Addressing FAA 14 CFR PART 450.141

A Comparison with RTCA DO-178C

genuen

ideas taking flight

Genuen's analysis of the Federal Aviation Administration's Part 450 Launch and Reentry License Requirements for Software Computing Systems

Abstract

Since its founding, Genuen has been providing its business partners with effective, timely avionics technology solutions, ensuring the safety of their software and computing products using RTCA DO-178C as the basis for software systems certification. The recently released Launch and Reentry License Requirements set forth in § 450.141 of the FAA's Title 14 Code of Federal Regulations detail the certification basis for computing systems in spacecraft launch and reentry vehicles. This document compares and contrasts § 450.141 with RTCA DO-178C, showing how Genuen can leverage its extensive experience in commercial aviation toward meeting the requirements of the space industry. The findings of this comparison show significant similarities and overlap between the two sets of regulations, most notably in the development and process sections, as well as their overall flexibility based on project type and needs. The major differences are where topics covered by § 450.141 are outside the scope of DO-178C (RTCA, 2011; FAA, 2020a).

Introduction

On September 30, 2020 the Federal Aviation Administration (FAA) submitted Part 450 of the Title 14 Code of Federal Regulations (14 CFR) for publication, which was driven by the Streamlining Launch and Reentry Licensing Requirements (SLR2) Final Rule. Section 450.141 provides specific requirements regarding licensing of Computing System Safety Items, which are defined as any software or data that implements a capability that, by intended operation, unintended operation, or non-operation, can present a hazard to the public.

Genuen has significant experience in developing and testing avionics systems utilizing the standard processes defined in RTCA DO-178C – Software Considerations in Airborne Systems and Equipment Certification (and prior versions of DO-178). Pursuant to this knowledge, this paper compares § 450.141 with DO-178C standards to understand the similarities and differences. The goal of this analysis is to define a process model based on the current Genuen knowledge base that supports fulfillment of the requirements of § 450.141 for licensing submittal for our current and future customers (RTCA, 2011; FAA, 2020a, p. 375).

Overview of Section 450.141

Part 450 defines the requirements for obtaining and maintaining a license from the FAA for launch and reentry (or both) of a space vehicle. Section 450.141 specifically addresses the prescribed hazard controls for safety-critical computing systems.

Note: Section 450.141 focuses on the safety requirements for software, whereas Section 450.143 describes the requirements of the hazard controls for safety-critical hardware.

Section 450.141 is broken into sections (a) through (d) as described below:

(a) § 450.141(a) Identification of Computing System Safety Items requires identification of the Computing System Safety Items and their associated Level of Criticality (FAA, 2020a, p. 378-380).

(b) § 450.141(b) Safety Requirements requires the identification, evaluation, implementation, and verification and validation for all Safety Requirements associated with each Computing System Safety Item (FAA, 2020a, p. 380-384).

(c) § 450.141(c) Development Process requires documentation of the Development Process used for implementation, verification, and validation of the Safety Requirements (FAA, 2020a, p. 384-389).

(d) § 450.141(d) Application Requirements defines the minimum set of documentation and data required for license application submittal (FAA, 2020a, p. 389-396).

AC 450-141.1A Computing Systems

In October 2020, the FAA issued Advisory Circular (AC) 450.141-1 Computing Systems to provide a means of compliance to § 450.141. On August 16, 2021, the FAA released Revision A updates to AC 450.141-1 under AC 450.141-1A. AC 450.141-1A was written to be very flexible, offering multiple ways to show compliance. Most of these are based upon other standards from the space and defense industries.

AC 450.141-1A defines a means to identify the computing system safety items that present hazards to the public. This is achieved through analysis of all software functions in a way that provides compliance with § 450.141(a). Partitioning may be used to separate safety from non-safety functions. The list of computing system safety items should include all software functions that perform safety-related functions based on functional hazard analysis per § 450.107(b). Appendix B of AC 450.141-1A provides two methods for conducting the computer system hazard analysis using either Software Failure Modes and Effects Analysis (SFMEA) or Software Fault Tree Analysis (SFTA), with corresponding examples for each. There are five methods provided by AC 450.141-1A for assigning criticality levels, all of which are based on the severity of the hazard to the public and the degree of control of the computing system safety item. AC 450.141-1A references several other industry documents for determining the degree of control and severity of hazard categories (FAA, 2020b, p. 16-18, 42-53).

