



Standard Practice for Ensuring Dependability of Software Used in Unmanned Aircraft Systems (UAS)¹

This standard is issued under the fixed designation F3201; 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.

1. Scope

1.1 This standard practice intends to ensure the dependability of UAS software. Dependability includes both the safety and security aspects of the software.

1.2 This practice will focus on the following areas: (a) Organizational controls (for example, management, training) in place during software development. (b) Use of the software in the system, including its architecture and contribution to overall system safety and security. (c) Metrics and design analysis related to assessing the code. (d) Techniques and tools related to code review. (e) Quality assurance. (f) Testing of the software.

1.3 There is interest from industry and some parts of the CAAs to pursue an alternate means of compliance for software assurance for small UAS (sUAS).

1.4 This practice is intended to support sUAS operations. It is assumed that the risk of sUAS will vary based on concept of operations, environment, and other variables. The fact that there are no souls onboard the UAS may reduce or eliminate some hazards and risks. However, at the discretion of the CAA, this practice may be applied to other UAS operations.

1.5 *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 FAA Standard:²

FAA 23.1309-1E System Safety Analysis and Assessment for Part 23 Airplanes

¹ This practice is under the jurisdiction of ASTM Committee F38 on Unmanned Aircraft Systems and is the direct responsibility of Subcommittee F38.01 on Airworthiness.

Current edition approved Sept. 1, 2016. Published September 2016. DOI: 10.1520/F3201-16.

² Available from Federal Aviation Administration (FAA), 800 Independence Ave., SW, Washington, DC 20591, <http://www.faa.gov>.

2.2 IEC Standard:³

IEC 62304 Medical Device Software—Software Life Cycle Processes

2.3 ISO Standards:⁴

ISO 9001 Quality Management Systems—Requirements

2.4 ICAO Standard:⁵

ICAO 9859 Safety Management Manual

2.5 NASA Standard:⁶

NASA Technical Briefs Making Sense out of SOUP (Software of Unknown Pedigree)

2.6 RTCA Standards:⁷

RTCA DO-178C Software Considerations in Airborne Systems and Equipment Certification

RTCA DO-278A Software Integrity Assurance Considerations for Communication, Navigation, Surveillance, and Air Traffic Management (CNS/ATM) Systems

RTCA DO-326 Airworthiness Security Process Specification

2.7 Military Standards:⁸

Department of Defense Joint Software System Safety Handbook

MIL-STD-882E Department of Defense Standard for System Safety

3. Terminology

3.1 Definitions of Terms Specific to This Standard:

3.1.1 *application programming interface (API)*—definition of the inputs and outputs for operations intended for use by other software modules.

3.1.2 *architecture*—architecture is made up of the definition of the sUAS Software components, the data that flows between

³ Available from International Electrotechnical Commission (IEC), 3, rue de Varembe, P.O. Box 131, 1211 Geneva 20, Switzerland, <http://www.iec.ch>.

⁴ Available from International Organization for Standardization (ISO), ISO Central Secretariat, BIBC II, Chemin de Blandonnet 8, CP 401, 1214 Vernier, Geneva, Switzerland, <http://www.iso.org>.

⁵ Available from International Civil Aviation Organization (ICAO), 999 Robert-Bourassa Blvd., Montreal, Quebec H3C 5H7, Canada, <http://www.icao.int>.

⁶ Available from U.S. National Air and Space Administration (NASA), 300 E. Street, SW, Suite 5R30, Washington, DC 20546, <http://www.nasa.gov>.

⁷ Available from Radio Technical Commission for Aeronautics (RTCA), 1150 18th St., NW, Suite 910, Washington, DC 20036, <http://www.rtca.org>.

⁸ Available from DLA Document Services, Building 4/D, 700 Robbins Ave., Philadelphia, PA 19111-5094, <http://quicksearch.dla.mil>.