



Designation: F3269 – 17

Standard Practice for Methods to Safely Bound Flight Behavior of Unmanned Aircraft Systems Containing Complex Functions¹

This standard is issued under the fixed designation F3269; 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 defines design and test best practices that if followed, would provide guidance to an applicant for providing evidence to the civil aviation authority (CAA) that the flight behavior of an unmanned aircraft system (UAS) containing complex function(s) is constrained through a run-time assurance (RTA) architecture to maintain an acceptable level of flight safety.

1.2 This practice will have the benefit of enabling highly automated UAS operations. It is envisioned that applicants will use this practice as a means of compliance for safe implementation of complex functions for routine operations.

1.3 Verification of complex functions is considered too challenging to use conventional software assurance methods such as RTCA DO-178C or IEC 61508. Certification challenges under these standards include generating required artifacts, such as requirements, elimination of unintended functionality, traceability/coverage, and test cases required for verification.

1.4 There is significant interest from industry and CAAs to have a standard practice to enable flight operations for UAS containing complex functions. Developing a certification path for these UAS technologies could also advance safety in General Aviation.

1.5 The following design tenets are offered to provide guidance to the UAS manufacturer as to the intended application of this standard.

1.5.1 The RTA Architecture is intended to be used for Complex Functions that would require an amount of effort that is beyond reasonably practicable to pass CAA conventional certification requirements.

1.5.2 The UAS manufacturer should engage in appropriate design, test, and validation activities to enable the Complex Function to perform as intended.

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, 2017. Published September 2017. DOI: 10.1520/F3269-17.

1.5.3 The complexity of the Recovery Control Function (RCF) deterministic commands should be minimized insofar as practicable.

1.5.4 Repeated invocation of an RCF during a single mission may be considered an indication of improper Complex Function performance.

1.5.5 An RTA design with multiple RCFs should consider the aircraft state, relative outcomes, and differences in RTA recovery times in prioritizing the recovery actions in the safety monitor.

1.5.6 The UAS manufacturer should strive to minimize false or nuisance triggers of one or more RCFs as these false alarms undermine user confidence in the system and impact operational efficiency.

1.6 *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, health, and environmental practices and determine the applicability of regulatory limitations prior to use.*

1.7 *This international standard was developed in accordance with internationally recognized principles on standardization established in the Decision on Principles for the Development of International Standards, Guides and Recommendations issued by the World Trade Organization Technical Barriers to Trade (TBT) Committee.*

2. Referenced Documents

2.1 ASTM Standards:²

F3201 Practice for Ensuring Dependability of Software Used in Unmanned Aircraft Systems (UAS)

F3178 Practice for Operational Risk Assessment of Small Unmanned Aircraft Systems (sUAS)

2.2 Civil Standards, Policy, and Guidance:

IEC 61508 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems³

² For referenced ASTM standards, visit the ASTM website, www.astm.org, or contact ASTM Customer Service at service@astm.org. For *Annual Book of ASTM Standards* volume information, refer to the standard's Document Summary page on the ASTM website.

³ Available from International Electrotechnical Commission (IEC), 3, rue de Varembe, 1st Floor, P.O. Box 131, CH-1211, Geneva 20, Switzerland, <http://www.iec.ch>.

RTCA DO-178C Software Considerations in Airborne Systems and Equipment Certification⁴

3. Terminology

3.1 Definitions of Terms Specific to This Standard:

3.1.1 complex function—software function or algorithm that may cause the UAS to operate in a manner that is difficult to predict due to compounded implications from factors such as sensor measurement precision, algorithm complexity, environmental variables (for example, gusts, traffic, electromagnetic effects, etc.), multi-core processing, probabilistic algorithms, fuzzy logic, machine learning, genetic algorithms, resource availability, and aircraft system state. These software functions or algorithms are sometimes referred to as “autonomous”, “non-deterministic”, “artificial intelligence”, “adaptive”, or “intelligent” algorithms.

3.1.2 continuous built-in test—component level tests that are critical for monitoring the integrity of data and health of the aircraft systems which are crucial for validating the data used for determining acceptable aircraft safety and stability and control.

3.1.3 decision delay—cumulative delays from the safety monitor and the RTA Switch.

3.1.4 input delay—cumulative delay from the sensed inputs and the RTA Input Manager.

3.1.5 non-pedigreed components—hardware and software items for which the UAS manufacturer does not or cannot produce sufficient evidence that these items on their own will operate within an acceptable level of risk based on the operational risk assessment.

