U.S. Department
of Transportation
**Federal Aviation
Administration**

Advisory Circular

Subject: Flight Abort Rule Development | **Date:** July 27, 2021 | **AC No:** 450.108-1
Initiated By: AST-1

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

Contents

Contents (continued)

Contents (continued)

Contents (continued)

Paragraph **Page**

Contents (continued)

Figures

1 PURPOSE.

This advisory circular (AC) provides guidance and a comprehensive method to demonstrate compliance with the requirements for the flight abort hazard control strategy in § 450.108, Flight Abort. Flight abort is one of the hazard control strategies identified in § 450.107.

1.1 Level of Imperatives.

This AC presents one, but not the only, acceptable means of compliance with the associated regulatory requirements. The FAA will consider other means of compliance that an applicant may elect to present. Throughout this document, the word "must" characterizes statements that directly flow from regulatory text and therefore reflect regulatory mandates. The word "should" describes a requirement if electing to use this means of compliance; variation from these requirements is possible, but must be justified and approved as an alternative means of compliance. The word "may" describes variations or alternatives allowed within the accepted means of compliance set forth in this AC. In general, these alternative approaches can be used only under certain situations that do not compromise safety.

2 APPLICABILITY.

2.1 The guidance in this AC is for launch and reentry vehicle applicants and operators required to comply with 14 CFR part 450. The guidance in this AC is for those seeking a launch or reentry vehicle operator license, and a licensed operator seeking to renew or modify an existing vehicle operator license.

2.2 The material in this AC is advisory in nature and does not constitute a regulation. This guidance is not legally binding in its own right, and will not be relied upon by the FAA as a separate basis for affirmative enforcement action or other administrative penalty. Conformity with this guidance document (as distinct from existing statutes and regulations) is voluntary only, and nonconformity will not affect rights and obligations under existing statutes and regulations. This AC describes acceptable means, but not the only means, for demonstrating compliance with the applicable regulations.

2.3 The material in this AC does not change or create any additional regulatory requirements, nor does it authorize changes to, or deviations from, existing regulatory requirements.

3 APPLICABLE REGULATIONS AND RELATED GUIDANCE DOCUMENTS.

3.1 Related U.S.C. Statute.

- 51 U.S.C. Subtitle V, Chapter 509.

3.2 Related FAA Commercial Space Transportation Regulations.

The following regulations from title 14 of the CFR must be accounted for when showing compliance with § 450.108. You can download the full text of these regulations from the U.S. Government Printing Office e-CFR or order a paper copy from the Government Printing Office, Superintendent of Documents, Attn: New Orders, PO Box 371954, Pittsburgh, PA, 15250-7954.

- Section 450.101, *Safety Criteria*.
- Section 450.107, *Hazard Control Strategies*.
- Section 450.113, *Flight Safety Analysis Requirements*.
- Section 450.115, *Flight Safety Analysis Methods*.
- Section 450.117, *Trajectory Analysis for Normal Flight*.
- Section 450.119, *Trajectory Analysis for Malfunction Flight*.
- Section 450.121, *Debris Analysis*.
- Section 450.123, *Population Exposure Analysis*.
- Section 450.131, *Probability of Failure Analysis*.
- Section 450.135, *Debris Risk Analysis*.
- Section 450.137, *Far-field Overpressure Blast Effects*.
- Section 450.139, *Toxic Hazards for Flight*.
- Section 450.143, *Safety-Critical System Design, Test, and Documentation*.
- Section 450.145, *Highly-Reliable Flight Safety System*.

3.3 Related FAA Advisory Circulars.

- AC 450.101-1A, *High Consequence Event Protection*, Revision A, dated May 20, 2021.
- AC 450.109-1, *Flight Hazard Analysis*, when published.
- AC 450-113-1, *Flight Safety Analysis: Levels of Fidelity*, when published.
- AC 450.115-1A, *High Fidelity Flight Safety Analysis*, Revision A, dated June 24, 2021.
- AC 450.115-2, *Medium Fidelity Flight Safety Analysis*, when published.
- AC 450.117-1, *Trajectory Analysis*, when published.
- AC 450.123-1, *Population Exposure Analysis*, when published.

- AC 450.131-1, *Probability of Failure Analysis*, when published.
- AC 450.123-1, *Far-field Overpressure Blast Effects Analysis*, when published.
- AC 450.139-1, *Toxic Hazards for Flight*, when published.
- AC 450.143-1, *Safety-Critical System Design, Test, and Documentation*, when published.

3.4 Documents Related to Subject AC.

- Range Commanders Council (RCC) 319 Flight Termination Systems Commonality Standard, June 2019, https://www.wsmr.army.mil/RCCsite/Documents/319-19_FTS_Commonality/319-19_FTS_Commonality.pdf.
- Ricketson, Tom, P. D. Wilde, and E. Larson, *Proposed Flight Abort Criteria to Ensure Public Safety during Commercial Launch and Reentry Operations*, 10th International Association for the Advancement of Space Safety Conference, Los Angeles, California, May 2019.
- Range Commanders Council (RCC) 321-20 *Common Risk Criteria Standards For National Test Ranges*, May 2020, https://www.wsmr.army.mil/RCCsite/Documents/321-20_Common_Risk_Criteria_Test_Ranges/321-20_Common_Risk_Criteria_Test_Ranges.pdf.
- Range Commanders Council (RCC) 321-20 *Common Risk Criteria Standards for National Test Ranges*: Supplement, May 2020, https://www.wsmr.army.mil/RCCsite/Documents/321-20_Common_Risk_Criteria_Supplement/321-20_Supplement.pdf.
- *Joint Advanced Range Safety System Algorithm Document*, Millennium Engineering and Integration Company.
- CASS Steering Committee, *Software Design Description (SDD) for the Core Autonomous Safety Software (CASS)*, USSF 30SW/SEAE, Vandenberg Space Force Base, CA.

4 DEFINITION OF TERMS.

For this AC, the following terms and definitions apply:

4.1 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.

4.2 Debris Footprint

A geographic region containing, with at least 97% confidence, all the hazardous debris impacts resulting from an event. See paragraph 6.2 of this AC for further explanation.

4.3 Hazard Footprint

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.

4.4 Residual Risk

The risk that remains after all hazard controls are accounted for in the flight safety analysis.

4.5 State Vector

A set comprised, at minimum, of the three-component position and three-component velocity associated with a point in time along a vehicle's trajectory. A state vector may also include vehicle mass, thrust, orientation, angular velocity, and other parameters.

4.6 Unintended Trajectory

A trajectory outside the normal trajectory envelope but within the limits of a useful mission.

5 ACRONYMS.

- AC – Advisory Circular
- AFSS – Autonomous Flight Safety System
- CE_C – Conditional Expected Casualties
- DADL – Duration of Acceptable Data Loss
- DLFT – Data Loss Flight Time
- FFBO – Far-Field Blast Overpressure
- FSL – Flight Safety Limit
- FSS – Flight Safety System
- GPS – Global Positioning System
- IIP – Instantaneous Impact Point
- RCC – Range Commanders Council
- U.S.C. – United States Code

6 INTRODUCTION.

6.1 Overview.

This AC provides guidance for a launch operator to develop flight safety limits and flight abort rules for launch of a space vehicle. It provides further explanation of the requirements in § 450.108(a) through (f), in chapters 7 through 12 of this AC. Chapter 13 contains a description of an acceptable procedure for a means of compliance that meets the regulations, organized as a series of steps in an analysis. Chapter 14 contains further explanation of the application requirements in § 450.108(g).

6.2 Footprints.

6.2.1 Debris Footprint.

Per paragraph 4.2, a debris footprint is *a geographic region containing, with at least 97% confidence, all the hazardous debris impacts resulting from an event*.

6.2.1.1 An event is the outcome of a breakup, where the uncertainties that are considered are those that exist at the time of the breakup event. It is probabilistic because there is uncertainty in the vehicle state vector due to measurement uncertainty, the fragmentation resulting from the breakup and associated physical properties of the debris, the environmental conditions, modeling approximations, and numerical simulation limitations.

6.2.1.2 There are several important aspects to understand when considering the footprint. First, this definition means ALL impacts from every fragment group should be contained for 97% of realizations of the event. Addition of more fragments or fragment groups always expands the region. This is a much higher threshold than simply containing 97% of impacts for every event. The debris footprint includes ALL fragment groups, bounding all the distributions.

6.2.2 Hazard Footprint.

Per paragraph 4.3, a hazard footprint is: *A debris footprint extended to include the 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.* This effectively means the debris footprint is expanded to include area surrounding the fragment impact where a casualty is possible. This casualty radius incorporates the extent of the area affected, such as due to bounce and roll of an inert fragment or the blast wave from an explosive fragment. There is uncertainty in the consequence modeling due to impact conditions, modeling approximations, and human response. For inert debris, energy for hazards at the surface of the Earth, 11 ft-lbf of impact kinetic may be used for the 1% threshold, and, for aircraft, one gram may be used.

6.2.3 Confidence of Containment.

The region for confidence of containment is computed by integrating the impact probability over area, in order of increasing probability density, until the integral is one minus the specified confidence is reached. All the area included in this integrated region is outside the containment region, thus defining a boundary. This boundary then occurs at an equi-probability contour, but the probability is not known without integration. For a bivariate normal distribution, the integration can be performed analytically. In this case, the relationship between sigma level, n_σ, and confidence of containment, C, is given by $n_\sigma = \sqrt{-2\ln\left(1-\sqrt[N]{C}\right)}$ where N is the number of impacts.

6.2.4 Example.

Let us consider 4 fragment groups, with index *I* and N_i fragment impacts, each with a bivariate normal distribution, with standard deviations, $\sigma_{x,i}$ and $\sigma_{y,i}$, in miles, as shown in Table 1 of this AC.

Table 1. Example Fragment Groups

	$\sigma_{x,i}$	$\sigma_{y,i}$	N_i
Group 1	1.0	1.0	2
Group 2	0.5	0.5	5
Group 3	1.5	1.3	20
Group 4	1.0	0.5	100

6.2.4.1 **Sigma and confidence**.

The sigma levels and 97% containment are shown in Figure 6-1, with groups 1 to 4 proceeding from left to right:

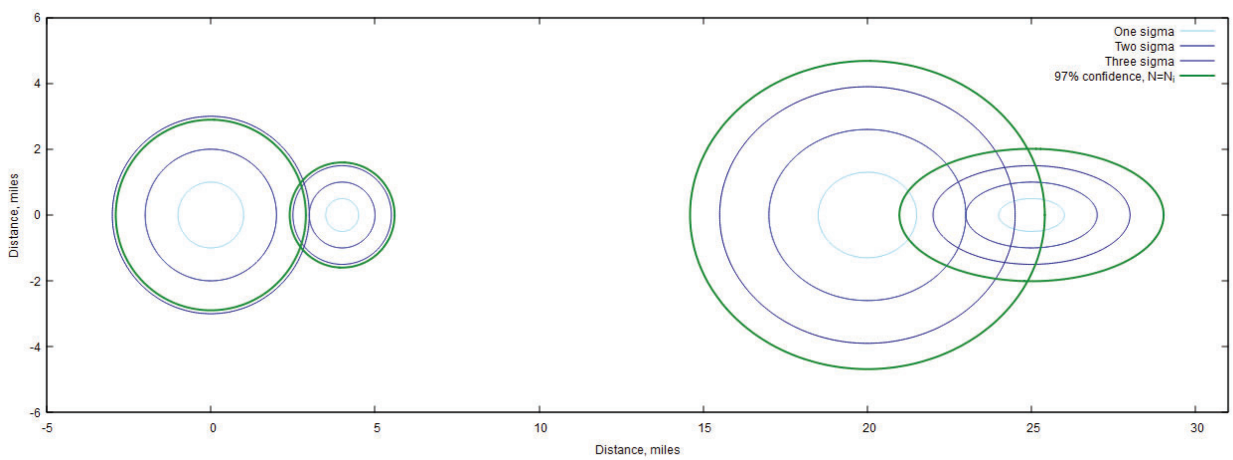


Figure 6-1: Comparison of Sigma Levels to Confidence Example

Note: The 97% confidence ellipse is slightly inside the three sigma level for group 1, where N_i is 2, but significantly outside for groups 3 and 4, where N_i is much larger.

6.2.4.2 **Debris Footprint**.

This example uses a simple approach to compute the debris footprint, which is guaranteed to be conservative. Instead of using the number of fragments for each group, the n_σ, for each group is computed using the sum of N_i. This accounts for the fact that fragment group distributions may overlap.[1] In this example, the sum is 127. The footprint is then the region bounding all of these, or for simplicity, the convex hull surrounding them, as shown in Figure 6-2. For the left three fragment groups, the change from N_i to the sum of N_i has a significant effect, because the right group has 80% of the fragments. The containment ellipse for the right group, with N increasing from 100 to 127, increases in size only slightly.

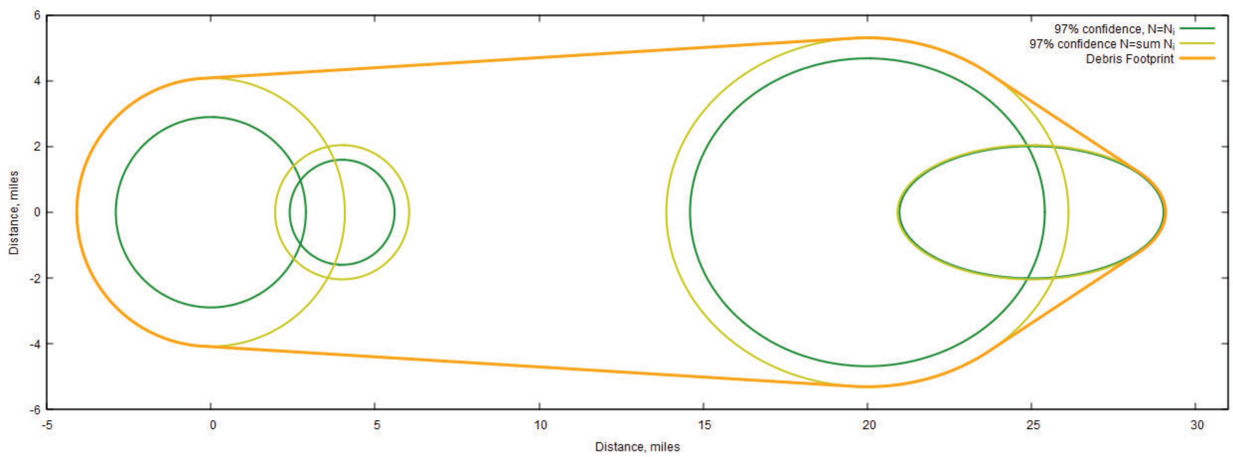


Figure 6-2: Debris Footprint Example

6.2.4.3 **Hazard Footprint**.

The hazard footprint is then computed by adding a distance around the debris footprint to account for hazards radiating from the impact point. In this example, 0.2 miles is used for illustration (see paragraph 13.4 for more discussion), as shown in Figure 6-3.

[1] Using the sum may appear excessively conservative. However, imagine the simple case of two identical fragment groups; in this case the containment of **each** is the same, but the containment of **both** is found with the equation where N is the sum of the number of fragments in each group. The conservatism is also limited because the N is used in taking the root of the confidence and then the natural log of this result.

