

Workshop on AC §450.101-1

High Consequence Analysis

Presented by:

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

Paul Wilde, Ph.D., FAA/AST


June 24, 2021

faa.gov/space



Federal Aviation
Administration

Agenda

- Background
- Chapter by chapter review of the Advisory Circular (AC)
 - A review of each topic, especially where there were comments
 - Open for questions at the end of each chapter
- There were numerous comments on the draft advisory circular, and over 20 revisions.
 - Where a substantive revision to the AC was made, the topic is marked with 
 - Comments are not specifically referenced
 - If the slides are not sufficiently responsive to comments, please ask through the Q&A or reach out to your AST contact



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.

Background on AC 450.101-1

This AC discusses §450.101(c) and related parts of §450.108 *Flight Abort*.

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

A Flight Safety System (FSS) is no longer required for all missions (or for all phases of flight).

Instead, the need for an FSS is based on:

- Collective risk (Expected casualties)
- Individual risk (Probability of casualty)
- High consequence risk (generally CE_C)

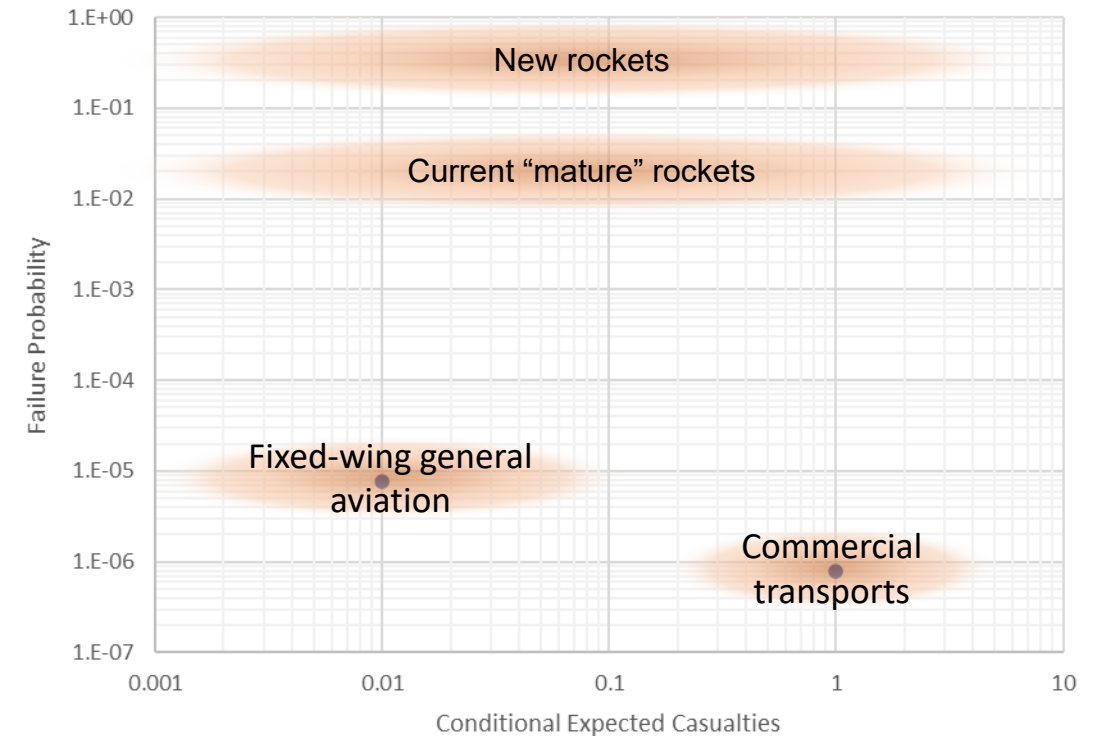


Why high consequence event protection?

Risk standards often consider comparisons to similar activities that have publicly-accepted **risk tolerance**.

