Audit by third party	
REVIEW PROCESS			
Management Review		NCR Follow Up Process	
Internal Ops QA Reviews		Ops QA Manual Review	
RECOMMENDATIONS			
DEFICIENCIES			

3. Flight Operations Management and Operations Manual

OPERATIONS AREA		AIR TRAFFIC & CAA COMPLIANCE	
Space & Staffing adequate		ATC Arrangements Approvals	
Crew Scheduling arrangements		NOTAM & Operations awareness	
Post Flight Documentation (inc batteries)		Radio procedures (if applicable)	
Flight and Duty Records		Search & Retrieval capabilities	
Operational notices to crew		Contingency Planning	
FLIGHT PLANNING		**OPERATIONAL PROCEDURES**	
General area information		Standard Operating Procedures (SOPs)	
Proximity to Airfield & Heliport Data, Alternate Landing areas		Two crew / Three operations	
Weight, balance and load sheet data		Crew Briefing including observers	
Performance, payload and fuel / battery calculations		Detect & Avoid Precautions, procedures	
Flight Planning Process (feasibility, Risk assessment, JSA)>		Stabilised approach & landing area criteria	
Meteorological Information (including wind measurement)		Landing and take-off area markers	
NOTAMs		Collision Avoidance procedures/functions	
RPA TYPE SECTION			

Technical data (recorded in OM)		Normal checklist	
Variations or approvals required		Abnormal checklist	
Performance data		Emergency checklist	
Serial number / registration /fire plate		Quick reference Handbook (QRH)	
OPERATIONS MANUAL CONTENT		**OBSERVERS, CREW & SECURITY**	
Terms of Reference		Cyber and other Security process	
Accountabilities		Observer training & briefing	
Operational policies		Battery handling and protection	
Amendment status/lep		Dangerous goods transport policy	
Type specific sections		Operational area procedures	
Training manual		Weather & temperature protection	
Specialised roles		Operational area Assessment	
Crew Health policies			
RECOMMENDATIONS			
DEFICIENCIES			

4. UAS Crew Training

TRAINING MANUAL		**TRAINING CHECK REQUIREMENTS**	
Designated Training UAS Pilots		BVLOS Rating	
Checked by Relevant CAA		Company Proficiency Check	
Initial Induction and recurrent training		Rating / approvals checks	
Training Manual Amendment Status		Night Flying approvals	
Training Process Observers		Post Absence Recency	
Adequate Training Hours		Emergency Procedures Check	
Other crew training including safety and support crew		Job specific checks (high risk inspections e.g. Power line inspection).	
QUESTIONNAIRES		**TRAINING RECORDS**	
Ops Procedures/Ops Manual		Scheduling & records	
Technical		Narrative Comment & Available to UAS crew	
Emergency equipment training		OH&S training	
ADDITIONAL TRAINING			
ERP Training (including equipment)		HUET/Sea Survival - BOSIET	
Dangerous goods Training (Lipo Batteries)		Wet Life Raft Drill	
CRM/ADM training		Technical Refresher	

UAS Safety and Risk Assessment Training		Fire Extinguisher/Smoke Drill	
Cyber and other Security		Conversion/Ground School	
First Aid		UAS Crew Maintenance Training	
UAS high risk environment TEM		Pilot & Crew daily inspections	
Other Training (specify)			
RECOMMENDATIONS			
DEFICIENCIES			

5. UAS controller skill and task evaluation

TASK DETAILS					
RPA Type		Date of Flight		Pilot/Controller	
RPA Reg. No		Number of flights		Observer & Crew	
RPA Serial No		Tot flight time		Certification Check	
UAS task type & location					

CONDUCT OF UAS FLIGHT TASK			
Flight Planning (JSA, Approvals, ATC)		Aircraft battery management	
Checklist usage & content (pre-despatch, pre-flight, toff & approach landing, pack up etc).		Control Station & component Battery management	
Take off / Landing area marking & planning		Software / Firmware updates valid	
Use & Suitability of Check-Lists		Use of Performance Data	
Knowledge of Emergency Drills & Alternates		Flight recording / running sheet	
Observer Briefing & Conduct		Observation of required Altitudes	
Confirmation wind, meteorological conditions		Performance monitoring	
Crew and Observers Briefings & Handling		Type, Accuracy & Technique of inspection (SOPs for high risk task)	
Detect & avoid procedures review		Approach Landing / alternate landing	

CRM in all Flight Phases		Checklist completion post operation	
Adherence to ATC Instructions (if applicable)		Pack up component checklists procedures	
RPA Handling		Airspace monitoring & awareness	
Handover/take over UAS Control procedures		Handover/takeover UAS observer	
POST UASTASK			
Completion of documentation/downloads		Observers & support crew debriefed	
UAS component Checklists complete		Retention of Post-Flight Documents	
OH&S recommendations observed for lifting		Event Register completed	
Maintenance issues recorded		Damaged parts recorded	
Battery log (defects) recorded		Maintenance entry made in log	
RECOMMENDATIONS			
DEFICIENCIES			

6. UAS Aircraft Documentation

RPA FLIGHT & TECHNICAL LOG			
UAS pilot/controller liaison/debrief		Discrepancies entered	
Technical Log content		Defects cleared	
Pre-Flight entries		Cert. of Maintenance Release or Equivalent	
Post-Flight entries		Battery Trend checks	
Battery log for Aircraft Utilised		Pre-flight specific to type recorded	
Battery log for Control unit utilised		Information transferred to Master Battery Log if required	
RPA APPROVALS / MODIFICATIONS		**AIRCRAFT / BATTERY LOG BOOKS**	
Master Status Lists		Aircraft/Engine Log Books inspected	
Controls Incl. Relevant CAA Monitoring		Cross References to Technical Log Entries	
Receipt and issue procedures		Modification List Complete	
Compliance Records		CAA signed off of modifications in req	

Master Battery log updated (if required)			
MAINTENANCE RECORDS		**DEFERRED DEFECTS**	
Record of work retained (>2 years)		Control of allowable defects	
Recording and signature		Quality assurance of genuine parts	
Back Up/disaster recovery for software		Control of allowable non-genuine parts	
Revision status/format		Adherence to Manufacturers guidelines	
Completed Work Entered Airframe/engine/ power plant Logs			
RECOMMENDATIONS			
DEFICIENCIES			

7. UAS Maintenance Quality Assurance

ORGANISATION		**QA MANUAL**	
Relevant CAA Approval		QA Policy defined in Operations Manual	
Maintenance Manager Approval		Terms of Reference	
Internal Quality Auditors		Quality Procedures	
Reporting Chain/Function		Review Process	
Conflicts of Interest (e.g. suppliers)		Amendment Status	
List of acceptable parts / suppliers		Protection against defective parts	
CONTROLS		**REVIEW PROCESS**	
External Audit by CAA, EASA, FAA		Management Review Board	
Internal Audit Plan (Frequency & Range)		Internal QA Review Meetings	
Compliance Monitoring		Contracts & Contractor/Supplier QA	
Random Quality Control Checks		Manuals, Procedures & Instructions	
Post Maintenance Release Checks		Software / Firmware protection	
Best practice monitoring			
QA TRAINING		**QUALITY RECORDS**	
Auditor Training		External Audit Reports	

Induction Training		Internal Audit Reports	
Recurrent Training		NCR/Follow-Up	
Maintenance / part defect training			
Part inspection training			
RECOMMENDATIONS			
DEFICIENCIES			

8. Maintenance & Part Management, Procedures & Training

MANAGEMENT		**CERTIFYING STAFF & CERTIFICATION**	
MCM/MPM/CMM content		Records complete and up to date	
Control of activities & effective communication		Authorisations defined & available to staff	
Certifying Staff		Authorisation doc. covers activities certified	
Responsibilities defined in MCM/MPM/CMM		Duplicate inspections/RII	
Personnel qualifications/experience appropriate		CRS issued by appropriately authorised staff	
Staff Numbers & Working Hours		CRS contains details of work carried out	
Work / Task / Shift handover procedures			
TECHNICAL LIBRARY, MANUALS & PROCEDURES			
Receipt/Issue control of manuals			
Master Amendment List (AL) & Accessibility			
Adequacy of Engineering Procedures/Tech Memos			
Type Manuals & Parts Catalogue			
Procedures - Relevant and Adequately descriptive			
Procedures - Readily available at workplace & fully cover work control			
Maintenance completed in compliance with schedule - sample			
RPA FLIGHT DATA MONITORING			
Procedures Manual detailing facilities, responsibilities, controls & organisation			
Manual - Include downloading, troubleshooting & maintenance procedures			

Thresholds defined. Analysis and trend monitoring procedures	
Included in MEL/OMEL with Operational Limitations	
Event reporting and system serviceability records	
Training plan and records for management, data interpretation & continuation training	
Data Management Plan	

MAINTENANCE AND RPA CARE TRAINING			
Policy & Programme in Place		Workshop/Overhaul	
Management Training		Recurrent Training	
Supervisor Development		Maintenance Manual updates	
Apprenticeship Scheme		Liaising with manufacture (updates)	
Type Ratings		Maintenance training records	

RECOMMENDATIONS

DEFICIENCIES

9. Maintenance Facilities, Equipment Planning & Storage

MAINTENANCE EQUIPMENT STOREAGE & FACILITIES			
Office - Management/Admin		Battery storage	
Avionics/Electrical Workshops		Battery support equipment (fire bags)	
Clean Workshops		Maintenance library	
Safety Equipment Area		Battery maintenance / safety area	
Location, Security & Segregation		Component segregation & storage	
Paint Shop		Test flight room / area	
No dangerous spills evident		Fire extinguisher	
Cleanliness & General Condition		Metal bin & water store for lithium battery fires	
Eyewash facility / First aid kit		General workplace HSE	
Tooling area (calibrated if required)		Flammable Storage	
Mobile Equipment		Fire control and testing regime	

