Workshop on Advisory Circular (AC) §450.108-1

Flight Abort Rule Development

Hosted by:

Pamela Hicks, FAA/AST

August 19, 2021

AST Commercial Space Transportation
Go for launch

faa.gov/space

Federal Aviation Administration

Agenda

Presentation includes:

- Background on ACs
- Review of the AC, chapter by chapter
  - A review of each topic
  - Open for questions at the end of each chapter
- Skipping chapters 1-2 (boilerplate), 3 (references) and 5 (acronyms)

WE ENCOURAGE DISCUSSION!

(we have up to two hours today)

NOTE

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

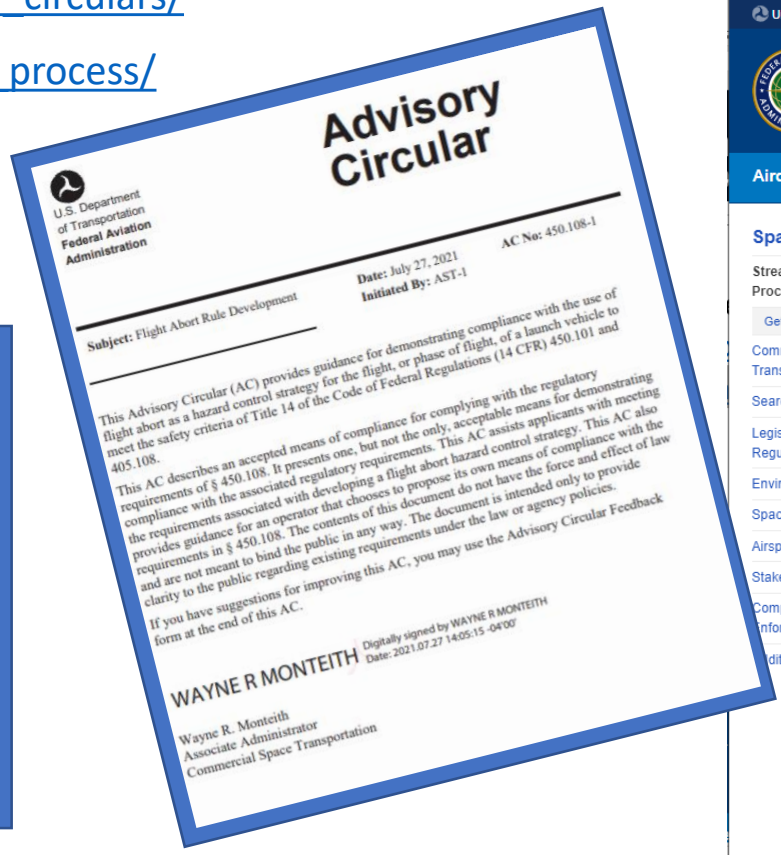
Where to Find the ACs on AST Part 450 Webpages

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.



U.S. Department of Transportation
Federal Aviation Administration

Advisory Circular

AC No: 450.108-1
Date: July 27, 2021
Initiated By: AST-1

Subject: Flight Abort Rule Development

This Advisory Circular (AC) provides guidance for demonstrating compliance with the use of flight abort as a hazard control strategy for the flight, or phase of flight, of a launch vehicle to meet the safety criteria of Title 14 of the Code of Federal Regulations (14 CFR) 450.101 and 405.108.

This AC describes an accepted means of compliance for complying with the regulatory requirements of § 450.108. It presents one, but not the only, acceptable means for demonstrating compliance with the associated regulatory requirements. This AC assists applicants with meeting the requirements associated with developing a flight abort hazard control strategy. This AC also provides guidance for an operator that chooses to propose its own means of compliance with the requirements in § 450.108. The contents of this document do not have the force and effect of law and are not meant to bind the public in any way. The document is intended only to provide clarity to the public regarding existing requirements under the law or agency policies.

If you have suggestions for improving this AC, you may use the Advisory Circular Feedback form at the end of this AC.

WAYNE R MONTEITH Digitally signed by WAYNE R MONTEITH Date: 2021.07.27 14:05:15 -04'00'

Wayne R. Monteith
Associate Administrator
Commercial Space Transportation

Background on Advisory Circulars

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.