- The **best** rockets historically have a reliability near 99% = 1% probability of failure per flight.
- Commercial airplanes are more than **10,000x more reliable** than rockets.
- A rocket failure can have comparable **consequences** (if impacting in the same location) to an aircraft crash, potentially much larger

Society is often less tolerant of one event that causes 10 casualties than ten events that cause a single casualty each (“catastrophe-aversion”)



Options for high consequence event protection



Part 450 offers three approaches for protecting from high consequence events:

- Demonstrated reliability
- Use of FSS to implement flight abort
- Analysis showing low enough risk of high consequence events
 - 450.101(c)(2) provides a metric: conditional expected casualties CE_C
 - 450.37 allows alternatives that have an equivalent level of safety (ELOS)
 - For most of the rest of 450.101, no ELOS is allowed

Even if CE_C low enough to not require FSS (<0.001), an operator may choose flight abort as a hazard control strategy to satisfy other safety criteria






Chapter 4 – Definitions

Chapter 5 – Overview


Chapter 4 *Definitions*

Provides the scope for terms used in the AC text. There are now five definitions:

- Failure mode 
 - Also added in High-Fidelity AC and discussed in Feb 24 workshop
- Maximum Conditional Expected Casualty
- Multiple Casualty Event 
- Phase of Flight
- Statistically Valid 
 - Also added in High-Fidelity AC and discussed in Feb 24 workshop

ACs only call out definitions of terms not defined in the regulation (§401.7), so review those definitions.

Chapter 5 *Overview*

- Recaps requirements from §101(c)
- Provides additional information about what constitutes a high consequence event 

High consequence events include incidents that could involve multiple casualties, massive toxic exposures, extensive property or environmental damage, or events that jeopardize the national security or foreign policy interests of the United States.

(also in the preamble to the final rule)



Chapter 4 – Definitions

Chapter 5 – Overview

Response to real-time feedback



Please submit questions through
<https://forms.gle/EoR4uvGSFGXWeiWA8>



Chapter 6 - Scope

Phase of flight

- High consequence event protection approach may be different for different phases of flight.
- Definition: A phase of flight is a period of flight between two milestones in the vehicle flight sequence, which is not necessarily a set period of time.
- Maximum duration:
 - Failure rate should be homogeneous
 - Include not more than one key flight safety event
- Minimum duration:
 - Sufficient to allow for implementation of a risk mitigation, including adequate time buffers to account for uncertainty
 - Related to significant period of flight (see section 8.4)
- Flight phase definitions should be consistent throughout a flight and based on physically observable phenomena

Chapter 6 - Scope

Controlled vs. uncontrolled areas

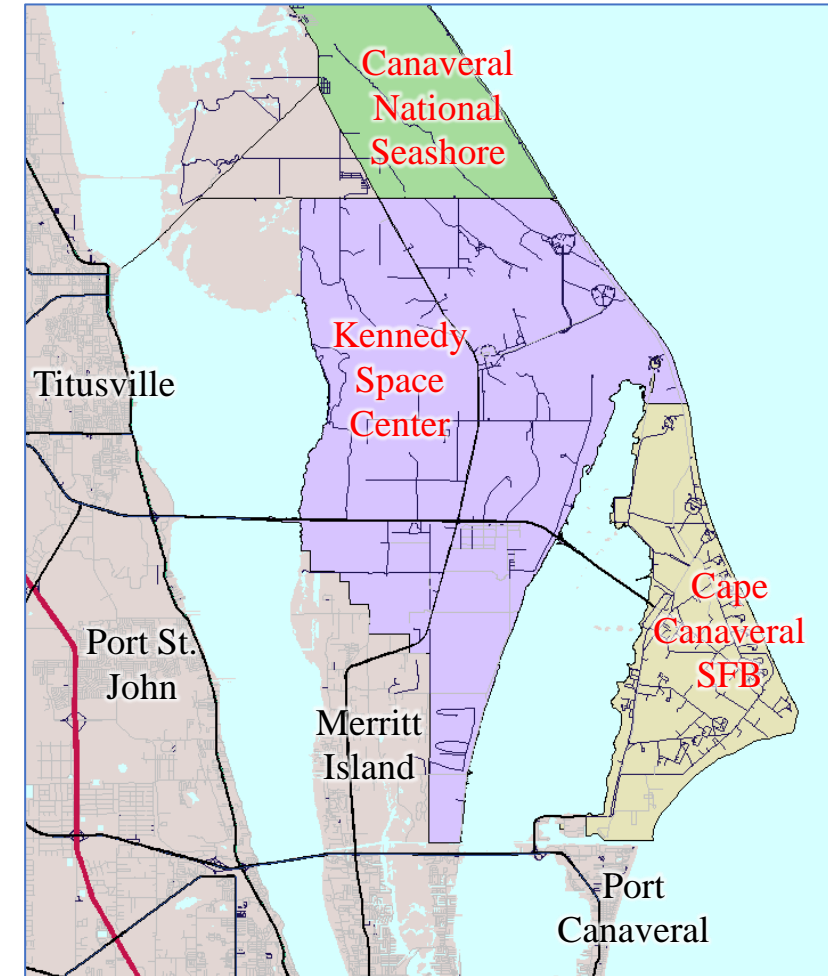
High consequence event protection is only required for uncontrolled areas (as defined in § 401.7)