RECOMMENDATIONS

DEFICIENCIES

10. RPA Inspection & Equipment Fit

RPA INSPECTION					
Type:		**Reg. No:**		**Year of Manufacture:**	
Date of Inspection:		**Serial No:**		**Hours:**	
				Supplier/Manufacturer	

EXTERIOR		RPA INTERIOR BAYS (if able)	
General external Condition		GPS connection wires	
Battery Fluid Leaks		Computer Data motherboard	
Control Surfaces, Rotor Blades		Wire connection servos	
Pitot Static vents		Corrosion or acid damage evident	
Lights (if fitted)		Camera / equipment connection or mounts	
Gimbals, connections, elastic tensions		Battery bay	
Undercarriage/Skids		Battery connections	
Flotation Equipment (if amphibian)		Internal leaks	
Automatic / Manual Activation Of Floats		Internal grease/lubricant	
Parachute hatch & bay (if fitted)		ELT (406, TSO C126 compliant, if required)	
Lock wire connections (corrosion)		Payload bay condition	
Hatch screws seated / condition		Transponder / Detect Avoid equip if fitted	
		EPGWS (sonar altimeter)	

RPA CONTROL STATION				DOCUMENTS & INFORMATION	
Type:		**Reg. No:**		**Year of Manufacture:**	
Date of Inspection:		**Serial No:**		**Supplier/ Manufacture:**	
General Appearance & Cleanliness				Flight Manual (electronic storage)	
Display type; FPV, Flight Plan Analogue/Glass/Apple/ Word				Weight Schedule	

Emergency power source		Operations Manual	
Emergency Equipment		Checklists - Normal/Emergency	
Radar Altimeter/ Sonar / GPS		Maps/Charts	
Set up for 2 Pilot Crew Operation		Approach Plates (as required by task)	
Weather info available?		Technical Log and modification checks	
Software / firmware update status		Certificates & Licences	
Cords / connections / leads		GPS Cards	
Control interface (joystick, keyboard)		Certificate of Airworthiness	
Emergency Land function		Certificate of Registration	
Return to land function			
Collision / Evasion function			
RECOMMENDATIONS			
DEFICIENCIES			

11. UAS transport and storage

RPA PARTS AND TOOLS STORAGE			
Stores Procedures Manual		Item location exercise	
Storage Areas and containers		Stock checks	
Storage of batteries		Adequate Spares Holding	
Controller Systems storage and log		Tools & Test Equipment	
Bogus / non génuine parts log			
RECOMMENDATIONS			
DEFICIENCIES			

12. Battery care & quality & safety assurance

STORAGE/DELIVERY SYSTEM			
Master battery log		Battery storage containers	

Batteries individually identified		Battery transport procedures	
Battery records inwards		Transfer of UAS battery log to master	
Expired or damaged batteries (outwards)		Battery performance trending	
PROCEDURES			
Battery change procedures		Training of personnel	
Flight task tracking sheet records		Test & equipment	
Emergency procedures		Environmental controls	
HSE Issue		Protective equipment (gloves, eyes)	
Dangerous goods awareness training		DG training records / recurrency	
RECOMMENDATIONS			
DEFICIENCIES			

13. Appendix A References

Ahn, J., & Chang, D. (2016). Fuzzy-based HAZOP study for process industry [Hazards Effects Management Process (HEMP) Risk Assessment Matrix]. *Journal of Hazardous Materials, 317, 303-311.*

Alexander, D. E. (2015). Disaster and Emergency Planning for Preparedness, Response, and Recovery. Oxford University Press.

AUVSI. (2019). *Trusted Operator Program: Protocol Certification Manual.* Association for Unmanned Vehicle Systems International. Retrieved, May 18, 2021. https://www.auvsi.org/topoperator

Brady, T. F. (2003, December). Emergency management: capability analysis of critical incident response. In *Winter Simulation Conference* (Vol. 2, pp. 1863-1867).

Federal Aviation Administration. (2015). Advisory circular 120-92B: Safety management systems for aviation service providers. documentLibrary/media/Advisory_Circular/AC_120-92B.pdf

Federal Aviation Administration. [FAA].(2021, August 22). Safety Management Systems:

Voluntary Implementation of SMS for Non-Part 121 Operators, MROs, and Training Organizations. FAA.Gov Retrieved August 22, 2020 from https://www.faa.gov/about/initiatives/sms/specifics_by_aviation_industry_type/air_operators/

Federal Aviation Administration. (2016). Safety risk management policy [national policy order 8040.4B]. documentLibrary/media/Order/FAA_Order_8040.4B.pdf

Federal Aviation Administration. https://www.regulations.gov/document/FAA-2019-0622-0003

Helmreich, R. L., Merritt, A. C., & Wilhelm, J. A. (1999). The evolution of crew resource management training in commercial aviation. *The International Journal of Aviation Psychology*, *9*(1), 19-32.

International Civil Aviation Organization. (2008). ICAO safety management systems (SMS) course module n 5 – risks. safety/afiplan/Documents/Safety%20Management/2008/SMS%20Worksh op/Modules/ICAO%20SMS%20Module%20N%C2%B0%205%20%E2% 80%93%20Risks%202008-11%20(E).pdf

International Civil Aviation Organization. (2009). Safety management manual (SMM): DOC 9859 AN/474 (2nd ed.).

International Civil Aviation Organization. (2013). Safety management manual (SMM): Doc 9859 AN/474 (2nd ed.).

International Civil Aviation Organization [ICAO]. (2018). *Safety Management Manual* (Doc 9859). International Civil Aviation Organization.

International Civil Aviation Organization. [ICAO]. (2021, 22 August). [Website]. UAS Toolkit. Xxxxx https://www.icao.int/safety/UA/UASToolkit/Pages/default.aspx

Lamb, T. L. Phillips, N., Nguyen, T. (2021). Quantum Safety Metrics Framework for Commercial Unmanned Aircraft Operators. *International Journal of Aviation, Aeronautics, and Aerospace, 8*(1)

Lamb, T. (2019). The changing face of airmanship and safety culture operating Unmanned Aircraft Systems. In Unmanned Aerial Vehicles in Civilian Logistics and Supply Chain Management (pp. 243-265). IGI Global.

Leveson, N. (2015). A systems approach to risk management through leading safety indicators. *Reliability Engineering and System Safety, 136*, 17-34.

Reason, J. (2016). *Managing the risks of organizational accidents*. Routledge.

Renner, S. (2001). Emergency exercise and training techniques . *Australian Journal of Emergency Management, 26*

Silver, N. (2012). *The Signal and the Noise: Why So Many Predictions Fail-But Some Don't*. Penguin.

Stolzer, A. J., Halford, M. C. D., & Goglia, M. J. J. (2015). *Safety Management Systems in Aviation*. Ashgate Publishing, Ltd.

Stoop, J., & Dekker, S. (2012). Are safety investigations pro-active?. Safety Science, 50(6), 1422-1430.

[i] The term Operator in this appendix refers to both the entity who has the approval to operate small commercial UAS operations which may be a sole pilot in command, or an organization who employs many pilots in command. In an organization, there is always an accountable manager for safety of operations, in addition to the individual responsibilities of the PIC of the aircraft (AUVSI, 2019; FAA, 2017).

Appendix B Task 3-3
Mathematical overview of the proposed PRA

---

1 Introduction

This document is a mathematical overview of the proposed probabilistic risk assessment (PRA) framework developed in the deliverables for FAA ASSURE A21 Phase 3, namely, the reports for Tasks 3-1, 3-2, and 3-3. The mathematical aspects of the proposed PRA model are summarized bt the PRA framework as a whole is not reviewed in full. This note is organized as follows:

- §2: "Review of main mathematical relationships in the proposed PRA model." The key mathematical constructs and relationships are briefly reviewed.
- §3: "Confidence intervals for the proposed PRA model." Classical results on confidence intervals are applied to the unconditional hazard outcome probabilities.
- §4: "Calculations used in the Task 3-3 scenario." The PRA model is applied to the scenario described in the Task 3-3 report.

2 Review of main mathematical relationships in the proposed PRA model

This section contains the following subsections:

- §2.1: "Notation: conventions and summary." A review of notational conventions and a summary of key notation.
- §2.2: "Review of main distributions used in the proposed PRA model." The categorical, Dirichlet, and beta distributions are reviewed.
- §2.3: "Hazard causes, hazard outcomes, their interaction, and parameter estimation." Review of the key ideas pertaining to hazard causes, hazard outcomes, how they interact, and how their underlying parameters may be estimated.
- §2.4: "Proactive and reactive mitigations." Review of how proactive mitigations affect the hazard cause distribution and how reactive mitigations affect the hazard outcome conditional distribution.
- §2.5: "Proposed application of PRA framework for sUAS CONOPS." Review of how the PRA framework may be used for making statistically informed decisions regarding risk for sUAS BVLOS CONOPS.

2.1 Notation: conventions and summary

Notational conventions and a summary of key notation are reviewed below.

2.1.1 Notational convention

Write $a \equiv b$ when a, b are equal by definition. Let $\mathbb{N}, \mathbb{Z}, \mathbb{R}$ denote the natural numbers ($\{1, 2, 3, \ldots\}$), the integers, and the real numbers, respectively, with $\mathbb{Z}_+$ and $\mathbb{R}_+$ the nonnegative integers and reals, respectively. For $(a, b) \in \mathbb{Z}^2$ with $a < b$, let $[a : b] \equiv \{a, a+1, \ldots, b-1, b\}$, and, for $k \in \mathbb{N}$, let $[k] \equiv [1 : k] = \{1, 2, \ldots, k-1, k\}$. If $\sigma \in \mathbb{R}^k$ is a vector, then $\sigma_\Sigma \equiv \sigma_1 + \cdots + \sigma_k$ denotes the sum of its components. If S is a list or set then $|S|$ denotes its cardinality.