AST Commercial Space Transportation
Go for launch

Workshop on Advisory Circular (AC) §450.108-1

Flight Abort Rule Development

Presented by:

Erik Larson, Ph.D., Marigold RISE LLC, contractor to FAA/AST

Tom Ricketson, FAA/AST

Paul Wilde, Ph.D., FAA/AST

August 19, 2021

faa.gov/space

Federal Aviation Administration

Background on AC 450.108-1

Part 417

In part 417, there were several sections of prescriptive requirements for flight abort rules

The flight abort requirements are possibly the most innovative element of the new regulations.

Part 450

- In part 450, these are consolidated to one section with performance requirements
  - Conditional expected casualty (CE_C) is a key performance metric; this is discussed AC 450.101.
- Per 450.101(c), a Flight Safety System (FSS) is no longer required for all missions (or for all phases of flight)
- No abort rules when FSS is not used

AC 450.108-1 Overview

AC organization

- Chapters 7-12 explain subsections (a) through (f), respectively, of 450.108
- Chapter 13 is an extensive discussion of an approach to meeting all the requirements
- Chapter 14 provides further explanation of the application submission requirements

Expanded discussion of two key terms

- Debris footprint
- Hazard footprint

} **Useful constructs for developing abort rules**

Explanation of statistical meaning of footprint

Chapter 4 – Definitions

There are six definitions:

- **Conditional limit –**
  - A flight safety limit through which a vehicle may fly, unless a critical vehicle parameter is outside its pre-established expected range or indicates an inability to complete flight within the limits of a useful mission
  - Generalization of a “gate”
- **Residual risk –**
  - The risk after all hazard controls are accounted for in FSA
  - This is what is compared to safety criteria for go/no-go
- **Unintended Trajectory**
  - A trajectory outside the normal trajectory envelope but within the limits of a useful mission.

ACs only define terms not defined in the regulation (§401.7).

Chapter 4 – Definitions

There are six definitions (continued):

- Debris footprint
- Hazard footprint

} Discussed in chapter 6

- State vector – (standard definition)

ACs only define terms not defined in the regulation (§401.7).

