Designation: F3178 – 16

Standard Practice for Operational Risk Assessment of Small Unmanned Aircraft Systems (sUAS)[1]

This standard is issued under the fixed designation F3178; the number immediately following the designation indicates the year of original adoption or, in the case of revision, the year of last revision. A number in parentheses indicates the year of last reapproval. A superscript epsilon (ε) indicates an editorial change since the last revision or reapproval.

INTRODUCTION

An operational risk assessment (ORA) offers to an applicant of small unmanned aircraft systems (sUAS) a standardized approach to examine their operations for potential hazards and assess those hazards for risk. The ORA is then used to mitigate or avoid risks associated with those hazards to achieve acceptable levels of safety. ORA is a key component of operational risk management (ORM), which seeks to identify hazards endemic to an operation, assign risks to those hazards based on quantitative and qualitative analysis, and mitigate unacceptable levels of risk. The main functions of the ORM are to: (*1*) Minimize risk to acceptable levels while providing a method to manage resources effectively; (*2*) Enhance decision-making skills based on systematic, reasoned, and repeatable processes; (*3*) Provide systematic structure to perform risk assessments; (*4*) Provide an adaptive process for continuous feedback through planning, preparation, and execution; and (*5*) Identify feasible and effective control measures, particularly where specific standards do not exist.

Through a risk-based approach to operations, design, and airworthiness, an applicant can quickly understand the operational environment and threats to the operation. The ORA offers a methodology to identify system and operational hazards, apply quantitative and qualitative analysis to those hazards, analyze the outputs of the ORA, and then apply appropriate mitigations to satisfy safety of flight requirements.

The ORA is an integral component of any sUAS application and is an important tool for gaining access to the national airspace, or especially into increasingly higher risk environments, such as controlled airspace where other manned aircraft are likely to be present.

1. Scope

1.1 This practice focuses on preparing operational risk assessments (ORAs) to be used for supporting small unmanned aircraft systems (sUAS) (aircraft under 55 lb (25 kg)) design, airworthiness, and subsequent operational applications to the civil aviation authority (CAA).

1.2 It is expected that manufacturers and developers of larger/higher energy sUAS designs, intended to operate in controlled airspace over populated areas, will adopt many of the existing manned aircraft standards in use. These include standards such as SAE ARP4754A and ARP4761, which prescribe a "design for safety" top-down design approach to ensure the sUAS designs can reasonably meet more stringent qualitative and quantitative safety requirements. The ORA, however, remains the same for all risk profiles and will be a part of any sUAS operation.

1.3 In mitigating and preventing incidents and accidents, it is understood that people generally do not seek to cause damage or injure others, and therefore, malicious acts are beyond the scope of this practice.

1.4 As part of the ORA, the applicant should clearly understand and be able to articulate their intended mission for purposes of assessing safety and providing information to regulators. This documentation of a sUAS operation (mission, or set of missions) is what many refer to as a concept of operations (CONOPS).

1.5 This practice is intended primarily for sUAS applicants seeking approval or certification for airworthiness or operations from their respective CAA, though sUAS manufacturers may consider this practice, along with other system safety

[1] This practice is under the jurisdiction of ASTM Committee F38 on Unmanned Aircraft Systems and is the direct responsibility of Subcommittee F38.02 on Flight Operations.

Current edition approved Nov. 1, 2016. Published January 2017. DOI: 10.1520/F3178-16.

design standards, as appropriate to identify sUAS design and operational requirements needed to mitigate hazards.

1.6 *Units*—The values stated in inch-pound units are to be regarded as the standard. The values given in parentheses are mathematical conversions to SI units that are provided for information only and are not considered standard.

1.7 *This standard does not purport to address all of the safety concerns, if any, associated with its use. It is the responsibility of the user of this standard to establish appropriate safety and health practices and determine the applicability of regulatory limitations prior to use.*

2. Referenced Documents

2.1 *SAE Standards:*[2]

ARP4754A Guidelines for Development of Civil Aircraft and Systems

ARP4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment

3. Terminology

3.1 *Definitions:*

3.1.1 *airworthiness, n*—condition in which the small unmanned aircraft systems (sUAS) (including the aircraft, airframe, engine, propeller, accessories, appliances, firmware, software, and control station elements) conforms to its design intent, including as defined by the type certificate (TC), if applicable, and is in condition for safe operation.

3.1.2 *applicant, n*—may be one of the following entities:

3.1.2.1 *manufacturer, n*—sUAS manufacturer that makes changes to the design of an sUAS with a civil aviation authority (CAA) airworthiness approval or kinds of flight operations or both not specifically allowed in the original airworthiness approval. A manufacturer may also be an operator.

3.1.2.2 *operator, n*—entity that applies for CAA approval to operate an sUAS with a CAA airworthiness approval for already approved flight operations or who seeks operational approval for additional kinds of flight operations not presently allowed under that airworthiness approval. If this entity proposes to operate sUAS for additional kinds of flight operations, then the entity shall use normal CAA processes to obtain airworthiness or operational approval or both for the additional kinds of flight operations. This entity can be the original equipment manufacturer (OEM), a manufacturer, or an entity that proposes to operate an sUAS procured from an OEM or a manufacturer.

3.1.2.3 *original equipment manufacturer, OEM, n*—sUAS manufacturer for the original airworthiness approval of a specific sUAS design and kinds of flight operations and an OEM may also be an operator.

3.1.3 *beyond visual line of sight, BVLOS, n*—operation when the individuals (for example, remote pilot in command (RPIC) or visual observer (VO)) responsible for controlling the flight of the small unmanned aircraft (sUA) cannot maintain direct visual contact with the sUA unaided other than by corrective lenses (spectacles or contact lenses) or sunglasses or both.

3.1.3.1 *Discussion*—Technological means may be used for determining the sUA's movement relative to intruding aircraft, obstacles, and terrain; observe the airspace for other air traffic or hazards; and determine that the sUA does not endanger the life or property of another.