Random quantities are denoted with a sans-serif font, e.g., $\mathsf{p}, \mathsf{q}, \mathsf{y}, \mathsf{z}$, while their realized values are denoted with a serif font, e.g., p, q, y, z. The notation $\{\mathsf{x} = x\}$ denotes the (probabilistic) event that random variable x

takes value x. If F is a probability distribution then the notation $\mathsf{x} \sim F$ indicates x is a random variable with that distribution; common distributions include the categorical, Dirichlet, and beta, presented below. The expectation, variance, covariance, and correlation of random variables, say (x, y), are denoted as $\mathbb{E}[\mathsf{x}]$, $\text{var}(\mathsf{x})$, $\text{cov}(\mathsf{x}, \mathsf{y})$, and $\rho(\mathsf{x}, \mathsf{y})$, respectively. Probability acronyms include random variable (RV), cumulative distribution function (CDF), complementary CDF (CCDF), probability mass function (PMF), probability density function (PDF), independent and identically distributed (IID), and confidence interval (CI).

2.1.2 Notation summary

Table 1 lists the key notation in the model.

Sym	Meaning
ϕ	a "null" event, e.g., no hazard cause or no hazard outcome
Y	finite set of non-null hazard causes
Y_ϕ	finite set of hazard causes, including the null cause
Z	finite set of non-null hazard outcomes
Z_ϕ	finite set of hazard outcomes, including the null outcome
y	hazard cause categorical RV $\mathsf{y} \sim \text{Cat}(\mathsf{p})$ with support Y_ϕ
p	a Dirichlet random distribution $\mathsf{p} \sim \text{Dir}(\bar{\sigma})$ with $\mathsf{p} = (\mathsf{p}_y, y \in Y_\phi)$ the distribution of y
$\bar{\sigma}$	(hyper-) parameters of Dirichlet distribution p on hazard causes, with $\bar{\sigma} = (\bar{\sigma}_y, y \in Y_\phi)$
z	hazard outcome categorical RV with conditional distribution $\mathsf{z}\|\{\mathsf{y} = y\} \sim \text{Cat}(\mathsf{q}^y)$, with support Z_ϕ
q^y	a Dirichlet random distribution $\mathsf{q}^y \sim \text{Dir}(\hat{\sigma}^y)$ with $\mathsf{q}^y = (\mathsf{q}^y_z, z \in Z_\phi)$ the distribution of $\mathsf{z}\|\{\mathsf{y} = y\}$
$\hat{\sigma}^y$	(hyper-) parameters of Dirichlet conditional distribution q^y on hazard outcomes, with $\hat{\sigma}^y = (\hat{\sigma}^y_z, z \in Z_\phi)$

Table 1: Notation used in the PRA model.

2.2 Review of main distributions used in the proposed PRA model

The three main distributions used in the proposed PRA model are the *categorical* distribution, the *Dirichlet* distribution, and the *beta* distribution, each defined below.

2.2.1 Categorical distribution

A categorical RV, say x, with finite support, say $\mathcal{X}$, is defined by a PMF, say p, on $\mathcal{X}$, i.e., $p = (p_x, x \in \mathcal{X})$, with $p_x \equiv \mathbb{P}(X = x)$, where $p_x \geq 0$ for $x \in \mathcal{X}$ and $\sum_{x \in \mathcal{X}} p_x = 1$.

2.2.2 Dirichlet distribution

A Dirichlet RV, say p, with finite dimension, say $k \in \mathbb{N}$, is defined by k (hyper-)parameters, say $\sigma = (\sigma_1, \ldots, \sigma_k) \in \mathbb{R}^k_+$, denoted $\mathsf{p} \sim \text{Dir}(\sigma)$. The Dirichlet distribution has as support the simplex of all possible distributions on k values, i.e., the realization of a Dirichlet RV is a probability distribution on a finite support of size k, i.e.,

$$\mathcal{P} \equiv \{p \in \mathbb{R}^k_+ : p_1 + \cdots + p_k = 1\}. \tag{1}$$

The PDF is

$$f_{\mathsf{p}}(p) = \frac{1}{B(\sigma)} \prod_{i \in [k]} p_i^{\sigma_i - 1}, \ p \in \mathcal{P} \tag{2}$$

where

$$B(\sigma) \equiv \frac{\prod_{i\in[k]} \Gamma(\sigma_i)}{\Gamma\left(\sum_{i\in[k]} \sigma_i\right)}, \tag{3}$$

and $\Gamma(\cdot)$ is the gamma function. Let $\sigma_\Sigma \equiv \sum_{i\in[k]} \sigma_i$ denote the sum of the hyper-parameters. The k random components of the Dirichlet distribution have the beta distribution with parameters $(\sigma_i, \sigma_\Sigma - \sigma_i)$, i.e.,

$$\mathsf{p}_i \sim \text{beta}(\sigma_i, \sigma_\Sigma - \sigma_i),\ i \in [k], \tag{4}$$

and as such, per the presentation below, the components have expectation and variance:

$$\mathbb{E}[\mathsf{p}_i] = \frac{\sigma_i}{\sigma_\Sigma},\ \text{var}(\mathsf{p}_i) = \frac{\frac{\sigma_i}{\sigma_\Sigma}\left(1 - \frac{\sigma_i}{\sigma_\Sigma}\right)}{\sigma_\Sigma + 1},\ i \in [k]. \tag{5}$$

2.2.3 Beta distribution

A beta RV, say x, with parameters $(\alpha, \beta) \in \mathbb{R}_+^2$, denoted $\mathsf{x} \sim \text{beta}(\alpha, \beta)$, has support $[0, 1]$ and PDF

$$f_{\mathsf{x}}(x; \alpha, \beta) = \frac{x^{\alpha-1}(1-x)^{\beta-1}}{B(\alpha, \beta)},\ x \in [0, 1], \tag{6}$$

where

$$B(\alpha, \beta) \equiv \frac{\Gamma(\alpha)\Gamma(\beta)}{\Gamma(\alpha + \beta)} \tag{7}$$

and $\Gamma(\cdot)$ is the gamma function. The mean and variance are

$$\mathbb{E}[\mathsf{x}] = \frac{\alpha}{\alpha + \beta},\ \text{var}(\mathsf{x}) = \frac{\alpha\beta}{(\alpha + \beta)^2(\alpha + \beta + 1)}. \tag{8}$$

The beta distribution arises in the context of this work primarily as the distribution of a single component of the Dirichlet distribution, as mentioned in the presentation above.

2.3 Hazard causes, hazard outcomes, their interaction, and parameter estimation

Hazard causes, hazard outcomes, their interaction, and estimation of their underlying parameters are reviewed in turn. Let ϕ denote a "null" event, either the null hazard cause or the null hazard outcome, both of which are defined below.

2.3.1 Hazard causes

A hazard cause is any condition or property connected with the sUAS CONOPS that is *i*) unexpected / irregular and *ii*) potentially problematic. Loosely speaking, it is anything that has "gone wrong." The phrase "potentially problematic" indicates that it may directly or indirectly contribute to an increased probability of one or more hazard outcomes, described below. Let Y denote the (finite, possibly empty) list of non-null hazard causes, with $Y_\phi = \{\phi\} \cup Y$, where the null hazard cause ϕ denotes "nothing wrong."

Let $\mathsf{y} \sim \text{Cat}(\mathsf{p})$ denote the hazard cause categorical RV, with support Y_ϕ, where $\mathsf{p} \sim \text{Dir}(\bar{\sigma})$ is the corresponding Dirichlet random distribution, with $\mathsf{p} = (\mathsf{p}_y, y \in Y_\phi)$ and hazard cause (hyper-)parameters $\bar{\sigma} = (\bar{\sigma}_y, y \in Y_\phi)$.

The assumption that y is a categorical RV directly corresponds to an assumption that at most one hazard cause may occur. While compound and/or simultaneous hazard causes are of course possible in practice, they are not supported under the model; this assumption, its motivation, and its implications are discussed at greater length in the Task 3-1 report.

The hazard cause (hyper-)parameters $\bar{\sigma} \in \mathbb{R}_+^{|Y_\phi|}$ directly represent the probabilities of each given hazard cause in that, for (y, p) and $y \in Y_\phi$, recall $\mathsf{p}_y \sim \text{beta}(\bar{\sigma}_y, \bar{\sigma}_\Sigma - \bar{\sigma}_y)$ with $\mathbb{E}[\mathsf{p}_y] = \bar{\sigma}_y/\bar{\sigma}_\Sigma$, and application of the total probability theorem yields:

$$\mathbb{P}(\mathsf{y} = y) = \int_0^1 \mathbb{P}(\mathsf{y} = y | \mathsf{p}_y = p) f_{\mathsf{p}_y}(p) \mathrm{d}p = \int_0^1 p f_{\mathsf{p}_y}(p) \mathrm{d}p = \mathbb{E}[\mathsf{p}_y] = \frac{\bar{\sigma}_y}{\bar{\sigma}_\Sigma}. \tag{9}$$

It is evident that the expression above constitutes a valid distribution, i.e., it is nonnegative and sums to one.