Chapter 4 – Definitions

Discussion

Floor open for questions/comments
Either verbally or via comments

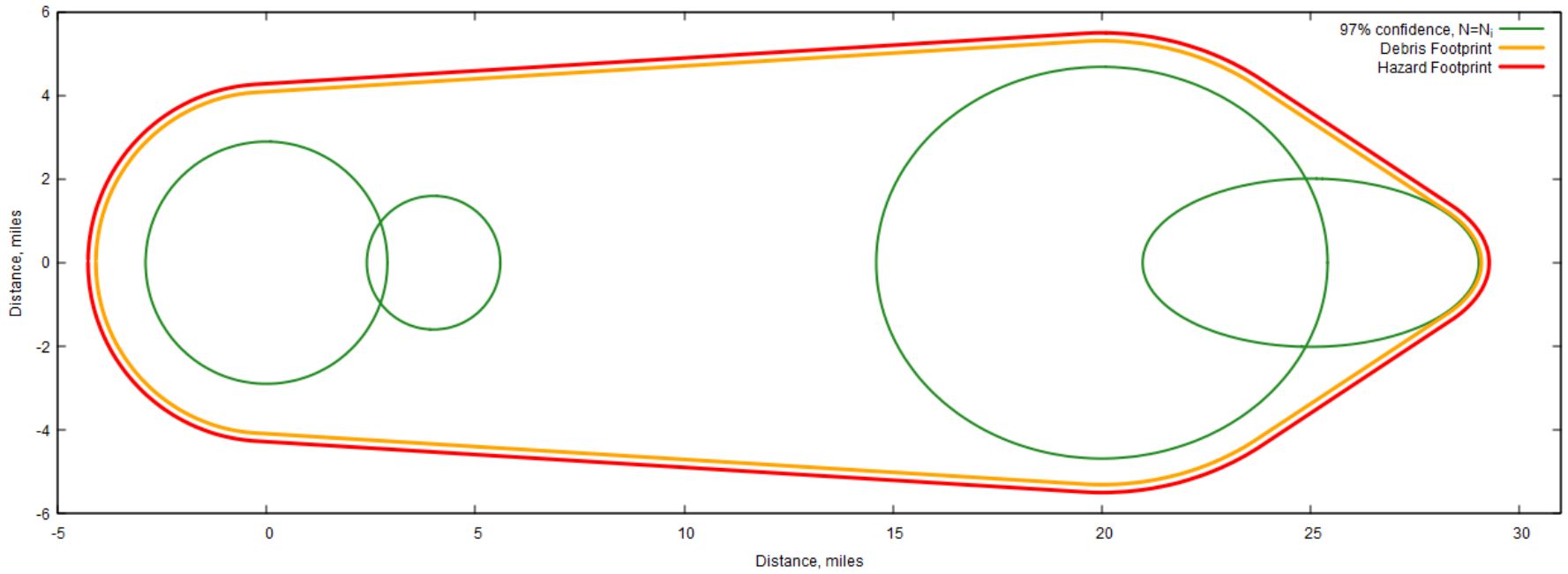
Chapter 6 - Introduction

"A **debris footprint** is a geographic region containing, with at least **97%** confidence, all the **hazardous debris** impacts resulting from an **event**."

- **All** impacts should be contained for 97% of the occurrences of the event, not 97% of fragments contained
- Fragments too small to cause injury are excluded
- The outcome of a breakup (or intact impact) – incorporates uncertainties subsequent to the failure initiation

Chapter 6 - Introduction

A **hazard footprint** is a debris footprint extended to include at least the region where the probability of casualty exceeds 1% from any impact included in the footprint (conditional on each impact), considering all hazards.



Chapter 6 - Introduction

Discussion

Floor open for questions/comments
Either verbally or via comments

Chapters 7&8 – Flight Abort Applicability and Requirements

Flight abort system and rules may be different for different phases of flight

- Abort can include
  - Destruct
  - Thrust termination
  - Contingency landing
  - Any combination
- Fundamentally, abort means that the primary objective changes from accomplishing the mission goals to ending the flight in a way to avoid adverse consequences.
  - Abort may also be used to protect crew or spaceflight participants, but they are not considered in the regulations or the AC (except that abort must not increase risk to the public)

Chapters 7&8 – Flight Abort Applicability and Requirements

Required reliability of FSS is based on CE_C (see AC 450.101-1).

- Highly-reliable FSS (450.145) for phases of flight where CE_C exceeds $1x10^{-2}$
  - This is the traditional RCC 319 FSS
- Safety-critical FSS (450.143) for phases of flight where CE_C exceeds $1x10^{-3}$
  - A highly-reliable FSS is acceptable
  - Level of rigor of this FSS expected to be higher as CE_C is closer to $1x10^{-2}$
  - This is a **new approach** aimed to help vehicles with lower potential consequence use a less expensive system. Being new, the FAA will work with each applicant to tailor the approach

An applicant should carefully consider when choosing an FSS reliability.

- A different launch/landing site or mission profile can significantly change the CE_C
- Switching to a high-reliability FSS later in development cycle could be expensive

Chapters 7&8 – Flight Abort Applicability and Requirements

Discussion

Floor open for questions/comments
Either verbally or via comments

Chapter 9 - Flight Safety Limits Objectives

The objectives of subpart (c) attempt to capture the **performance standards** for flight abort

Per (c)(1), abort should ensure compliance with safety criteria of 450.101:

- **Collective risk for people on land and in/on water**
  - Especially important in launch/landing area as deviations usually have a significant effect on risk.
  - Usually less important in overflight where a deviation doesn't significantly change risk
- **Individual risk for people on land, in/on water, and in aircraft**
  - Flight abort can shift where keep-out areas are located, and thus must be accounted for in this determination. Flight abort can be used to manage these to occur in areas easier to control.
- **Risk to critical assets**

These are cumulative requirements across phases of a flight, not considering each phase separately.

Chapter 9 - Flight Safety Limits Objectives

Option 1

Within each phase of flight, **flight safely limits can be based on two options:**

1. Abort providing containment (c)(6)

- This is an updated version of the former beta>3 psf requirement, now prevent hazardous debris from affecting uncontrolled areas
  - Controlled areas and oceanic areas are excluded
  - Hazardous: debris capable of causing a casualty due to any hazard
- The objective is to simplify the analysis in phases where containment can be easily demonstrated, such as over broad open areas
- Some missions can use containment for all phases of flight

Chapter 9 - Flight Safety Limits Objectives

Option 2

Within each phase of flight, **flight safely limits can be based on two options (continued):**

2. Risk & consequence

Prevent increased risk (c)(2)

- An obvious objective abort: if the mission is no longer useful, abort before risk is increased!
- See forthcoming AC 450.119-1 regarding limits of a useful mission

Chapter 9 - Flight Safety Limits Objectives

Option 2

2. Risk & consequence (continued)

Limit CE_C for abort cases (c)(4)