3.1.4 *concept of operations, CONOPS, n*—user-oriented document that describes systems characteristics and limitations for a proposed system and its operation from a user's perspective.

3.1.4.1 *Discussion*—A CONOPS also describes the user organization, mission, and objectives from an integrated systems point of view and is used to communicate overall quantitative and qualitative system characteristics and operational procedures to stakeholders.

3.1.5 *control station, CS, n*—interface used by the remote pilot or the person manipulating the controls to control the flight path of the sUA.

3.1.6 *extended visual line of sight, EVLOS, n*—operation when the sUA cannot be seen by the individual responsible for see and avoid with vision that is unaided by any device other than corrective lenses or sunglasses or both and where the location of the sUA is known through technological means; however, the individual responsible for see and avoid shall be able to see intruding aircraft with vision unaided by any device other than corrective lenses or sunglasses or both so that the sUA can be maneuvered clear of collision with other aircraft, terrain, or obstacles, or combinations thereof.

3.1.6.1 *Discussion*—Either the remote pilot in command (RPIC) or, alternatively, the visual observer (VO) can use said technological means for determining the location of the sUA to determine its movement relative to intruding aircraft, obstacles, and terrain; observe the airspace for other air traffic or hazards; and determine that the sUA does not endanger the life or property of another.

3.1.7 *fly-away, n*—unintended flight outside of operational boundaries (altitude/airspeed/lateral) as the result of a failure of the control element or onboard systems or both.

3.1.8 *hazard, n*—potentially unsafe condition resulting from failures, malfunctions, external events, errors, or combinations thereof and this term is intended for single malfunctions or loss of function that are considered foreseeable based on either past service experience or analysis with similar components in comparable manned aircraft applications or both.

3.1.9 *likelihood, n*—estimated probability or frequency, in quantitative and qualitative terms, of a hazard's effect or outcome.

3.1.10 *non-participant, n*—any individual in the vicinity of a sUAS operation who is not participating in the operation of the sUAS.

3.1.11 *operational risk assessment, ORA, n*—engineering evaluation of the proposed design and operation of the sUAS,

[2] Available from SAE International (SAE), 400 Commonwealth Dr., Warrendale, PA 15096, http://www.sae.org.

its intended mission, and proposed area of operation to determine potential risk to persons and property and identify mitigation strategies to reduce that potential risk reasonably through operating procedures or limitations.

3.1.12 *operational risk management, ORM, n*—continual, cyclic, process and the evaluation of the effectiveness of those controls, which includes risk assessment, risk decision making, and implementation of risk controls, that results in acceptance, mitigation, or avoidance of risk.

3.1.13 *pilot, n*—person other than the RPIC who is controlling the flight of a sUAS under the supervision of the RPIC.

3.1.14 *qualitative, adj*—those analytical processes that apply mathematical or numerically based methods to assess the system and airplane safety.

3.1.15 *radio line of sight, RLOS, n*—operational state in which radio communications are over distances where the path between the transmitter and receiver is not obstructed by the curvature of the earth or other obstructions such as terrain or structures.

3.1.16 *reliability, n*—determine that a system, subsystem, unit, or part will perform its intended function for a specified interval under certain operational and environmental conditions.

3.1.17 *remote pilot-in-command, RPIC, n*—person who is directly responsible for and is the final authority as to the operation of the sUAS; has been designated as remote pilot in command before or during the flight of an sUAS; and holds the appropriate CAA certificate for the conduct of the flight.

3.1.18 *residual risk, n*—any risk that remains after mitigation or other control actions.

3.1.18.1 *Discussion*—Residual risk is usually accepted if it is within the risk tolerance of the applicant or CAA or both.

3.1.19 *risk, n*—composite of predicted severity and likelihood of the potential effect of hazards.

3.1.20 *risk mitigations, n*—means to reduce the risk of a hazard.

3.1.21 *safety risk, SR, n*—projected likelihood and severity of the consequences or outcomes from an existing hazard or situation.

3.1.21.1 *Discussion*—The outcome may be an accident or an "intermediate unsafe event/consequence" may be identified as the "worst credible outcome."

3.1.22 *severity, n*—consequence or impact of a hazard's effect or outcome in terms of degree of loss or harm.

3.1.23 *shall versus should versus may, v*—use of the word "shall" implies that a procedure or statement is mandatory and must be followed to comply with this practice, "should" implies recommended, and "may" implies optional at the discretion of the applicant.

3.1.23.1 *Discussion*—Since "shall" statements are requirements, they include sufficient detail needed to define compliance (for example, threshold values, test methods, oversight, and reference to other standards). "Should" statements are provided as guidance towards the overall goal of improving safety and could include only subjective statements. "Should" statements also represent parameters that could be used in safety evaluations and could lead to development of future requirements. "May" statements are provided to clarify acceptability of a specific item or practice and offer options for satisfying requirements.

3.1.24 *small unmanned aircraft, sUA, n*—unmanned aircraft weighing less than 55 lb (25 kg) on takeoff, including everything that is on board or otherwise attached to the aircraft.

3.1.25 *small unmanned aircraft system, sUAS, n*—small unmanned aircraft (under 55 lb (25 kg)) and its associated elements (including communication links and the components that control the sUA) that are required for the safe and efficient operation of the sUA in a national airspace system.

3.1.26 *unmanned aircraft system, UAS, n*—unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the RPIC to operate safely and efficiently in a national airspace system.

3.1.27 *visual line of sight, VLOS, n*—with vision that is unaided other than by corrective lenses or sunglasses or both, the pilot or visual observer shall be able to see the sUA throughout the entire flight to determine its movement relative to intruding aircraft, obstacles, and terrain; observe the airspace for other air traffic or hazards; and determine that the sUA does not endanger the life or property of another.

