Workshop on Advisory Circular (AC) 450.141-1A

Computing System Safety

Presented by:

Jay Naphas, FAA/AST
Diane Doran, FAA/AST

September 23, 2021
Advisory Circulars (ACs) are being used to supplement streamlined regulations by the Federal Aviation Administration (FAA), Commercial Space Transportation (AST).

The goals of the ACs are to:

- Further explain the meaning of the regulatory text and its intent
- Provide a means of compliance

The ACs are guidance, not a regulation, and so compliance is voluntary.

To demonstrate compliance using an AC, the entire AC must be implemented. This means that the FAA must approve any variance from a “should” statement in the AC.
DISCUSSION IS ENCOURAGED

We have up to two hours today, with incremental periods for Q&A as we step through the chapters of the AC.

NOTE:
Answers by presenters are preliminary; a future revision of the AC is the official response.
Discussion

Floor open for questions/comments
Either verbally or via comments
Objectives of § 450.141

To produce understanding of computing systems and how to make them safe
• Each requirement is designed to drive understanding of an aspect of safe software
• Together, the requirements produce the minimum level of understanding needed to know that computing systems are safe for the public

To fit with a wide range of development processes
• Each requirement is a goal of any safe development process
• Requirements are technology-independent

To work constructively with system safety
• Requirements build on the foundation laid by system safety analyses
• Requirements establish confidence in safe computing system behaviors
• Requirements facilitate understanding of human-computer and computer-hardware interfaces
Structure of § 450.141

Computing system found in a safety role (FHA, SFMEA, etc) 450.107 or 450.141(a) requires

Severity assessment 450.141(a)(2)
Degree of control assessment 450.141(a)(2)

combine into

Criticality assessment 450.141(a)(2)
determines

Computing System Safety Item description requirements 450.141(d)(1)
Minimum development rigor 450.141(c)
Verification and validation requirements 450.141(b)(4), (c)(6), and (d)
Structure of the AC

Walks through the regulation
• Each requirement has one or more means of compliance

Describes a method to document compliance
• Software safety is iterative

Appendices provide supplemental information
• Appendix A provides sample safety requirements
• Appendix B provides sample software safety analysis methods
• Appendix C provides lessons learned from spacecraft failures and aircraft accidents
• Appendix D provides lessons learned from commercial, military, and experimental aircraft accidents

Advisory Circulars are not mandatory
AC 450.141-1A has two means of compliance:

1. Tailoring RCC 319-19 or later
   - Recommended for FSS, AFSS, and other dedicated safety systems
   - Tailored version must be tailored during pre-application consultation and included in the application

2. Direct compliance
   - Follows chapters 6 through 9 of AC 450.141-1A
Discussion

Floor open for questions/comments
Either verbally or via comments
Regulation

FAA revised proposed § 450.111 and re-designated it as § 450.141.

Replaces prescriptive requirements with performance-based standards and provides increased flexibility for operators to demonstrate compliance.

Scales level of rigor based on each computing system’s system-level criticality by severity and degree of control, rather than by degree of autonomy.

Section 450.141 requires the identification and assessment of the public safety-related computing system requirements, functions, and data items in order to streamline the evaluation of computing system safety.

§ 450.141 Computing Systems.

(a) Identification of Computing System Safety Items. An operator must identify:

(1) Any software or data that implements a capability that, by intended operation, unintended operation, or non-operation, can present a hazard to the public; and

(2) The level of criticality of each computing system safety item identified in subparagraph (1), commensurate with its degree of control over hazards to the public and the severity of those hazards.
§ 450.141(a) In Practice

Section 6 of AC 450.141-1A

“Computing system safety item” means any software or data that implements a capability that, by intended operation, unintended operation, or non-operation, can present a hazard to the public, and the criticality of each computing system safety item, commensurate with its degree of control over hazards to the public and the severity of those hazards.

- Includes software that could interfere with the operation of a computing system safety item, as well as each computing system safety item’s human and hardware interfaces

Identified computing system safety items should be evident in a standalone document, FHA, or other system safety product

- Applicant and FAA should agree on the list of computing system safety items prior to application submission
Identifying Computing System Safety Items

System Safety Analyses may identify Computing System Safety Items (CSSI)

- Section 6.1
- CSSI is a collection of software or data that can present a hazard to the public
- Evident as a cause or control to a hazard in functional hazard analysis
- Evident in software requirements derived from system safety analyses
Define severity levels (Section 6.2.3)

- Adapt existing standards to public safety
  - Most definitions include public and 1\textsuperscript{st} party people
  - Inclusion of 1\textsuperscript{st} party may elevate severity, especially with cleared areas
  - Applicants can tailor definitions for public safety
- Inherit severity categories from functional hazard assessment
  - Relies on accurate and consistently applied severity definitions
Assessing Criticality

Define control levels using one of several methods (Section 6.2.4)

- Assume high degree of control for all CSSI
- RCC 319-19 software categories (for flight safety systems)
- MIL-STD-882E software control categories and software criticality index
- NASA-GB-8719.13 software control categories and software risk index
- Fault tolerance categories

Criticality assessments drive minimum acceptable rigor in development and testing

Highly-reliable flight safety systems can reduce degree of control, typically from “Autonomous” to “Redundant fault-tolerant”
Floor open for questions/comments
Either verbally or via comments
Section 450.141(b) requires an operator to develop safety requirements for each computing system safety item.