- Uncontrolled areas only include land (not ocean)

Controlled areas:

- **Prevent** unauthorized access or otherwise ensure that no unauthorized persons are present
- **Manage the location** of any persons that are present
- **Coordinate** protection measures with controlling authority

A controlled area may include much more than just the launch or re-entry site.



Chapter 6 – Scope

Response to real-time feedback



Please submit questions through
<https://forms.gle/EoR4uvGSFGXWeiWA8>



Chapter 7 – Flight Abort

The first option for managing high consequence events is a highly-reliable FSS (compliant with §450.145) – which was always required by Part 417.

If any FSS is used, flight abort rules must comply with § 450.108.

Note: CE_C does NOT need to be computed if an FSS compliant with §450.145 prevents debris in uncontrolled areas, per §450.108(c)(6).

There were no comments submitted regarding chapter 7 nor any updates in the revised AC.



Chapter 7 – Flight Abort

Response to real-time feedback



Please submit questions through
<https://forms.gle/EoR4uvGSFGXWeiWA8>



Conditional Expected Casualty (CE_C)

CE_C is the specified metric for evaluating high consequence event protection

The FAA chose CE_C because

- Provides objective measure for when an FSS is unnecessary
- Straightforward to calculate along with E_C
- Consistent with past practices regarding FSS needs
- Precedent set in past waiver evaluations

Other approaches for quantifying the potential for high consequence events are available, but CE_C is a pragmatic solution

- Does not require significant additional resources (for each mission)
- Not overly sensitive to uncertainties in analysis method and input data
- Sufficient data exists to validate thresholds

Chapters 8-11 cover different aspects of CE_C

Chapter 12 discusses alternatives

Chapter 8 – Scope of CE_C

What is CE_C ?

- The average number of serious injuries (or worse) given that a “specified event” occurs.
- For 450.101(c)(2) and 450.108, the “specified events” are the occurrence of any reasonably foreseeable failure mode within any significant period of flight.

Hazards

- Debris – usually most important hazard for CE_C
- Far-field Blast Overpressure (FFBO) - normally compliance with E_C criterion also satisfies CE_C
- Toxic
 - For in-flight breakups, normally compliance with E_C criterion also satisfies CE_C
 - Needs to be considered for intact tank impact (e.g. hypergolic propellants)

Chapter 8 – Scope of CE_C

What is a “reasonably foreseeable failure mode”?

- Failure mode: a category of potentially hazardous events that share significant similarity in system response, prior to consideration of mitigations or hazard control strategies
 - Group of events by the conditions at the time of failure
 - Different outcomes may occur within the same failure mode
 - A vehicle response mode considers both initial conditions and outcome
 - Example: a stuck control system could result in structural failure or intact impact depending only on the random time of occurrence, so these are the same failure mode
- Reasonably foreseeable
 - For FSA: identifiable through the system safety process, including events that have occurred in the past for similar vehicles.
 - Not associated with a probability threshold.



Chapter 8 – Scope of CE_C

What is a “significant period of flight”?



The key test: would analysis with a shorter interval result in a meaningfully different outcome?

- A shorter interval is a more stringent criteria because CE_C is averaged over the interval.

Qualitatively:

- If it is long enough for a mitigation, such as flight abort, to materially decrease the public risks or consequences. This should consider latency and uncertainty in the abort response.
- Short enough that exposed population density does not significantly change.