3.1.6 pedigreed components—hardware and software items for which the UAS manufacturer produces sufficient evidence that these items on their own will operate within an acceptable level of risk based on the operational risk assessment.

3.1.7 pre-defined limits—defined not-to-exceed restrictions that, if exceeded, would create a safety hazard. These “hard limits” are determined from the operational risk assessment (for example, taking into account vehicle characteristics, CONOPS, etc.).

3.1.8 recovery control function—a pedigreed function or software algorithm to return the UAS to a safe state. For example, a sequence of commands that causes the UAS to land safely, to maneuver in space, return to level flight, or deploy a flight recovery system.

3.1.8.1 RCF complete—the system state where the RCF has been effective in ensuring the UAS will not violate its pre-defined limits.

3.1.8.2 RCF delay—the cumulative delay from each RCF.

3.1.8.3 RCF response delay—the delay between the initiation of the RCF and RCF complete.

3.1.8.4 RCF trigger thresholds—the thresholds in the safety monitor which the UAS manufacturer sets to ensure that action

is taken before the UAS violates a pre-defined limit. These “soft limits” trigger the safety monitor to command the RTA switch to an appropriate RCF and account for all delays between command of the RTA switch and the execution of the recovery action.

3.1.9 run-time assurance architecture—a system of pedigreed components that implements real-time monitoring, prediction, and fail-safe recovery mechanisms that bounds the flight behavior of a non-pedigreed complex function to ensure the safety of a UAS. Includes the components in Fig. 1.

3.1.9.1 RTA input manager—a function or device that integrates sensor data and monitors sensor state.

3.1.9.2 RTA recovery time—the delay between the inputs to the RTA architecture and RCF complete. RTA recovery time includes the RTA response time plus vehicle dynamics, human response time (if implemented), etc.

3.1.9.3 RTA required inputs—data from sensors, discrete state indicators, vehicle state monitors, and other sources that describe the aircraft state and its environment.

3.1.9.4 RTA response time—the delay between the inputs to the RTA architecture and the activation of each recovery control function. RTA response time is the system end-to-end delay and includes input delay, decision delay, and RCF delay. See Fig. 2.

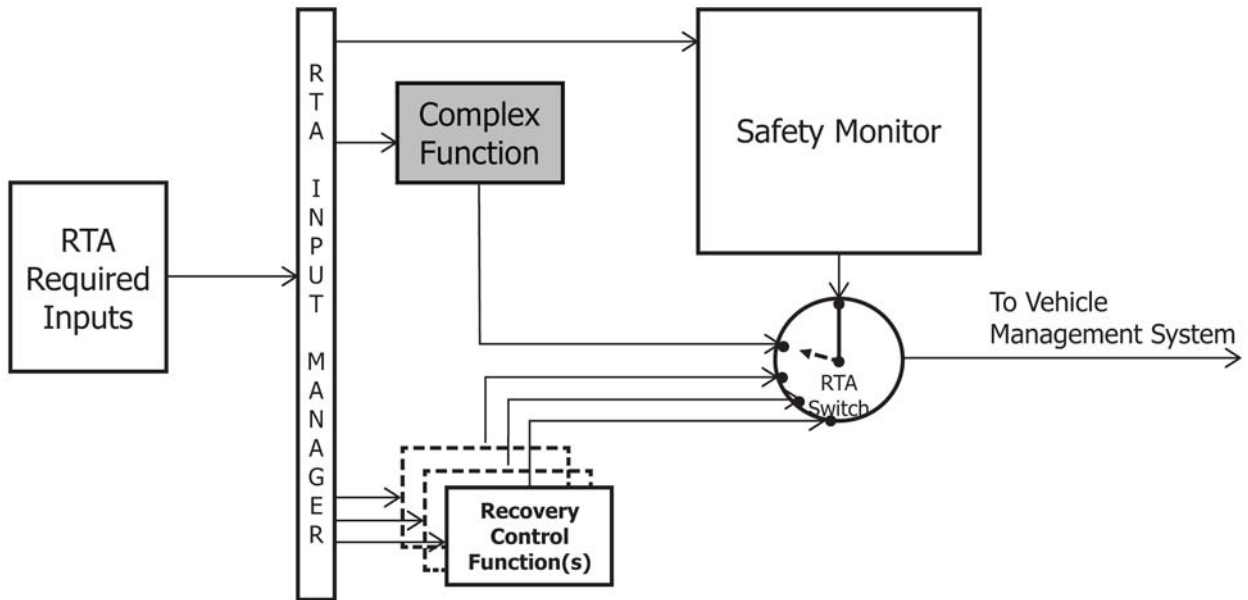
3.1.9.5 RTA switch—a function or device that receives control commands from the safety monitor which determines whether the complex function or specific recovery control functions are sending commands to the aircraft systems to execute the appropriate action. The RTA switch ensures that only a single function is sending commands to the vehicle management system.