“Safety requirements” means computing system requirements that specify attributes or functionality that have public safety significance. Identification of this subset of requirements related to public safety is essential to focus an operator’s safety efforts on those parts of the computing system safety item that have public safety consequences.

Example of a means of compliance for § 450.141 can be found in AC 450.141-1, “Computing System Safety.”

§ 450.141 Computing Systems.

(b) Safety Requirements. An operator must develop safety requirements for each computing system safety item. In doing so, the operator must:

1. Identify and evaluate safety requirements for each computing system safety item;
2. Ensure the safety requirements are complete and correct;
3. Implement each safety requirement; and
4. Verify and validate the implementation of each safety requirement by using a method appropriate for the level of criticality of the computing system safety item. For each computing system safety item that is safety critical under § 401.7, verification and validation must include testing by a test team independent of the development division or organization.
§ 450.141(b) In Practice

Computing system safety items implement safety requirements (Section 7)

- Identify safety requirements for each computing system safety item (Section 7.1)
  - Safety requirements are a subset of software or system requirements
- Validate the safety requirements (complete and correct, Section 7.2)
  - Should check that the safety requirements are consistent with the system’s safety requirements
  - Should check that the safety requirements fully specify all needed safety functionality
- Implement the safety requirements
  - As normal for computing system requirements
- Verify and validate the implementation of safety requirements (Section 7.3)
  - Includes IV&V for safety-critical computing system safety items
“Safety requirements” are design requirements that have public safety consequences

• Describe safety-related design attributes and functionality
• Examples in AC Appendix A

**Complete safety requirements (Section 7.2.1)**

• Define set from design and system safety/software safety documentation
• Ensure completeness with a feedback loop through testing and operation

**Correct safety requirements (Section 7.2.2)**

• Relies on identification of system requirements and design requirements
  • Checked by independent analysts, testers, and operators
• Expected to be a cyclical refinement process
Implementing and Verifying Safety Requirements

Implement safety requirements as with any other design requirements

Independent verification and validation required for safety-critical CSSI (Section 7.3.1)

- Essential to ensuring public safety and the safety of property (§ 401.7)
- IV&V should:
  - Be managed independent of the development process
  - Use incentives that encourage thoroughness
  - Have latitude to check for undocumented requirements
  - Provide feedback and findings to development team in a timely manner

Verification and validation should be proportional to criticality (Section 7.3.2)

- Testing is preferred whenever feasible
- Optimal methods are often specific to the system
Floor open for questions/comments
Either verbally or via comments
The final rule calls for a development “process,” rather than a “plan,” that achieves the same objectives as a development plan but affords applicants greater flexibility to structure their processes. Operators need not employ a separate development process for each computing system safety item. The development process for each computing system safety item must be appropriate to the level of criticality of the computing system safety item and must satisfy the criteria listed in § 450.141(c), at a minimum.

§ 450.141 Computing Systems.

(c) Development Process. An operator must implement and document a development process for computing system safety items appropriate for the level of criticality of the computing system safety item. A development process must define:

1. Responsibilities for each task associated with a computing system safety item;
2. Processes for internal review and approval—including review that evaluates the implementation of all safety requirements—such that no person approves that person’s own work;
3. Processes to ensure development personnel are trained, qualified, and capable of performing their role;
4. Processes that trace requirements to verification and validation evidence;
5. Processes for configuration management that specify the content of each released version of a computing system safety item;
6. Processes for testing that verify and validate all safety requirements to the extent required by paragraph (b)(4);
7. Reuse policies that verify and validate the safety requirements for reused computing system safety items; and
8. Third-party product use policies that verify and validate the safety requirements for any third-party product.
Performance requirements for development processes scale with criticality

- Assignments of responsibility for development tasks, usually by position or title (8.2.1)
- Review processes, typically for requirements vetting, implementation, and testing (8.2.2)
- Training and qualification process for personnel in safety-related development roles (8.2.3)
- Process for tracing requirements to verification and validation evidence (8.2.4)
  - Should link each requirement to V&V thereof, enabling verification of a complete safety requirement set
- Configuration management to specify version content per computing system safety item (8.2.5)
  - See also 450.103(c)
- Testing process rigor proportional to criticality, with IV&V for safety-critical computing system safety items (8.2.6)
- Reuse policy (8.2.7)
  - Should define evaluation and testing processes
- Third-party policy (8.2.8)
  - Should define acceptance, evaluation, and testing processes
Assign responsibilities for safety tasks
• Often by position and qualification
• Accomplished when the applicant documents who did each safety task for each CSSI