The AC states that one second intervals are an acceptable approach

- The above qualitative statements provide guidance as to an Equivalent Level of Safety (ELOS)



Chapter 8 – Scope of CE_C

We have covered:

- Definition of CE_C
- Reasonably foreseeable failure modes
- Significant period of flight

Still to come:

- Calculating CE_C
- Discrete simulation approach
- Evaluating CE_C results
- Alternatives

Response to real-time feedback



Please submit questions through
<https://forms.gle/EoR4uvGSFGXWeiWA8>



Chapter 9 – Calculating CE_C

If an “event” is a specified failure mode in a given period of flight:

$CE_C = E[C|Event]$ is related to E_C as:

$$E_C = \sum_{EventSet} Pr(Event) E[C|Event]$$

Therefore, CE_C is simply the conditional E_C for each realization, R , of an event, weighted by the probability:

$$E[C|Event] = \frac{E_C(Event)}{Pr(Event)} = \frac{\sum_{R \in Event} Pr(R) E[C|R]}{\sum_{R \in Event} Pr(R)}$$

Often within the set, all realizations have the same probability, so this is simply

$$E[C|Event] = \frac{\sum_{R \in Event} E[C|R]}{N_R}$$

Example

Pr(R)	E[C R]
2.0E-08	1.07E-11
1.0E-08	1.76E-11
1.0E-08	4.81E-12
1.0E-08	2.62E-11
2.0E-08	3.58E-11

$$\sum_{R \in Event} Pr(R) = 7.0E - 8$$

$$\sum_{R \in Event} Pr(R) E[C|R] = 9.50E - 11$$

$$CE_C = E[C|Event] = 1.36E - 3$$



Chapter 9 – Calculating CE_C

Computation

- In an analysis, the conditional E_C for a realization, $E[C|R]$, is the average number of casualties resulting from a simulation of the failure mode within a specified period.
- This is inherent in the calculation of debris (450.135), FFBO (450.137) and toxic (450.139) risk. If the same event leads to multiple hazards, they must be combined.
- The key element is that the calculation **must separate** failure modes and time intervals.

Accuracy

- Standard: 75% confidence that CE_C is below the threshold of interest
 - Need a standard because CE_C is more sensitive to sampling methods and data resolution than E_C
 - A mathematically rigorous confidence interval may not be necessary; this could be demonstrated with a reasonable justification

Chapter 9 – Calculating CE_C

Implementation

The FAA has found that implementing calculation of CE_C in existing flight safety software is a small development effort.

- No new models are needed
- Just need to include logic to compute within suitable logic and write out values

Advantages

- Computing CE_C in design is far less expensive than including a highly-reliable FSS
- The use of CE_C provides a basis for a structured approach for developing flight safety limits

Tools

- Launch operators have modified in-house tools to support
- AVRA-DR by ARCTOS is known to compute CE_C ; inquire with other providers

Chapter 9 – Calculating CE_C

We have covered:

- Definition of CE_C
- Calculating CE_C

Still to come:

- Discrete simulation approach
- Evaluating CE_C results
- Alternatives

Response to real-time feedback



Please submit questions through
<https://forms.gle/EoR4uvGSFGXWeiWA8>



Chapter 10 – Using Discrete Simulations

Purpose

- The AC provides **an acceptable approach** for computing 75% confidence CE_C as part of a High-Fidelity Flight Safety Analysis (HFFSA)
- An HFFSA produces breakup state vectors (BSVs)
 - BSVs represent outcome(s) predicted from a discrete failure simulation.
 - Each is a “realization” per the previous discussion.
 - A BSV includes uncertainty, and an average $E[C | BSV]$ is computed based on
 - Impact distributions of fragments (§ 121)
 - Relative probability of each BSV (trajectory sampling per §§ 117 or 119)
 - Population exposure (§ 123)
 - Consequence modeling, including vulnerability (§§ 135, 137, 139)



Chapter 10 – Using Discrete Simulations

Basic approach

- Define a threshold $T_{\text{tiny}} = 1\%$ of CE_C threshold
- Compute at least 300 failure simulations for each failure mode in each interval
 - 300 was determined by analysis of a variety of missions
- If a 99.7% of simulations result are below threshold, criteria is satisfied
- If not, and there are also not enough significant samples, more simulations must be run
- Once there are enough samples, AC presents equations to compute 75% confidence upper bound on CE_C
- More simulations MAY be run to narrow the confidence bounds

The method is not mathematically rigorous but has been demonstrated to produce conservative results across many scenarios.