2.3.2 Hazard outcomes

A hazard outcome is any result or effect connected with the sUAS CONOPS that is *i*) dangerous or costly to people, the sUAS, other sUAS's in its vicinity, or the built environment, and *ii*) directly or indirectly connected to one or more hazard causes. Loosely speaking, it is anything that falls in the category of a "adverse effect." Let Z denote the (finite, possibly empty) list of non-null hazard outcomes, with $Z_\phi = \{\phi\} \cup Z$, where the null hazard outcome ϕ denotes "no adverse effect."

Let z denote the hazard outome categorical RV, with support Z_ϕ, which is specified in terms of its conditional distribution given y, the hazard cause RV. Namely, for each $y \in Y_\phi$, conditioned on specification of hazard cause y, set $\mathsf{z}|\{\mathsf{y} = y\} \sim \text{Cat}(\mathsf{q}^y)$, where $\mathsf{q}^y \sim \text{Dir}(\hat{\sigma}^y)$ is the corresponding Dirichlet random distribution, with $\mathsf{q}^y = (\mathsf{q}_z^y, z \in Z_\phi)$ and hazard outcome (hyper-)parameters $\hat{\sigma}^y = (\hat{\sigma}_z^y, z \in Z_\phi)$.

The assumption that z is a categorical RV directly corresponds to an assumption that at most one hazard outcome may occur. While compound and/or simultaneous hazard outcomes are of course possible in practice, they are not supported under the model; this assumption, its motivation, and its implications are discussed at greater length in the Task 3-1 report.

The hazard outcome (hyper-)parameters $\hat{\sigma}^y \in \mathbb{R}_+^{|Z_\phi|}$ directly represent the conditional probabilities, assuming $\mathsf{y} = y$, of each given hazard outcome in that, for (z, q) and $(y, z) \in Y_\phi \times Z_\phi$, recall $\mathsf{q}_z^y \sim \text{beta}(\hat{\sigma} y_z, \hat{\sigma}_\Sigma^y - \hat{\sigma}_z^y)$ with $\mathbb{E}[\mathsf{q}_z^y] = \hat{\sigma}_z^y/\hat{\sigma}_\Sigma^y$, and application of the total probability theorem yields:

$$\mathbb{P}(\mathsf{z} = z | \mathsf{y} = y) = \int_0^1 \mathbb{P}(\mathsf{z} = z | \mathsf{y} = y, \mathsf{q}_z^y = q) f_{\mathsf{q}_z^y}(q) \mathrm{d}q = \int_0^1 q f_{\mathsf{q}_z^y}(q) \mathrm{d}q = \mathbb{E}[\mathsf{q}_z^y] = \frac{\hat{\sigma}_z^y}{\hat{\sigma}_\Sigma^y}. \tag{10}$$

It is evident that the expression above constitutes a valid distribution, i.e., it is nonnegative and sums to one.

Write $\hat{\sigma} \equiv (\hat{\sigma}^y, y \in Y_\phi)$, which is viewed as an $|Z_\phi| \times |Y_\phi|$ matrix with entries $\hat{\sigma}_z^y$ in row z column y.

2.3.3 Interaction of hazard causes and hazard outcomes

The connection between the distributions of (y, z) and their corresponding Dirichlet distributions (p, q) is clarified by application of the total probability theorem: for $(\mathsf{y}, \mathsf{z}, \mathsf{p}, \mathsf{q})$ and $z \in Z_\phi$:

$$\mathbb{P}(\mathsf{z} = z) = \sum_{y \in Y_\phi} \mathbb{P}(\mathsf{y} = y) \mathbb{P}(\mathsf{z} = z | \mathsf{y} = y) = \sum_{y \in Y_\phi} \mathbb{E}[\mathsf{p}_y] \mathbb{E}[\mathsf{q}_z^y] = \sum_{y \in Y_\phi} \frac{\bar{\sigma}_y}{\bar{\sigma}_\Sigma} \frac{\hat{\sigma}_z^y}{\hat{\sigma}_\Sigma^y}. \tag{11}$$

It is evident that the expression above constitutes a valid distribution, i.e., it is nonnegative and sums to one.

It is also evident that the model is insensitive to linear scaling of the Dirichlet hyper-parameters, $\bar{\sigma}$ and $\hat{\sigma}$, and as such it is natural to normalize these to have unit sum, i.e., $\bar{\sigma}_\Sigma = 1$ and $\hat{\sigma}_\Sigma^y = 1$ for each $y \in Y_\phi$. We henceforth assume this normalization, under which the equations above become:

$$\mathbb{P}(\mathsf{y} = y) = \bar{\sigma}_y, \quad \mathbb{P}(\mathsf{z} = z | \mathsf{y} = y) = \hat{\sigma}_z^y, \quad \mathbb{P}(\mathsf{z} = z) = \sum_{y \in Y_\phi} \bar{\sigma}_y \hat{\sigma}_z^y. \tag{12}$$

2.3.4 Parameter estimation and CONOPS modeling

The vector $\bar{\sigma}$ and the matrix $\hat{\sigma}$ are the two types of model parameters, and each such parameter is to be estimated either from observation or from an environmental / dynamic model of the relevant CONOPS.

The number of model parameters is $|\bar{\sigma}| = |Y_\phi|$ hazard cause parameters and $|\hat{\sigma}| = |Y_\phi||Z_\phi|$. More precisely, because of the parameter normalization identified above, identification of $|Y|$ distinct non-null hazard causes and $|Z|$ distinct non-null hazard outcomes requires *i)* $|Y|$ independent hazard cause parameters and *ii)* $|Y|(|Z|+1)$ independent hazard outcome parameters.

As discussed in the Task 3-1 report, the interest in limiting the number of model parameters is the key motivation behind the categorical distribution assumptions for hazard causes and hazard outcomes. Even with such assumptions in place, however, it is evident that model parsimony (and, thereby, model tractability) is improved by restricting the lists of non-null hazard causes and outcomes to those with a non-negligible (i.e., not "de minimus") probability of occurrence.

While any parameter may be estimated by either observations or modeling, it is anticipated that it is more likely that the hazard cause parameters may be estimated by observation while the hazard outcome parameters may be estimated by modeling. Specifically, hazard causes parameters may be directly estimated by conducting repeated independent trials and tracking the frequency of occurrence of each hazard cause (malfunction), while hazard outcome parameters, which measure the conditional probability of an adverse effect resulting from an assumed hazard cause, are likely to be most easily obtainable from a corresponding environmental or dynamic model of the CONOPS.

2.4 Proactive and reactive mitigations

Mitigations, in the context of the PRA model, comprise any modification of an original CONOPS that affects, either indirectly or directly, the distribution on and/or the impact of hazard outcomes. Proactive (indirect) and reactive (direct) mitigations are discussed in turn.

2.4.1 Proactive mitigations

Proactive (indirect) mitigations affect the probability of one or more (non-null) hazard causes, thereby (indirectly) affecting the probability of a non-null hazard outcome. Examples of proactive mitigations include, but are not limited to, improved sensing, actuation, and communications mechanisms, battery backup, and flight stabilization, i.e., any step taken that reduces the probability of occurrence of a non-null hazard cause.

Formally, with $Y_\phi, \mathsf{y}, \mathsf{p}, \bar{\sigma}$ the list of hazard causes, the categorical hazard cause RV, the Dirichlet hazard cause random distribution, and the hazard cause (hyper-)parameters of the nominal (non-mitigated) CONOPS, let $Y'_\phi, \mathsf{y}', \mathsf{p}', \bar{\sigma}'$ denote the same with one or more proactive mitigations applied. With $\hat{\sigma}$ common between the unmitigated and mitigated scenarios, let z, z' denote the hazard outcome RVs, with unconditional hazard outcome distributions r, r', respectively. Specifically, $r \equiv (r_z, z \in Z_\phi)$ and $r' \equiv (r'_z, z \in Z_\phi)$, where

$$\begin{aligned} r_z &\equiv \mathbb{P}(\mathsf{z} = z) = \sum_{y \in Y_\phi} \bar{\sigma}_y \hat{\sigma}^y_z \\ r'_z &\equiv \mathbb{P}(\mathsf{z}' = z) = \sum_{y \in Y'_\phi} \bar{\sigma}'_y \hat{\sigma}^y_z. \end{aligned} \tag{13}$$

As an example, suppose, for simplicity, that a specific proactive mitigation affects only a specific non-null hazard cause $y^* \in Y$, e.g.,

$$\bar{\sigma}'_y = \begin{cases} \bar{\sigma}_y, & y \in Y \setminus \{y^*\} \\ \bar{\sigma}_y - \delta, & y = y^* \\ \bar{\sigma}_y + \delta, & y = \phi \end{cases}, \tag{14}$$

i.e., the mitigation reduces the parameter $\bar{\sigma}_{y^*}$ corresponding to hazard cause y^* by δ and, to preserve normalization, the null hazard cause is increased by the same amount. Then, the change in the (unconditional) probability of hazard outcome z is

$$\begin{aligned} r'_z - r_z &= \sum_{y \in Y'_\phi} \bar{\sigma}'_y \hat{\sigma}^y_z - \sum_{y \in Y_\phi} \bar{\sigma}_y \hat{\sigma}^y_z = \sum_{y \in Y_\phi} (\bar{\sigma}'_y - \bar{\sigma}_y) \hat{\sigma}^y_z \\ &= (\bar{\sigma}'_\phi - \bar{\sigma}_\phi)\hat{\sigma}^\phi_z + (\bar{\sigma}'_{y^*} - \bar{\sigma}_{y^*})\hat{\sigma}^{y^*}_z \\ &= \delta \hat{\sigma}^\phi_z - \delta \hat{\sigma}^{y^*}_z = \delta(\hat{\sigma}^\phi_z - \hat{\sigma}^{y^*}_z) \end{aligned} \tag{15}$$

Observe, for z a non-null hazard outcome, it is expected that the conditional probability of the hazard outcome is higher under hazard cause y^* than under a null hazard cause, i.e., $\hat{\sigma}^\phi_z < \hat{\sigma}^{y^*}_z$, while the reverse is true for the case when $z = \phi$ is the null hazard outcome.