For defining the safety requirements per § 450.141(b), AC 450.141-1A describes a means of compliance by identification, formal inspections, implementation, and verification. Appendix A provides examples of generic safety requirements for computing system safety items. This includes safety requirements specific to the computing system safety item functionality, including power requirement, anomaly/fault detection and responses, interfaces, maintenance, and other functional requirements. Appendix A also includes safety requirements relating to process, such as Verification and Validation, Configuration Management, Standards, Security, etc. (FAA, 2020b, p. 29-41)

AC 450.141-1A also provides guidance for compliance to the safety measures required for the development process called out under § 450.141(c). The development process should be based on the level of criticality of each computing system safety item identified within § 450.141(a). Based on the level of rigor required, the process should become more stringent, adding to the confidence level that the safety requirements have been properly implemented and verified. Use of industry standards are encouraged to provide a compelling rationale for acceptance of the development process (FAA, 2020b, p. 18-26).

As defined above, § 450.141(d) addresses the requirements for the licensing application (FAA, 2020a, p. 389-396). AC 450.141-1A merely summarizes these requirements. The application must include the following:

- Computing system safety items with associated level of criticality
- Safety requirements for each computing system safety item
- Documentation of the development process from requirements through verification and validation
- Evidence of implemented requirements and associated test artifacts (FAA, 2020b, p. 27-28).

Note: The FAA also indicates that there will be a second Advisory Circular coming out in the third quarter of 2021 to address compliance to § 450.141 for Mission Data Loads (AC 450.141-2).

DO-178C Overview

One of the standards with which Genuen has significant experience is RTCA DO-178C. RTCA is an organization which creates industry standards that are recognized and referenced by Federal Aviation Administration (FAA) regulations. DO-178C provides comprehensive guidance for the development of airborne software. It has become the universal basis for development of airborne software in avionics applications and is seen as a fundamental process model for both hardware and software standards across multiple industries (RTCA, 2011).

The purpose of DO-178C is to define the lifecycle processes that must be followed and the objectives that must be met to certify airborne software. DO-178C provides graduated levels of process rigor based on Design Assurance Levels (DAL). These span from A–E and are based on the impact of possible software failure (A being catastrophic to the safety of the aircraft, operators, or passengers; E having no effect on safety). Higher DAL levels have increasingly stringent processes that must be followed in order to achieve certification, and the specifics of these processes are defined as objectives (RTCA, 2011).

The current DO-178C process includes the following fundamental components:

- Planning (RTCA, 2011, p. 25-30).
- Development (RTCA, 2011, p. 31-38).
- Verification (RTCA, 2011, p. 39-52).
- Configuration Management (RTCA, 2011, p. 53-60).
- Quality Assurance (RTCA, 2011, p. 61-64).
- Certification (RTCA, 2011, p. 65-67).

DO-178C is widely considered one of the most rigorous and stringent software product development standards. It requires a comprehensive understanding of not only the process guidelines, but also the intent of the objectives and the required supporting documentation.

DO-178C is part of a suite of standards in the aerospace industry that includes:

- DO-254, which sets similar requirements for complex hardware used in mission-critical avionics
- SAE ARP4754A, which addresses system-level concerns
- SAE ARP4761 which addresses the safety assessment process
- (RTCA, 2011; 2005; SAE, 2010; 1996).

Comparing Section 450.141 to DO-178C

In some ways, comparing Title 14 CFR Part 450.141 to DO-178C is like comparing an apple tree with an apple. In this case, DO-178C would be like a big apple on a tree that only yields a few apples. DO-178C only maps to part of § 450.141(b) and all of § 450.141(c). The sections below address these differences, including not only the extensions beyond DO-178C (apple tree to apple), but also comparing the process sections of § 450.141 with the process sections of DO-178C (apple to apple) (FAA, 2020a; RTCA 2012).