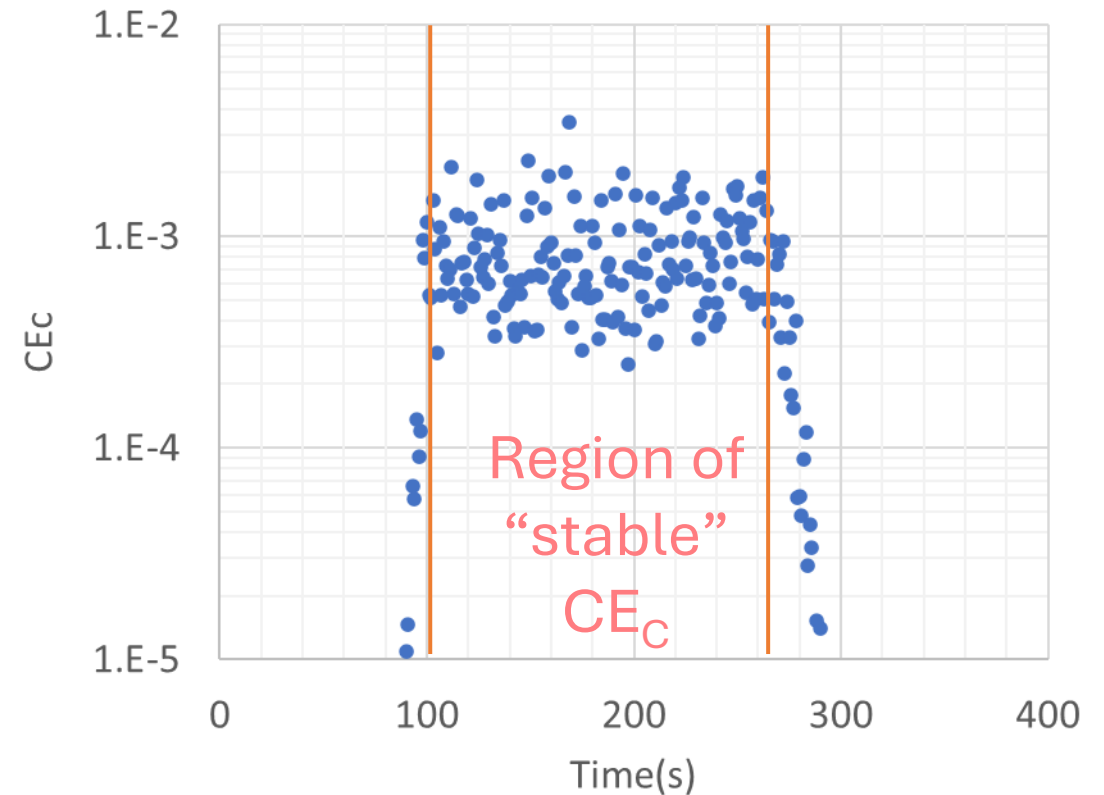
Chapter 10 – Using Discrete Simulations

In evaluating the CE_C approach, analysis of some datasets showed a large scatter of CE_C as a function of time; this resulted from simulation limitations, not physics.



Thus, the FAA will allow averaging over a larger time interval where CE_C is stable, but noisy.

The FAA plans to investigate alternative approaches to reduce the modeling scatter.



Chapter 10 – Using Discrete Simulations

We have covered:

- Definition of CE_C
- Calculating CE_C
- Discrete simulation approach

Still to come:

- Evaluating CE_C results
- Alternatives

Response to real-time feedback



Please submit questions through
<https://forms.gle/EoR4uvGSFGXWeiWA8>



Chapter 11 – Evaluating CE_C Results

Timeline of CE_C



CE_C has two purposes: the need for an FSS and determining flight safety limits

Initial CE_C analysis should be performed

- Early in vehicle design to determine the flight phases for which an FSS may be required and the required reliability of the FSS
- Without consideration of FSS action
- In a way that is not sensitive to particulars of vehicle variations, trajectory design, winds, etc.

