Designation: F3269 – 21

Standard Practice for Methods to Safely Bound Behavior of Aircraft Systems Containing Complex Functions Using Run-Time Assurance[1]

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.

INTRODUCTION

This practice defines an architecture using Run-Time Assurance (RTA) in conjunction with unassured functions or commercial off-the-shelf (COTS) functions that have not been developed to traditional aerospace standards and processes. This section provides the scope, applicability, and intended use for the understanding of this practice.

The practice is organized as follows: *(1)* An introduction, background, and scope to provide context for applying the capabilities defined in this practice to unmanned aircraft system (UAS) certification, or operational approval, or both. *(2)* Definitions of key terms and abbreviations. *(3)* Description of a Run-Time Assurance (RTA) architecture. *(4)* Appendixes that contain Examples of RTA in systems and supplemental information. *(a)* Ground Collision Avoidance System (GCAS) as an Example RTA. *(b)* Machine Learning AI Autopilot (MLAA). *(c)* Run-Time Assurance for a Neural Network-Based Adaptive Flight Control of an Unmanned Aircraft. *(d)* Run-Time Assurance for Risk-Based Operation. *(e)* Example Implementation of Timing and Latency Requirement. *(5)* A list of documents referenced herein.

BACKGROUND

There is significant interest from industry and civil aviation authorities (CAA) to have a standard practice to enable new and novel technologies used in UAS operations containing unassured or COTS functions/systems, or both, to be used on certified aircraft and aviation systems. From this point forward, "functions/systems" will be referenced as "functions." Developing a certification path for these technologies may also introduce greater safety to aviation.

In this practice, the term *Complex Function* (CF) may be any function, algorithm, component, or system that has not been subject to accepted CAA or aerospace design assurance practices, or both (DO-178C, DO-254, ARP4754A, etc.). Motivations to use such an unassured function arise from the need or desire to use commercial, off-the-shelf systems or parts that have algorithmic complexity, probabilistic algorithms, fuzzy logic, environmental uncertainties, or no pedigree. The complexity may also come from factors associated with new and novel technologies such as sensor measurement precision, nondeterministic algorithms, data-driven algorithms, or artificial intelligence (for example, machine learning, genetic algorithms). A complex function may be any combination of software or hardware.

Traditional approaches to digital avionics design begin with the assumption that each software and hardware component on an aircraft contribute independently to the safe operation of the platform. At the core of this process is an assessment of the risks associated with the functional failure of each system, assembly, or component to ensure that the aircraft meets the required safety objectives. This is known as design-time assurance.

This practice describes a run-time assurance method, which may be used as an alternative means to or in combination with design-time assurance. RTA mitigates the risk of complex function misbehavior by managing the system's use of the Complex Function output. The RTA includes a safety monitor, which monitors the complex function or the behavior the complex function has on the system, or both, at run-time. In the event the safety monitor determines that the complex function is not operating correctly, or is driving the system to an unsafe state, it disengages the complex function and initiates a recovery function.

This practice provides an RTA architecture and best practices that provide guidance to an applicant for ensuring that the behavior of an unmanned aircraft system (UAS) containing complex functions maintains the acceptable level of safety.

At the time of this practice's development, there is no accepted formal guidance material for certifying commercial UAS containing complex functions. Emerging CAA certification guidance, processes, and concepts have been considered in the development of this practice.

[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 July 15, 2021. Published November 2021. Originally approved in 2017. Last previous edition approved in 2017 as F3269–17. DOI: 10.1520/F3269-21.

1. Scope

1.1 The scope of this practice includes the following:

1.1.1 A set of components that comprise an RTA system.

1.1.2 Requirements and best practices to determine safe boundaries and RTA system coverage.

1.1.3 Requirements and best practices for an RTA system and RTA components, as applicable.

1.1.4 Appendixes with examples that demonstrate key RTA system concepts.

1.2 RTA components are required to meet the design assurance level dictated by a safety assessment process. Guidance for the safety assessment process may be found in references appropriate for the intended operations (ARP4754A, ARP4761, Practice F3178, etc.).

1.3 This practice was developed with UAS in mind. It may be applicable for aspects of manned aircraft certification/approval, as well as aviation ground systems. The scope of this practice is also envisioned to allow a variety of aircraft implementations where a human may perform the role of either the Complex Function or a Recovery Function.

1.4 The scope of this practice does not cover aspects of hardware/software integration. These should be considered separately during the development process.

NOTE 1—This practice does not suggest a one-size-fits-all strategy knowing that not all use cases may fit well into this architecture. There may exist additional components required to satisfy specific applications to the practice.

1.5 The values stated in inch-pound units are to be regarded as standard. No other units of measurement are included in this standard.

1.6 *Table of Contents:*

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

1.8 *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.*