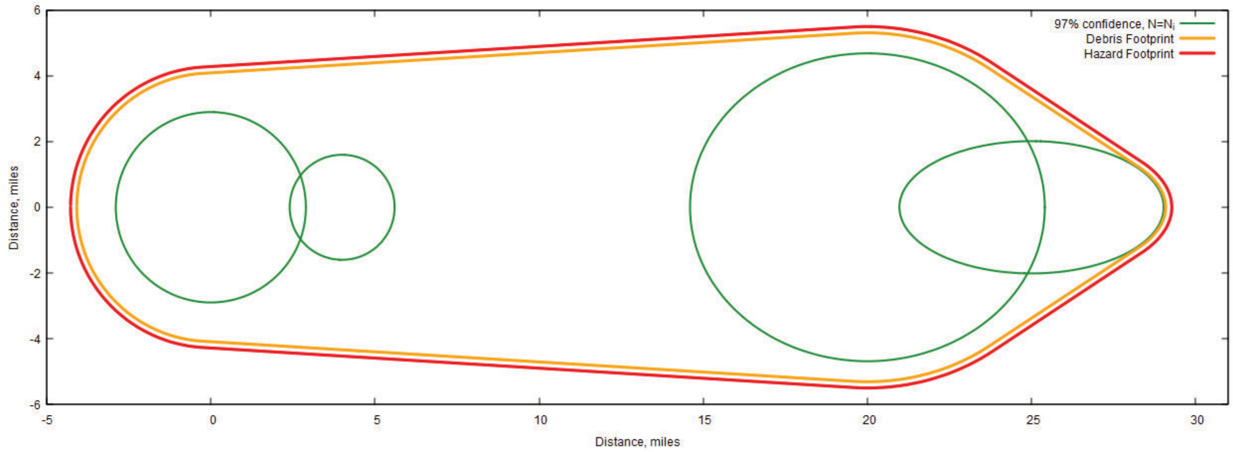


Figure 6-3: Hazard Footprint Example

7 FLIGHT ABORT APPLICABILITY.

7.1 Use of Flight Abort as a Hazard Control Strategy.

The operator is responsible for the safe conduct of all licensed activities and authorized to provide final approval to proceed with licensed activities. One method of limiting collective risk is a flight safety system, and in many cases such a system is required to protect against high consequence events in accordance with § 450.101(c). In accordance with § 450.108(a), the requirements in § 450.108 apply to any operation that uses a flight safety system as a hazard control strategy for the flight, or phase of flight, of a launch or reentry vehicle to meet the safety criteria of § 450.101. These requirements apply to all phases of flight for which the abort system is used to meet the risk requirements and may be necessary to protect against a high consequence event in uncontrolled areas; see AC 450.101-1, *High Consequence Event Protection*, regarding clarification on phases of flight. In accordance with § 450.101(c) an operator must use flight abort as a hazard control strategy if the consequence of any reasonably foreseeable vehicle response mode, for any significant period of flight, is greater than 1×10^{-3} CE_C for uncontrolled areas, unless § 450.101(c)(3) is satisfied. A period of flight would be significant if it is long enough for a mitigation, such as flight abort, to decrease the public risks or consequences materially from any reasonably foreseeable failure mode.

Note: Sections 450.101(c)(2) and (c)(3) allow an operator to demonstrate it has sufficiently protected against a high consequence event by demonstrating CE_C values of any reasonably foreseeable failure mode, in any significant period of flight below $1 \text{ x } 10^{-3}$ or by establishing the launch or reentry vehicle has sufficient demonstrated reliability as agreed to by the Administrator based on conditional expected casualties criteria during that phase of flight.

Note: If an operator cannot ensure by means other than flight abort that it has sufficiently protected against a high consequence event (as measured by CE_C), the way to satisfy § 450.101(c) is to use flight abort consistent with the requirements in § 450.108.

7.2 **Focus on Protecting the Public**.

A flight abort may be implemented in a variety of ways, as diverse as a pilot choosing a contingency landing site to an autonomous termination system destroying the vehicle. In all cases of abort, the primary objective changes from accomplishing the mission goals to ending flight in a way to avoid adverse consequences. There are limits to the capability of an abort system to mitigate risk. When control continues after abort the objective is to redirect the flight so landing or impact minimizes the exposed population. In this case, the potential for a secondary failure that results in hazards should be considered. When control (and thrust) are terminated the objective is to minimize the hazard posed by the vehicle, although the absolute minimum can never be positively identified (no known system exists that, for example, vaporizes all possible debris). Thus, it is assumed that flight abort results in some hazardous impacts. In accordance with § 450.115(b)(1), the demonstration of acceptable risk must include the use of mitigations. Thus, the flight safety analysis should account for post-abort physical processes that influence flight of a controlled vehicle and the effective casualty area, such as subsequent aerothermal breakup, melting, or vaporization, as well as the potential for structural failure and breakup of a falling object. Flight abort in the context of part 450 is focused on protecting the public and critical assets. An operator may choose to use flight abort to protect personnel on-board the vehicle as well, but that is not covered by these regulations, except to the extent that the pilot may be a component of the flight safety system. Therefore, whenever risk or high consequence events are discussed in the regulations or this document, they do not consider personnel on-board the vehicle. The primary objective for flight abort in the context of this AC is protecting the public and critical assets.

7.3 **Clarity of Flight Abort Rules**.

It is critically important that flight abort rules be clearly defined in advance of initiating flight. More specifically, in accordance with § 450.108(g)(2), an applicant must describe how each flight safety limit and flight abort rule is evaluated and implemented during vehicle flight, including the critical parameters and quantitative criteria that will be used. When humans are a part of the flight safety system, they should have a very clear understanding of the flight abort rules, and the human-system interface needs to be accounted for in accordance with § 450.108(d)(4) when establishing the time delay between the violation of a flight abort rule and the time when the flight safety system is expected to activate.

8 FLIGHT SAFETY SYSTEM REQUIREMENTS.

The flight safety system requirements for a phase of flight are prescribed by the magnitude of the risk of high consequence events, in accordance with § 450.108(b)(1) and (b)(2). Consequence is measured by the maximum conditional expected casualties (CE_C) in uncontrolled areas of any reasonably foreseeable failure mode in any significant period of flight within the phase. As discussed in the AC 450.101-1, *High Consequence Event Protection*, an alternate measure of the risk may be used to evaluate high consequence risk, such as a risk profile, if the measure and threshold are approved by the FAA Administrator.

8.1 **Highly-reliable Flight Safety System (FSS)**.

If the maximum CE_C is greater than 1×10^{-2}, § 450.108(b)(1) requires a highly-reliable flight safety system (FSS) that meets the requirements of § 450.145. The FAA has identified *Range Commanders Council, Range Safety Group, Flight Termination System Commonality Standard, RCC 319* (see first reference in paragraph 3.4 of this AC) as an existing means of compliance to demonstrate high-reliability of an FSS. The FAA will work with applicants to tailor RCC 319 in order to comply with § 450.145. Section 450.35(a)(3) requires an operator to obtain acceptance from the FAA for a means of compliance for § 450.145(b) in advance of submitting an application. Therefore, a tailored RCC 319 used as a means of compliance for § 450.145(b) must be submitted to the FAA for acceptance prior to being included in a license application.

8.2 **Safety-critical FSS**.

Section 450.108(b)(2) states that if the maximum CE_C is between 1×10^{-2} and 1×10^{-3} an operator must use a flight safety system that meets the requirements of § 450.143 and discussed in AC 450.143-1 *Safety-Critical Systems.* Historically, the FAA has found that operations launching or reentering in remote locations or for stages that only overfly sparsely populated regions have a CE_C between 1×10^{-2} and 1×10^{-3}.

8.3 **FSS Requirements**.

An operator usually determines which FSS system to use early in a vehicle design process. Therefore, it is generally helpful to identify early which set of requirements the FSS must meet. If an applicant chooses to use a highly-reliable FSS, an applicant must meet the requirements of § 450.145, and no CE_C analysis is required to determine the FSS requirements in accordance with § 450.108(b). This is because meeting the requirements of § 450.145 also satisfies the requirements of § 450.143. Alternatively, an applicant may compute the CE_C to determine whether an FSS is required, in accordance with § 450.101(c)(2), and, if so, the reliability standards the FSS must be met, per § 450.108(b). The CE_C analysis must be performed without consideration of the FSS, as the results will determine the requirements for the FSS. Paragraphs 8.1 and 8.2 of this AC describe how this CE_C analysis affects the FSS requirements. An approach to determine CE_C is described in AC 450.101-1 *High Consequence Event Protection*. For evaluation of the effectiveness of the flight abort rules, per § 450.108(d)(5), the reliability of the flight safety system should be determined. For a highly-reliability FSS, meeting the requirements of § 450.145, a reliability of 99.9% may be used.

9 FLIGHT SAFETY LIMITS OBJECTIVES.

9.1 Introduction.

In accordance with § 450.108(f)(2), the FSS must abort flight when valid, real-time data indicate the vehicle has violated any flight safety limit developed in accordance with § 450.108. An operator must define when a flight abort must be initiated in order to achieve objectives listed in § 450.108(c), including to ensure compliance with the public safety criteria of § 450.101(a) and (b). An operator must develop flight safety limits that meet the constraints set in § 450.108(d). For example, an operator must determine flight safety limits that account for the reliability of the FSS, in accordance with § 450.108(d)(5). This is a necessary aspect of a flight safety limits analysis because a critical objective is to ensure that the public and critical assets are protected from high consequence events given any intended flight abort action, and the reliability of the FSS can have a substantial influence on the predicted consequences of a flight abort action. There are several conditions that must be captured in the development of flight safety limits in accordance with § 450.108(c).

Note: In accordance with § 450.115(a), an operator's flight safety analysis method must account for all reasonably foreseeable events and failures of safety-critical systems during nominal and non-nominal launch or reentry that could jeopardize public safety.

9.2 Compliance with Risk Requirements.

In accordance with § 450.108(c)(1), the first objective is to develop flight safety limits to achieve compliance with the requirements of § 450.101(a) and (b). This, of course, includes collective risk criteria for expected casualties in § 450.101(a) for launch and in § 450.101(b) for reentry. In addition, flight safety limits also influence individual risk protection. For example, flight safety limits may be used to limit the region that exceeds the threshold for individual probability of casualty. This may be a better approach than evacuating a region, especially if the region is uncontrolled or a difficult-to-clear marine area. Regardless, it is critical that hazard areas be developed taking the flight safety limits into account; in accordance with § 450.133(a)(2) the flight hazard area analysis must account for any hazard controls implemented, which of course includes flight abort.

Note: Section 450.101(c) requires an operator to protect against a high consequence event only in uncontrolled areas, whereas the safety requirements in § 450.101(a) and (b) are not limited to uncontrolled areas, but instead apply to both controlled and uncontrolled areas. Thus, there are different considerations for developing flight safety limits based on where the exposed population is located.

9.3 **Prevent Increased Risk**.

The second objective of the flight safety limits, in accordance with § 450.108(c)(2), is to prevent continued flight from increasing risk in uncontrolled areas if the vehicle is unable to achieve a useful mission. It has been general practice in the safety community to contain debris, and this is an option via § 450.108(c)(6). Section 450.108(c)(2) captures the same intent, but with the recognition that a vehicle may deviate from the limits of a useful mission during a period where hazard containment is not possible. In this case, the requirement is to define a flight safety limit that prevents continued flight from increasing public risks, though some risk from either flight abort or continued flight may be unavoidable. Flight safety limits must be placed to ensure the lower-risk strategy is used, per § 450.108(d)(6), whether aborting flight once the vehicle has departed from the limits of a useful mission or allowing the flight to continue, at least until a location is reached where abort would reduce the risk. The concepts of “useful mission” and “limits of a useful mission” are discussed in AC 450.117-1, *Trajectory Analysis*. Evaluation of increased risk in § 450.108(c)(2) should consider risks of casualty from any hazard, including debris, toxic release, or explosions, including far-field blast overpressure (FFBO) effects.

9.4 **Prevent Anomalous Flight over Populated Areas**.

The third objective of the flight safety limits, in accordance with § 450.108(c)(3), is to prevent the vehicle from entering a period of materially increased public exposure in uncontrolled areas, including before orbital insertion, if 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. The intent of this regulation is to prevent unnecessarily exposing the general public to hazards when degraded vehicle health is identified. This flight abort situation commonly has been called a “gate,” but since the definition of a gate varies, the regulations state a clearer, performance-based requirement. In this document, the term “conditional limit” is used to refer to abort rules of this type. If the critical vehicle parameters fail to remain within the pre-established expected range or indicate an inability to complete flight within the limits of a useful mission at the location of a conditional limit, then the operator is required to initiate flight abort to accomplish a controlled ending to flight at the conditional limit.

9.4.1 Materially Increased Exposure.

A period of materially increased public exposure includes the beginning of a period when the vehicle will pose a hazard to a populated landmass prior to orbital injection. Overflight of continental areas and islands with substantial population generally constitutes a period of materially increased public exposure, while overflight of islands with small populations or other areas of sparse population generally do not. An applicant may use a CE_C greater than 1×10^{-2} as a threshold for materially increased risk in any significant period of flight from any on-trajectory failure mode. In general, a standoff from the landmass is advised to avoid hazards within several miles of a shore, due to high coastal vessel traffic. Orbital insertion also results in a material increase in public exposure due to the possibility of a random reentry from a vehicle that cannot achieve a minimum safe orbit. A vehicle that must reach orbit to achieve a useful mission would require flight abort in accordance with § 450.108(c)(3) if a minimum safe orbit cannot be reached.

9.4.2 Selecting Appropriate Critical Vehicle Parameters.

The critical vehicle parameters used to evaluate whether abort should be initiated generally depend on the vehicle type and mission. Ideally, critical parameters would determine that no anomaly exists that would prevent a successful mission at the time of validation. However, this perfect test is not practically possible. Therefore, critical parameters must be compared against pre-established expected ranges, per § 450.108(c)(3). The ranges are those whose values (individually or collectively) can indicate the inability to complete the upcoming phase of flight within the limits of a useful mission. For the final conditional limit for orbital missions, an important test is whether the vehicle is capable of reaching an orbit with a perigee greater than 70 nautical miles altitude.

9.4.2.1 The criteria used for determining whether to allow passage through a conditional limit or to terminate flight at the limit should use at least the same vehicle flight status parameters as the criteria used for determining whether to terminate flight at flight safety limits for this flight phase. For example, if a flight safety limit is a function of instantaneous impact point (IIP) location, the criteria for determining whether to allow passage through a conditional limit should also be a function of IIP (and potentially other parameters).

9.4.2.2 The flight abort rules should permit the vehicle to cross the conditional limit only if there is no indication that the vehicle's performance has become erratic and the vehicle is flying within the limits of a useful mission.

9.4.2.3 Erratic behavior should be assessed through quantitative metrics, such as angular velocity, growing vehicle oscillation, and stagnant IIP. In addition, if a human is making the flight abort decision, then a flight rule should also permit flight abort if the vehicle is erratic due to any other data. Human application of the erratic flight rule, however, is subject to significant judgment, and sufficient quantitative rules are a far more reliable solution, both for safety and for mission assurance. The operator must select parameters and their acceptable ranges that are appropriate for the vehicle and mission, with consideration of the ability to measure and act on the parameters, in accordance with § 450.108(c)(3).

9.4.2.4 Specific examples of critical vehicle parameters and associated pre-established expected ranges include:

- IIP latitude and longitude, as compared to a pre-established polygon;
- Direction of motion of the IIP (i.e. parallelism or convergence);

- Minimum impact range that the last suborbital stage must achieve, if the succeeding stage is to attain a useful orbit and a minimum orbit (perigee > 70 nautical miles);
- Pressure of a tank, as compared to minimum thresholds (e.g. verifying pressurized fluid will flow when required) or maximum thresholds (e.g. avoiding rupture);
- Motor chamber pressure;
- Orientation and/or angular velocity;
- Acceleration of the vehicle, verifying that motor is producing anticipated thrust; and
- Altitude at perigee, given the current position and velocity, verifying that minimum orbit can be achieved with remaining thrust.

9.4.2.5 The expected range for each critical vehicle parameter (or parameter set) should also be determined. The analysis should assess if a variety of trajectories, including all normal trajectories, are acceptable for passing through the conditional limit. The values of each critical parameter should be determined at the conditions when the validation will occur. The pre-defined expected range should encompass the range of values each of which are typically extended by a 20% margin to account for uncertainty, though this margin may vary on a case-by-case basis.

9.5 **Preventing High Consequence Events**.

The fourth objective of flight safety limits, in accordance with § 450.108(c)(4), is to prevent conditional expected casualties greater than 1×10^{-2} in uncontrolled areas due to flight abort or due to flight outside the limits of a useful mission from any reasonably foreseeable off-trajectory failure mode in any significant period of flight. Many of the phrases here match § 450.101(c), and AC 450.101-1 *High Consequence Event Protection*, provides guidance on the terminology used to define what constitutes a failure mode. This objective requires that abort actions do not produce high consequence events. This requirement does not apply to failure modes that lead to already minimized consequence before a vehicle exits the limits of a useful mission. For example, in a simple case, this requirement does not apply to an on-trajectory engine explosion. Also, loss-of-thrust is not considered an off-trajectory failure mode. Nor does it apply to a failure which causes breakup soon after initiation, such as a malfunction turn at high dynamic pressure that quickly causes structural failure before the vehicle exits the limits of a useful mission. In this context, breakup soon after initiation of a failure includes any breakup expected to occur before the minimum period necessary to implement a risk mitigation, such as flight abort or propellant dispersal. The CE_C limit in § 450.108(c)(4) applies to failures where vehicle begins to exit the limits of a useful mission and the vehicle would not be expected to breakup prior to this.