Review and approval processes
• Similar to code reviews, but can be a distributed, iterative process
• Accomplished when reviews are documented to have been independent

Training processes should put appropriately trained/experienced people in safety roles
• Methods are applicant-specific
• AST verifies that the applicant has a sound method and standards
More Development Process Requirements

Define processes that trace requirements to verification and validation evidence

• Connect computing system requirements to tests/analyses or other evidence of implementation

• Evaluation focuses on potential errors or gaps in traceability

Configuration management sufficient to specify the content of each released version

• CM is a broader discipline; this is the minimum

• Accomplished when the applicant has records of what has flown and will fly

Verification and validation in proportion to criticality

• Tests should check implementation of safety requirements at a minimum

• Often needs test plans, descriptions, and results in addition to analyses
Previously developed CSSI (reused or 3rd party)

- Verify and validate safety requirements for reused and 3rd party CSSI
- Includes COTS, GOTS, and legacy CSSI
- Should evaluate the differences between prior uses or design documents and its use in the system
- Need not replicate tests or analyses conducted by supplier, but should ingest data into the applicant’s safety analyses
Considerations for development processes

- Is not a means of compliance in itself
- Discusses concepts that may aid applicants in accomplishing elements of safe development
  - Software implementation analysis (8.3.1)
  - Development standards (8.3.2)
  - Quality assurance (8.3.3)
  - Formal inspections (8.3.4)
  - Anomaly reports (8.3.5)
  - Maintenance and repair of computing system hardware (8.3.6)
  - Maintenance of computing system software (8.3.7)
  - Building maintainable software (8.3.8)
Discussion

Floor open for questions/comments
Either verbally or via comments
Section 450.141(d) contains the application requirements for this section. Each of the five requirements in paragraph (d) mirrors a key aspect of computing system safety, allowing the applicant and FAA to understand the rigor of development in terms of public safety. This structure is meant to reflect the typical formats of computing system safety data submissions received by the FAA to date.

These application requirements need not be met in separate documents.

§ 450.141 Computing Systems.

(d) Application Requirements. An applicant must:

1. Identify and describe all computing system safety items involved in the proposed operations;
2. Provide the safety requirements for each computing system safety item;
3. Provide documentation of the development processes that meets § 450.141(c);
4. Provide evidence of the execution of the appropriate development process for each computing system safety item; and
5. Provide evidence of the implementation of each safety requirement.
Requires documentation of (a-c)

- Identify and describe computing system safety items, including their criticality (9.1)
- Provide safety requirements for each computing system safety item (9.2)
- Document a process that meets (c)(1)-(8) (9.3)
- Provide evidence of execution of the appropriate development processes (9.4)
  - Note which development process applied to each computing system safety item and which process path options are used
  - Provide artifacts of the development process that verify that the computing system safety item followed the process
- Provide evidence of the implementation of each safety requirement (9.5)
  - Test record, analysis, or other verification evidence per process
Key Revisions in 1A

• Revised definitions of “risk” and “risk mitigation”
  • Risk: Measure that takes into consideration, for hardware, the probability of occurrence and the consequence of a hazard to a population or installation. For computing systems, risk takes into consideration the computing system’s contributions to hazard causation or mitigation and the consequence of a hazard to a population or installation.
  • Risk Mitigation: Process of reducing either the likelihood or the severity of a risk for hardware. For software, risk mitigation is the process of reducing the severity, reducing the degree of control, or validating and verifying correct control.

• Functional Hazard Analyses conducted to meet 450.107 or 109 can, when appropriately configured, meet 450.141(a)
Key Revisions in 1A

• Reasonably foreseeable faults are those that an analyst can discover through methodical assessment of the system.
  • Could depend on:
    • Programming language
    • Hardware configuration
    • Other computing systems that interact with the vehicle

• Fault tolerance analysis should:
  • Identify the conditions under which each tolerance is acceptable
  • Identify each computing system safety item by fault tolerance
  • Describe the measures in place to limit risk for each CSSI
Key Revisions in 1A

• Clarified that configuration management processes start when an initial baseline configuration is defined
• Updated discussion of verification and validation, expanding on approaches to testing and test documentation
• Clarified the role of maintenance in computing system safety as:
  • For software, the ongoing process of adapting software to changing hardware and system requirements
  • For computing system hardware, preventing or mitigating CSSI hardware failures
Floor open for questions/comments
Either verbally or via comments
Upcoming Workshops

• October 13, 1330
  AC 450.103-1  System Safety Program

• Date/Time TBD (October):
  AC 450.173-1 Mishap Plan-Response, Reporting, and Investigation Requirements
Where to Find the ACs on AST Part 450 Webpages

Links to ACs:

https://www.faa.gov/regulations_policies/advisory_circulars/
https://www.faa.gov/space/streamlined_licensing_process/

To ensure your comments and questions are considered in a future revision of the AC, please submit via the Feedback Form: https://www.faa.gov/documentLibrary/media/Form/FAA1320-73.pdf
Attachments to this form are welcome.