3.1.28 *visual observer, VO, n*—person who is designated by the RPIC to assist the RPIC and the person manipulating the flight controls of the sUAS to see and avoid other air traffic or objects aloft or on the ground.

4. Summary of Practice

4.1 This practice is intended to provide an understanding of the risk assessment process as a baseline standard for applicants of sUAS designs and operations covered under the "small" designation of a CAA kinetic energy spectrum and that are not generally designed with the rigorous design assurance standards that exist in more complex unmanned aircraft with higher kinetic energy characteristics.

4.2 It is expected that manufacturers of larger/higher energy UAS designs, which are intended to operate in controlled airspace over populated areas, will adopt many of the unmanned aircraft standards in use, such as SAE ARP4754A and ARP4761, that prescribe a "design for safety" top down design approach to ensure the sUAS designs can reasonably meet the more stringent qualitative and quantitative safety requirements.

4.3 The industry "best practices" embodied herein are subject to continuous improvement as safety theory develops and more advanced technologies facilitate greater safety knowledge and application or methods for clarification develop and refine.

5. Significance and Use

5.1 *Use*—This practice is intended for use by parties who desire access to the national, or international, airspace as regulated by their respective CAA(s) either for a vehicle design (airworthiness) or a vehicle's use (operational approval). In this practice, it is recognized the varying levels of complexity, need

for risk assessment(s), and due diligence that should be determined in an ongoing dialogue between the CAA and the applicant. Users should consider their requirements, the purpose that the ORA is to serve, and their risk acceptance level before undertaking the ORA. Use of this practice does not preclude other initiatives or processes to identify hazardous conditions or assess and mitigate associated risks.

5.2 *Risk Reduced, not Eliminated*—No ORA can eliminate all risk or uncertainty with regard to operations. Preparation of an ORA in accordance with this practice is intended to reduce, but may not necessarily completely eliminate, the risk of an operation in which system complexity is minimal, the operation is conducted in a lower risk environment, and the likelihood for harm to people or property, though present, is reduced to an acceptable level. As mission complexity increases, the operational environment may become less risk tolerant. For example, as the kinetic energy associated with the aircraft increases, more complex assessment/analysis tools and greater time may be required to conduct the ORA.

6. Concept of Operations (CONOPS)

6.1 *Purpose*—This section provides guidance to applicants on suggested data an descriptions to include in their CONOPS so that they may better evaluate safety of the operation in the ORA and provide the documentation needed to obtain approval from a CAA to conduct operations. It is up to the applicant to reach agreement with the CAA on the specific contents and format of any CONOPS required. This guidance is not meant to be an exhaustive listing of what is required for approvals or to provide a completed CONOPS to a regulator. Rather, it is meant to clarify some of the key elements that a CAA and the applicant may take into consideration to determine if risks are acceptable.

6.2 *Operational System Description of the Primary Elements of a sUAS*—The aircraft, control station, crew, control link, and data/telemetry communications link parameters shall be documented as follows (where applicable):

6.2.1 *Aircraft*—Description of limitations, normal procedures, emergency procedures, supplemental information, and systems information as it pertains to each type of sUA desired to be operated. Specific detail should be given to onboard subsystems critical for the safety of flight including, but not limited to, flight guidance systems, power plant, fuel and batteries, propellers and rotors, electrical systems and equipment, radio and navigation equipment, and so forth.

6.2.2 *Control Station*—Description of structure, components, mobility, and occupancy, if applicable.

6.2.3 *Crew Members*—Description of required crew members and their responsibilities, credentials, experience, or training, or combinations thereof.

6.2.4 *Command and Control (C2) Link*—Description of frequency and power, susceptibility to compromise and mitigation strategies, and range of operation.

6.2.5 *Data/Telemetry Communications Link*—Description of data and telemetry being gathered and strategies for using data/telemetry to assure safe operations.

6.3 *Description of Operational Scenarios for the sUAS:*

6.3.1 *Define the Operations*—Include a brief description of the types of operations that are allowed in the application. For example, types of operations include agriculture, line inspection, industrial inspection, photography, surveying, research, and film or television production.

6.3.2 Describe the nature of the applicant's business (manufacturer, operator, system integrator, and so forth).

6.3.3 Define geographic operating boundaries (lack of specifics implies very broad national airspace system (NAS) access).

6.3.4 Describe any intent to launch/fly/recover over private property with owner's permission (implies very limited NAS access).

6.3.5 Define the minimum and maximum operating characteristics as well as all other operationally relevant flight characteristics of the aircraft.

6.3.6 Describe intentions to operate within VLOS or outside of VLOS or both: BVLOS, EVLOS, night operations, inclement weather, and so forth.

6.3.7 Identify the occupants of the proposed operating area (both on the ground and in the air).

6.3.8 Describe location of the control station.

6.4 *Summary of the Anticipated sUAS Operations from the Perspective of Other Users of the Airspace and Those on the Ground:*

6.4.1 Identify types of airspace in which the sUAS is to be flown in as well as any special considerations to be taken because of the type of airspace in which it is being flown.

6.4.2 Give launch and recovery details/location(s).

6.4.3 Identify and describe the operation's proximity to people, vehicles, structures, and infrastructure on the ground as well as their density.

6.4.4 Identify and describe the aircraft's proximity to other NAS users.

6.4.5 Identify the meteorological conditions in which operations are intended or likely to occur (visual/instrument, icing, and so forth) and, if other than visual meteorological conditions, the equipment provided to allow such operations.

6.4.6 Identify the flight rules in which operation is intended (visual/instrument flight rules).

6.4.7 Identify whether the geographic and airspace boundaries are physically contiguous.

6.4.8 Identify the automation level (autopilot, manual control, stabilization assistances, return to home, loiter/position hold, height hold, course lock, waypoint navigation, point of interest orbit, and so forth.