Hazard Analysis

As indicated, § 450.141(a) does not correspond to any processes within the scope of DO-178C. Section 2.0 of DO-178C discusses the system aspects relating to software development, which includes discussion regarding the System Safety Assessment process and how that applies to the Software Levels. It is indicated that the System Safety Assessment process is part of the system life cycle processes, which references SAE ARP47574A. It should also be noted that SAE ARP4761 provides a detailed process for completing a System Safety Analysis on Civil Airborne Systems, and it is also referenced as a driving process within ARP4754A (RTCA, 2011; 2005; SAE, 2010; 1996).

Therefore, § 450.141(a) would be better compared to SAE ARP4754A, but that evaluation is beyond the scope of this paper.

Levels of Rigor

Both § 450.141 and DO-178C define software levels that establish the level of rigor necessary for compliance. In both cases, this level is defined by the degree of control (the contribution of the software to the failure), which comes out of the system safety assessment process, and the severity of that failure condition (FAA, 2020a; RTCA 2012).

DO-178C provides a very thorough description of the Failure Condition Categories defining the severity level. These 5 categories (Catastrophic, Hazardous, Major, Minor, and No Safety Effect) map directly to the 5 software DALs, Level A through Level E respectively (FAA, 2020a; RTCA 2012).

AC 450.141-1A provides multiple methods for determining the Level of Criticality, most of which are based on software control categories and consequence classifications from other Industry Standard documents. These include documents such as RCC 319-19, MIL-STD-882E, and NASA-GB-8719.13. This provides more flexibility in defining the Level of Criticality based on the applicant's area of familiarity. Additionally, the Level of Criticality can be determined by the computing system safety item's fault tolerance (defined by a table in AC 450-141-1A) or by just selecting the highest level of criticality and applying the accompanying safety standards to all system safety items (FAA, 2020b; RCC, 2019; DOD, 2012; NASA, 2004).

Hazard Assessment – Public Versus Aircraft, Crew, and Passengers

It should be noted that the failure condition categories or consequence classifications between the DO-178C and AC 450.141-1A are evaluating the hazards to different impacted group. The failure condition categories in DO-178C discuss the impacts to the flight crew, passengers, and loss of aircraft, whereas the consequence classifications in AC 450.141-1A address the hazard impacts to the public (FAA, 2020b; RTCA 2012).

Process Versus Plans

Unlike the submittal of Plan documents prior to development described in DO-178C, AC 450.141-1A indicates that the Development Process needs only to be documented and submitted as part of the license application. For 450.141, there is no need for approval of the process prior to executing the development when using the process laid out in AC 450.141-1A. However, prior buy-in from the FAA is required when using a tailored RCC 319-19 development process (FAA, 2020b; RTCA 2012; RCC, 2019).

Tailoring RCC 319-19

AC 450.141-1A indicates a tailored RCC 319-19 process can be used as the software development process for developing computing system safety items. However, it also indicates that applicants should carefully consider the requirements of RCC 319-19 prior to tailoring for computing system safety components that are not part of a Flight Termination System. This seems to indicate that unless your computing system safety item is a Flight Termination System or part of a Flight Termination System, it may not be advisable to tailor the RCC 319-19 to meet the safety requirements of the software development process (FAA, 2020b; RCC, 2019).

Coverage of Plans

At the highest level, the development process defined in AC 450.141-1A and required by § 450.141 covers the plans called for in DO-178C. Aside from minor differences in levels of rigor, the expectations of the Software Development Plan (SDP) and Software Verification Plan (SVP) are included within the § 450.141 development process. In contrast, the Software Quality Assurance Plan (SQAP) and the Software Configuration Management Plan (SCMP) identified in DO-178C are not completely required by the § 450.141 development processes. Additionally, the DO-178C Plan for Software Aspects of Certification is somewhat irrelevant for § 450.141 except for the definition of the software life cycle and software life cycle data (FAA, 2020b; 2020a; RTCA, 2012).

Note: There is no mention of Tool Qualification within the AC 450.141-1A, although a similar process may be required to provide a compelling argument for acceptance of the license application package if a tool is used to develop or verify a critical part of a computing system safety item.