3.1.10 safety monitor—continually monitors aircraft state to determine if the aircraft is or is predicted to exceed pre-defined limits. As necessary it will control the safety switch to enable execution of the recovery control function (including determining which recovery control function is executed if more than one exists).

3.1.11 shall versus should versus may—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 supplier, manufacturer, or operator. Since “shall” statements are requirements, they include sufficient detail needed to define compliance (for example, threshold values, test methods, oversight, and references to other standards). “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.

3.1.12 vehicle management system—elements critical to maintaining normal flight and to executing all recovery control functions. Requirements for the VMS are derived from other standards and may include certified autopilots, inner-loop flight controls, outer-loop flight controls, etc.

⁴ Available from Radio Technical Commission for Aeronautics (RTCA), 1150 18th NW, Suite 910, Washington, DC 20036, www.rtca.org.



- Pedigreed components
- Non-pedigreed component

FIG. 1 Functional Components of a Generic Run-Time Assurance Architecture

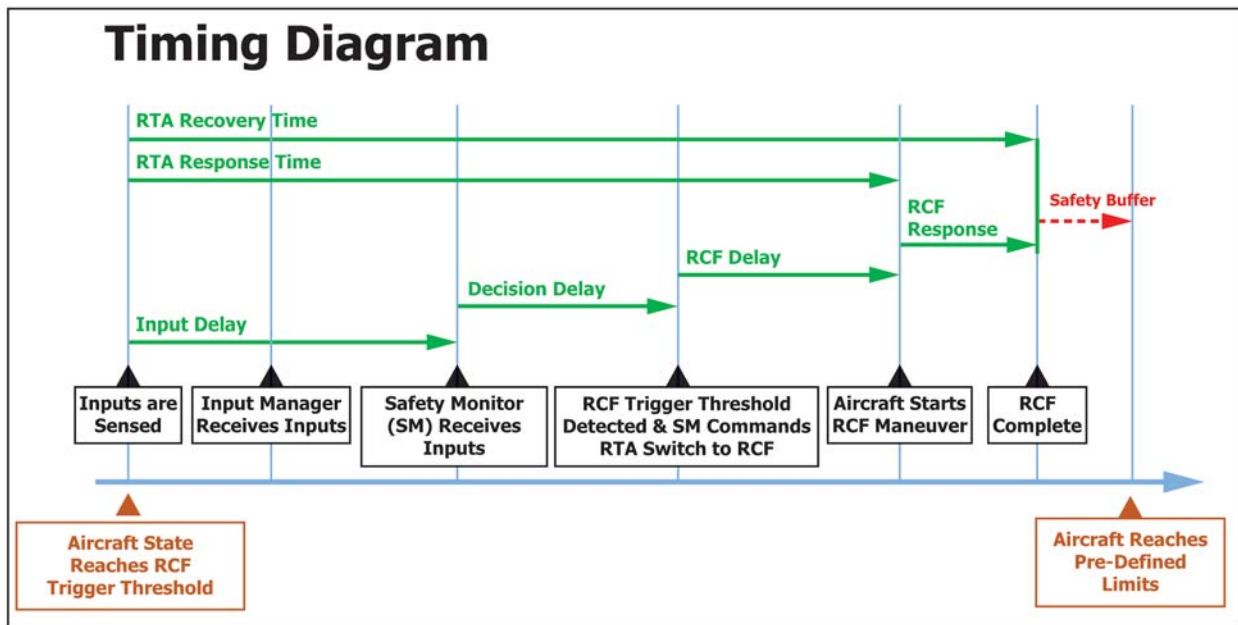


FIG. 2 RTA Response Timing Diagram

3.2 Acronyms:

3.2.1 CAA—Civil Aviation Authority.

3.2.2 CF—Complex Function.

3.2.3 ORA—Operational Risk Assessment.

3.2.4 RCF—Recovery Control Function.

3.2.5 RTA—Run-time assurance.

3.2.6 SM—Safety Monitor.

3.2.7 UAS—Unmanned Aircraft System.

3.2.8 VMS—Vehicle Management System.

4. Applicability

4.1 The focus of this practice is UAS operations, including extended visual line of sight and beyond visual line of sight operations. At the discretion of the CAA, this practice may be applied to other UAS or other aviation operations, based on a