6.4.9 Identify minimum crew and their roles.

6.4.10 Identify pilot/aircraft ratio (1:1 and so forth).

6.4.11 Identify day or night operations or both.

6.4.12 Define plan for safety of crew members.

6.4.13 Describe community outreach plans, if any, being used to minimize risk (notices to airmen (NOTAMs), operational awareness information distributed to flying/non-flying public, outreach meetings with municipalities, airports, and so forth).

6.4.14 Describe when/if flight plans will be filed with air traffic control (ATC).

6.4.15 Identify liaisons with ATC, if necessary.

6.4.16 Identify accident and incident reporting procedures.

6.4.17 Summary of any sUAS interaction with ATC and traffic management as well as see-and-avoid strategies.

6.4.18 Describe communication means between the crew members and other air traffic in the area (direct voice, visual, radio, and so forth).

6.4.19 Detail plans involving command and communication functions between different components of the sUAS and other NAS stakeholders.

6.4.20 Describe command and communication functions between the various components of the sUAS (aircraft, control station, control link, observers, and so forth).

6.4.21 Describe the security of the C2 link.

6.4.22 Describe the physical security of the crew members and control station.

6.4.23 Describe ability to maintain real-time situation awareness (terrain, weather, obstacles, and traffic).

6.4.24 Describe the number of pilots, hand-off procedures between control stations (direct, daisy-chain, and so forth) and, if more than one pilot is used, procedures to ensure only one PIC is in control of the operation.

6.4.25 Describe lost-link procedures for loss or interruption of positive control.

6.4.26 Describe emergency procedures (in the event of lost link, the UA shall squawk appropriate code if transponder equipped).

6.5 *Non-VLOS Operational Considerations*—For the following flight operations, address the specific factors necessary to maintain safe operational control of the aircraft, accurate knowledge of its location, and the capability to see and avoid other traffic or objects aloft or on the ground:

6.5.1 EVLOS.

6.5.2 EVLOS using VOs who are collocated with the PIC.

6.5.3 EVLOS using VOs who are not collocated.

6.5.4 EVLOS using VOs using aided vision.

6.5.5 Daisy chaining of VOs or VOs on a moving platform (chase plane, boat, vehicle, and so forth).

6.5.6 BVLOS.

6.5.7 BVLOS when the PIC and VO are unable to track visually the aircraft because of night-time flying visual meteorological conditions (VMC).

6.5.8 BVLOS using technological support to PIC only.

6.5.9 BVLOS using technological support to the PIC and VO requiring aided vision or technological support or both.

6.5.10 Night operations using technological support to PIC or VO or both.

6.6 The above suggested elements of a CONOPS will assist applicants in both evaluating their operation as part of safety management processes and provide a foundation of documentation needed to ensure all parties to the operation understand the mission context and safety overall. As noted in Section 7, a complete and fully vetted CONOPS will provide applicants a framework to evaluate safety in an organized and deliberate way without underestimating or overextending the scope of their effort in conducting an ORA. With this foundation document to refer to, applicants will find that the work of conducting an ORA will be streamlined, more efficient, and produce cost savings in operations overall.

7. Operational Risk Assessment (ORA)

7.1 *Introduction*—System safety is the discipline and practice of identifying, analyzing, and mitigating hazards of a particular system, program, project, or activity using a "systems" approach throughout its life cycle. The application of safety management systems (SMS) methodology is a best practice in aviation operations for overall safety and risk management. System safety analysis and use of a structured hierarchy of controls (to affect hazards and their associated risks) during unmanned system design, manufacturing, modification, or integration is the precondition of an applicant's SMS program. There are several system safety and SMS process outputs that can serve as evidence to support an applicant's case that a sUAS or sUAS operation is safe. An applicant can show an unmanned system will be operated safely by providing approval authorities evidence of hazards identified, analyzed, and mitigated. Applicants of unmanned aircraft operations should scale their system safety analysis for hazards and mitigations needed to the level of rigor appropriate for their CONOPS, which should include operational size, complexity, and mission scenario as discussed in Section 6. Just as there are multiple sizes and missions of unmanned systems, there are multiple ways to approach safety hazard identification, analysis, mitigation, and documentation of residual risk to be provided to CAA or approval authorities. A key to successful and appropriate evidence to support arguments that an unmanned system and its operation is safe lies in appropriately determining severity and likelihood of undesired events occurring during mission execution.

7.1.1 An operational risk assessment for any system shall document the system, its operation (including mission scenario or CONOPS), and the hazards identified that might occur as a result of unexpected or expected events during a mission. Next, applicants shall show how those hazards will be addressed and mitigated to manage adverse results within the operation. Once mitigations have been determined, the residual risk will be assessed and accepted or rejected by the CAA or approval authority charged with approving the operation. However, before seeking CAA approval of any residual risk, the applicant shall determine its risk tolerance, that is, the level of residual risk acceptable to the applicant. This risk tolerance should include a rationale to support selection of the risk criteria that supports an organization's risk tolerance.

7.1.2 To provide information adequately about the operation, the applicant should determine the appropriate detail needed for the system and its operation based on complexity of the system and is operational environment. This system/mission description is explained in detail in Section 6. The CONOPS and ORA are tightly coupled since higher than acceptable risks identified in the ORA may often need to be mitigated by operational procedures or limitations that are documented in the CONOPS. When such operational changes result in acceptable risk levels, the associated risk mitigations are documented in the ORA. This relationship is illustrated in Fig. 1.