- Only off-trajectory failure modes are considered (excludes loss-of-thrust)
- In this case, the CEC should be evaluated just for some of the outcomes of each failure more within each significant period of flight:
  - Where abort is predicted to occur AND where no abort is predicted, but the vehicle is outside the limits of a useful mission
- The **core objective is to prevent an action (abort) from leading to a high consequence event**; it is considered worse if a safety action causes negative consequences than if no action does
  - But “not aborting” on errant flight is no better

Chapter 9 - Flight Safety Limits Objectives

Two additional objectives:

1. Per (c)(3), **Perform a "health check" before entering a period of materially increased exposure**

- Vehicle health is assessed by evaluating vehicle parameters that provide signs of whether the vehicle is behaving normally, which are more than just the parameters assessed as flight safety limits
    - Examples: chamber or tank pressure, IIP direction, orientation
- The idea is that an anomalous vehicle should be terminated in a region of negligible risk instead of being allowed to fly to a period where there is significant risk

Chapter 9 - Flight Safety Limits Objectives

Two additional objectives (continued):

2. Per (c)(5), **terminate before environment compromises the flight safety system**

- Any system, including FSS, has limits as to the physical environment it can withstand
- Flight should be terminated before this occurs (if the vehicle has potential to violate a limit)
- Especially important for a safety-critical system, instead of highly-reliable, because margins likely smaller

Chapter 9 - Flight Safety Limits Objectives

Discussion

Floor open for questions/comments
Either verbally or via comments

Chapter 10 – Flight Safety Limits Constraints

The constraints in (d) **are elements that must be considered while developing flight safety limits**. These describe the attributes of the analysis that is used to develop limits.

Developing limits is tightly connected to the flight safety analysis.

- (d)(1) – same failure modes as identified in probability of failure (131) and evaluation of malfunction trajectories (119)
- (d)(2) – physics of generation and transport, for debris (121), FFBO (137), and toxic (139)
  - This means that the IIP is not sufficient for determination of abort limits, but the breakup/explosion of a vehicle should be considered
  - Transport includes drag and wind effects for debris and focusing for FFBO, which are usually most important in the launch/landing area

Chapter 10 – Flight Safety Limits Constraints

Two constraints deal with time:

1. d(3) discusses how long a vehicle should be allowed to fly when the FSS is not receiving valid data, called Duration of Acceptable Data Loss (DADL),

- Data Loss Flight Times (DLFT), Green Numbers, and No Data Destruct Times (NDDT) are examples of these, but this requirement does not specify a particular approach
- Need to balance preventing malfunction flight with potential for terminating a good vehicle
  - Data loss could be caused by a failure that leads to malfunction flight (common cause)
  - Data loss could be an *expected* gap (e.g. plasma blackout) or *unexpected* problem
    - BAD outcome: Abort could lead to increased risk as well as loss of mission
- There are many principles listed in the AC that guide the determination of DADL

Chapter 10 – Flight Safety Limits Constraints

Two constraints deal with time (continued):

2. (d)(4) requires that the system delays be accounted for, because abort is not immediately effective when a limit is violated. This means limits must be adjusted so abort is accomplished in time to provide the protection for which it is intended.

Delays include:

- Hardware
  - Includes consideration for possible residual thrust
  - May be significant when abort is complex (e.g. capsule escape)
- Software
  - Algorithm processing, also includes built-in delays to account for data noise (missing from AC)
- Communication
  - Transmission to the ground
- Humans: Safety officer decision, Pilot procedure

The delays are shortest for autonomous on-board systems

Chapter 10 – Flight Safety Limits Constraints

(d)(5) requires consideration of FSS reliability in the residual risk analysis

- The potential for failure of the FSS to activate can significantly affect E_C, especially when
  - A “safety-critical” FSS is used
  - There are much higher density populations being protected by the limits
- Not required for CE_C when containment is used for a phase