Proactive mitigations are not guaranteed to function correctly. Let $s \in [0,1]$ denote the probability an attempted proactive mitigation fails and $1-s$ the probability it succeeds, and let $\mathsf{s} \sim \text{Ber}(s)$ be the corresponding Bernoulli failed deployment indicator RV. Let $\bar{\sigma}', \bar{\sigma}$ denote the (hyper-)parameters for the hazard causes when the mitigation succeeds and fails, respectively. Then, the hazard outcome unconditioal probabilities are computed using the total probability theorem, as follows:

$$\begin{aligned} r_z &= \mathbb{P}(\mathsf{z} = z) \\ &= \mathbb{P}(\mathsf{z} = z | \mathsf{s} = 0)\mathbb{P}(\mathsf{s} = 0) + \mathbb{P}(\mathsf{z} = z | \mathsf{s} = 1)\mathbb{P}(\mathsf{s} = 1) \\ &= (1-s) \sum_{y \in Y_\phi} \bar{\sigma}'_y \hat{\sigma}^y_z + s \sum_{y \in Y_\phi} \bar{\sigma}_y \hat{\sigma}^y_z \\ &= \sum_{y \in Y_\phi} ((1-s)\bar{\sigma}'_y + s\bar{\sigma}_y)\hat{\sigma}^y_z = \sum_{y \in Y_\phi} \bar{\sigma}^{(s)}_y \hat{\sigma}^y_z. \end{aligned} \tag{16}$$

Thus, the effect of the potential failure of the proactive mitigation is that the (hyper-)parameters for the hazard causes become the convex combination of the (hyper-) parameters when the proactive mitigation succeeds and fails, i.e., $\bar{\sigma}^{(s)} \equiv (1-s)\bar{\sigma}' + s\bar{\sigma}$.

2.4.2 Reactive mitigations

Reactive (direct) mitigations affect the conditional probability of one or more hazard outcomes, thereby (directly) affecting the (unconditional) probability of those outcomes. Examples of reactive mitigations include, but are not limited to, parachutes, emergency landing protocols, software interrupt and override protocols, and collision evasion protocols, i.e., any steps that may be taken upon recognition of one or more non-null hazard causes which reduce the probability of one or more non-null hazard outcomes.

Formally, let $Y' \subset Y$ denote the subset of hazard causes for which the proposed reactive mitigation(s) affect the conditional hazard outcome probabilities, and let $\hat{\sigma} = (\hat{\sigma}^y, y \in Y_\phi)$ denote the matrix of (hyper-)parameters for the conditional hazard outcome distributions. For $y \in Y'$, let $\hat{\sigma}^{y,'} = (\hat{\sigma}^{y,'}_z, z \in Z_\phi)$ denote the modified conditional distributions on hazard outcomes for the hazard causes affected by the reactive mitigation. Let z, z' denote the hazard outcome RVs, with unconditional hazard outcome distributions r, r', respectively. Specifically, $r \equiv (r_z, z \in Z_\phi)$ and $r' \equiv (r'_z, z \in Z_\phi)$, where

$$\begin{aligned} r_z &\equiv \mathbb{P}(\mathsf{z} = z) = \sum_{y \in Y_\phi} \bar{\sigma}_y \hat{\sigma}^y_z \\ r'_z &\equiv \mathbb{P}(\mathsf{z}' = z) = \sum_{y \in Y_\phi \setminus Y'} \bar{\sigma}_y \hat{\sigma}^y_z + \sum_{y \in Y'} \bar{\sigma}_y \hat{\sigma}^{y,'}_z \end{aligned} \tag{17}$$

As an example, suppose, for simplicity, that a specific reactive mitigation affects all the non-null hazard outcomes but only for one specific non-null hazard cause $y^* \in Y$, e.g.,

$$\hat{\sigma}_z^{y,'} = \begin{cases} \hat{\sigma}_z^y, & y \in Y \setminus \{y^*\} \\ \hat{\sigma}_z^y - \delta, & y = y^*, z \in Z \\ \hat{\sigma}_z^y + |Z|\delta, & y = y^*, z = \phi \end{cases}, \tag{18}$$

i.e., the mitigation reduces each parameter $\hat{\sigma}_z^{y^*}$, corresponding to hazard (cause, outcome) pair (y^*, z) by δ while the corresponding null outcome conditional probability $\hat{\sigma}_\phi^{y^*}$ is increased by $|Z|\delta$ to preserve normalization. Then the change in the (unconditional) probability of hazard outcome z is

$$\begin{aligned} r'_z - r_z &= \sum_{y \in Y'} \bar{\sigma}_y \hat{\sigma}_z^{y,'} - \sum_{y \in Y'} \bar{\sigma}_y \hat{\sigma}_z^y = \sum_{y \in Y'} \bar{\sigma}_y (\hat{\sigma}_z^{y,'} - \hat{\sigma}_z^y) \\ &= \bar{\sigma}_{y^*} (\hat{\sigma}_z^{y^*,'} - \hat{\sigma}_z^{y^*}) = \begin{cases} -\bar{\sigma}_{y^*}\delta, & z \in Z \\ \bar{\sigma}_{y^*}|Z|\delta, & z = \phi \end{cases}. \end{aligned} \tag{19}$$

Thus, under this particular example, each non-null hazard outcome unconditional probability is reduced by $\bar{\sigma}_{y^*}\delta$ while the null hazard outcome unconditional probability is increased by $\bar{\sigma}_{y^*}|Z|\delta$.

Reactive mitigations are not guaranteed to function correctly. Let $s \in [0,1]$ denote the probability an attempted reactive mitigation fails and $1-s$ the probability it succeeds, and let $\mathsf{s} \sim \text{Ber}(s)$ be the corresponding Bernoulli failed deployment indicator RV. Let $\hat{\sigma}', \hat{\sigma}$ denote the (hyper-)parameters for the hazard outcomes when the mitigation succeeds and fails, respectively. Then, the hazard outcome unconditioal probabilities are computed using the total probability theorem, as follows:

$$\begin{aligned} r_z &= \mathbb{P}(\mathsf{z} = z) \\ &= \mathbb{P}(\mathsf{z} = z|\mathsf{s} = 0)\mathbb{P}(\mathsf{s} = 0) + \mathbb{P}(\mathsf{z} = z|\mathsf{s} = 1)\mathbb{P}(\mathsf{s} = 1) \\ &= (1-s) \sum_{y \in Y_\phi} \bar{\sigma}_y \hat{\sigma}_z^{y,'} + s \sum_{y \in Y_\phi} \bar{\sigma}_y \hat{\sigma}_z^y \\ &= \sum_{y \in Y_\phi} \bar{\sigma}_y ((1-s)\hat{\sigma}_z^{y,'} + s\hat{\sigma}_z^y) = \sum_{y \in Y_\phi} \bar{\sigma}_y \hat{\sigma}_z^{(s),y} \end{aligned} \tag{20}$$

Thus, the effect of the potential failure of the reactive mitigation is that the (hyper-)parameters for the hazard outcomes are the convex combination of the (hyper-) parameters when the reactive mitigation succeeds and fails, i.e., $\hat{\sigma}^{(s)} \equiv (1-s)\hat{\sigma}' + s\hat{\sigma}$.

2.5 Proposed application of PRA framework for sUAS CONOPS

The previous discussion has established a mechanism that, given a vector $\bar{\sigma}$ and a matrix $\hat{\sigma}$ as inputs, computes as output the unconditional distribution on hazard outcomes, $r \equiv (r_z, z \in Z_\phi)$ with $r_z \equiv \mathbb{P}(\mathsf{z} = z) = \bar{\sigma}^T \hat{\sigma}_z$, as well as the impact of both proactive and reactive mitigations on the model. As discussed in greater detail in the Task 3-1 report, this mapping from $(\bar{\sigma}, \hat{\sigma})$ to r is a key part, but only a part, of the larger PRA framework for sUAS CONOPS. The PRA operator may consider the following proposed PRA process:

1. Identify the relevant state descriptor of the proposed CONOPS, to ensure that any statistical tests or environmental / dynamic models used to estimate parameters $(\bar{\sigma}, \hat{\sigma})$ are directly relevant to the CONOPS.

2. Identify critical instants in the CONOPS where risk assessment should be performed.

3. Define a relevant risk matrix with likelihood categories (rows) and severity categories (columns) and assign risk categories (e.g., very low, low, medium, high) to each entry in the matrix.

4. Assign severity categories to each of the identified non-null hazard outcomes, look up the likelihood category for the computed unconditional probabilities for the non-null hazard outcomes, and use the risk matrix to lookup the risk category for each such outcome.

5. Apply mitigations, update the input parameters, update the calculcated unconditional probabilities for the non-null hazard outcomes, update the risk categories for these outcomes, and perhaps continue to apply additional mitigations until the risk categories are acceptably low.

6. Devise a mechanism or decision rule that makes a triage decision on the overall CONOPS (e.g., approved, denied, or requires further investigation) as a function of the risk categories associated with each non-null hazard outcome, for each critical flight instance.

3 Confidence intervals for the proposed PRA model

While the previous section presented the PRA model using point estimates for both input parameters and output values, this section incorporates CIs for both input and output values, the latter being approximated using the classical delta method. This section contains the following subsections.

