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