The result depends on the

- Deviation capability during the phase (450.119)
- Debris list (450.121)
- Effective casualty area(s) (450.135, 450.137, and/or 450.139)
- Population density in the exposed area (450.123)



Chapter 11 – Evaluating CE_C Results

If flight abort is used as a hazard control strategy, then a **mission-level CE_C analysis** should be performed, in order to satisfy 450.108

- In conjunction with the development of flight safety limits
- Considering the effects of both abort or non-abort
- In a way that is not sensitive to particulars of trajectory variability and winds.
- Compared to initial analysis, also incorporates
 - More detailed malfunction trajectory analysis, including flight safety limits
 - Effects of abort on consequences (debris, FFBO, toxic)

Results in locations of flight safety limits, including conditional limits (gates)

Chapter 11 – Evaluating CE_C Results

We have covered:

- Definition of CE_C
- Calculating CE_C
- Discrete simulation approach
- Evaluating CE_C results

Still to come:

- Alternative to CE_C

Response to real-time feedback



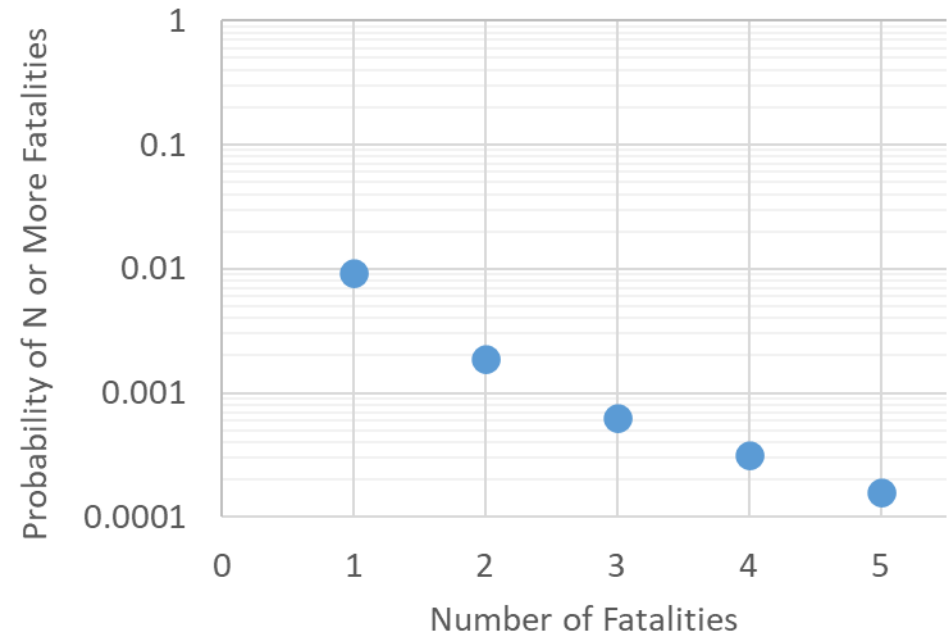
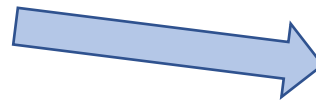
Please submit questions through
<https://forms.gle/EoR4uvGSFGXWeiWA8>



Chapter 12 – Alternative Means of Compliance

Alternative 1: conditional risk profile

- AC allows an ELOS if the conditional risk profile for a launch or reentry mission, in terms of casualties is at least an order of magnitude below the GA conditional CE_C
- Generally, entails more input data and more sophisticated calculations than CE_C



US General Aviation Ground Fatalities per Fatal Accident 1982-2019 (NTSB data)

Alternative 2: Conditional risk

RCC 321 Supplement describes another (more simplified and conservative) method to screen for excessive catastrophic risk.