- §3.1: "Selective review of CIs". Classical concepts from elementary probability and statistics pertaining to CIs are briefly reviewed.
- §3.2: "Selective review of the delta method". The delta method is a widely-used tool in probability and statistics to estimate the variance of a random variable that is a (nonlinear) function of input random variables.
- §3.3: "Application of the delta method to the proposed PRA model". The delta method is specialized to the proposed PRA model, specifically to the unconditional probabilities of hazard outcomes.

3.1 Selective review of CIs

This selective review of CIs includes three subsections: *i*) CIs for normal RVs, *ii*) CIs for binomial RVs approximated from CIs for normal RVs, and *iii*) CIs for binomial RVs approximated as Poisson RVs. Fix $\alpha \in (0,1)$ as the target confidence level, i.e., a $\alpha \times 100$ % CI is sought.

3.1.1 CIs for IID normal trials

Let $\mathsf{w} = (\mathsf{w}_i, i \in [N])$, for $N \in \mathbb{N}$, denote IID normal RVs, with $\mathsf{w}_i \sim N(\mu, \nu)$. Here, assume the mean μ is fixed but unknown and assume the standard deviation ν is fixed and known. The objective is to derive a CI for the unknown mean μ in terms of a suitable statistic of the RVs w, namely, the sample mean, $\bar{\mathsf{w}} = (\mathsf{w}_1 + \cdots + \mathsf{w}_N)/N$.

Fact. Observe, $\bar{\mathsf{w}} \sim N(\mu, \nu/\sqrt{N})$. The $\alpha \times 100$ % CI for μ has random endpoints

$$\bar{\mathsf{w}} \pm \frac{c(\alpha)}{\sqrt{N}}\nu, \tag{21}$$

where $c(\alpha) = \Phi^{-1}((1+\alpha)/2)$, $\Phi(\cdot)$ is the CDF for the standard normal distribution, and $\Phi^{-1}(\cdot)$ is the inverse of Φ. For example, choosing $\alpha = 0.95$ yields $c = \Phi^{-1}((1+\alpha)/2) \approx 1.96$, while $\alpha = 0.9999999$ yields $c \approx 5.326723886681888$.[1]

[1] e.g., in Mathematica, `InverseCDF[NormalDistribution[0, 1], (1 + α)/2]`.

Proof. Standardize the RV $\bar{\mathsf{w}}$ as the RV $\bar{\mathsf{f}}$, i.e.,

$$\bar{\mathsf{f}} = \frac{\sqrt{N}}{\nu}(\bar{\mathsf{w}} - \mu) \sim N(0,1), \tag{22}$$

so that, using $\Phi(c) = \mathbb{P}(\mathsf{z} \leq c)$, for $\mathsf{z} \sim N(0,1)$, and $\Phi(-c) = 1 - \Phi(c)$, the probability that $\bar{\mathsf{f}}$ is in the interval $[-c, +c]$, for some $c > 0$, is

$$\mathbb{P}(-c \leq \bar{\mathsf{f}} \leq +c) = \Phi(c) - \Phi(-c) = 2\Phi(c) - 1. \tag{23}$$

Fixing $\alpha = 2\Phi(c) - 1$ and solving for c yields $c(\alpha) = \Phi^{-1}((1+\alpha)/2)$, so that

$$\begin{aligned}
\mathbb{P}(-c(\alpha) \leq \bar{\mathsf{f}} \leq +c(\alpha)) &= \alpha \\
\mathbb{P}\left(-c(\alpha) \leq \frac{\sqrt{N}}{\nu}(\bar{\mathsf{w}} - \mu) \leq +c(\alpha)\right) &= \alpha \\
\mathbb{P}\left(-\frac{c(\alpha)}{\sqrt{N}}\nu \leq \bar{\mathsf{w}} - \mu \leq +\frac{c(\alpha)}{\sqrt{N}}\nu\right) &= \alpha \\
\mathbb{P}\left(+\frac{c(\alpha)}{\sqrt{N}}\nu \geq \mu - \bar{\mathsf{w}} \geq -\frac{c(\alpha)}{\sqrt{N}}\nu\right) &= \alpha \\
\mathbb{P}\left(\bar{\mathsf{w}} - \frac{c(\alpha)}{\sqrt{N}}\nu \leq \mu \leq \bar{\mathsf{w}} + \frac{c(\alpha)}{\sqrt{N}}\nu\right) &= \alpha
\end{aligned} \tag{24}$$

The asserted Fact now follows immediately from the last expression. ■

3.1.2 CIs for binomial RVs approximated from normal RVs

Let $\mathsf{x} = (\mathsf{x}_i, i \in [N])$, for $N \in \mathbb{N}$, denote IID Bernoulli trials, with $\mathsf{x}_i \sim \text{Ber}(\theta)$, for fixed but unknown $\theta \in (0,1)$, and let $\mathsf{n} = \mathsf{x}_1 + \cdots + \mathsf{x}_N \sim \text{bin}(N, \theta)$ denote the correponding number of succeses. The objective is to derive an approximate CI for the unknown probability of success, θ, in terms of a suitable statistic of the RVs x.

The normal approximation to the binomial, suitable for large N and θ not too close to either 0 or 1, allows the derivation of the following approximate CI for θ. Observe, $\bar{\mathsf{f}} = \mathsf{n}/N$ has an approximately normal distribution for large N, with mean θ and variance $\theta(1-\theta)/N$, i.e.,

$$\bar{\mathsf{f}} \sim N\left(\theta, \sqrt{\frac{\theta(1-\theta)}{N}}\right). \tag{25}$$

Define $\tilde{\nu}$ as an approximation of ν, estimated using the realization of the statistic $\bar{f}$,

$$\nu = \sqrt{\theta(1-\theta)} \approx \tilde{\nu} \equiv \sqrt{\bar{f}(1-\bar{f})}. \tag{26}$$

Adapting the CI for normal RVs yields the following $\alpha \times 100$ % approximate CI for θ.

Fact. An approximate $\alpha \times 100$ % CI for θ, suitable for large N and $\bar{f} \in (0,1)$, has random endpoints

$$\bar{\mathsf{f}} \pm \frac{c(\alpha)}{\sqrt{N}}\sqrt{\bar{\mathsf{f}}(1-\bar{\mathsf{f}})}, \tag{27}$$

where $c(\alpha) = \Phi^{-1}((1+\alpha)/2)$, $\Phi(\cdot)$ is the CDF for the standard normal distribution, and $\Phi^{-1}(\cdot)$ is the inverse of Φ.

Observe that the interval has zero width if $\bar{f} = 0$ or $\bar{f} = 1$, as will be the case when there are either no or all successes observed in the N trials. As this edge case has practical relevance, it is of interest to consider the alternate CIs for binomial RVs given below.

3.1.3 CIs for binomial RVs approximated from Poisson RVs

Let $\mathsf{x} = (\mathsf{x}_i, i \in [N])$, for $N \in \mathbb{N}$, denote IID Bernoulli trials, with $\mathsf{x}_i \sim \text{Ber}(\theta)$, for fixed but unknown $\theta \in (0,1)$, and let $\mathsf{n} = \mathsf{x}_1 + \cdots + \mathsf{x}_N \sim \text{bin}(N,\theta)$ denote the correponding number of successes, where θ is considered to be "small". The objective is to derive an approximate CI for the unknown probability of success, θ. If there are n successes in N trials then the one-sided CI for θ, denoted $[0, \bar{f}]$, has right endpoint $\bar{f}$ given by the unique solution of the equation, with (N, n, α) as parameters:

$$\mathbb{P}(\text{bin}(N, \bar{f}) \leq n) = 1 - \alpha. \tag{28}$$

Equivalently, $\bar{f}(N, n, \alpha)$ is the solution of

$$\sum_{k \in [0:n]} \binom{N}{k} \bar{f}^k (1-\bar{f})^{N-k} = 1 - \alpha. \tag{29}$$

When N is "large" and n is "small', it is natural to leverage the Poisson approximation to the binomial, namely

$$\mathbb{P}(\text{bin}(N, f) \leq n) \approx \mathbb{P}(\text{Po}(\lambda) \leq n), \ \lambda = Nf. \tag{30}$$

In other words, under the Poisson approximation, the right endpoint is $\bar{f} = \lambda/N$, where λ is given by the unique solution of the equation, with (n, α) as parameters:

$$\mathbb{P}(\text{Po}(\lambda) \leq n) = 1 - \alpha. \tag{31}$$

Equivalently, $\lambda(n, \alpha)$ is the solution[2] of

$$\mathrm{e}^{-\lambda} \sum_{k \in [0:n]} \frac{\lambda^k}{k!} = 1 - \alpha. \tag{32}$$

The approximate value $\bar{f}(N, n, \alpha)$ is then $\lambda(n, \alpha)/N$.