7.1.3 As shown in Fig. 1, if an ORA results in an unacceptable risk, changes need to be made in the product itself in the way in which the product will be operated (documented in the

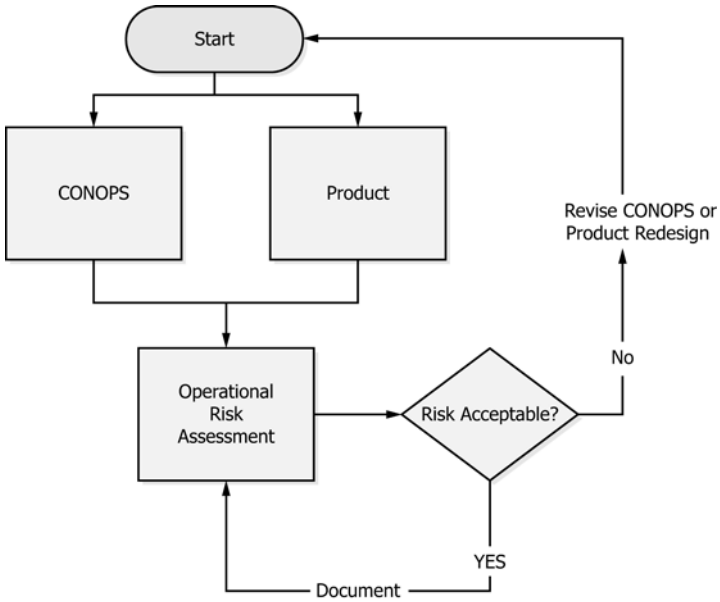

FIG. 1 CONOPS and ORA Relationship Flowchart

CONOPS) or in required training before operation. It is also critical that applicants understand that conducting sUAS operations in a manner other than intended in the original CONOPS plans or as the product was designed will change the results of the ORA. This should immediately trigger a stop to the operation until the changes to assumptions and assertions made in the original ORA are resolved and updated and CAA approval obtained if needed.

7.1.4 Introduced in 7.2, hazard identification is a process that should take into account a full understanding of how the product will be used and operationally deployed. Without a firm plan for both product use and limitations, applicants risk missing new hazards introduced through change or existing hazards that are untraceable when CONOPS or product details are inadequate or unavailable.

7.2 *Hazard Identification:*

7.2.1 *Introduction*—For the purpose of sUAS safety risk management, the term hazard is better understood as a condition that could cause or contribute to unsafe operation of sUAS with regard to persons or property on the surface or in the air. For example, hazardous conditions typically create an environment in which an accident is more likely to occur. Hazards, and hazardous conditions in sUAS operations, are normal and expected components of operations. However, with the appropriate mitigations, hazards and hazardous conditions can be managed and accepted to ensure operations can and will be conducted safely. Hazards should be identified for the sUAS, operational environment, crew, traffic in the air, and people or property on the ground. Hazards can be identified through site surveys, flight data-monitoring programs, training programs, review boards, expert risk panels, investigations, audits, and inspections. Potential failures shall be considered by an applicant in the ORA, and therefore, Appendix X1 has been included to help identify common failures to sUAS.

7.2.2 *Property on the Ground*—Hazards assessed for property on the ground should include infrastructure items such as substations, high-power electrical transmission lines, water treatment plants, and so forth. They may also include sensitive areas for flight such as schools, hospitals, or large gatherings of people.

7.2.3 *Hazard Tracking System*—Hazards should be identified, documented, tracked, and managed through a hazard tracking system that should fit the needs of the organization and allow safety managers to review and treat hazards actively and efficiently. The hazard tracking system complexity should be appropriate to the size of the operation and should fit the needs and budget of the applicant.

7.2.4 *Voluntary Reporting System*—Applicants should consider establishing a voluntary, anonymous, non-punitive safety reporting system that allows employees to report safety issues without fear of reprisal. Employees should be encouraged to help identify hazards to improve the overall safety of the organization. These hazards can then be used in addition to those identified as part of the ORA activity and to assess fully safety in the ORM process.

7.3 *Risk Analysis:*

7.3.1 *Introduction*—Following hazard identification, a risk analysis shall be performed. Risk analysis describes the process of characterizing the nature and level of risk associated with each of the previously identified hazards. A measurement of risk is established through the combination of likelihood and severity, that is, the likelihood of a hazard occurring and the severity of that hazard. The level of risk associated with a hazard is established by mapping the component measures of severity and likelihood to a qualitative or quantitative index or scale as detailed in Tables 1-4. The most common and accessible tool used to illustrate this mapping is the safety risk matrix. The definitions and construction of the risk matrix may be tailored to the specific organizational or operational needs or both of each applicant.

7.3.2 The definitions of each level of severity and likelihood need to be defined in terms that are realistic and reasonable for

TABLE 1 Severity Definitions

Severity of Occurring Hazard		
Severity Level	Definition	Value
Catastrophic	Non-sUAS equipment destroyed (such as electrical transmission lines, substation, water treatment facility, and so forth); multiple fatalities.	5
Hazardous	Large reduction in safety margins; vast reduction in ability to complete duties accurately; single fatality or serious injury; major equipment damage.	4
Major	Significant reduction in safety margins; reduction in the ability of pilots to cope with adverse operating conditions as a result of increased workload; serious accident; injury to persons.	3
Minor	Nuisance; minor incident.	2
Negligible	Little or no negative consequence.	1

TABLE 2 Likelihood Definitions

Likelihood of Hazard Occurring During an Operation		
Likelihood Level	Definition	Value
Frequent	Likely to occur many times	5
Occasional	Likely to occur sometimes	4
Remote	Unlikely, but possible, to occur	3
Improbable	Very unlikely to occur	2
Extremely Improbable	Almost inconceivable to occur	1

TABLE 3 Example Risk Matrix

Severity	Likelihood				
	Extremely Improbable (1)	Improbable (2)	Remote (3)	Occasional (4)	Frequent (5)
Catastrophic (5)	5	10	15	20	25
Hazardous (4)	4	8	12	16	20
Major (3)	3	6	9	12	15
Minor (2)	2	4	6	8	10
Negligible (1)	1	2	3	4	5

TABLE 4 Example Risk Categories

Risk Score	Risk	Description
1 to 4	Low	Acceptable without review
5 to 11	Moderate Risk	May be acceptable with review
12 to 19	High Risk	Shall be mitigated
20 to 25	Very High Risk	Unacceptable

the operational environment. This realistic definition of severity and likelihood for each hazard ensures each applicant's tools for dealing with hazards are applicable for the environment, operation, or system design encountered, or combinations thereof. An example of severity and likelihood definitions can be found in Table 1. A value is assigned to each severity and likelihood level to be used subsequently in a risk matrix.