9.6 Abort Prior to Failure of Flight Safety System (FSS).

The fifth objective of the flight safety limits, in accordance with § 450.108(c)(5), is to initiate flight abort to prevent the vehicle state from reaching identified conditions that are anticipated to compromise the capability of the flight safety system if further flight has the potential to violate a flight safety limit. A real-time determination of whether a particular failure may evolve to violate a flight safety limit is not always possible. The operator must determine in preflight analyses (system safety analysis, link analysis, etc.) which failure modes can compromise the capability of the FSS, in accordance with § 450.108(c)(5). The operator should then perform analysis to determine if those failure modes can potentially violate a flight safety limit. If it finds a failure mode that can potentially violate a flight safety limit, the operator must develop flight safety limits and abort rules that protect against those modes in accordance with § 450.108(c)(5). If the ability to reach a flight safety limit via a particular failure mode is uncertain, the assumption should be made that it is possible during any phase of flight where flight abort is used as a hazard control strategy. In addition, flight safety limits and abort rules should be established to prevent the vehicle from exceeding the acceptable environments of the abort system in accordance with § 450.108(c)(5). For example, if the abort system is qualified to withstand a certain vibration environment, then limits and rules should be in place to abort in order to prevent the system from exceeding the established vibration level.

9.7 Containment Alternative.

An alternative objective, in accordance with § 450.108(c)(6), is to initiate flight abort to prevent debris capable of causing a casualty due to any hazard from affecting uncontrolled areas using a flight safety system that complies with § 450.145, in lieu of meeting §§ 450.108(c)(2) and (4). Containment means no hazard footprint (see definition 4.3) from any event, ignoring failures of the flight safety system, will impact an uncontrolled area. This containment strategy relieves the operator of needing to perform a consequence analysis but may be incompatible with mission requirements. Hazard containment achieves the goals of §§ 450.108(c)(2) and (4) because neither risk nor high consequence will be present in uncontrolled areas when hazard containment is provided. This can be achieved by complying with the legacy § 417.213. This strategy is not an option when hazard containment is not possible during a phase of flight. For example, if overflight of uncontrolled areas occurs on a useful mission trajectory during a phase of flight when flight abort is used as a hazard control strategy, an operator cannot claim containment during this phase and must meet §§ 450.108(c)(2) and (c)(4). To comply with § 450.108(c)(6), flight abort capability must be maintained until § 450.108(e) is applicable.

10 FLIGHT SAFETY LIMITS CONSTRAINTS.

Section 450.108(d) describes the constraints of flight safety limits. An operator must determine flight safety limits that satisfy each of the constraints identified in § 450.108(d).

10.1 Extent of Flight Safety Limits Analysis.

Section 450.108(d)(1) requires that flight safety limits account for temporal and geometric extents on the Earth's surface of any reasonably foreseeable vehicle hazards under all reasonably foreseeable conditions during normal and malfunctioning flight. The intent of this requirement is that the flight safety limits account for any area that could potentially be hazarded for any phase of flight that uses flight abort as a hazard control strategy. This includes the duration and region that could be affected by malfunction or abort. The entire region of the Earth's surface that could be hazarded must be considered until the time the hazard has ended.

10.2 Consideration of Hazards.

Section 450.108(d)(2) requires that flight safety limits account for physics of hazard generation and transport, including uncertainty. This is further discussed in AC 450.115-1 *High Fidelity Flight Safety Analysis*. Hazard generation refers to the process by which a vehicle produces a hazard. Transport is how the hazard moves from the source to an exposed person or a critical asset. For debris risk from an in-air breakup, hazard generation includes the fragmentation of a vehicle and uncertainty in fragment properties. Transport of debris is the propagation from each breakup location to impact accounting for all foreseeable forces that can influence any debris impact location and all foreseeable sources of impact dispersion in accordance with § 450.121(c)(1) and (2). For a loss-of-thrust or lift vector control, this includes modeling of the fall of the intact vehicle; consideration of whether it will structurally fail during the fall and if so, the associated fragments; the explosion, toxic release, fire, etc. at impact (generating a new hazard); then, the propagation of that hazard (e.g. a blast wave or toxic cloud). Also, for intact impact scenarios, the potential for FFBO hazards must be considered in accordance with § 450.137. For an in-air toxic release, hazard generation would account for the time-release history of the toxic species, and transport would be how the toxic species spread through the air.

10.2.1 <u>Debris Dispersion</u>.

For most of flight, the particulars of hazard generation and transport are of minimal importance in the development of flight safety limits. Outside of the launch or landing area, it is typically sufficient to consider debris dispersion effects to determine the extent of the hazard. Risk calculations account for all consequences, such as if there is undispersed propellant, but this has little effect on the size of the region that is hazarded. In the launch or landing area however, the size of the region hazarded, such as due to toxics or FFBO, can be significantly expanded beyond the debris dispersion area (which may be small in these areas) due to the transport of these hazards. Likewise, typically wind effects have a negligible effect on risk outside the launch or landing area. Generally, wind cannot affect the impact location of hazardous debris by more than a few miles and any wind effects are typically insignificant compared to dispersions from other sources. Outside of the launch or landing a buffer may be used to account for this variability when developing flight safety limits, provided the analysis demonstrates the adequacy of the buffer to meet the flight safety limits objectives. In the near launch or landing area, the acceptability of flight safety limits is determined through the flight safety analysis, where risks must be evaluated using latest winds or a prelaunch availability study in accordance with §§ 450.135(a) and 450.137(a). It is not generally necessary for flight safety limits to vary based on wind conditions, but it is conceivable that mission flexibility could be enhanced if they were in some situations.

10.3 Considering Data Loss.

Section 450.108(d)(3) requires that flight safety limits account for the potential to lose valid data necessary to evaluate the flight abort rules. The development of suitable limits is a precursor to meeting the requirement in § 450.108(f)(2)(iii). This AC uses the term "Duration of Acceptable Data Loss (DADL)" to encompass various approaches used previously to develop data loss flight times (DLFT), green numbers, or no data destruct times (NDDT). To implement a DADL limit, if at any point in flight all tracking data are lost, the abort system begins a data loss countdown timer with a duration predefined based on vehicle parameters at the time of data loss. When the countdown timer reaches zero, flight abort action is taken. Historically, the duration has typically been a function of only the flight time at data loss, but more sophisticated functions based on more parameters (e.g. position or IIP) may be used. Of course, this section only applies to periods in flight where the abort system is active.

10.3.1 Background.

A particular challenge in determining data loss criteria is the uncertainty as to the cause of data loss. If the data loss is the only failure, and the vehicle continues to fly normally, then taking abort action would result in increased risk (even in open ocean areas due to ships and aircraft). But if data loss is related to a failure that also causes deviation from a flight path, then risk may be reduced by aborting flight. In many cases, data loss is not a safety concern, such as due to:

- Expected behavior, such as communication gaps or sensor drop-out, from which the data stream is expected to return;
- Unexpected sensor or communication problems where no failure affecting flight has occurred; or
- Vehicle break up, such that flight abort would have no effect.

However, data loss could also indicate a safety issue, such as a sensor or communication failure that leads to bad data to the guidance system, or partial vehicle breakup where there is still a free-flying motor. Malfunction flight can also be a cause of data loss. The challenge is that in real-time, when data loss occurs, it is not known whether the vehicle is still operating correctly or not.

10.3.2 Partial Data Loss.

In most situations, the minimum required data are position and velocity of the vehicle. However, sometimes, different data may be sufficient to continue flight if it can be used to demonstrate that the vehicle is still normal. If this is the case, clear rules should define which parameters are required, and the flight conditions under which the set of required parameters changes.

10.3.3 Core Principles.

Because the vehicle state is unknown, it cannot be determined in real-time as to whether termination or continued flight is the better choice. The goals of flight safety action are still the same: reduce risk (especially high consequence events) and terminate before the ability to terminate is lost.[2] Every active motor should either have an Inadvertent Separation Destruct System (ISDS) or a flight safety system based on the state of the motor, in order to prevent free-flying motors, unless the motor can be physically contained outside of uncontrolled areas. The following principles should be used to develop data loss flight times.

a. If the vehicle is outside the limits of a useful mission, termination should occur immediately (subject to paragraph 10.3. of this AC).

b. Termination should occur before the vehicle could reach the following (any of these options is acceptable), accounting for the state of the vehicle at the time of data loss:

  i. Violating a position or IIP-based flight safety limit (e.g. the former part 417 approach for DLFTs),

  ii. Reaching the limits of a useful mission, or

  iii. Having a hazard footprint that reaches an uncontrolled area.

c. If data is lost while the vehicle is within the normal flight envelope, data loss flight times should be long enough to allow for reasonably expected data loss scenarios.

d. If uncontrolled populated regions are hazarded at the time of data loss, termination should be delayed until hazards from the vehicle would no longer hazard the uncontrolled area if the vehicle were operating normally. Additional study would be appropriate if this would lead to increased likelihood of impacting regions of higher population density.

e. No abort action should be taken based on data loss whenever the vehicle is no longer able to reach a flight safety limit, including having reached orbital insertion.

[2] Terminating quickly upon data loss also helps reduce the potential hazard area, which is helpful for post-accident response. However, this is not as relevant for on-board autonomous safety systems, as loss of data to the flight termination decision computer may or may not indicate loss of data to external systems. And only those external systems are relevant for post-accident response.

f. The operator may choose not to implement data loss flight abort limits at any state where:

   i. The only reachable flight safety limits are not required in order to meet § 450.108.

   ii. The vehicle's state vector has reached a state where a flight safety system would not materially decrease the collective risk or the risks from a high consequence event.

10.4 **Consideration of Time Delay**.

Part 450.108(d)(4) requires that flight safety limits account for the time delay, including uncertainties, between the violation of a flight abort rule and the time when the FSS is expected to activate. Time delays are important in a flight safety limits analysis because the decision to abort flight must be made in time to achieve the flight safety limits objectives in accordance with § 450.108(d)(4). This is not possible unless the time delay between the violation of a flight abort rule and the time when the FSS is expected to activate is known. The delay is the total time from the actual violation of a flight safety limit until the abort action is finally accomplished, also called the latency of the abort action. Examples of flight abort being finally accomplished are (1) when the IIP stops moving following a destruct action, and (2) when the net thrust reaches zero following a thrust termination action. The delay may include hardware, software, communication, and human-in-the-loop contributions from tracking systems, data processing systems, display systems, command control systems, and flight safety systems.

10.4.1 Hardware Delays.

Hardware delays are typically less than one second unless intentionally lengthened, and may include:

- Processing time of the navigation unit (e.g. delay of the GPS receiver to determine position);
- Time on the vehicle to activate the abort. This is the time from terminate signal

  received on the vehicle until the thrust or controlled glide is stopped. For example, on a thrust termination system this includes the time to fully shutdown a turbopump and end any residual thrusting; and

- Intentional delays to allow escape of a vehicle component prior to abort.

10.4.2 Software Delays.

Software delays include:

- The time to process received data (e.g. decommutation), to transform the data to other formats and coordinate systems,
- Filter delays;
- For systems with a person on the ground to initiate a destruct, the time to generate displays;
- For automated systems, the time to process rules and issue a terminate signal; and

- Intentional delays to allow escape of a vehicle component prior to abort.

10.4.3 Communication Delays.

Communication delays consider the transmission time of data. This includes both transmission from the measurement system to the abort rule system and from the abort rule system to the system that effects the abort.

10.4.4 Safety Officer Decision Duration.

When a human is in the loop, the human delay is usually the most significant, and also has significant uncertainty. For a safety officer, this is the time to process the decision and send the abort. The delay depends on the training of the safety officer, and the verification sources they are tasked to monitor (confirming violation across multiple tracking sources, hearing violations through multiple communications, or similar). In some cases, safety officers are trained to activate the abort *before* a flight safety limit violation, and thus the effective latency for their action may be negative. However, in most cases, safety officers react when a vehicle violates a limit, and thus the latency is slightly positive. There is also a typical constraint that safety officers have a longer delay when the vehicle appeared nominal prior to the failure. The decision delay, including uncertainty, should be based on studies of safety officer responses to simulated malfunction flight. The appropriate measurement is the delay should be between the time the displays show a violation and the safety officer initiates abort. This should be evaluated considering noise and different types of failures.

10.4.5 Pilot Abort Action Duration.

When a pilot is implementing the abort, there is a delay between making the abort decision or receiving the direction to abort and completing the action to initiate abort. This process must be considered and must account for the entire time until the abort initiation sequence is completed in accordance with § 450.108(d)(4).

10.5 **Consideration of FSS Reliability**.

Section 450.108(d)(5) requires that an operator must determine flight safety limits that account in individual, collective, and conditional risk evaluations, both for proper functioning of the flight safety system and failure of the flight safety system. Thus, the risks from a failed abort must be considered in evaluation of § 450.101(a) and (b) and § 450.108(c)(4). Thus, the outcomes of malfunction flight where the FSS fails should be included in the residual risk, with a conditional probability of one minus the reliability of the FSS. The conditional probability of risks from proper function of the FSS should either be the reliability of the FSS or one. Note, however, that § 450.108(c)(6) obviates the need for a conditional risk analysis per § 450.108(c)(4) if the FSS complies with § 450.145 and abort prevents debris capable of causing a casualty due to any hazard from affecting uncontrolled areas, in accordance with § 450.108(c)(6). While § 450.108(d)(5) requires that an operator account in its conditional risk evaluation both for the proper functioning of the FSS and the failure of the FSS, an operator would not be required to perform a conditional risk evaluation if it is in compliance with § 450.108(c)(6), because § 450.108(c)(4) would not apply. In this case, the applicant should still assess the collective and individual risk from a failure of the flight safety system in accordance with § 450.108(d)(5).

10.6 **Abort Should Never Increase Risk**.

Section 450.108(d)(6) requires that flight safety limits be designed to avoid flight abort that results in increased collective risk to the public in uncontrolled areas, compared to continued flight. This is a common-sense requirement that taking abort action should not present a higher risk to the public than not taking abort action. This can affect the location of the flight safety limits. A best practice is that flight safety limits analysis would minimize all foreseeable consequences, not just those to people on the ground or to the extent necessary to meet the public safety criteria.

10.6.1 Best Practice For Flight Safety Limit Locations.

For example, placing flight safety limits in areas where flight abort might place debris on a busy shipping lane or air corridor is not a best practice when other locations for the limits could meet the public safety criteria and consequence criteria, and still provide space for the vehicle to execute a useful mission. Also, as a malfunctioning vehicle's hazard footprint migrates towards a populated area, the consequence to people on the ground from a flight abort will increase from a low number and possibly reach the proposed consequence limit. The best practice for identifying the location for a flight safety limit on such trajectory is not at the last location where an abort would still result in meeting the consequence criteria, which would presumably result in a consequence close to the limit, but at a location that minimizes the consequence. This approach could result in flight safety limits that provide debris containment, or nearly so, while also allowing normal flight and flight within the limits of a useful mission without triggering an abort.

10.6.2 Selecting Lowest Risk Alternative.

It is not possible to evaluate every possible location of flight safety limits, so it is impossible to determine with certainty the absolute minimum risk location for limits. However, it is possible to evaluate for each malfunction trajectory that the risks from aborting due to flight safety limits are equal to or less than the risks from not aborting at all. This should be done by comparing the CE_C between abort action, and allowing continued flight. It is also possible to qualitatively assess the impact areas resulting from abort action and identify areas where risks might be reduced through a modification to the flight safety limits. If there is potential for a material reduction in risk, then alternative flight safety limits should be evaluated and the lowest risk alternative selected.

10.7 **Risk on any Useful Mission Trajectory**.