Chapter 12 – Alternative Means of Compliance

Response to real-time feedback

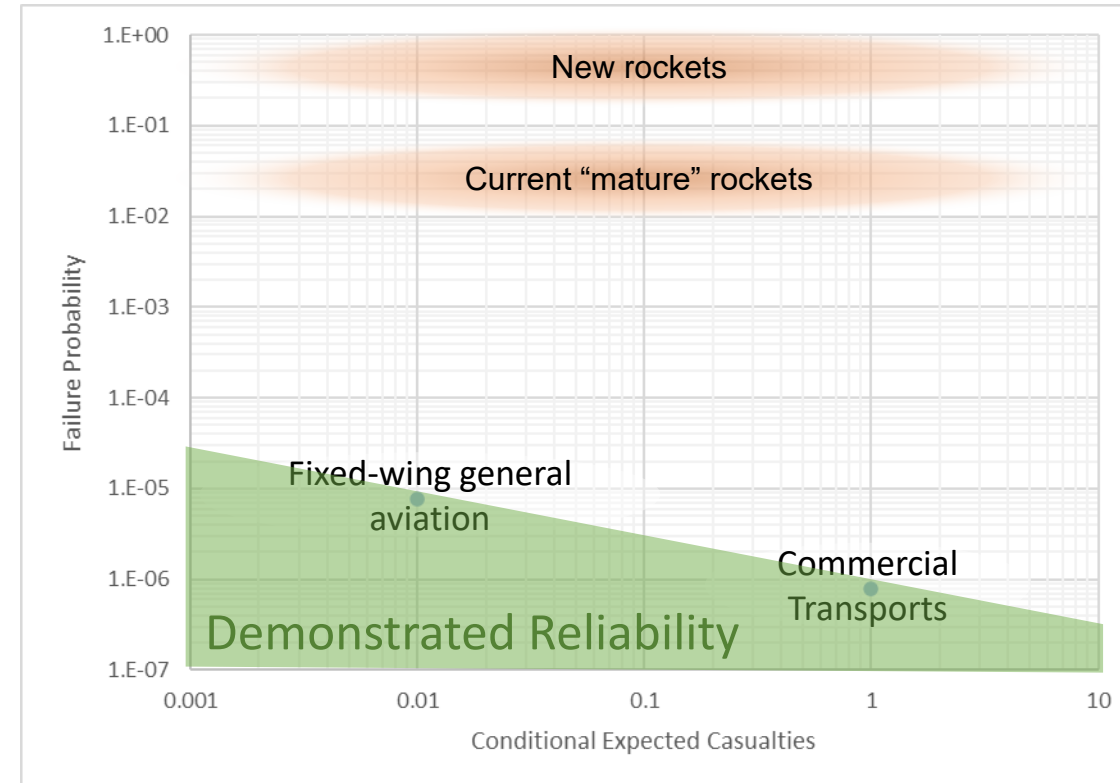


Please submit questions through
<https://forms.gle/EoR4uvGSFGXWeiWA8>



Chapter 13 – Demonstrated Reliability

- Demonstrated reliability standard in this AC is *currently* expected to be met only in some phases of flight when an aircraft carries a rocket.
 - Expect to accept standard airworthiness or an experimental airworthiness certificate (EAC) in conjunction with a rigorous flight test program
- The FAA anticipates that other suborbital rockets might achieve the demonstrated reliability standard in this AC in a decade or two.
 - This requires substantial flight history AND a rigorous system safety process.
- Full history data does not need to be shown for specific vehicle hardware, but for a vehicle configuration, such as for an aircraft type.



Chapter 13 – Demonstrated Reliability

Casualties vs. fatalities



- Casualties (serious injuries) are an appropriate metric for the public safety.
- For aircraft, ground fatalities data are tracked better than ground casualties.
- Difference between empirical data (on ground fatalities from aviation accidents) and predicted casualties (from launch/reentry operations) justifies some margin.
- The core principle is that the reliability standard will be based on the hazard the vehicle presents
 - A vehicle of comparable size and effective casualty area to a small aircraft would need reliability like a small aircraft
 - A vehicle with a larger effective casualty area necessitates an even higher demonstrated reliability comparable to that of commercial aircraft.



Chapter 13 – Demonstrated Reliability

Response to real-time feedback



Please submit questions through
<https://forms.gle/EoR4uvGSFGXWeiWA8>



Additional Upcoming Guidance

Flight abort

Population Exposure

Malfunction Trajectory Analysis

Medium Fidelity FSA

FFBO

Toxics



Further questions

- Background
- Definitions
- Scope of High Consequence
- Flight abort
- Demonstrated Reliability
- CE_C
 - Scope
 - Calculating
 - Discrete simulation approach
 - Evaluating results
 - Alternatives

Response to real-time feedback



Please submit questions through
<https://forms.gle/EoR4uvGSFGXWeiWA8>



Contact

ASTWorkshops@faa.gov

AST Commercial Space
Transportation
Go for launch.

faa.gov/space



Federal Aviation
Administration