7.3.3 To determine the appropriate severity level as defined in Table 1 for a given hazard, an applicant shall identify the potential for death or injury to people and damage to property. To determine the appropriate likelihood score, the applicant shall assess the likelihood of a hazard's occurrence. The use of quantitative data relating to frequency of occurrence is generally preferred over qualitative data. Absent quantitative data, the example definitions in Table 2 may be used to estimate values.

7.3.4 To estimate likelihood, many sources may be consulted including: system safety assessments, mishap reports, historical reports of flight hours, and subject matter experts chosen because of their experience with other aircraft systems and their ability to transfer that expertise to the sUAS and its relevant mission and related hazards.

7.3.5 A risk matrix allows the assessor to assign a risk score to each hazard, which is composed of a severity value and likelihood value. Grading each hazard component separately allows for a straightforward but also more objective and rational identification of high risks and prioritization of mitigations. Averaging risks with different characteristics, or excessively splitting risk, could mask important elements of the assessment generating new risks. The risk score is the severity value (from Table 1) multiplied by the likelihood value (from Table 2). The final risk score is between 1 and 25.

7.3.6 Risk scores are placed into the risk matrix per their severity and likelihood values. In Table 3, an example of a risk matrix comprised of scores calculated by multiplying the severity times the likelihood scores is shown. The risk is scored as a value between 1 and 25 to categorize the risk as low, moderate, high, and very high, which are further defined in Table 4.

7.3.7 The definitions in Table 1 and Table 2 and risk scores in Table 3 and Table 4 should be used unless tailored alternative definitions or a tailored matrix or both are approved by CAAs. While these tables have subjective elements, Tables 1-4 represent a recognized method of providing quick and effective risk analysis.

7.3.8 *Interpreting Results*—After calculating risk scores, hazards should be ranked from most to least serious safety effect (very high- to low-risk levels) to find the overall level of risk of the operation in the application of this risk matrix. Hazards may be assessed as very high level of risk, a high level of risk, a moderate level of risk, or a low level of risk. Very high levels of risk may be deemed unacceptable under any circumstance and may need to be eliminated. High levels of risk shall be mitigated by eliminating the hazard, lessening the severity of the hazard, or reducing the likelihood of the hazard occurring. Moderate levels of risk may be deemed acceptable upon review, potentially in combination with a mitigation to reduce the hazard's residual risk. Low levels of risk are acceptable and require no action. The acceptance levels for various types of outcomes (death, damage to the sUAS, damage to property, loss of sUAS without loss of life, and so forth) may differ depending on the mission, pilot, organization, and CAA. It is essential for the applicant to establish when risks can be tolerated and when risk is deemed unacceptable and shall be further mitigated. Determination of risk tolerance should be independent of the risk analysis and its associated outcomes. For example, the applicant may not allow a risk score (severity value times likelihood value) of 20 or higher: an

organization may require modification to design, operational environment, crew training, or other to reduce the risk score.

7.3.9 *Concurrence on Acceptable Risk*—For type certification or other aviation authority approval, the governing approval authority should concur with the acceptable risk determination. Unacceptable risks may require a higher level of design assurance or redesign or both, additional operational mitigations reflected in an updated CONOPS, or vehicle design changes. All unacceptable risks shall be addressed.

7.3.10 *Mitigating Risk*—The risk to people (participating or third parties) and property may be mitigated by design requirements, operational mitigations, or geographic limitations, or combinations thereof. If operational constraints, design requirements, or geographic limitations are insufficient for mitigating the risk to people and property, the sUAS may be redesigned, operational limitations revised, additional design assurances provided, or some combination of actions as specified in an updated CONOPS.

8. Common Operational Mitigations for sUAS

8.1 *Training*—sUAS crew training is a key method of risk mitigation. Pilot and crew member abilities to identify hazards are enhanced through training related to flight operations and airspace rules. Through the proper training, pilots and crews are able to develop the critical thinking required for appropriate response to hazards and an overall attitude of safety. For instance, training in standard pre-flight activities will lower overall risk as crews conduct disciplined checks and assessments of mission plans in association with current conditions present at the time of each flight. As a result, properly trained sUAS operators know that risk is reduced through mitigations identified during pre-flight planning hazard assessment.

8.1.1 Training may also dictate the level of pilot capability and knowledge. For flights conducted at or below controlled airspace, training received from another sUAS operator, an online course, or CAA ground school class may provide the requisite knowledge needed to understand airspace rules, aircraft limitations, and operational rules of the sUAS operational environment. Operations at altitudes greater than 400 ft (122 m) above ground level (AGL) may require a license or certification of training commensurate with the increased responsibilities associated with higher altitudes, controlled airspace integration, or generally more complex airspace environments. Either way, it is important to understand and abide by the relevant CAA's requirements for licensing or certification of crew and aircraft before crews participate in the operation or take to the controls of the sUAS during a mission.

8.1.2 System knowledge may also be enhanced through pilot and crew training. Knowledge of critical performance parameters of a sUAS, such as maximum command and control link range and lost-link protocols, is a precondition for flight. For example, if a directional antenna is used, one may choose to improve the antenna performance by physically pointing the antenna towards the aircraft in a more optimal manner consistent with its design. These practices offer a means to avoid potential lost-link hazards. System knowledge is also important in recovering from unusual attitudes and avoiding high-risk maneuvers.