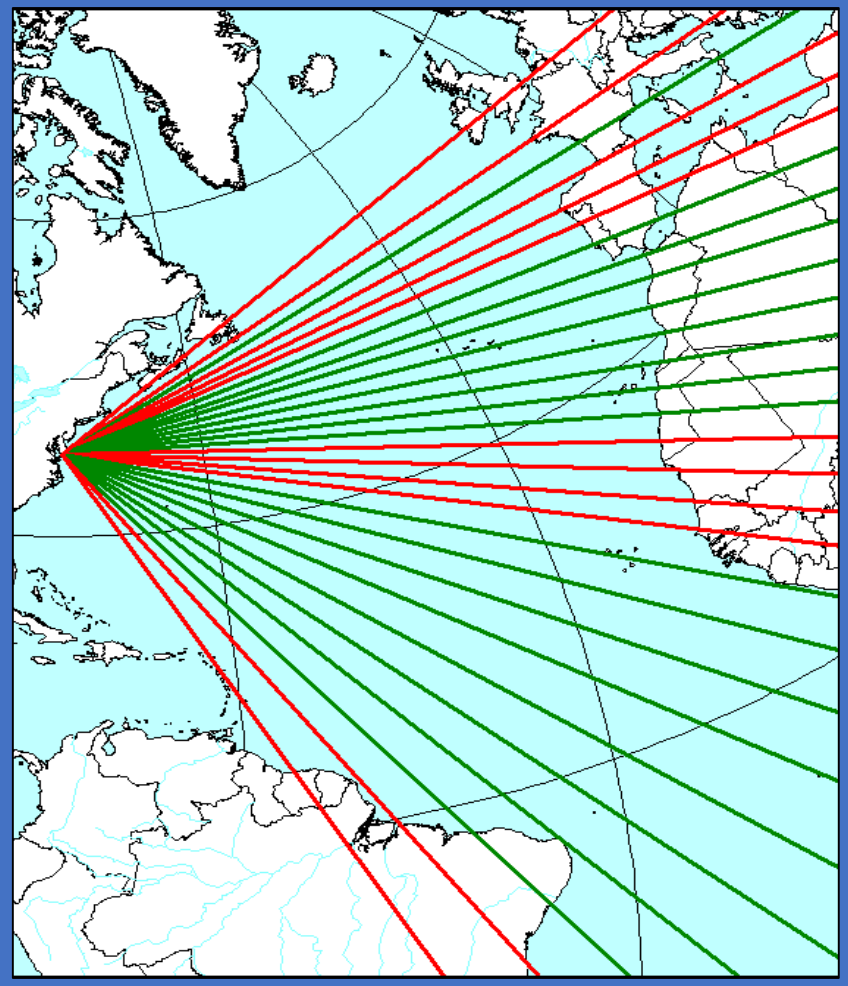
(d)(6) requires that abort should never increase risk

- Common sense, but impossible to prove that the optimal abort location has always been selected
- Guidelines for pragmatic application are discussed in AC
- Minimum requirement: compare risk with abort at flight safety limits to the same malfunction analysis without abort

Chapter 10 – Flight Safety Limits Constraints

(d)(7) requires that every mission within the limits of a useful mission that can fly without abort meets E_C requirements

- This is a critical step that reduces the useful mission envelope to a **safe** useful mission envelope
- More complex missions require consideration of a variety of trajectories within the limits sufficient to ensure that trajectories that could potentially violate the limits are identified
- Risk evaluation should be the same approach as used to satisfy 135, 137, and 139, for each trajectory examined, but not considering off-trajectory failures



Notional example: Figure for eliminating azimuths

Chapter 10 – Flight Safety Limits Constraints

Discussion

Floor open for questions/comments
Either verbally or via comments

Chapter 11 – End of Flight Abort

When flight abort is used as a hazard control strategy, sometimes it is best to end the use of flight abort, as it no longer improves safety.

- Example: downrange overflight

In order to end flight abort:

- No further key flight safety events
- Abort would not materially decrease risk from high consequence events
- Evaluation of critical parameters (e.g. a downrange gate)

Chapter 11 – End of Flight Abort

Discussion

Floor open for questions/comments
Either verbally or via comments

Chapter 12 – Flight Abort Rules

Part (f) states:

1. Data must be available to evaluate the flight safety limits under all reasonable conditions.

- Common sense: a limit is not useful if the data is not available in-flight to evaluate it
- Could fail if
  - During flight, a limit relies on future knowledge
  - Requires excessive subjective judgment
  - Data is no longer available due to changing vehicle environment

2. The flight safety limits developed above must be implemented as abort rules
  - Need to specify that limits will be implemented in the launch, in order to clarify decision-making process.

Chapter 12 – Flight Abort Rules

Discussion

Floor open for questions/comments
Either verbally or via comments

Chapter 13 – Means of Compliance

Describes a means of achieving all the requirements for flight safety limits, both objectives and constraints.