Section 450.108(d)(7) requires an operator to ensure any trajectory within the limits of a useful mission that is permitted to fly without abort would meet the collective risk criteria of § 450.101(a)(1) or (b)(1) when analyzed as if it were the planned mission in accordance with § 450.213(b)(2). This analysis should, at a minimum, account for the collective risk due to planned hazardous debris as well as the potential for on-trajectory failure modes. The philosophy behind § 450.108(d)(7) is to allow a non-normal flight to continue as long as the mission does not pose an unacceptable conditional risk given the present trajectory. An example of missions that fall into this category are missions that lift-off on an incorrect flight azimuth, usually due to a software input error, such as the Ariane 5 failure on January 25, 2018. Apart from the programming error, these vehicles may be healthy and are not expected to fail more frequently than a flight without the programming error, so these flights should be allowed to continue if they meet the collective risk criteria on the present azimuth (including the risk from planned debris impacts on the present flight azimuth). If they do not, such flights would be required, in accordance with § 450.108(d)(7), to implement an abort before the point in flight where the collective risk criteria would be exceeded.

10.7.1 Variety of Trajectories.

It is of course, impossible to evaluate every possible trajectory within the limits of a useful mission to meet § 450.108(d)(7). Instead, this requirement should be met by evaluating the risk for a variety of trajectories in the envelope, each with normal trajectory dispersions and accounting for all failure modes and planned events. The requirement states that the risk criteria must be met for any trajectory within the limits. This does not require every possible trajectory within the limits to be examined. Instead a sufficient set is one that includes the edges of the limits and those identified, by inspection or analysis, that overfly population centers that could result in risks exceeding the criterion.

10.7.2 Risk Evaluation.

Risk evaluation must follow a methodology for flight safety analysis consistent with § 450.115, but need only evaluate collective risk metrics. Usually risks are not significantly changed within the useful mission envelope for failures very early in flight, when the useful mission envelope is small compared to the distance to exposed population. Thus, FFBO and toxic risks are often not relevant for this analysis. Analyzing a variety of trajectories is most important for examining debris risks when a vehicle has a larger limit of useful missions. It is best practice to optimize flight abort rules to define a minimal set that provides adequate protection while eliminating duplicate or unnecessary rules that add complexity to the flight safety system implementation. Further, flight safety limits can help to reduce financial responsibility obligations determined in accordance with 14 CFR Part 440 requirements. This includes preventing intact impacts with non-trivial remaining explosive or toxic materials.

11 END OF FLIGHT ABORT.

For some mission scenarios, at some point in flight, abort can no longer mitigate risk. Section 450.108(e) states that a flight does not need to be aborted to protect against high consequence events in uncontrolled areas beginning immediately after critical vehicle parameters are validated, if the vehicle is able to achieve a useful mission and certain conditions are met for the remainder of flight. Specifically, the conditions which must be present are: (1) flight abort would not materially decrease the risk from a high consequence event, and (2) there are no key flight safety events. In these situations, flight abort no longer provides any effective mitigation of high consequence events. This addresses a common occurrence during a period of planned overflight of an uncontrolled area immediately preceding orbital insertion.

11.1 Key Flight Safety Events.

In order to comply with § 450.108(e)(2) key flight safety events must be identified. The definition in § 401.7 states that a "key flight safety event" means a flight activity that has an increased probability of causing a failure compared with other portions of flight. Additional guidance is provided in AC 450.101-1, *High Consequence Event Protection*, in the discussion of phases of flight (a phase of flight cannot include a key flight safety event).

11.2 Material Decrease in Risk of High Consequence Events.

The evaluation of § 450.108(e)(1) requires definition of material decrease. A material decrease does not include cases where the risks are already two orders of magnitude below the threshold of interest. A material decrease does not include small reductions, specifically a reduction smaller than coefficient of variation of irreducible uncertainty in input data. Typically, the two most significant irreducible uncertainties are the population distribution and the outcome of a failure. For population, it is impossible to obtain data on the exact location (including sheltering) of every individual affected by a launch or reentry. For failure outcomes, there is uncertainty in the dynamics of breakup and in the flight of a vehicle between failure and impact. Thus, if CE_C is used as a metric, a reduction in CE_C by a factor of less than two is not a material decrease (based on empirical evidence). And likewise, if CE_C is below $1E^{-3}$, it is not a material decrease.

11.3 Evaluation of Critical Parameters.

If the two conditions above are valid for the remainder of flight, then flight abort may be disabled. When flight abort is disabled, a conditional limit—a flight safety limit which includes validation of critical parameters—should be used. This is identical to that described in paragraph 9.4 of this AC.

12 FLIGHT ABORT RULES.

Flight safety limits as developed to meet the Part 450 regulations are implemented as rules for flight. These rules must be implemented as part of flight, in accordance with § 450.108(f), to ensure that a determination can be made on whether flight abort must be implemented.

12.1 **Data Availability**.

In accordance with § 450.108(f)(1) vehicle data required to evaluate flight abort rules must be available to the flight safety system under all reasonably foreseeable conditions during normal and malfunctioning flight. Flight abort rules are not useful if the data to evaluate them is not available to inform the flight abort decision during flight. There are three examples of situations that challenge the availability of vehicle data needed to facilitate flight abort rule evaluation. First, that a flight abort rule (or limit) could rely on knowledge of the future. An example would be a rule that states that flight abort should occur if a vehicle will pose a hazard to a location. The point of the analysis above is to develop limits that achieve this goal with available information. Second, a rule could be based on subjective judgment that is either impossible to evaluate in the case of an autonomous system or too reliant on discretion of the safety officer. An example of this is the “obviously erratic” rule. While this is an important safety precaution for failures that have not been foreseen, it cannot be relied on to terminate a vehicle for any failure that is foreseeable. Third, a rule could rely on data, which is no longer available to the decision system where the rule might be violated. An example of this would be a downrange flight safety limit, which the vehicle might violate when it is below the horizon of a tracking system critical to the evaluation of a flight abort rule.

12.2 **When Flight Abort Must Occur**.

12.2.1 Implementing Flight Safety Limits.

The FSS must abort flight when valid, real-time data indicates the vehicle has violated any flight safety limit developed in accordance with § 450.108(f)(2)(i). This is simply the requirement that in real-time, flight parameters must be evaluated relative to the flight safety limits developed above and abort action taken when violated. It is, of course, insufficient to develop limits, but then ignore them during an actual mission.

12.2.2 When Flight Safety System nears Incapacitance.

Section 450.108(f)(2)(ii) requires that the FSS must abort flight when the vehicle state approaches identified conditions that are anticipated to compromise the capability of the FSS and further flight has the potential to violate a flight safety limit. This is the implementation of the flight safety limit developed to meet the objective in § 450.108(c)(5).

12.2.3 Invalid Track Data.

Section 450.108(f)(2)(iii) requires that the FSS must abort flight in accordance with methods used to satisfy § 450.108 (d)(3), if tracking data is invalid and further flight has the potential to violate a flight safety limit. This is the implementation of the flight safety limit developed to meet the constraint in § 450.108(d)(3), and the approach is discussed in paragraph 10.3 of this document.

13 FLIGHT SAFETY LIMITS MEANS OF COMPLIANCE.

This chapter describes a means of achieving all the requirements for flight safety limits, both objectives and constraints. These steps are expected to be applied for evaluation of a single intended flight or a small set of similar flights. The analysis results for the full range of licensed operations do not need to be submitted with the application. To comply with § 450.108(f)(2), the applicant needs to demonstrate their process for a representative mission, then use the same process during a flight. The following steps provide a methodology:

1. Start with an envelope of trajectories sufficient to characterize variability and uncertainty during normal flight in accordance with § 450.117 and that encompass the limits of a useful mission, per § 450.119(a)(3).
2. Evaluate and adjust the envelope, so § 450.108(d)(7) can be satisfied, reducing the envelope if some portions do not meet acceptable risk criteria. During this step, portions of the envelope which could lead to debris on uncontrolled areas are also identified.
3. Evaluate the potential for ending flight abort, applying § 450.108(e).
4. Identify potential flight safety limit types, based on system capabilities, so § 450.108(f)(1) can be satisfied.
5. Perform time delay analysis (system latency), satisfying § 450.108(d)(4).
6. Determine buffers accounting for credible malfunction flight, satisfying § 450.108(d)(1).
7. Define candidate quantitative criteria for each limit type, satisfying §§ 450.108(c)(2), (4), and (5). Note that compliance with § 450.108(c)(6) is an alternative to §§ 450.108(c)(2) and (4).
8. Define conditional limits,[3] satisfying § 450.108(c)(3).
9. Validate that rules as defined can be supported by the system, satisfying § 450.108(f)(1).
10. Adjust the limits to reduce risk, in accordance with § 450.108(d)(6), and/or better meet mission secondary objectives.
11. Assess residual risk, including CE_C, and refine as necessary, verifying that all objectives of § 450.108(c) and constraints of § 450.108(d)(6) are satisfied, using flight safety analysis per subpart C, satisfying §§ 450.108(d)(1) and (2), subject to the requirements of § 450.108(d)(5).
12. Compute durations of acceptable data loss, satisfying § 450.108(d)(3).

[3] A "conditional limit" is a performance-based requirement similar to a "gate" concept. See paragraph 9.4 of this AC.

13.1 **Trajectory Envelope**.

The initial "trajectory envelope" should describe the extent of where the vehicle may fly and still be within the limits of a useful mission, in accordance with § 450.119(a)(3). According to § 401.7, a useful mission is one that can attain one or more objectives. The limits of a useful mission means the trajectory data or other parameters that bound the performance of a useful mission, including flight azimuth limits. These must incorporate all uncertainty and variability that exists, in accordance with §§ 450.117(a)(1) and (2). This should include, but not be limited to, wind variability, performance uncertainty, mission initiation time variability, and launch platform variability. The variability should encompass just the planned operations for which the flight safety limits are intended to be applied. Trajectories that fly on an unplanned guidance program (e.g. incorrect azimuth) may still be useful if an objective can be met. These are examples of unintended trajectories. These trajectories may become the boundaries of what is considered useful; however, their extents must be separated from the extents of normal flight including only uncertainty and variability (not failures), in accordance with § 450.117(a).

13.1.1 Trajectories That Characterize Variability.

When an operator develops flight safety limits for a family of missions, they must also incorporate the variability in mission objectives in accordance with § 450.117(a)(1). AC 450.117-1, *Trajectory Analysis* describes the development of such trajectories. For flight abort rule development, the maximum extent in time, position, and impact point should be considered. The traditional three-sigma trajectories (as described in the former 14 CFR Part 417) about the nominal trajectory may be a starting point. However, the analysis should use actual trajectory simulations rather than constructed trajectories,[4] unless the use of actual trajectories is operationally prohibitive and it is shown that use of constructed trajectories produce equal or higher risk estimates and hazard areas for all mission profiles. Numerous trajectories should be simulated to reflect the extremes of normal flight in all phases of flight. In some cases, intermediate trajectories are also necessary to ensure that risk is acceptable across the range of useful missions, especially when a large fan of possible trajectories is considered useful. The intermediate trajectories should be identified as those that overfly population centers where the population density divided by IIP rate is comparatively high.

13.2 **Trajectory Envelope Evaluation**.

The second step, in accordance with § 450.108(d)(7) is to ensure that all trajectories within the envelope described in paragraph 13.1 of this AC meet the risk criteria of § 450.101(a)(1) or (b)(1) when analyzed as if it were the planned mission in accordance with § 450.213(b)(2), but applying the special conditions described here. This requirement should be met by evaluating the risk for a variety of normal and unintended trajectories, each with normal trajectory dispersions and accounting for failure modes

[4] The distinction between simulated and constructed is as follows: a simulated trajectory is a self-consistent physically-realizable trajectory, whereas a constructed (or "synthetic") trajectory may be assembled by using state vectors from different trajectories at different times to define extremes, and thus is not necessarily physically realizable.

and planned events. The specific trajectories should be selected with the method described in paragraph 13.2 of this AC. Risk evaluation must follow a methodology for flight safety analysis consistent with § 450.115, with three special conditions. First, each selected trajectory should be evaluated as if it were the nominal trajectory, and risk should be computed considering normal trajectory dispersions. Second, this analysis need only evaluate collective risk metrics, not individual risks or high consequence events. Third, the failure probability may be allocated only to on-trajectory failures, as described in paragraph 13.2 of this AC. The third condition is a simplification that facilitates efficient analyses, which should only be used in cases where the "on-trajectory" failures occur on a trajectory that is the result of a malfunction (e.g. incorrect azimuth).

13.2.1 Trajectory Selection.

This analysis normally begins by analyzing the nominal, the edges of the envelope, and those trajectories which can lead to debris on the most densely populated areas. The assessment should also analyze trajectories that may concentrate hazards on significant populated areas, by having the slowest impact point traverse rate (longest dwell time) for the ballistic coefficients of fragments with significant consequence, a short time span of high probability of failure, etc. Particular attention should be paid to the impact areas associated with jettisoned items, especially if an unintended trajectory could place them over land instead of water, in accordance with § 450.133.

- · In most cases, the envelope analysis is likely to be straightforward, but a more complex envelope (e.g. gaps or special restrictions) may require a more extensive analysis to satisfy § 450.108(d)(7). For example, for overflight, an envelope analysis could be performed to show that a series of windows of azimuth are available, but flight is not allowed over the most densely populated cities. An even more complex example is an inland suborbital air-drop mission, where the envelope analysis could be performed to show that the drop point and ignition locations should be constrained to a certain volume, and then later in flight, trajectories can include larger volumes.
- In order to accomplish § 450.108(c)(3), the analysis should also identify the portions of the envelope that approach an uncontrolled area with materially increased public exposure. It is often clear which areas are likely to be affected: overflight of continents and significant islands within the geographic extent of the useful missions.

13.2.2 Failure Probability Allocation.

There are different approaches to assessing a particular useful mission trajectory with respect to § 450.108(d)(7).

- The total failure probability may be allocated to each on-trajectory failure mode separately, or just the most hazardous on-trajectory failure mode, while retaining the allocation with respect to the mission timeline for each failure mode being studied. This reduces the extent of the analysis compared to including off-trajectory failure modes but may require a different approach if conservatism results in non-compliance with § 450.108(d)(7). If any on-trajectory failure mode is excluded, the operator should provide evidence why the included failure mode(s) provide conservative results.

- An operator may distribute the total failure probability across just the on-trajectory failure modes, while retaining the allocations with respect to the mission timeline and relative likelihoods of each of these failure modes. This reduces the extent of the analysis compared to including off-trajectory failure modes but may require a different approach if conservatism results in non-compliance with § 450.108(d)(7).
- All on-trajectory and off-trajectory failures modes may be considered, retaining their allocations with respect to the mission timeline and relative likelihoods.

Note: For all three approaches, allocation of the failure probability to flight time should be performed with the consideration for variability in the mission timeline.[5] When critical events on an examined useful mission trajectory differ from the nominal timeline, the allocation with respect to time should be adjusted to correspond correctly to the events.

13.3 **Evaluating Ending Flight Abort**.

An applicant frequently wishes to turn off the capability for flight abort for some period towards the end flight, such as in the period before reaching orbit. Normally, flight abort is ended prior to reaching orbit, in order to prevent accidental initiation of abort resulting in orbital debris. For landings, flight abort may also be ended prior to touchdown, in order to prevent accidental abort on the ground.

13.3.1 Determining When Abort Can Be Ended.

Determination of when flight abort may be ended should be evaluated by first selecting a set of trajectories that span the acceptable envelope identified in paragraph 13.2 of this AC. For each trajectory, the CE_C vs. time (see AC 450.101-3 *High Consequence Event Protection*) should be computed for all foreseeable failure modes, back to the last key flight safety event, per § 450.108(e)(2). For each significant period of flight, the CE_C should be computed as if the termination system acted immediately upon failure, $CE_C^{\text{best}}(t)$, where *t* represents the time of failure. This is the minimum CE_C that can be reasonably expected from taking abort action. Likewise, the maximum CE_C over all other failure modes should be identified for each significant period of flight, $CE_C^{\text{other}}(t)$. Per the discussion in paragraph 11.2 of this AC, evaluation should be performed to determine if, at any time, abort would result in a material decrease in CE_C. This occurs at any time that $CE_C^{\text{other}}(t)>1E^{-3}$ and $CE_C^{\text{other}}(t)>2\,CE_C^{\text{best}}(t)$. This time, t_{end} represents the earliest possible nominal time that abort could be ended.