8.2 *Remote Flight Pathways*—To reduce risk through geographical operational limitations, an applicant may choose to fly sUAS in remote areas or avoid flight paths over nonparticipants or both. Remote operations may also require avoiding flying near structures.

8.3 *Minimize Pilot Tasking*—Hazards arising from human (pilot) error can be reduced by avoiding task overload. For example, when a pilot receives an alert, particularly an alert annunciating imminent danger, the pilot should focus their attention on key responsive tasks. The control station, including its interface, should not overload the pilot with information or tasks that degrade or impede the pilot from safe flight. An additional crew member tasked with operating the payload may help to mitigate the risk of overtasking for PIC.

8.4 *Standard Operating Procedures*—Standard operating procedures (SOPs) should be developed that are consistent with sUAS manufacturer information. All crew members should train to these procedures to reduce operational risk.

8.5 *Mission Go/No-Go Criteria*—Similar to manned aviation, sUAS applicants shall determine their go/no-go criteria in advance. The go/no-go criteria encompass more than simply assessing sUAS limitations. In addition, pilot capability, awareness of the relevant geography (including proximity to people), current and changing weather conditions across the entire flight path, and system limitations, among other factors, inform the final go/no-go decision.

8.6 *Procedural Changes in Specific Flight Environments*—Pilots and crew members may need to incorporate additional operational limitations, flight procedures, maintenance processes, inspections, and so forth depending on the flight environment. For example, if a sUAS operates in a particularly harsh environment, the frequency of inspections may need to be increased and additional maintenance performed. Additional systems may also require monitoring during flight; however, limitation should never be reduced without specific CAA approval.

9. Operation (Mission) System Configuration Management and Data Requirements

9.1 *Introduction*—The following section outlines mission and system configuration management and associated data requirement best practices to be included as part of applicant applications and ORA considerations. Overall change management practices should be adhered to regardless of whether the change occurring is within the mission concept, aircraft configuration, use of a sUAS, or the interaction between sUAS subsystems. The principles of change management and associated data requirements are part of the overall safety management of a program regardless of the size or scope of involved program's operations. The CAA may have mandatory configuration management and change management requirements. For type certification, there exist data retention requirements and approval requirements of any changes to the sUAS (including software elements). Coordination with the CAA throughout these processes is vital.

9.2 *System Configuration Management (CM) Plan*—The sUAS applicants should establish a standard CM plan for

maintaining sUAS equipment and software as a fundamental supporting element of operational risk assessments and in support of the operations and system configuration component of operations. A CM approach provides a sUAS applicant a method to implement the policies, procedures, techniques, and tools to manage system changes, evaluate proposed changes to a sUAS CONOPS or ORA, track the status of changes to any system element, and maintain an inventory of sUAS systems and operations with associated documentation through the sUAS life cycle.

9.2.1 Changes to system and design requirements of the sUAS should be approved and documented according to a CM plan, and should reflect accurately the system design and operational status. Furthermore, the applicant is responsible for asserting that the sUAS is airworthy and safe for the intended flight.

9.3 *Data Requirements*—Proper data management throughout the ORA life cycle is essential to support a robust safety management process. Data management is the continuous development and maintenance of processes and procedures to assure that an applicant has the necessary data in an organized, reliable, appropriate, current form with configuration control. Establishing data attribute requirements, and a data management plan, enables effective hazard identification and risk mitigation. Data to be collected should include, but are not limited to:

9.3.1 CONOPS-related data that supports the ORA;

9.3.2 Hazards identified in the ORA;

9.3.3 Severity and likelihood scoring for the hazards identified and rationale for their scoring;

9.3.4 Mitigations that were implemented to diminish the overall risk to an acceptable level or at the level the acceptance of risk verified and mission approved;

9.3.5 Continued operational safety data, such as accidents, incidents, and significant sUAS failures that may impact ORA results or assumptions or both; and

9.3.6 The source of all data gathered in 9.3.1 – 9.3.5 and the data and time of the operations for which they were considered.

10. Keywords

10.1 airworthiness; concept of operations; control; design; operation; operational effects; ORA; risk assessment; system failure

APPENDIXES

(Nonmandatory Information)

X1. COMMON FAILURES TO sUAS BY CATEGORY

X1.1 sUAS share some common characteristics that are often considered vulnerable to loss of function and should be addressed within the ORA. The following list of function losses (organized by category) serves as a preliminary guide for an ORA. While an ORA considers many, if not all, of the potential failures identified in the following, others may exist that are peculiar to a specific UAS and also require review.

X1.1.1 *Power/Prop, Electrical Powered*—Electronic speed control failure, propulsion battery failure, motor failure—electrical fault, motor failure—structure or bearings failure, propeller structural or connection failure, wiring or connector failure, and fire.

X1.1.2 *Power/Prop, Internal Combustion Powered*—Engine control failure, fuel delivery or fuel contamination failure, motor failure—lubrication system failure, motor failure—ignition system failure, motor failure—structure or bearing failures, propeller structural or connection failure, and fire.

X1.1.3 *Flight Control (Includes Stabilization and Guidance)*—Avionics battery or power supply failure, control computer failure, actuators/servo failure, global positioning system (GPS) receiver failure, GPS antenna failure, inertial measurement unit (IMU) failure, and wiring or connector failure.

X1.1.4 *Communications*—Transmitter failure, receiver failure, external interference/EMI/EMC, self-generated interference/EMI/EMC, and wiring or connector failure.

X1.1.5 *Human/Ground*—Inadequate training, improper reaction, inadequate man-machine interface, misjudgment—weather, inadequate procedures, excessive workload, fatigue, and ergonomics.

X1.1.6 *Miscellaneous*—Physical environment (wind, rain, and icing), GPS obstruction, and communications link obstruction.

X2. EXAMPLES OF HAZARD OR FAILURE IDENTIFICATION AND MITIGATION PRACTICES

X2.1 See Table X2.1 for examples of hazard of failure identification and mitigation practices.