Software Quality Assurance

Unlike DO-178C, which requires a specific Software Quality Assurance Plan (SQAP), the guidance in AC 450.141-1A only states that quality assurance "may support the achievement of performance objectives" for licensing with § 450.141. Additionally, AC 450.141-1A indicates that quality assurance "could evaluate the validity of system safety data" (RTCA 2012; FAA, 2020b).

AC 450.141-1A provides two references for software quality assurance methods, NASA Software Assurance and Software Safety Standard (NASA-STD-8739.8), and NASA Software Engineering and Assurance Handbook (NASA-HDBK-2203) (2020a; 2020b).

Configuration Management

AC 450.141-1A requires an adequate Configuration Management (CM) process for continuing efficacy of each released version of the computing system safety item.

Note: There is no mention of Tool Qualification within the AC 450.141-1A, although a similar process may be required to provide a compelling argument for acceptance of the license application package if a tool is used to develop or verify a critical part of a computing system safety item.

Software Quality Assurance

Unlike DO-178C, which requires a specific Software Quality Assurance Plan (SQAP), the guidance in AC 450.141-1A only states that quality assurance "may support the achievement of performance objectives" for licensing with § 450.141. Additionally, AC 450.141-1A indicates that quality assurance "could evaluate the validity of system safety data" (RTCA 2012; FAA, 2020b).

AC 450.141-1A provides two references for software quality assurance methods, NASA Software Assurance and Software Safety Standard (NASA-STD-8739.8), and NASA Software Engineering and Assurance Handbook (NASA-HDBK-2203) (2020a; 2020b).

Configuration Management

AC 450.141-1A requires an adequate Configuration Management (CM) process for continuing efficacy of each released version of the computing system safety item.

This configuration management and control process should be in force during the entire life cycle of the program, from initiation of development through retirement. It should include control of project documentation, source code, object code, data, development tools, test tools, environments (hardware and software), and test cases (FAA, 2020b).

Unlike DO-178C, there is no concept of Control Categories (CC1 and CC2) defined in AC 450.141-1A. Instead, the focus is on the ability to capture a Configuration Index for each release and to maintain future releases. This CM process includes capturing of baselines and traceability from safety requirements to the tests and test results. Additionally, the CM process must include a method for tracking changes between baselines (FAA, 2020b, MTC 2012).

Traceability

Traceability in AC 450.141-1A focuses on tracing from the safety requirements to the test evidence. There is no indication of tracing to the code as being required like it is for most DAL levels in DO-178C. Though not required, it could be possible to trace to the tests through the code. That method of testing/tracing does not appear to be prohibited (FAA, 2020b).

Development Standards

Unlike DO-178C, use of development standards is not required by AC 450.141-1A. However, AC 450.141-1A also states that "referencing a standard may produce a compelling rationale for the acceptance of a development process". RCC 319-19 is identified as a possible means to use for compliance. AC 450.141-1A also references the use of safety standards, which are not covered by DO-178C. MIL-STD-882 or GEIA-STD-0010A include approaches for analyzing risk and classifying hazards (FAA, 2020b; RCC, 2019; RTCA, 2012; DOD, 2012; SAE, 2018).

Verification and Validation

A similar level of rigor to those defined in AC 450.141-1A for development and implementation of safety requirements should also be applied to testing. Therefore, the testing expectations are based on the level of criticality assigned to the computing system safety item for which the test is defined, with the highest level of criticality verified by an independent department or organization. AC 450.141-1A does not specify the level of testing, but it does imply that this will be tied to the standards used to define the level of criticality. The AC does define test types (unit, interface, system, stress, and regression) that may be used, although testing is not limited to these types. It also defines another set of verification tests that can be used: equivalence partitioning, boundary value, error guessing, statement coverage, decision coverage, function coverage, and call coverage. Unlike DO-178C, there is no mention of multiple condition decision coverage (MCDC), which is required for DAL A development. This seems to imply that MCDC is not necessary within AC 450.141-1A, but that level of detail will need to be verified through the other referenced standards being used for compliance (FAA, 2020b; RTCA, 2012).