3.2 Selective review of the delta method

The delta method approximates the variance of an (output) RV that is a known function of one or more (input) RVs. Let $h : \mathbb{R}^k \to \mathbb{R}$ be a real-valued function, typically nonlinear, with argument $t = (t_1, \ldots, t_k)$. Let $\mathsf{t} = (\mathsf{t}_1, \ldots, \mathsf{t}_k)$ be the input RVs and let $\mathsf{u} = h(\mathsf{t})$ be the output RV. The delta method approximates the variance of u, i.e., $\text{var}(\mathsf{u})$, using a first-order Taylor series approximation of h around the point $\tilde{t} = (\tilde{t}_1, \ldots, \tilde{t}_k)$, the expectation of t, i.e., $\mathbb{E}[\mathsf{t}_i] = \tilde{t}_i$ for $i \in [k]$. Thus, the nonlinear $u = h(t)$ is approximated as the linear $\tilde{u} = \tilde{h}(t)$, where

$$\begin{aligned} h(t) &\approx \tilde{h}(t) = h(\tilde{t}) + \nabla h(t)|_{t=\tilde{t}}(t - \tilde{t}) \\ &= h(\tilde{t}) + \sum_{i \in [k]} \left.\frac{\partial h(t)}{\partial t_i}\right|_{t=\tilde{t}} (t_i - \tilde{t}_i) \end{aligned} \tag{33}$$

Then, for random t, i.e., t, the RV $h(\mathsf{t})$ is approximated as $\tilde{h}(\mathsf{t})$, i.e.,

$$h(\mathsf{t}) \approx \tilde{h}(\mathsf{t}) = h(\tilde{t}) + \sum_{i \in [k]} \left.\frac{\partial h(t)}{\partial t_i}\right|_{t=\tilde{t}} (\mathsf{t}_i - \tilde{t}_i). \tag{34}$$

Taking expectations of both sides yields, by linearity of expectation,

$$\mathbb{E}[h(\mathsf{t})] \approx \mathbb{E}[\tilde{h}(\mathsf{t})] = \tilde{h}(\mathbb{E}[\mathsf{t}]) = \tilde{h}(\tilde{t}) = h(\tilde{t}). \tag{35}$$

[2] For example, in Mathematica, `Solve[CDF[PoissonDistribution[λ],n]==1-α,λ]`

The corresponding variance is

$$\begin{aligned}\mathrm{var}(h(\mathsf{t})) &\approx \mathrm{var}(\tilde{h}(\mathsf{t}))\\ &= \mathrm{var}\left(h(\tilde{t})+\sum_{i\in[k]}\frac{\partial h(\tilde{t})}{\partial t_i}(\mathsf{t}_i-\tilde{t}_i)\right)\\ &= \mathrm{var}\left(\sum_{i\in[k]}\frac{\partial h(\tilde{t})}{\partial t_i}\mathsf{t}_i\right)\\ &= \sum_{i\in[k]}\left(\frac{\partial h(\tilde{t})}{\partial t_i}\right)^2\mathrm{var}(\mathsf{t}_i)+2\sum_{i<j}\frac{\partial h(\tilde{t})}{\partial t_i}\frac{\partial h(\tilde{t})}{\partial t_j}\mathrm{cov}(\mathsf{t}_i,\mathsf{t}_j) \qquad (36)\end{aligned}$$

Thus, RV u has approximate mean $h(\tilde{t})$ and approximate variance $\mathrm{var}(\tilde{h}(\mathsf{t}))$, the latter expressed in terms of the partial derivatives of h and the variances and covariances of t.

3.3 Application of the delta method to the proposed PRA model

The Iverson bracket notation is employed below, i.e., $[S]=1$ (0) if S is true (false).

Let u denote a Bernoulli RV $\mathsf{u}=[\mathsf{z}=z]$ for the categorical hazard outcome RV z and some element z of its support, with the CI for $r_z=\mathbb{P}(\mathsf{z}=z)=\mathbb{P}(\mathsf{u}=1)$ to be estimated from either direct or indirect trials.

3.3.1 CI on r_z via direct trials and the Poisson approximation

Direct trials would consist of N IID Bernoulli RVs $(\mathsf{u}_1,\ldots,\mathsf{u}_N)$ with trial $i\in[N]$ recording the value of the Bernoulli RV $\mathsf{u}_i=[\mathsf{z}_i=z]$, of which $n\in[0:N]$ constitute "success." With $\alpha\in(0,1)$ the target confidence level, the Poisson approximation CI for r_z is $[0,\bar{r}_z]$ where $\bar{r}_z=\lambda(n,\alpha)/N$, and $\lambda(n,\alpha)$ is the solution of $\mathbb{P}(\mathrm{Po}(\lambda)\leq n)=1-\alpha$.

The primary reason that direct trials are not used in the context of the proposed PRA is that the direct trials require direct observations of hazard outcomes, whereas a much more common and feasible testing mechanism is to conduct direct observations of hazard causes.

3.3.2 CI on r_z via indirect trials and the delta method

Indirect trials may yield a CI for r_z using the delta method on the function

$$r_z=\sum_{y\in Y_\phi}\bar{\sigma}_y\hat{\sigma}_z^y=h(\bar{\sigma},\hat{\sigma}_z). \qquad (37)$$

The term "indirect trials" means trials are conducted in order to produce estimates of each of the input parameters, namely, $(\bar{\sigma},\hat{\sigma}_z)$. The partial derivatives are

$$\frac{\partial h(\bar{\sigma},\hat{\sigma}_z)}{\partial\bar{\sigma}_y}=\hat{\sigma}_z^y,\quad \frac{\partial h(\bar{\sigma},\hat{\sigma}_z)}{\partial\hat{\sigma}_z^y}=\bar{\sigma}_y. \qquad (38)$$

The RVs corresponding to the parameters are all Bernoulli, i.e.,

$$[\mathsf{z}=z]=\sum_{y\in Y_\phi}[\mathsf{y}=y][\mathsf{z}=z|\mathsf{y}=y] \qquad (39)$$

with expectations

$$\mathbb{E}[[\mathsf{y}=y]]=\bar{\sigma}_y,\quad \mathbb{E}[[\mathsf{z}=z|\mathsf{y}=y]]=\hat{\sigma}_z^y, \qquad (40)$$

variances

$$\text{var}([\mathsf{y}=y]) = \bar{\sigma}_y(1-\bar{\sigma}_y), \quad \text{var}([\mathsf{z}=z|\mathsf{y}=y]) = \hat{\sigma}_z^y(1-\hat{\sigma}_z^y), \tag{41}$$

and covariances, for $y \neq y'$ both in Y_ϕ:

$$\text{cov}([\mathsf{y}=y],[\mathsf{y}=y']) = \mathbb{E}[[\mathsf{y}=y][\mathsf{y}=y']] - \mathbb{E}[[\mathsf{y}=y]]\mathbb{E}[[\mathsf{y}=y']] = -\bar{\sigma}_y\bar{\sigma}_{y'} \tag{42}$$

It is straightforward to show that all other covariances are 0. Substitution yields:

$$\text{var}([\mathsf{z}=z]) \approx \tilde{\text{var}}([\mathsf{z}=z]) = \sum_{y\in Y_\phi}[\hat{\sigma}_z^y\bar{\sigma}_y(1-\bar{\sigma}_y) + \bar{\sigma}_y\hat{\sigma}_z^y(1-\hat{\sigma}_z^y)] - 2\sum_{(y,y')\in Y_\phi : y<y'} \hat{\sigma}_z^y\hat{\sigma}_z^{y'}\bar{\sigma}_y\bar{\sigma}_{y'} \tag{43}$$

Recall that the $\alpha \times 100$ % CI for μ using an estimator $\bar{\mathsf{x}}$ from N IID trials of a normal RV with unknown mean μ and known or estimated standard deviation σ is $\bar{\mathsf{x}} \pm \frac{c(\alpha)}{\sqrt{N}}\sigma$. Applying this to the current context, using the estimated mean and variance for r_z yields an approximate CI for r_z given by

$$h(\bar{\sigma},\hat{\sigma}_z) \pm \frac{c(\alpha)}{\sqrt{N}}\sqrt{\tilde{\text{var}}([\mathsf{z}=z])}, \tag{44}$$

Here, the values of the components of $(\bar{\sigma},\hat{\sigma}_z)$ are obtained from the indirect trials.

4 Calculations used in the Task 3-3 scenario

The Task 3-3 report describes a practically motivated but hypothetical scenario (i.e., a CONOPS) in which an sUAS flies BVLOS to deliver a package. The specific details of the scenario are in the report and are not repeated here. The purpose of this section is to represent the scenario in terms of the PRA model, and to then compute the unconditional hazard outcome probabilities, both as point estimates and as CIs, both with and without the proposed parachute (reactive) mitigation. This section contains the following subsections:

- §4.1: "Scenario specification". The essential components of the scenario are reviewed.
- §4.2: "Point estimates for the proposed scenario". Point estimates of the non-null hazard outcome unconditional probabilities are computed.
- §4.3: "Confidence intervals for the proposed scenario". Confidence intervals on the non-null hazard outcome unconditional probabilities are computed.

4.1 Scenario specification

The following components of the scenario allow it to be represented within the proposed PRA model:

1. There are four equally likely non-null hazard causes, $Y = (1,2,3,4)$;
2. There are two non-null hazard outcomes, $Z = (b,p)$: i) hitting the built environment ("b"), and ii) hitting a person ("p"). It is assumed that i) a null hazard outcome is guaranteed under a null hazard cause, ii) the conditional distribution on hazard outcomes is the same for each of the non-null hazard causes, with $\hat{\sigma}_b = 0.200$ the (conditional) probability of hitting the built environment and $\hat{\sigma}_p = 0.006$ the (conditional) probability of hitting a person, both conditioned under a (any) non-null hazard cause.
3. All CIs are to be computed with $\alpha = 0.9999999$;
4. There are $N = 3,100$ hazard cause trials, each of which results in a null hazard cause;

5. The only mitigation applied to the CONOPS is the use of a parachute; this is a reactive mitigation which is always attempted if any non-null hazard cause is present. The mitigation may or may not succeed, i.e., the parachute may or may not deploy. To assess this, it is assumed that $M = 1,045$ trials are conducted, each of which resulted in a successful parachute deployment. If the parachute is successfully deployed, then it is assumed that the hazard cause is effectively mitigated, in the sense that a null hazard outcome is guaranteed. If the parachute deployment fails, however, then the conditional distribution on the hazard cause remains as it was in the absence of the mitigation.