TABLE X2.1 Examples of Hazard or Failure Identification and Mitigation Practices

Failure Condition	Description	Mitigation Examples
Fly-away	This failure condition occurs when an unmanned aircraft fails to respond to any ground control system commands, proceeds on a route unknown to the pilot, and continues on a pathway until fuel exhaustion. These failure conditions create significant risk to other aircraft and persons. Therefore, it is incumbent upon the applicant to understand if their sUAS is vulnerable to this failure condition.	The applicant should understand all scenarios where the aircraft could enter a "flight not under control of the pilot" mode. For those systems with pre-programmed flight paths (typically invoked upon lost comm or lost C2 link events), the pilot should assure that the aircraft follows a specific, known flight path upon a C2 link failure condition. The pilot and sUAS designer should know the deterministic behaviors of the aircraft.
Loss of electrical power to aircraft systems, such as command and control or motors driving sUAS propulsion, or GPS, and so forth	Electrical power typically is used by the aircraft to power flight computers (autopilot), control surfaces (actuators or servos), GPS, radio, and so forth. The electrical system for a sUAS typically is one distribution system with voltages affected by components within that electrical power distribution system or the system being powered. Therefore, a failure in the electrical power distribution system, its components, its power source, and so forth may cause sUAS critical systems failures.	The pilot should check all connections before flight. The battery capacity should be sufficient as determined by briefing and flight plan before launch. All flight control surface movements should be confirmed. A pre-flight checklist should be prepared and followed by the pilot to assure that the electrical system is intact and functional. An inspection and maintenance plan should be developed by the pilot to include both manufacturer recommendations and those actions responsive to the particular flight environment, mission, and pilot.
Loss of thrust	A thrust loss could occur because of partial or catastrophic engine failure, engine control failure, propeller failure, environmental factors (such as icing), fuel loss, and so forth.	The pilot should include a propulsion system check before launch. This check may include a pre-flight engine power check to assure engine availability for the mission. An inspection and maintenance plan should be developed by the pilot including not only the actions recommended by the manufacturer but also actions that may be necessary because of the flight environment specific to the CONOPS.
Loss of communications with sUAS (commonly referred to as a lost link)	Radio failure, antenna failure, interference from other systems, weak signal, range exceedance, and so forth may cause loss of communications (lost C2 link).	Before flight, the pilot shall assess radio communications via a consistent procedure, including exercising the flight controls to assure the communications link is intact and functional.
Lost GPS (either a signal from the satellite or a failure of the GPS systems on the sUAS)	Most sUAS systems depend on GPS links for navigation and control of the aircraft. Loss of GPS may occur because of interference from other radio signals, loss of the GPS itself (because of GPS failure, loss of electrical power to the GPS, and so forth), shadowing caused by proximity to other structures or land formations, and so forth.	Before flight, the pilot shall assess the GPS by confirming its performance: signal strength, sufficient satellites in view, and accurate position of the stationary aircraft. The pilot will assess the intended flight path to assess if GPS loss may occur. The pilot may choose alternate flight paths to decrease the chance of GPS loss.
Loss of sUAS control as a result of "hijack" (another entity takes control of the sUAS)	sUAS radio links may be vulnerable to other signals, intentional and unintentional, which could cause the aircraft to deviate from its intended flight path. Although no aircraft failure may be present, the aircraft may no longer be controlled by its pilot.	The pilot should assess the radio link before flight and immediately after flight. The pilot may choose to use encrypted communications links.
Loss of flight control (this scenario comprises failure of flight control surfaces or the auto-pilot, and so forth)	Flight control failures may comprise system failures (such as control surface actuators and servos), flight computer failures (provides incorrect flight control signal to the control surface actuator), and so forth.	Before flight, the pilot will assess all control surface function by actuating and observing proper movements of surfaces.
Control station failure	Control station failures may occur as a result of loss of electrical power, system failure (of components or systems within the ground control system such as the ground control computer or iPad or other), software failure (such as software), and so forth.	The control station may possess a backup power supply or ensure that the remote control elements are charged to a satisfactory level before every flight. The pilot will exercise the ground control system to assure its appropriate operation before flight.
Impacts of rain, snow, dust, or other environmental factors	Environmental conditions may affect the sUAS including: carburetor icing for gasoline/diesel fueled engines; radio signal deformation as a result of rain or snow; icing that affects control surface movement; water exposure of the avionics; humidity affecting connectors; and so forth.	The pilot may limit sUAS operations for those environments that may cause or are likely to cause aircraft system failures. The pilot should follow manufacturer limitations.
Fuel degrades	Fuel impacts may include: fuel starvation caused by inadequate fuel for the mission; fuel contamination that affects engine operation; fuel mix failures wherein oil is over or under mixed into the fuel; and so forth.	Fuel quality may be assured through a fuel-handling procedure. The fuel procedure should include a "mix" process for fuels that require oil or other additives.
Fuel system failures	Fuel measuring system failures may result in loss of power, fuel sloshing may cause fuel measurement error, fuel measuring system components may fail, fuel tank leakage, and so forth.	Fuel quantity initially loaded into the aircraft may be measured for certainty of total usable fuel on board. Fuel estimation programs, software that estimates fuel usage and compares this value to fuel quantity reported, may provide additional confidence.
Electrical capacity failures	Batteries play a critical role for many UASs. Battery capacity is impacted by: improper charge/discharge cycles, failure to follow manufacturer's battery conditioning protocol, physical abuse to a battery (such as dropping), storing the battery in extreme cold (allowing the battery to freeze) or too hot condition (allowing the battery to exceed its recommended maximum temperature), and so forth.	The pilot should obtain battery inspection and maintenance information directly from the battery manufacturer. The battery voltage may provide additional insight for the ground control system display. Battery handling procedures may prevent too cold or hot events.