- A step-by-step approach that provides a method to achieve the requirements.
- May be applied to a single flight or a series of similar flights
  - Some steps may apply for all flights of a vehicle

Chapter 13 – Means of Compliance

1. **Develop trajectory data**
   - Normal trajectories per 450.117, characterizing uncertainty and variability
   - Limits of a useful mission per 450.119(a)(3)
2. **Identify the subset of the useful mission trajectories that meet risk requirements**
   - Intended to be simplified version of normal FSA (no malfunction trajectories)
   - This tends to be more complicated as the limits of a useful mission are larger
3. **Evaluate ending flight abort (e.g. downrange gate)**
   - Can flight abort be ended?
   - Where?

Chapter 13 – Means of Compliance

4. **Identify potential flight safety limit types**
   - Normally standard limits used for each range / vehicle
   - Sometimes new limits needed for significantly different missions
5. **Perform time delay (system latency) analysis**
   - Normally done just once for each flight safety system / vehicle
6. **Determine buffers**
   - Abort limits should not be too close to normal flight
     - Don’t want noise triggering abort
     - Need to give time for abort system to react (especially if human)
   - If possible, abort before hazard can reach uncontrolled areas

Chapter 13 – Means of Compliance

7. **Determine candidate quantitative parameters for flight safety limits**
   - This is a complicated step, AC attempts to provide a defined process for what has been a qualitative, approximate exercise
   - This section provides definitions for each type of limit and a process for developing the parameters for each
   - Normally a subset of limits are used
8. **Define conditional limits, if needed**
   - Conditional limits come in different types depending on the geometry of the exposed population to the mission
   - Two key steps:
     - Determining the conditional limit evaluation trigger(s)
     - Establishing the ranges for critical vehicle parameters

Chapter 13 – Means of Compliance

9. **Validate the system can support the rules**
    - For ground-based systems, verify that communication will be maintained
    - Ensure that uncertainty is not too large
    - Test implementation in software
10. **Verify risk reduction**
    - Confirm 108(d)(6) is satisfied, either by inspection or numerical analysis

Chapter 13 – Means of Compliance

9. Assess residual risk

- Perform flight safety analysis to ensure that E_C and CE_C criteria are satisfied
  - P_C is managed by hazard areas

10. Compute durations of acceptable data loss

- This is complex, because many data loss scenarios are not connected to malfunction flight, but some have common-cause with malfunction
- Also complicated because the problem is a lack of knowledge – have to consider what the vehicle could be doing

Chapter 13 – Means of Compliance

Discussion

Floor open for questions/comments
Either verbally or via comments

Chapter 14 – Application Requirements

The application should present:

- Approach to complying with the requirements
  - Analysis procedure by which objectives and constraints are satisfied and verified
  - If end of flight abort is used, how it is evaluated and applied
  - Process for ensuring limits are accurately incorporated in mission rules
- Definitions of flight safety limits and critical parameters
  - Algorithms necessary for evaluation should be included
    - They are usually simple, but critical
  - AC includes example for IIP limits

Chapter 14 – Application Requirements

The application should present (continued):

- Products (for a representative mission)
  - Flight safety limits quantitative values
  - Critical parameters
  - Graphic depiction of limits
    - Together with normal trajectory range and limits of a useful mission and relevant uncontrolled areas
    - All should be shown in the coordinate system of the limit
  - Vehicle data elements used to assess against limits, and conditions for availability

Chapter 14 – Application Requirements

Discussion

Floor open for questions/comments
Either verbally or via comments

Additional Upcoming Guidance

- Normal Trajectory Analysis
- Population Exposure Analysis
- Probability of Failure Analysis
- High-Fidelity Malfunction Trajectory Analysis
- Medium Fidelity Flight Safety Analysis
- Far-field Blast Overpressure Risk Analysis
- Toxic Risk Analysis

Upcoming Workshops

- August 25, 1 PM Eastern:
  AC 450.109-1 Flight Hazard Analysis
- Date/Time TBD (September):
  AC 450.173-1 Mishap Plan-Response, Reporting, and Investigation Requirements
- Date/Time TBD (September):
  AC 450.141-1 Computing Systems and Software
- Date/Time TBD (September):
  AC 450.117-1 Normal trajectory Analysis

AST Commercial Space Transportation
Go for launch

Contact

ASTWorkshops@faa.gov

faa.gov/space

Federal Aviation Administration