---

[5] For example, for a failure where the vehicle thrust is degraded and engine shutdown may occur later than normal, the failure probability rate during the period of degraded thrust should consider that the total thrusting time is longer than for a normal flight. Also, failure rates for subsequent phases of flight should not be transitioned to until those phases begin on the new mission timeline.

13.3.2 Establishing a Conditional Limit.

This time, t_{end}, is then used to develop a conditional limit for the criteria where the flight abort will be ended. A conditional limit is based on other parameters, such as IIP or position. These should be established so that the nominal trajectory crosses them after t_{end}. The conditional limit thus usually should be placed so that a nominal vehicle would cross it later in flight than the nominal time, and so that the failure trajectories that led to reducible CE_C do not cross the conditional limit and potentially end the abort capability. These flight safety limits should then be evaluated to ensure that the CE_C criteria for materially decreased, as discussed in the previous paragraph, are satisfied. This is especially important for failures that occur in the period just preceding the conditional limit. Conditional limits are further discussed in paragraph 13.9 of this AC.

13.4 **Acceptable Envelope Definition**.

The acceptable mission envelope is then determined by starting with the envelope of the limits of a useful mission and eliminating portions that would violate the collective risk criteria of §§ 450.101(a)(1) or 450.101(b)(1). The trajectories from the selection above that violate the risk criteria are used to describe what portions of the initial envelope should be removed. The remaining *acceptable trajectory envelope* encompasses only trajectories that meet the collective risk requirement, either when intentionally designated as the planned mission in accordance with § 450.213(b) or when the "nominal trajectory" is in fact an unintended trajectory that is the result of a malfunction (e.g. incorrect azimuth).

13.4.1 African Overflight Example.

A simple example of the application of this are missions from the Eastern Range that fly over Africa. Trajectories which overfly the coastal areas of Western Africa may meet mission objectives, but the risks associated with flying over these densely populated areas may exceed the risk criteria. Thus, the allowed envelope may need to be restricted to only trajectories which avoid overflight of these regions.

13.4.2 Hazard Footprints and Debris Footprints.

For evaluating hazard extent, a hazard footprint should be used. A hazard footprint is an extension of a debris footprint. A debris footprint is a geographic region containing, with at least 97% confidence, all the hazardous debris impacts resulting from an event. The debris footprint should be computed from the probability density distribution of debris impacts from an event (e.g. a breakup scenario). For flight safety limit evaluation, the debris footprint may be computed either by using a mean wind, and adding a ten-mile radius to account for wind variability, or using a more physically accurate modeling approach. A hazard footprint extends the debris footprint to include the region where the probability of casualty exceeds 1% from any impact included in the footprint (conditional on each impact), considering all hazards. The extended area is based on the distance from the impact location where a casualty could occur. For inert debris, one thousand feet may be assumed, or an analysis could demonstrate a smaller value. If propellant could remain at impact, the explosive radius and/or toxic cloud drift distance should be accounted for (these require analysis to identify the distance to the

1% probability of casualty). This distance should then be applied to expand the debris footprint polygon in each direction.

13.4.3 Potential for Hazards in Uncontrolled Areas.

The analysis must determine the specific limits that describe the portions of the envelope that lead to debris on such areas, in accordance with § 450.108(d)(2), which must consider all hazardous debris (as defined in § 401.7), in accordance with § 450.135(b)(1). For downrange overflight of a continental area, the first state vector in a trajectory where a hazard footprint from an on-trajectory failure reaches an uncontrolled area defines the minimum state vector. It is best practice to leave a "near-shore gap" of at least 10 miles between the shoreline and the hazard footprint to protect local ship and boat traffic. These state vectors should be determined across the acceptable envelope of useful trajectories. Also, for an island or land overflight, the last state vectors for which the hazard footprint includes the landmass (including a near-shore gap) should also be identified. This identification includes development of a hazard footprint that accounts for all sources of dispersion. For an island, left and right extents of trajectories that would affect the island should be determined as well, again accounting for debris uncertainty.

13.4.4 Categorizing State Vectors.

The product of this analysis is the set of state vectors from all trajectories describing a useful mission that have acceptable risk. These will be used in the subsequent parts of this analysis to define the flight safety limits. Each state vector of the selected trajectories should then be identified in two ways.

1. If it is in the portion of a trajectory that causes exceedance of the collective risk criteria.
2. Whether a breakup at the state vector would lead to debris in an uncontrolled area.

13.5 Identify Potential Flight Safety Limit Types.

Federal Ranges have used different types of flight safety limits and flight abort rules depending on instrumentation available, the dynamics of the vehicle, and the geography of the region(s) being protected. Execution of the flight abort rules can be via a ground-based safety officer (e.g. Mission Flight Control Officer), an automated ground-based system, an on-board autonomous flight safety system (AFSS), and/or a pilot. The flight abort rule types described in paragraph 13.5 of this AC apply to any of these types of systems.

13.5.1 Flight Abort Rule Types.

Flight abort rules fall into two categories. Rules monitor either vehicle health, regardless of the geographic position, or vehicle state vector (and their associated instantaneous impact point) relative to the environment. Flight safety limits are the quantitative criteria on which either type of rule is evaluated.

13.5.2 Vehicle Health Based Rules.

Rules that are based on vehicle health must be used in order to ensure that the abort system is not compromised before an abort can be achieved and before reaching a flight safety limit, in accordance with § 450.108(c)(5), (d)(3), (f)(2)(ii), and (f)(2)(iii). Example metrics for this category include electrical power stability, vibration limits, thermal limits, acceleration limits, vehicle angular rate limits, sensor quality requirements, chamber pressure, and data loss. For qualified abort systems, the applicant should identify the vibration, thermal, and motion-based limits based on the qualification standards. Identification of such rules for a pilot-in-the-loop abort system is outside the scope of this advisory circular. Paragraph 13.13 of this AC discusses the development of the duration of acceptable data loss. Data consistency rules define the approach for dealing with inconsistent input data. This approach should include a voting scheme. In cases where all navigation data (GPS, IMU, etc.) is lost, abort must occur in accordance with the duration of acceptable data loss, in accordance with § 450.108(f)(2)(iii).

13.5.3 Vehicle State Vector Guidelines.

Rules based on vehicle state vector and associated IIP should aim to meet the following pragmatic guidelines to achieve the flight safety limits objectives and constraints. It is also helpful for the applicant to allow for accurate prediction of the hazard location with adequate time to allow rerouting of aircraft, when real-time aircraft hazard mitigation is used.

1. Ensure the vehicle moves downrange (when applicable).
2. Prevent significant cross-range deviations.
3. Prevent intact impact with significant remaining propellant.

13.5.4 Most Common Flight Safety Limit Types.

The most common types of flight safety limits are the following. In many cases, debris containment and risk requirements can be met with a combination of only these three types.

1. Maximum altitude vs. downrange limits, to meet guideline 1.
2. Fixed Termination Line based on Instantaneous Impact Points (IIP), either based on vacuum or drag-corrected prediction, to meet guideline 2.
3. Minimum altitude vs downrange distance, to meet guideline 3 and assist with real-time aircraft hazard mitigation.

13.5.5 Less Common Flight Safety Limit Types.

Other types of flight safety limits are less commonly used:

1. Moving termination lines based on IIP[6], to meet guidelines 1, 2, 3, and assist with real-time aircraft hazard mitigation.
2. Azimuth limits, based on vehicle velocity vector to meet guideline 2.
3. Flight path angle limits, to meet guideline 3 and assist with real-time aircraft hazard mitigation.
4. Fixed minimum altitude, if the vehicle is falling, to meet guideline 3.
5. Optical tracking systems (skyscreens) to meet guidelines 1, 2, and 3 in the launch area.

13.5.6 Flight Safety Limits Constraints.

In accordance with § 450.108, there are also two constraints that must be considered when developing flight safety limits of any of the types above, when containment is not achieved. Conditional limits (see paragraph 13.9) are usually also a part of the strategy to meet these constraints:

1. In accordance with § 450.108(d)(6), do not abort in areas that would increase the collective risk (measured with E_C) to the public in uncontrolled populated areas, compared to continued flight.
2. In accordance with § 450.108(c)(4), do not abort in areas that would exceed 1×10^{-2} conditional expected casualties for off-trajectory failure modes.

13.5.7 Flight Safety Limit Types not addressed in this AC.

The above types are described in this document and explained in more detail in paragraph 13.8 of this AC. Other types of limits include seawalls, retrograde IIP, and present-position-based termination lines, but these are not common and not further discussed. Vertical plane charts and straight up times are not discussed. They are only used for historical reasons and have generally been found to be redundant with other simpler or more versatile rules. Finally, “obviously erratic” rules are usually in place when abort action is initiated by a human, which can help to prevent loss of command capability for ground-based systems to meet § 450.108(c)(5) and (f)(2)(ii), but these cannot be relied on in a safety analysis, due to the ambiguity as to when they would be violated. Any similar rule should be based on parameters that can be measured (such as body rates) with limits based on negative outcomes when exceeded (such as loss of FSS control). The selection of the flight abort rule types typically depends on range equipment or AFSS design, but the collective set must meet the requirements of § 450.108.

[6] An example of moving IIP limits are what has historically been called “chevrons.”

13.6 **Determining Abort System Latency**.

A time delay analysis must determine the abort system latency, including uncertainties, in accordance with § 450.108(d)(4). See paragraph 10.4 of this document for the considerations in determining latency. The delays should be determined through system testing and should consider any changes during flight, such as longer communication paths or retransmission points. An adequate analysis should diagram all steps in the process and determine delays from each part, with a resolution of 0.1 second or better. The *uncertainty* in the delay must also be determined to meet § 450.108(d)(4). For autonomous systems, a one-sigma uncertainty in the total time delay of 0.1 seconds is typical. When a human is in the loop, the uncertainty is much larger.

13.7 **Buffer Development**.

Mission assurance is benefited when there is margin between flight safety limits and vehicles on a potentially useful mission. Therefore, a buffer between the trajectories that define the limits of a useful mission and any flight safety limit may be used when the hazard footprint does not intersect populated areas. When the hazard footprint from the normal trajectory does intersect populated areas, then risk evaluation should be done to determine the optimal location for flight safety limits.

13.7.1 Malfunction Trajectories.

To determine the buffer, malfunction trajectories for the failure mode that leads to the most rapid credible deviation of the vehicle from the normal flight envelope should be used. The failure that generates this is typically a guidance system failure that aims the vehicle in a new direction and turns the vehicle as fast as physically possible in that direction. Ideally, in that simulation, the vehicle attitude is controlled to ensure that structural limits are not exceeded during the failure. In many cases a simpler model is used that simply turns the vehicle as fast as the control system will allow (or even immediately). The initiation times for trajectory generation should occur at sufficiently frequent intervals from launch until the vehicle is orbital or returns to ground. Sufficient frequency for low thrust-to-weight ratio (e.g. less than three) flight periods is typically one second or less near significant exposure areas or any maneuvers, and five seconds or less during steady state—but may need to have higher frequency for high thrust-to-weight vehicles in accordance with § 450.119(b)(3). See AC 450.117-1, *Trajectory Analysis*, for more information on malfunction trajectory generation.

13.7.2 Determining Minimum Buffer.

The buffer is based on the minimum malfunction duration. This minimum should always be accounted for—that is flight safety limits should always include this buffer, but sometimes it is not necessary to explicitly follow the process described below. To determine the minimum buffer, use the following steps:

1. Define a target time delay duration between the onset of a failure and the initiation of flight abort. Typically, no less than the desired *minimum* data loss flight time, e.g. 5 seconds.
2. Generate failure trajectories that deviate as rapidly as physically possible (i.e. the vehicle could fly and remain substantially intact) from the envelope of trajectories

as described above. The duration of the failure trajectories after failure initiation should extend at least up to the maximum time delay duration from step one.

3. Capture all the potential mid-flight state vectors that are predicted during each failure trajectory flyout, with a frequency of one hertz or better, typically at intervals shorter than the minimum time delay duration divided by ten. State vector data to be captured should include any data that is expected to be tested in a flight safety limit (e.g. position, velocity, acceleration, orientation, and angular velocity, as required by the selected flight abort rules).
4. If flight safety limits are based on instantaneous impact points (IIP), compute the IIP for all captured state vectors using an equivalent algorithm and parameters as will be used in the real-time mission to evaluate the flight abort rule. IIP prediction may be a Kepler propagation (although this is significantly different from the actual impact point), a vacuum propagator accounting for the J2 term of gravity, or with a three-degree-of-freedom (position but no orientation) simulation accounting for drag (either with constant ballistic coefficient or with a drag coefficient depending on speed). Importantly, the applicant should use the same methodology in planning as will be used by the real-time system to evaluate any flight abort rules based on IIP.

13.7.3 Determining Maximum Buffer.

The maximum buffer is for periods of flight when the hazard footprints from normal trajectories are not close to uncontrolled areas. When they are close to uncontrolled areas, a risk based approach should be used to identify good placement of flight safety limits, i.e. "contain if you can, otherwise use risk." Hazard footprints should be computed for sufficient failure trajectory state vectors to enable identification of the region that could lead to hazards reaching uncontrolled areas. The steps are:

1. Generate failure trajectories that deviate as rapidly as physically possible from the edges of the envelope of trajectories as described above. Adequate sampling should be used both in failure time and in the plane of the turn failure.
2. Identify the last state vector in each failure trajectory where the hazard footprint does not reach an uncontrolled area. Failure trajectories which would result in structural failure of the vehicle prior to the footprint reaching uncontrolled areas may be discarded.
3. This set of last state vectors should be used when developing a maximum buffer for flight safety limits.

13.8 **Defining the Quantitative Parameters of the Flight Safety Limits**.

The general process for determining quantitative parameters of flight safety limits is to identify an envelope in the appropriate projection/transformation of state vectors for each limit type (recall that one limit type is not generally sufficient to meet all of the flight abort objectives and constraints). This envelope, which should define a continuous line (e.g. defined by IIP), becomes a flight safety limit.

13.8.1 Four Types of Trajectory State Vectors.

There are four types of trajectory state vectors that result from paragraph 13.2, *Trajectory Envelope Evaluation* of this AC. (For this discussion, the "uncontrolled areas" also includes the near-shore gap discussed in paragraph 13.4 of this AC).

1. Within normal flight (as defined in § 401.7) which:
   a. Do not result in hazardous debris effects in uncontrolled areas with 97% confidence of containment ("Type 1a: normal/no risk").
   b. May result in hazards in uncontrolled areas ("Type 1b: normal/with risk").
2. Outside normal flight but inside the acceptable useful mission envelope which:
   a. Do not result in hazardous debris effects in uncontrolled areas ("Type 2a: useful/no risk") with 97% confidence of containment.
   b. May result in hazards in uncontrolled areas ("Type 2b: useful/with risk").

13.8.2 Three Sets of State Vectors.

There are (potentially) three sets of state vectors from paragraph 13.7 of this AC (Buffer Development).

- Set A: Within a short duration failure from the normal envelope, inside the minimum buffer, from paragraph 13.7 of this AC (but not also in set C).
- Set B: From extreme failures that lead to debris in uncontrolled areas from paragraph 13.8 of this AC (but not also in set C).
- Set C: That meet both conditions.

13.8.3 State Vectors Projected onto Planes.

An applicant should project or transform the state vectors in these datasets on to two-dimensional planes corresponding to the independent variable(s) and metrics of the flight safety limits identified in paragraph 13.5 of this AC. Examples of all of these are shown in the following figures for an sample mission from Wallops Flight Facility that flies over a portion of South America.

13.8.3.1 Figure 13-1 of this AC illustrates the trajectories for Types 1a and 1b, within the expected normal trajectory variation, i.e. due to guidance and performance uncertainty. The green points are from Type 1a: normal/no risk, for which the vehicle hazards do not affect an uncontrolled area, and the blue are for state vectors were the hazards do intersect uncontrolled areas (Type 1b: normal/with risk). These are shown projected in two ways; the left one is an altitude vs downrange distance plot, and the right one shows instantaneous impact points on a map. Both views could be used for defining abort limits. For this trajectory set, no hazardous debris impacts affect uncontrolled areas early in flight, but only during this segment of overflight of South America. This demonstrates where to locate the conditional limit. It should be near the latest green state vector that is the last one before the blue points adjusted for the abort system latency. For example, if the latest green state vector is for T+230 seconds and the latency is 2 seconds, the conditional limit would be placed at the state vector at T+228 seconds for this trajectory on this azimuth.