4.2 Point estimates for the proposed scenario

Point estimates are computed first and then without the parachute mitigation; the section closes with a summary of the computed values.

4.2.1 Point estimates without the parachute mitigation

The assumed $N = 3,100$ hazard cause trials, each of which is assumed to be successful, i.e., assumed to result in a null hazard cause, allows a calculation of the $\alpha \times 100\%$ CI on the probability of a non-null hazard cause. Namely, the solution of $\mathbb{P}(\text{Po}(\lambda) \leq n) = 1 - \alpha$ for λ given $n = 0$ and the given α is

$$\lambda = 16.118095651484676, \tag{45}$$

and the resulting CI is $[0, \bar{f}]$ with

$$\bar{f} = \frac{\lambda}{N} = 0.005199385694027315. \tag{46}$$

This yields hazard cause parameters

$$\bar{\sigma} = (\bar{\sigma}_\phi, \bar{\sigma}_1, \bar{\sigma}_2, \bar{\sigma}_3, \bar{\sigma}_4) = (1 - \bar{f}, \bar{f}/4, \bar{f}/4, \bar{f}/4, \bar{f}/4). \tag{47}$$

The assumptions regarding the conditional hazard outcome distribution yield

$$\hat{\sigma} = \begin{bmatrix} 1 & \hat{\sigma}_\phi & \hat{\sigma}_\phi & \hat{\sigma}_\phi & \hat{\sigma}_\phi \\ 0 & \hat{\sigma}_b & \hat{\sigma}_b & \hat{\sigma}_b & \hat{\sigma}_b \\ 0 & \hat{\sigma}_p & \hat{\sigma}_p & \hat{\sigma}_p & \hat{\sigma}_p \end{bmatrix}, \tag{48}$$

with

$$\hat{\sigma}_\phi \equiv 1 - \hat{\sigma}_b - \hat{\sigma}_p = 1 - 0.200 - 0.006 = 0.794. \tag{49}$$

With $\bar{\sigma}, \hat{\sigma}$ in hand, the unconditional probabilities $r_b = \mathbb{P}(\mathsf{z} = b)$ and $r_p = \mathbb{P}(\mathsf{z} = p)$ may be computed:

$$\begin{aligned} r_b &= \bar{\sigma}_\phi \hat{\sigma}_b^\phi + 4\bar{\sigma}_i \hat{\sigma}_b^i = (1 - \bar{f}) \cdot 0 + 4\frac{\bar{f}}{4}\hat{\sigma}_b = \bar{f}\hat{\sigma}_b = 0.001039877138805463 \\ r_p &= \bar{\sigma}_\phi \hat{\sigma}_p^\phi + 4\bar{\sigma}_i \hat{\sigma}_p^i = (1 - \bar{f}) \cdot 0 + 4\frac{\bar{f}}{4}\hat{\sigma}_p = \bar{f}\hat{\sigma}_p = 0.00003119631416416389 \end{aligned} \tag{50}$$

4.2.2 Point estimates with the parachute mitigation

If the parachute deployment is unsuccessful, the hazard outcome conditional distribution remains as $\hat{\sigma}$ in (48). If successful, however, then the governing assumptions ensure the hazard outcome conditional distribution become

$$\hat{\sigma}' = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \tag{51}$$

i.e., no non-null hazard outcome is possible, regardless of the hazard cause. Let $\check{s}$ be the fixed but uknown probability of a failed parachute deployment, and let $\check{\sigma}$ be the corresponding hazard outcome conditional distribution matrix, i.e.,

$$\check{\sigma} = \begin{cases} \hat{\sigma}, & \text{w.p. } \check{s} \\ \hat{\sigma}', & \text{w.p. } 1-\check{s} \end{cases} \tag{52}$$

Let $(\check{r}_b, \check{r}_p)$ denote the unconditional probabilities of the two hazard outcomes under the parachute mitigation, i.e.,

$$\begin{aligned} \check{r}_b &= \check{s}\bar{\sigma}^T\hat{\sigma}_b + (1-\check{s})\bar{\sigma}^T\hat{\sigma}'_b = \check{s}\bar{f}\hat{\sigma}_b \\ \check{r}_p &= \check{s}\bar{\sigma}^T\hat{\sigma}_p + (1-\check{s})\bar{\sigma}^T\hat{\sigma}'_p = \check{s}\bar{f}\hat{\sigma}_p \end{aligned} \tag{53}$$

The assumed $M = 1,045$ parachute deployment trials, each of which is assumed to succeed, allows a calculation of the $\alpha \times 100\%$ CI on the probability of a failed parachute deployment. Namely, the solution of $\mathbb{P}(\text{Po}(\lambda) \leq n) = 1-\alpha$ for λ given $n = 0$ and the given α is (as before)

$$\lambda = 16.118095651484676, \tag{54}$$

and the resulting CI is $[0, \hat{s}]$ with

$$\check{s} = \frac{\lambda}{M} = 0.015424014977497298. \tag{55}$$

Substitution yields

$$\begin{aligned} \check{r}_b &= \check{s}\bar{f}\hat{\sigma}_b = 0.0000160390805636925 \\ \check{r}_p &= \check{s}\bar{f}\hat{\sigma}_p = 0.000004811724169107 75. \end{aligned} \tag{56}$$

4.2.3 Point estimate summary

In summary, the relevant input values are

N	M	$\hat{\sigma}_b$	$\hat{\sigma}_p$	α
$3,100$	$1,045$	0.200	0.006	0.9999999

(57)

and the following unconditional hazard cause probabilities are computed:

Probability of hitting built env., no parachute	0.001039877138805463
Probability of hitting a person, no parachute	0.00003119631416416389
Probability of hitting built env., with parachute	0.0000160390805636925
Probability of hitting a person, with parachute	0.000004811724169107 75

(58)

4.3 Confidence intervals for the proposed scenario

Specializing the approximate variance expression, $\tilde{\text{var}}([\mathsf{z} = z])$ to the scenario yields:

$$\begin{aligned} \tilde{\text{var}}([\mathsf{z} = b]) &= \bar{f}\hat{\sigma}_b\left[1 - \frac{\bar{f}}{4} + 1 - \hat{\sigma}_b - \frac{3}{4}\bar{f}\hat{\sigma}_b\right] \\ \tilde{\text{var}}([\mathsf{z} = p]) &= \bar{f}\hat{\sigma}_p\left[1 - \frac{\bar{f}}{4} + 1 - \hat{\sigma}_p - \frac{3}{4}\bar{f}\hat{\sigma}_p\right] \end{aligned} \tag{59}$$

Combining the mean and variance estimates yields the CIs for (r_b, r_p):

$$\begin{aligned} r_b &: \bar{f}\hat{\sigma}_b \pm \frac{c(\alpha)}{\sqrt{N}}\sqrt{\bar{f}\hat{\sigma}_b\left[1 - \frac{\bar{f}}{4} + 1 - \hat{\sigma}_b - \frac{3}{4}\bar{f}\hat{\sigma}_b\right]} \\ r_p &: \bar{f}\hat{\sigma}_p \pm \frac{c(\alpha)}{\sqrt{N}}\sqrt{\bar{f}\hat{\sigma}_p\left[1 - \frac{\bar{f}}{4} + 1 - \hat{\sigma}_p - \frac{3}{4}\bar{f}\hat{\sigma}_p\right]} \end{aligned} \tag{60}$$

For the specified α, calculation yields

$$c(\alpha) = 5.326723886681888. \tag{61}$$

Substituting the parameter values yields the CIs on (r_b, r_p):

$$\begin{aligned} r_b &: 0.00103988 \pm 0.00413671 = [0, 0.00517659] \\ r_p &: 0.0000311963 \pm 0.000754309 = [0, 0.000785506]. \end{aligned} \tag{62}$$

In the case where the parachute mitigation is applied, the CI estimates become

$$\begin{aligned} \check{r}_b &: \check{s}\bar{f}\hat{\sigma}_b \pm \frac{c(\alpha)}{\sqrt{N}}\sqrt{\check{s}\bar{f}\hat{\sigma}_b\left[1 - \frac{\bar{f}}{4} + 1 - \check{s}\hat{\sigma}_b - \frac{3}{4}\check{s}\bar{f}\hat{\sigma}_b\right]} \\ \check{r}_p &: \check{s}\bar{f}\hat{\sigma}_p \pm \frac{c(\alpha)}{\sqrt{N}}\sqrt{\check{s}\bar{f}\hat{\sigma}_p\left[1 - \frac{\bar{f}}{4} + 1 - \check{s}\hat{\sigma}_p - \frac{3}{4}\bar{f}\check{s}\hat{\sigma}_p\right]} \end{aligned} \tag{63}$$

i.e., the quantities $\hat{\sigma}_b, \hat{\sigma}_p$ are replaced by $\check{s}\hat{\sigma}_b, \check{s}\hat{\sigma}_p$, respectively. Computation yields:

$$\begin{aligned} r_b &: 0.0000160391 \pm 0.00054126 = [0, 0.000557299] \\ r_p &: 0.0000004812 \pm 0.0000938196 = [0, 0.0000943007]. \end{aligned} \tag{64}$$

In summary:

CI on hitting built env., no parachute	$0.00103988 \pm 0.00413671 = [0, 0.00517659]$
CI on hitting a person, no parachute	$0.0000311963 \pm 0.000754309 = [0, 0.000785506]$
CI on hitting built env., with parachute	$0.0000160391 \pm 0.00054126 = [0, 0.000557299]$
CI on hitting a person, with parachute	$0.0000004812 \pm 0.0000938196 = [0, 0.0000943007]$

(65)