Application Requirements

Section 450.141(d) calls out the application requirements for licensing by the FAA of software computing systems as part of launch or reentry spacecraft. This is unlike RTCA DO-178C, which does not address requirements for licensing or certification of the aviation software, but instead provides the process that the FAA recognizes for use during certification of avionics or other aviation components containing software.

The application process for certification of aircraft components falls outside of scope of RTCA DO-178C but is covered by other FAA specific processes. Like Part 450 which covers Launch and Reentry License Requirements, the FAA also has Title 14 CFR Parts 23, 25, 27, and 29 to cover Airworthiness Standards for Normal Category Airplanes, Transport Category Airplanes, Normal Category Rotorcraft, and Transport Category Rotorcraft respectively. Parts 23, 25, 27, and 29 allow for certification of individual avionics systems separately through Technical Standard Orders (TSO) that are specific to each avionic system functionality. The TSO is usually where DO-178C is invoked as the preferred process for software development. Additionally, the TSO defines the requirements for certification of the avionic system, similarly to § 450.141(d) (FAA, 2020a; RTCA 2012).

Comparison Summary

When applying for a Computing System license against the requirements of Title 14 Code of Federal Regulations Part 450.141, experience with DO-178C can be very useful, specifically when looking at parts of § 450.141(b) and all of § 450.141(c). Although there are some minor differences in the processes, the overall structure of the development corresponds nicely. The level of rigor based on the Level of Criticality defined for the Computing System Safety Item in AC 450.141-1A translates closely with the Design Assurance Levels defined in DO-178C, with the exception that there may not be an AC 450.141-1A equivalent to the most critical and stringent DAL A. Following DO-178C processes with the right level of rigor would exceed the requirements described in § 450.141(b) and all of § 450.141(c) (FAA, 2020a, RTCA 2012).

Without detailed analysis, it appears that following process of SAE ARP4761 and SAE ARP4754 would fulfil the requirements of § 450.141(a) and the hazard assessment of § 450.141(b). Section 450.141(d) compliance is met by providing the documentation for the computing system safety items, requirements, development process, and test evidence (SAE, 2010; 1993; FAA, 2020a).

References

Department of Defense. (2012). *MIL-STD-882E Department of Defense standard practice: system safety*. http://everyspec.com/MIL-STD/MIL-STD-0800-0899/MIL-STD-882E_41682/.

Federal Aviation Administration. (2020a). *14 CFR Part 450.141: Streamlined launch and reentry license requirements.* https://www.faa.gov/space/streamlined_licensing_process/media/SLR2_Final_Rule_450.pdf.

Federal Aviation Administration. (2021). Advisory Circular 450.141-1: Computing system safety. https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_450.141-1A_Computing_System_Safety_20210816_v1_(002).pdf.

National Aeronautics and Space Administration. (2004*). NASA-GB-8719: NASA software safety guidebook.* https://standards.nasa.gov/standard/osma/nasa-gb-871913.

National Aeronautics and Space Administration. (2020a). *NASA-STD-8739: Software assurance and software safety standard.* https://standards.nasa.gov/standard/osma/nasa-std-87398.

National Aeronautics and Space Administration. (2020b). *NASA-HDBK-2203): Software Engineering and Assurance Handbook.* https://standards.nasa.gov/standard/oce/nasa-hdbk-2203.

Radio Technical Commission for Aeronautics. (2012). *RTCA DO-178C: Software considerations in airborne systems and equipment certification.* https://global.ihs.com/doc_detail.cfm?document_name=RTCA%20DO%2D178&item_s_key=00088334.

SAE International. (1996). *ARP4761: Guidelines and methods for conduction the safety assessment process on civil airborne systems and equipment.* https://www.sae.org/standards/content/arp4761/.

SAE International. (2010). *ARP4754A: Guidelines for development of civil aircraft and systems.* https://www.sae.org/standards/content/arp4754a/.

SAE International. (2018). *GEIASTD0010A: Standard best practices for system safety program development and execution.* https://www.sae.org/standards/content/geiastd0010a/.