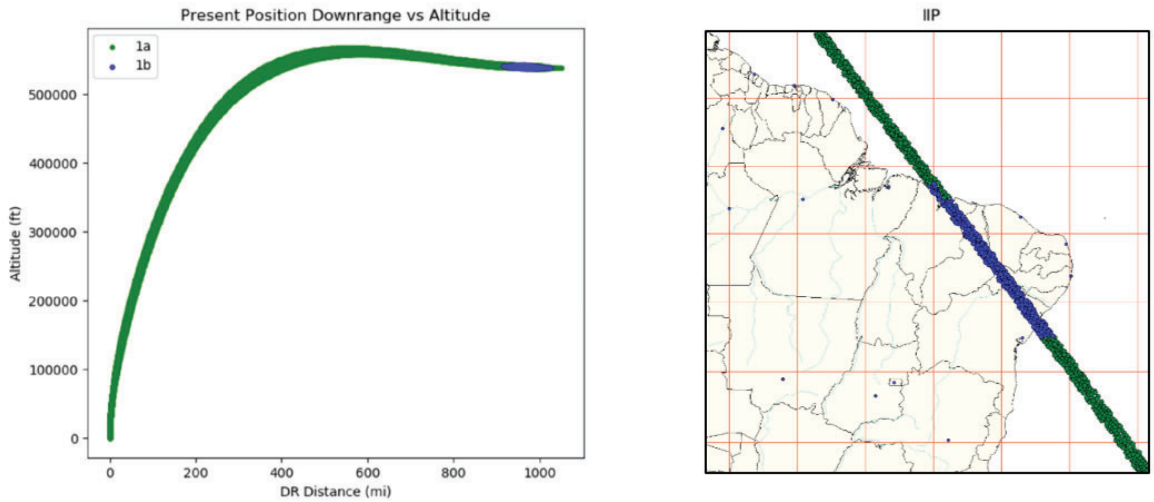


Figure 13-1: Projected points in the Normal Trajectory Range

13.8.3.2 The points from Type 2 are shown in Figure 13-2 of this AC and represent the range of useful missions. The mission spread is much wider, presuming that a later correction could allow the payload to reach the correct orbit or that a range of orbital inclinations would still result in a useful mission. An applicant would analyze these trajectories in accordance with paragraph 13.2 of this AC to determine that the collective risks for each one is acceptable. The orange points are those that do not have hazards impacting in uncontrolled areas (Type 2a: useful/no risk), whereas the red ones do (Type 2b: useful/with risk).

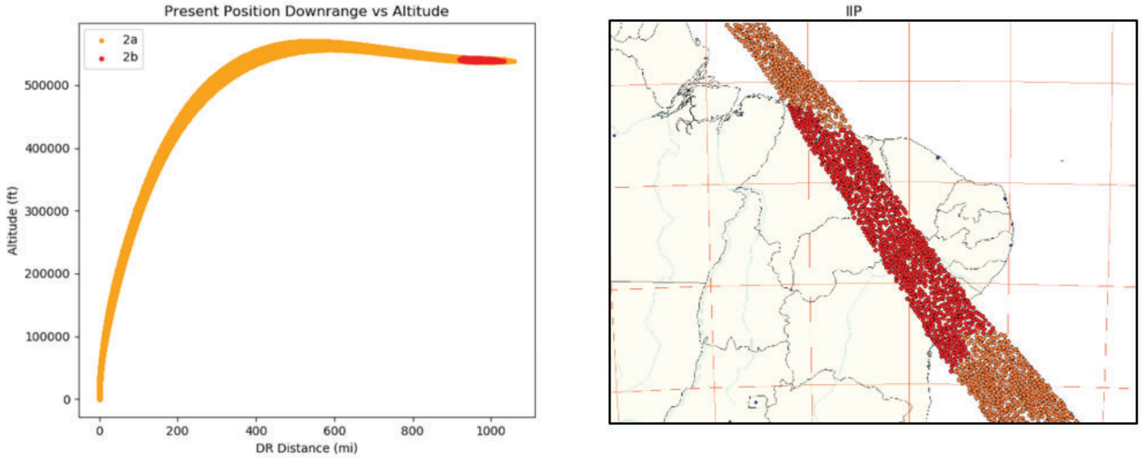


Figure 13-2: Projected points in the Range of Useful Missions

13.8.3.3 The sets that result from failure trajectories (sets A, B and C) are shown in Figure 13-3 and Figure 13-4. Figure 13-3 shows the launch area. In this example, the uncontrolled area includes a 10 mile offset from the coast, except there is a gap directly off the coast of the launch facility. There are many failures (purple dots, set B & C) that can reach uncontrolled areas. The IIP (right plot) shows that these are outside the short duration failures (yellow, set A), thus it is possible to use IIP limits that provide a sufficient buffer around useful missions while still protecting uncontrolled areas. This would not be possible using only altitude versus distance limits. This is illustrated by the yellow dots overlapping the purple dots. This of course occurs since failures that reach uncontrolled areas are primarily going crossrange, which this projection cannot depict. This is the reason that elevation limits are typically coupled with azimuth limits or with IIP-based limits. Altitude vs. distance limits can be developed to control failures in some directions, provided they do not abort trajectories within the normal envelope.

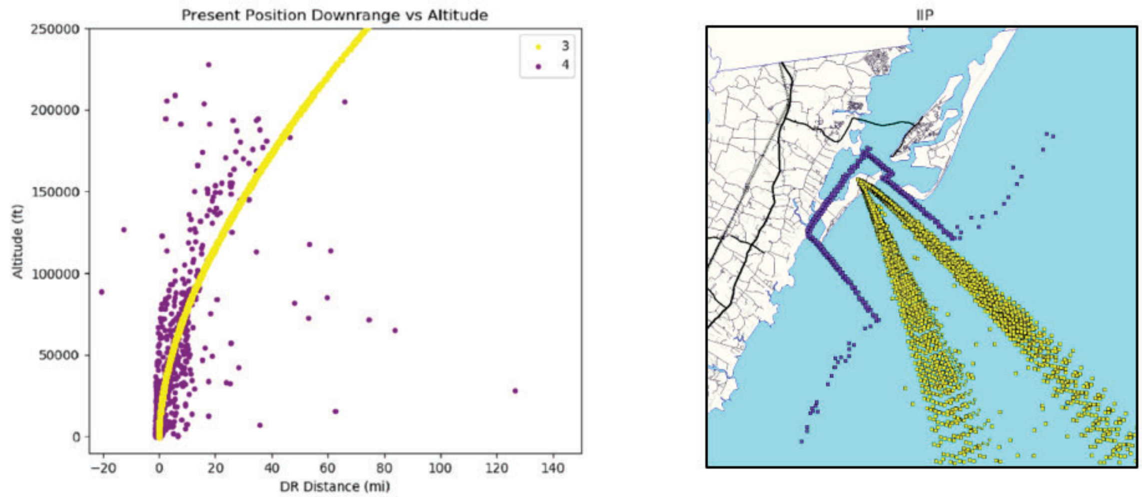


Figure 13-3: Projected points for Failure Trajectories, Launch Area

13.8.3.4 Figure 13-4 shows the same sets as the previous figure, but now for the downrange area. The uncontrolled region through which useful missions pass has been excluded. These figures would allow setting flights safety limits for both IIP and range versus altitude.

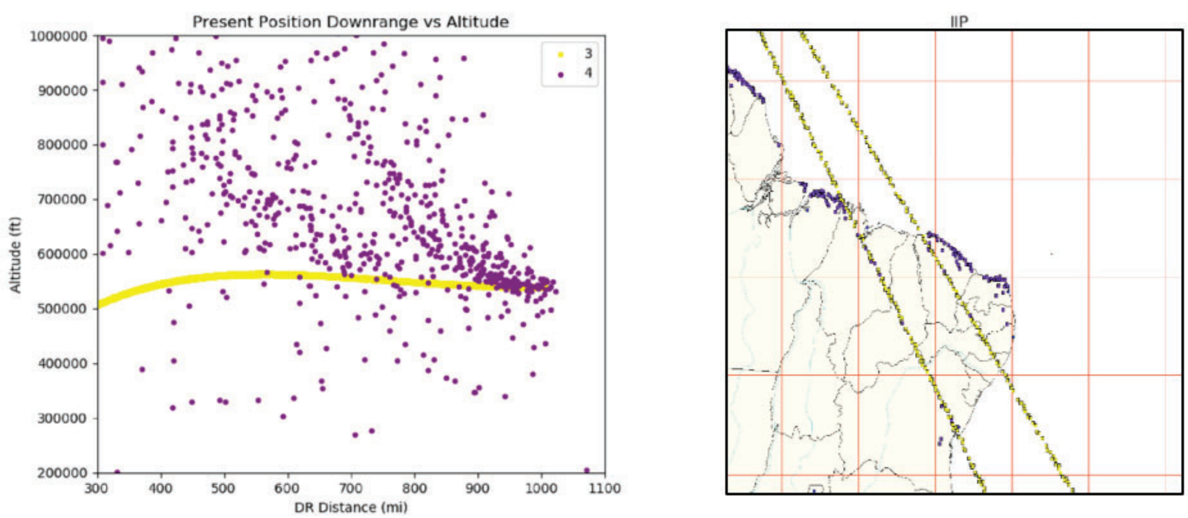


Figure 13-4: Projected points for Failure Trajectories, Downrange

13.8.4 Establishing Flight Safety Limits from State Vector Projections.

For all flight safety limits (FSLs) a piecewise continuous series of line segments should be created using the data shown in the plots above. For mission assurance purposes, the line segments would typically be outside the points for normal and useful trajectories (sets 1 and 2) and short duration failures (set A). The FSL line segments should also be inside the set of points for extreme failures (set B), but in some cases this is inconsistent with being outside the first group; in this case a combination of flight safety limits should be used in conjunction. This process prevents continued flight from increasing risk in uncontrolled areas if the vehicle is unable to achieve a useful mission, in accordance with § 450.108(c)(2). If there are points inside the normal or useful missions that impact uncontrolled areas with materially increased public exposure (sets 1b and 2b), a conditional limit must be established, in accordance with § 450.108(c)(3). Conditional Limits are discussed in paragraph 9.4 of this AC. The number of line segments may be limited by the system used to evaluate the rule (display or automated algorithm, where limits may be due to memory space, computation time, or complexity of display).

13.8.5 Maximum Altitude.

A maximum altitude limit is simply a limit where the vehicle's position must be below a line which is a function of downrange distance. The trajectory points described above are converted into the altitude vs. downrange coordinate system (as illustrated in the figures above). The definition of downrange should correspond to the algorithm that will be used to evaluate the rule in real-time; it may be either a tangent-plane downrange distance or a great circle arc-distance. The envelope is the line drawn above the normal trajectory points, subject to the rules in the conditions above.

13.8.6 Minimum Altitude.

The minimum altitude limit is analogous to the maximum altitude limit, and a similar process is used to create it, but with a few additional considerations. There are competing objectives on how low of an altitude to set the flight safety limit. For a termination that results in an explosive destruct, which leads to significant imparted velocities, activation in the upper atmosphere or above can cause a large spread of debris, thus subjecting a larger area to hazardous debris impacts, contrary to safety goals. However, allowing a wayward, but controlled, vehicle (such as due to a guidance programming error) to descend leads to inability to predict the location for a very hazardous object in time to warn aircraft. In this situation, it is likely better to terminate flight, so that the hazarded region can be better predicted, in order that aircraft can be moved. The minimum altitude rule can be effective at mitigating the hazards from an intact impact with significant remaining propellant, including near-field and far-field blast overpressure.

13.8.6.1 If a vehicle is falling and no longer thrusting and without significant lift capability, and the abort is destructive, then it is usually better to let it continue to fall and terminate at a low altitude. Thus, in these situations an operator should have separate rules for vehicles that have lost thrust than those that are thrusting. For non-destructive abort (e.g. fuel venting), there is no need to wait to terminate flight, because the resulting debris will not significantly spread, and therefore abort should occur as soon as a violation occurs.

13.8.6.2 The minimum altitude rule can be effective at mitigating the hazards from an intact impact with significant remaining propellant, including near-field and far-field blast overpressure.

13.8.7 Fixed IIP Limit.

A fixed IIP limit is a geographic boundary where the vehicle's instantaneous impact point (vacuum or accounting for drag) must remain inside. To create fixed IIP-based limits, the process is similar to the altitude limits, except now a closed "hull" is created. The collection of IIPs associated with the appropriate sets of state vectors is used. The IIPs should be transformed to an azimuthal equidistant projection, with the origin at some point along the nominal trajectory (normally the launch point), in order to adequately account for the curvature of the Earth's surface. A polygon containing all the IIPs defines the hull. A limited number of vertices are used, in order to not cause problems for computation time or displays. Usually the created hull is convex but this is not required. The vertices are translated to geodetic coordinates and the flight safety limits are great circles that connect these coordinates.

13.8.8 Moving IIP Limit.

A moving IIP limit is an extension of the fixed IIP limit concept. Moving IIP limits are simply a set of fixed IIP limits that are each active for a specific time period (or other independent variable). Chevron lines, as have been used at the Eastern Range for many years, are an example of moving IIP limits. Moving IIP limits have the advantage that they can meet nearly all the guidelines described above and could in some situations be sufficient to meet § 450.108(c)(1), (c)(2), (c)(3), (c)(4) and (c)(6) without any other flight safety limits. They contain the IIP at a specific location as a function of time, vehicle speed, or other variable. Thus, an uprange deviation, a downward (or slow) vehicle, and cross-range deviations all may violate the limit, depending on how the moving IIP limits are designed. To develop moving IIP limits, a similar process may be used as for fixed IIP limits except that time filtering is now performed (reference paragraph 13.8 of this AC). Therefore, the analyst should first define the time interval between moving IIP limits. This is normally the same as the time delay duration identified in paragraph 13.7 of this AC. For each time interval, all the points which have a flight time in the interval are used, then a hull surrounding the points is created (usually in an equidistant azimuthal projection). The moving IIP limits then are activated by the real-time system during the relevant interval.

13.8.9 Azimuth Limit.

An azimuth limit constrains the azimuth (angle in the horizontal plane) of the vehicle's velocity vector to be within predefined limits during a specified duration of flight. The limits are given as "left" and "right" azimuths and are calculated in an equidistant azimuthal coordinate system with the origin at the launch point. Usually the limits are given relative to the nominal trajectory azimuth but may be given as azimuth from north. The azimuth limit is usually constant, starting from vehicle tip-over and extending until the vehicle has reached a certain downrange distance or a certain time of flight, usually just in the launch area. The same process as is used for other limits can also be used, where the limit azimuths are found by plotting the vehicle azimuth as a function of flight time or downrange distance.

13.8.10 Flight Path Angle Limit.

A flight path angle limit references the angle of the vehicle's velocity vector relative to the local horizontal and is usually defined as a function of flight time or downrange distance. There may be both minimum and maximum flight path angle limits. This limit type is very helpful after a vehicle has pitched over to quickly identify a malfunction that causes the vehicle to accelerate downward, which is useful for protecting aircraft. This limit type may be more effective than a minimum altitude limit for early flight loss-of-thrust events. A flight path angle limit is created in the same method as above on a two-dimensional surface where flight path angle is a piecewise continuous function of either time or downrange distance below (and/or above) the nominal flight path.

13.8.11 Skyscreen.

A skyscreen is a human visual observation facility that is arranged to constrain the vehicle's azimuth and elevation as viewed from a particular location(s). A skyscreen is also referred to as "the wire." The observer's viewpoint is aligned through a physical guide, toward the expected flight field, with the bounds of an acceptable flight demarcated across this field of view (by using wires or ropes strung across a truss structure, ink lines drawn on a transparent plate, or similar physical cues for the flight envelope). Usually a back azimuth observer is used, viewing along the vehicle launch azimuth, while a cross-range observer verifies that the vehicle has initiated the pitch program properly, is moving downrange, and is flying between its upper and lower altitude bounds.

13.8.11.1 The skyscreen method is usually a backup or supplement to more technological systems, as it only works when weather, distance, and vehicle acceleration are compatible with the human eye's ability to track the vehicle. The abort instruction is usually communicated to the safety officer with a handheld radio, so this method may also have a slower response than some flight safety systems (such as AFSS), while potentially having a faster response than other flight safety systems (such as when multiple tracking screens and multiple telemetry sources should be double-checked, before abort).

13.8.11.2 To develop the limit, for each observer location the azimuth and elevation angles for the state vector sets are computed. Then a set of connected line segments, one to the left and one to the right (which transition to above and below for a cross-range observer) of the points is identified. These bounds are represented on the observer's physical view field, allowing visual identification of a flight, which is violating this envelope.

13.9 **Conditional Limits**.

There are three purposes of conditional limits: 1) to avoid aborting a vehicle in a region of elevated public risk, 2) to prevent a vehicle that cannot achieve a useful mission from hazarding uncontrolled areas, when the option exists to abort the vehicle before such a hazard is possible, and 3) to avoid discontinuation of flight abort capability prematurely during the flight of an malfunctioning vehicle. A conditional limit is a flight safety limit for which abort occurs only if the vehicle is not performing within expected parameters and should be used to comply with § 450.108(c)(3) and (e). If 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, then flight abort is initiated. Conditional limit replaces the term "gate," which does not have a consensus definition.

13.9.1 Placement of Conditional Limits.

In accordance with § 450.108(c)(3), conditional limits should be placed prior to a period of materially increased public exposure, as discussed in paragraph 9.4 of this AC. The trajectories used to compute the CE_C and collective risk should be selected to pass directly over the region of exposure but treated as though they were the planned trajectory, consistent with the technique described in paragraph 13.2 of this AC. A minimum requirement of § 450.108(c)(3) is that the vehicle must be able to achieve a useful mission where risk is acceptable after passing through the limit (see paragraph 13.2 of this AC).

13.9.1.1 When a conditional limit is used, the conditional limit segment should be located so that all acceptable useful mission trajectories pass through the conditional limit prior to the period of materially increased public exposure or achieving orbit. Similarly, in accordance with § 450.108(d)(7) all unacceptable useful mission trajectories must reach a flight safety limit prior to the period of materially increased public exposure if the period of exposure would cause the entire trajectory to exceed the risk limits in § 450.101(a)(1) or (b)(1). This may result in some trajectories in a fan of useful mission trajectories reaching a conditional limit while others reach hard flight safety limits that are contiguous with the conditional limits. An operator may choose to abort some vehicles outside of the normal mission envelope but within the limits of a useful mission if a conservative approach is preferred when approaching a period of materially increased public exposure, even if the trajectory does not require abort in accordance with § 450.108(d)(7). In accordance with § 450.108(d)(6), such aborts, like all aborts, must not increase collective risk to the public in uncontrolled areas compared to continued flight. Paragraph 13.7 of this AC discusses how to identify the range of state vectors within the trajectory envelope, which can hazard uncontrolled areas. A conditional limit should be located in advance of these state vectors for each trajectory in accordance with § 450.108(c)(3).

13.9.1.2 For an orbital launch, the conditional limit to determine the ability of a vehicle to reach a minimum safe orbit should be placed as late as possible but may be influenced by factors such as the imminent loss of flight abort control; the narrow range during which to evaluate the flight against the criteria used to judge performance; the presence of a period of materially increased public exposure just prior to orbital insertion, etc.

13.9.2 Extents of Conditional Limits.

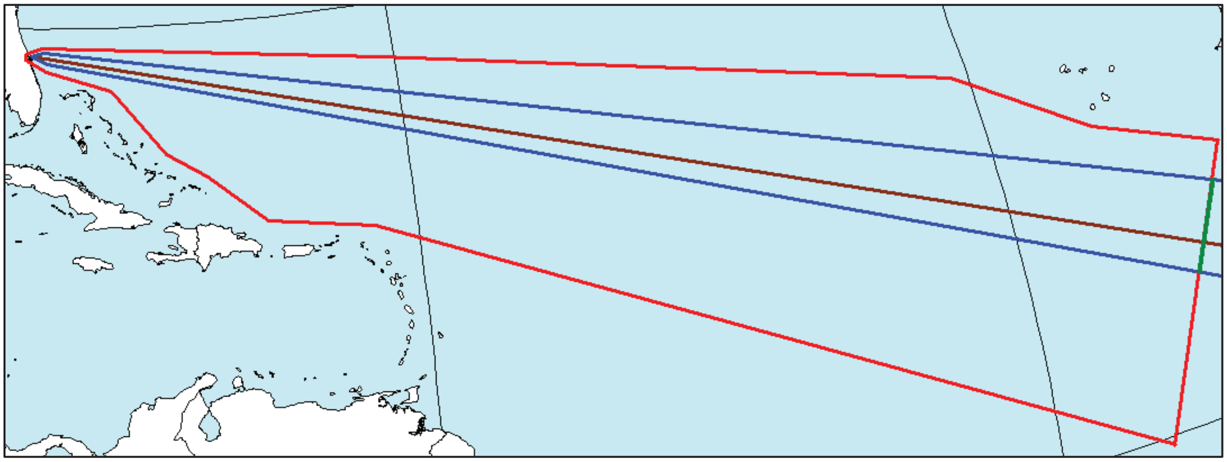
Conditional limits should be no wider than the extent of the acceptable useful mission trajectories plus the uncertainty in tracking (which is typically very small), and not include any buffer from paragraph 13.7 of this AC. This is consistent with § 450.108(c)(2) which requires flight abort in order to prevent continued flight from increasing risk in uncontrolled areas if the vehicle is unable to achieve a useful mission. For some unique mission profiles, it may be possible for vehicles outside the limits of a useful mission (for example, outside of the useful azimuth range) to pose a smaller risk through continued flight than through flight abort when approaching a period of materially increased public exposure. Such trajectories would have to have some exposure to the public at the location of the conditional limit, otherwise abort would reduce the risk prior to the period of increased exposure. An operator should search for better locations to place the conditional limit, before deciding that continued flight presents the lowest risk for a trajectory that can no longer achieve an objective.

13.9.3 Fundamental Geometries of Conditional Limits.

A conditional limit can occur in four fundamental geometries.

13.9.3.1 **No Flight Safety Limits Subsequent to Conditional Limit**.

A first geometry is when there are no flight safety limits subsequent to the conditional limit, which is the typical case when ending flight abort in accordance with § 450.108(e). This is a typical "head-on gate" or "orbital gate", such as those used for flights from the Eastern Range that overfly Europe or Africa. The flight safety limits typically have a significant buffer around normal flight while over broad ocean areas, but then come together where there is a narrow conditional limit, as shown in Figure 13-5. This conditional limit should be placed prior to any of the state vectors that can lead to hazardous debris effects in uncontrolled areas. When a conditional limit of this type is reached, the flight safety system is usually safed. The point in the trajectory where the vehicle performance and health are assessed may be prior to the conditional limit, or the conditional limit may be moved uprange, if the ability of a vehicle to reach orbit is best measured at a location other than at a flight safety limit placed to contain debris. In this case, the location where the parameters used as metrics for the ability to reach orbit are measured may be followed by flight safety limits that provide debris containment up until a period of overflight, when the flight safety limits would cease and no abort would occur. The significant buffer around normal flight is acceptable over the broad ocean areas because continued flight does not increase risk to uncontrolled areas in this case, and because the vehicle could potentially recover from a perturbation and resume flight within the limits of a useful mission.



Note: *All lines are in impact point space. Brown is nominal, blue is envelope of useful missions, red are fixed IIP limits, and green is the conditional limit.*

Figure 13-5: Example of head-on Conditional Limit

13.9.3.2 **Conditional Limits for Uncontrolled Areas Encompassed by Limits of a Useful Mission**.

A second geometry is when the uncontrolled area is completely encompassed by the envelope of useful missions, such as an island. This is typically used by the Eastern Range around Bermuda. In this case, the entire island is surrounded by a conditional limit where abort occurs when entering the region if the vehicle is not within expected parameters. Inside this region is a region where no abort should occur because continued flight is likely to reduce risk as compared to aborting near Bermuda. Normal flight safety limits still exist further to the left and right of the region. This is illustrated in Figure 13-6 of this AC.

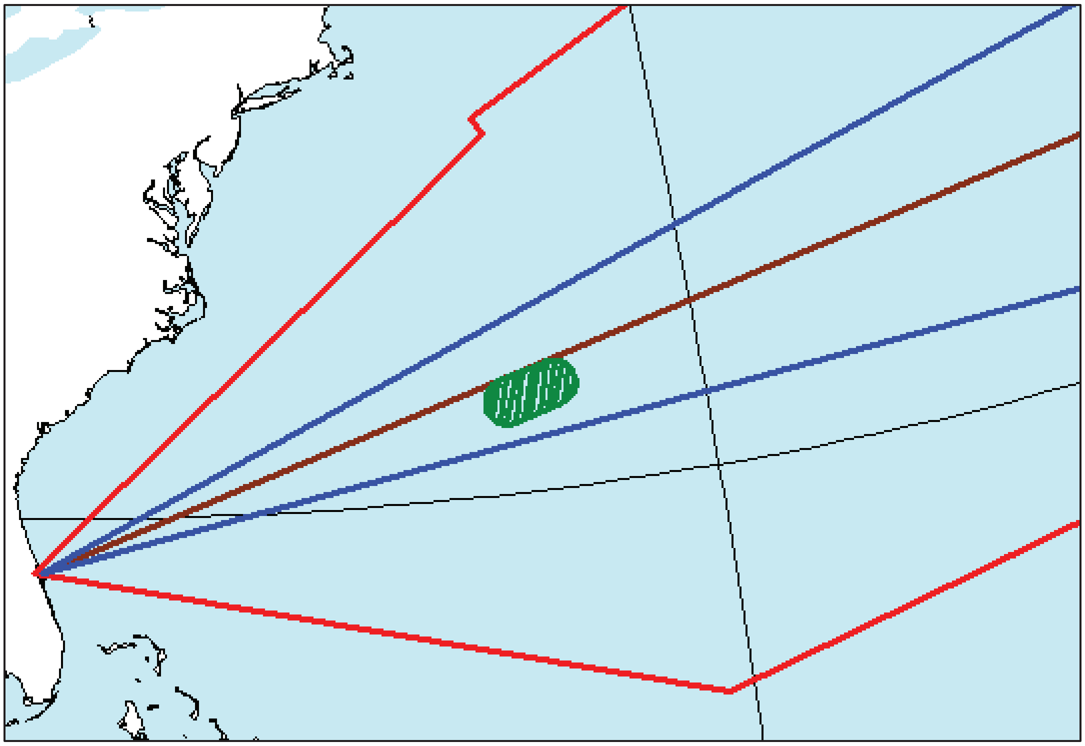


Figure 13-6: Example of Conditional Limit Around an Island

13.9.3.3 **Conditional Limits for Limits of a Useful Mission Encompassed By Uncontrolled Areas**.

A third geometry is when the uncontrolled area has greater lateral extent than the range of useful missions, but the vehicle will traverse the uncontrolled area before reaching orbit or ground impact as illustrated in Figure 13-7 of this AC. In this case, there should be a conditional limit prior to the uncontrolled area crossing, a region where limits are carefully examined to ensure abort reduces risk over continued flight, and then return to a typical abort region after the uncontrolled area crossing is complete. The exact location of flight safety limits in this example should be established in such a way as to minimize the possibility of an abort increasing risk over allowing continued flight, in order to meet§ 450.108(d)(6). This may require additional analysis, and the best approach may be to allow the flight to continue if it exits the limits of a useful mission after it passes the conditional limit. The best approach may vary depending on the direction that the vehicle deviates.

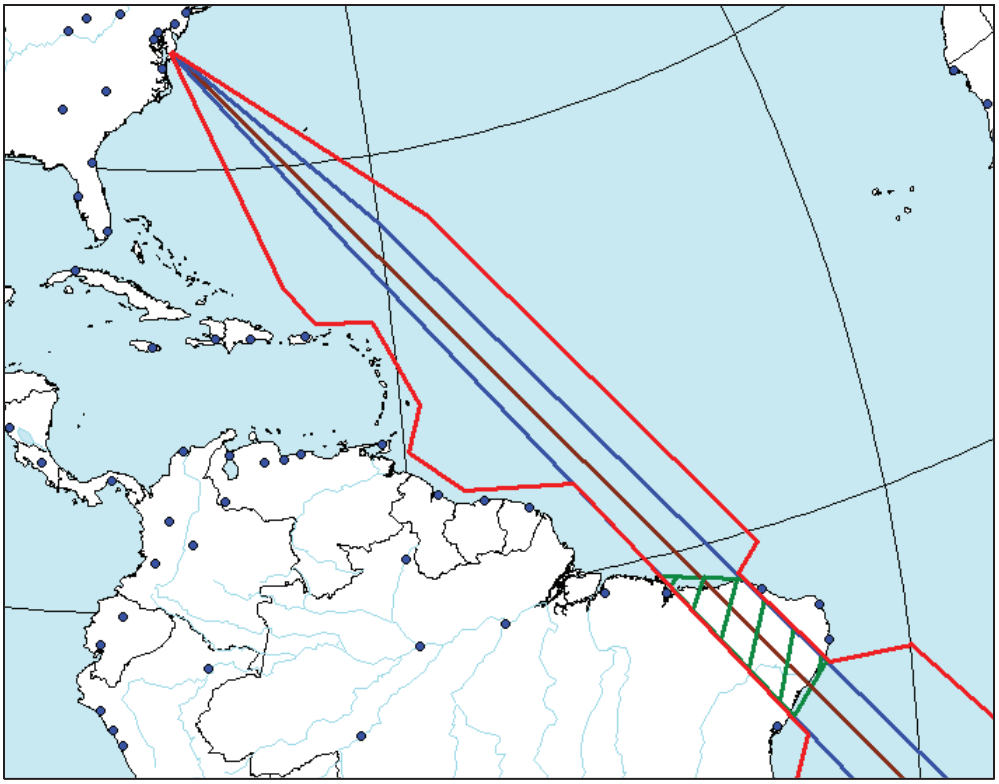


Figure 13-7: Conditional Limit Region around Uncontrolled Area

13.9.3.4 **Mixed Conditional Limits**.

The fourth geometry is a combination of geometries two and three. One way this occurs is when an uncontrolled area extends only to one side of the envelope. This has been used by the Eastern Range for northerly azimuth flights that fly along the coast of North America and is commonly called a "lateral gate." This is illustrated in Figure 13-8 of this AC, where the hashed box shows an area where flight safety limits should be carefully evaluated to ensure abort reduces risk.

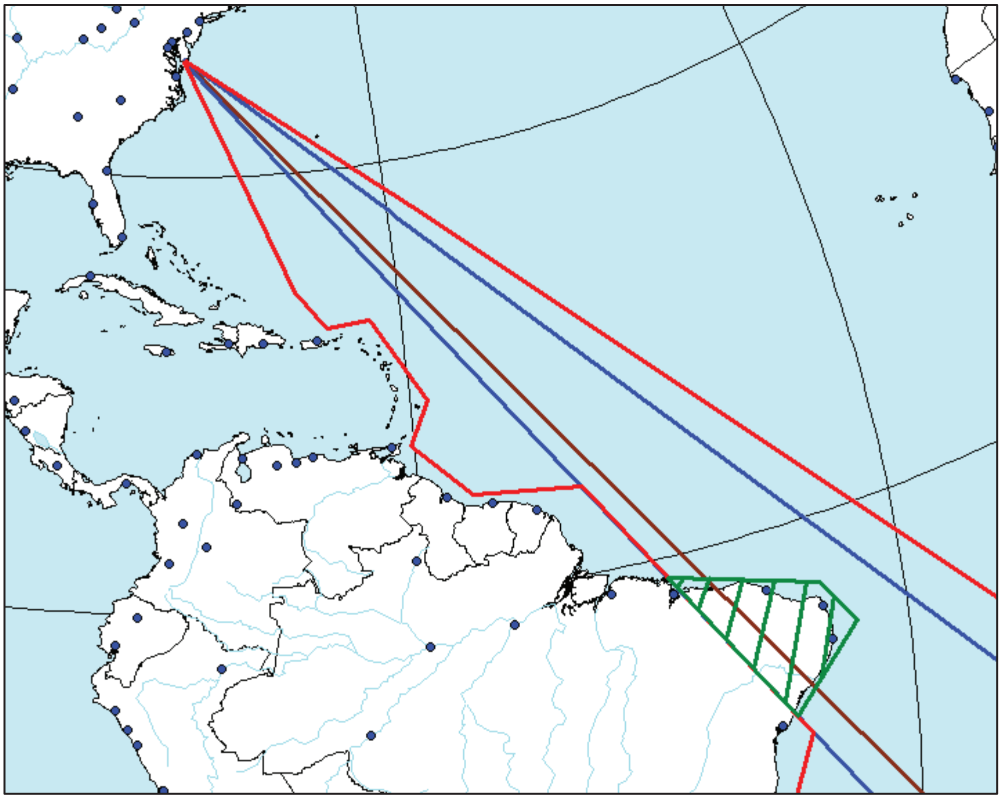


Figure 13-8: Mixed Conditional Limits

13.9.3.5 **Mixed Conditional Limits where Flight Safety Limits Should be Expanded.**

A similar situation occurs when an island is near the edge of the range of useful mission trajectories. Effectively this results in the same geometry results. However, in this case the flight safety limit should typically be expanded (unless it is protecting other uncontrolled areas) to avoid debris impacting on the island from an abort, in accordance with § 450.108(d)(6).

13.9.4 Multiple Conditional Limits.

A mission may have more than one period of overflight over an uncontrolled area, and in these cases, conditional limits may need to be drawn at the start of each uncontrolled area crossing to meet § 450.108(c)(3). Periods of materially increased public exposure should be separated depending on whether it is possible to initiate flight abort between them while not increasing risk to uncontrolled areas through abort. For example, a series of islands may be too closely spaced to implement abort as the hazard footprint moves from island to island, until the hazard moves away from the last island. These islands should be assessed collectively when deciding if they represent a period of materially increased public exposure. If there is an opportunity to initiate abort between periods of materially increased public exposure without increasing risk to uncontrolled areas, the regions of exposure should be assessed separately when deciding whether to protect them with conditional limits. While the above examples have all been represented geographically, conditional limits may be developed for other types of flight safety limits using the same approach.

13.9.5 Parameters Used for Flight Abort Decision.

In accordance with § 450.108(c)(3), abort action is taken at a conditional limit to prevent the vehicle from entering a period of materially increased public exposure in uncontrolled areas, including before orbital insertion, if 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. Likewise, § 450.108(e) requires the equivalent verification of critical parameters prior to ending abort. Paragraph 9.4 of this AC discusses an acceptable means for selecting critical parameters and their associated values.

13.10 **Validating Rules**.

It is critical to validate the rules to satisfy § 450.108(f)(1) and (d)(6). There are two important validations.

- First, the rules must be able to be implemented by the system used to obtain the input data and effect the abort in accordance with § 450.108(f)(1). To verify that the system can support the rules, if the abort decision is not on the vehicle, then the communication of an abort signal to the vehicle must be ensured. For telemetry data, the ability of the ground station to receive the data, including geometry considerations and atmospheric and plume attenuation effects should be accounted for.
- Second, although it is rarely an issue with modern measurement systems, it should be ensured that the uncertainty in the measurements does not pose an unacceptable possibility of rule violation for an acceptable useful mission. An unnecessary abort caused by measurement error would potentially violate § 450.108(d)(6).
- Each rule should be validated following a testing plan to ensure that their implementation within software or incorporation with hardware systems is functional. This testing should be repeated at various stages of development and

implementation to ensure that they remain functional as operations commence. Testing of software should be performed in accordance with AC 450.141-1.

13.11 **Verifying Risk Reduction**.

This paragraph and its subparagraphs discuss two approaches to verifying that limits are not increasing risk, to meet § 450.108(d)(6): by inspection (i.e. when hazardous debris from abort at flight safety limits is contained with at least 97% confidence with respect to uncontrolled areas) and by numerical analysis (compare CE_C of each failure trajectory with and without abort).

13.11.1 Verification by Inspection.

In many cases, it can be easily shown that flight safety limits do not increase risk, and in fact reduce risk. For most missions, most of the hazards from abort are contained to broad ocean or controlled areas. Except in the launch and landing area, this can be demonstrated by examination of the debris ellipses resulting from abort scenarios. If they are clearly separated from uncontrolled areas, then the risk is de minimis, and then risk has clearly not been increased. In some situations, a similar approach can be used, even if the debris ellipses slightly impinge on uncontrolled areas, when it is clear that risks would be increased (or at least cannot be reduced) if the safety limits were moved. An example of this is near overflight of Bermuda from the Eastern Range. If the limit of a useful mission pass over the island, flight abort would increase risk if action were taken as soon as the vehicle departed from the limits of a useful mission. In this case, flight safety limits could be moved further away from the normal flight envelope without exposing additional uncontrolled areas. The figure below illustrates how the debris footprints can be confirmed to not touch the island after flight is aborted using flight safety limits that are designed to avoid abort over Bermuda. In this example, the margin between the island and the footprint is minimal, and could be improved with further edits to the flight safety limits.

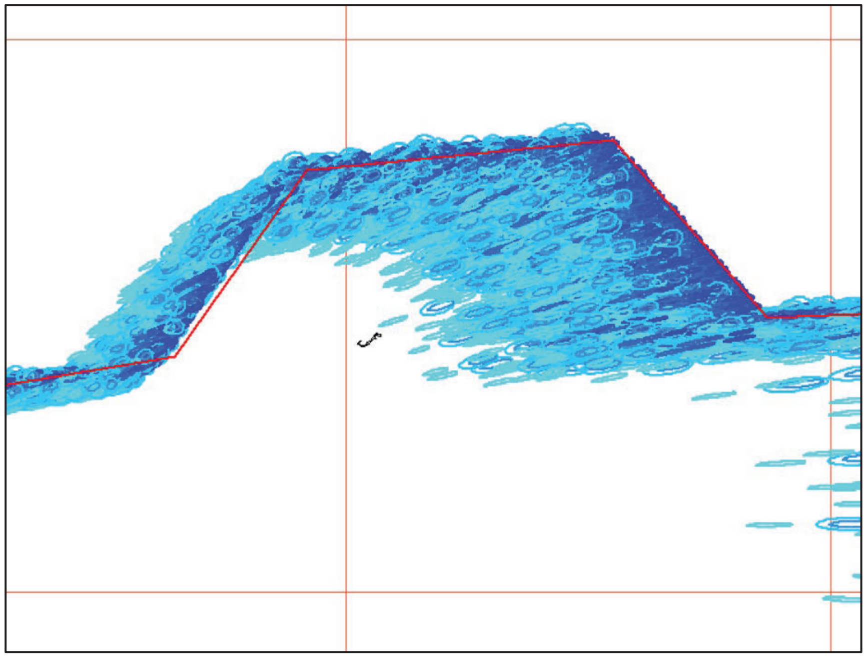


Figure 13-9: Risk Reduction by Inspection

13.11.2 Verification by Numerical Analysis.

For other situations, a numerical analysis should be used to meet § 450.108(d)(6) because inspection is not conclusive. In this case, for each simulated failure trajectory used in the risk analysis, the risk with the abort system activating and with it failing should be compared. The conditional risk for each trajectory should be equal to or less than allowing flight to continue. If the abort has higher risk than continued flight, then the flight safety limits should be adjusted. If these cases are found, the process should return to at least paragraph 13.8, or if there is no solution with the flight abort rule set chosen, paragraph 13.5 of this AC.

13.12 **Assessing Residual Risk**.

The rules then should be incorporated into the flight safety analysis, where the limits are applied to all trajectories, and the residual risk computed. Residual risk is the risk that remains after all hazard controls have been accounted for in the flight safety analysis. Accounting for flight abort includes accounting for the flight safety limits (paragraphs 13.8 and 13.10 of this AC), the reliability of the flight safety system (paragraph 10.5), and the outcome of the abort action (paragraph 10.2).

13.12.1 Compliance with Flight Safety Criteria.

There are several risk metrics that must be verified in accordance with § 450.115(a), using the flight safety analysis method appropriate to the determined level of fidelity:

- That the collective casualty expectation in § 450.101(a)(1) or (b)(1) is not exceeded, including people in both controlled and uncontrolled areas, and both the general public and neighboring operations personnel,
- That the individual risk criteria in § 450.101(a)(2) or (b)(2) can be met through acceptable mitigations (such as keep-out areas), including people in both controlled and uncontrolled areas, and both the general public and neighboring operations personnel, and
- That critical assets are adequately protected, in accordance with § 450.101(a)(4) or (b)(4).

13.12.1.1 These are accomplished by performing a flight safety analysis for the mission, including debris (§ 450.135), far-field blast overpressure (§ 450.137), and toxic (§ 450.139) risk analyses. These analyses aggregate results from all phases of flight. If the risk criteria are not satisfied, the limits of a useful mission and/or flight safety limits may be modified, and the flight safety limits analysis described in this paragraph should then be performed again.

13.12.1.2 To ensure compliance with individual risk and aircraft risk requirements (§ 450.101(a)(2) and (3) or § 450.101(b)(2) and (3)), the development of flight hazard areas must also account for flight abort for each phase of flight where it is used in accordance with § 450.133(a)(2). If practical flight hazard areas cannot be developed such that these safety criteria are met, the limits of a useful mission and/or flight safety limits may be modified, and the flight safety limits analysis described in this paragraph should then be performed again.

13.12.2 High Consequence Event Protection.

In addition, for each phase of flight, the residual risk analysis must either demonstrate containment with a highly-reliable FSS in accordance with § 450.108(c)(6) or be in compliance with high consequence event protection requirements in accordance with § 450.108(c)(4), as discussed in paragraph 9.5 of this AC.

13.12.2.1 **Containment**.

To demonstrate containment for a phase of flight, the analysis must demonstrate that no flight abort or other event results in hazardous effects in uncontrolled areas, per § 450.108(c)(6). For phases including overflight of uncontrolled areas, this option cannot be used, as hazards cannot be contained. It may also be impossible in launch or landing areas, as containment may not be achieved. To demonstrate compliance with this approach, an analysis should compute hazard footprints for the worst-case breakup scenario. The hazard footprints should be computed for failure trajectories that initiate at a maximum of one second intervals and approach flight safety limits at the most rapid pace (i.e. random attitude trajectories where the IIP trace is most perpendicular to an IIP-based flight safety limit). The state vector for the abort along each failure trajectory should be determined by considering the time the limit is violated plus the time delay of the FSS with a three-sigma uncertainty. If none of the polygons overlap uncontrolled areas, then the hazards are contained. If they do overlap, then the more sophisticated analysis in the following paragraph should be used.

13.12.2.2 **Analysis**.

If hazardous effects cannot be demonstrated to be contained, then prevention of high consequence events must be demonstrated through a conditional expected casualty analysis, in accordance with § 450.108(c)(4). For this, the first step is to compute the CE_C in each significant period of flight where flight abort or flight outside the limits of a useful mission may be an outcome for each reasonably foreseeable off-trajectory failure mode. The CE_C results from various end states, such as break-up due to aerodynamic loads or FSS activation, from flight abort and flight outside the limits of a useful mission should be averaged together to compute the mean CE_C for each significant period of flight. In part 450, CE_C only considers population in uncontrolled areas. The risks associated with a failure of the abort system (accounting for its failure probability) must be accounted for in the CE_C analysis in accordance with § 450.108(d)(5). If the maximum CE_C developed through this method is not greater than 1×10^{-2}, then high consequence event protection is demonstrated. If this analysis does not demonstrate compliance with high consequence event protection, the limits of a useful mission and/or flight safety limits may be modified, and the flight safety limits analysis should then be updated accordingly.

13.13 **Determining Durations of Acceptable Data Loss**.

To determine the duration of acceptable data loss, the principles described in paragraph 10.3 of this AC need to be applied to the particular operation. This discussion first will apply to the situation where the flight abort decision system can identify whether the vehicle was within the normal envelope, on an unintended trajectory, or outside the limits of the useful mission. This is the preferred situation, as it leads to more informed decisions and provides more margin. Paragraph 13.14 of this AC discusses development of data loss flight times when the decision system does not know this information (e.g. some current autonomous systems). While a real-time footprint could also be used, that is outside the scope of this AC.

13.13.1 Outside the Limits of a Useful Mission.

The first rule regarding data loss is simple: if the vehicle is outside the limits of a useful mission (see AC 450.119-1) when data loss occurs, flight should be terminated, unless the hazard footprint of the vehicle is over a populated area.

13.13.2 Baseline Data Loss Durations.

The baseline situation is for vehicles that are within the normal trajectory envelope and the hazard footprint does not intersect an uncontrolled populated area. To compute durations of acceptable data loss, the same malfunction trajectories are generated as for the buffer analysis in paragraph 13.7 of this AC, where failure trajectories initiate from sample states within the normal trajectory envelope. Each trajectory is evaluated for when it either intersects a flight safety limit, leaves the limits of a useful mission (hereinafter called "boundary"), or has a hazard footprint intersecting a populated uncontrolled area. The applicant may choose which of these types of boundaries to use.

13.13.2.1 **Trajectory Evaluation**.

The trajectories are analyzed to determine when structural limits would be exceeded and when a boundary is reached. All trajectories where a structural limit is reached first are discarded. For each trajectory where this does not occur, the duration from the failure initiation to the time the flight safety limit is reached is calculated (as illustrated in Figure 13-10). The trajectories are then grouped by time of failure (or another suitable independent parameter, such as down range distance at failure). For each group, the minimum duration is then the maximum allowable duration of data loss. Usually, the durations are simplified, both using constant values for intervals of failure initiation time (not linear interpolation) and truncating to whole seconds.

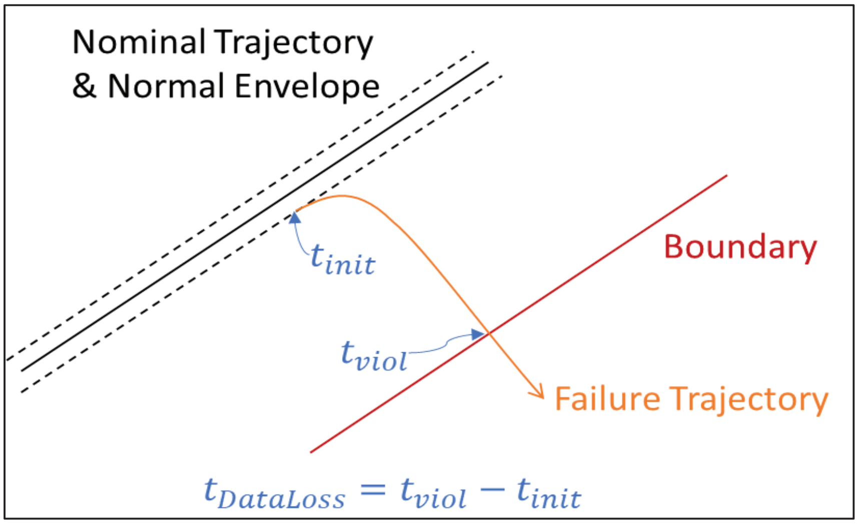


Figure 13-10: Data Loss Calculation for Normal Envelope

13.13.2.2 **Cannot Reach Terminate Lines**.

If the vehicle is approaching a conditional limit and there are no flight safety limits after the conditional limit, data loss flight abort limits should not be used once the vehicle reaches a point where the time to the conditional limit is less than the time required to reach a flight safety limit.

13.13.2.3 **Comparison to Expected Data Loss**.

These data loss durations should be compared to the anticipated data loss scenarios while a flight is otherwise normal. An example of this situation is reacquisition of GPS signal, but other demonstrated data loss scenarios could also apply. Since it is higher risk to abort flight than allow normal flight to continue, abort should not occur unless there is reasonable likelihood that a failure has occurred. Thus, evidence of expected data loss should be examined, and the abort duration should be no less than the 99% confidence of the duration for which data should have been restored. If the duration is not within this limit, then the approach to developing data loss durations could be refined, the flight safety limits adjusted, and/or the mission adjusted.

13.13.3 Durations during Overflight of Populated Areas.

If the planned mission features overflight of populated uncontrolled areas, and subsequently exits this situation where abort is still used as hazard mitigation, there are additional considerations. This is because the consequence of aborting a vehicle that has not failed, except for data loss, to uncontrolled areas is higher than allowing continued flight. Abort is still usually an appropriate safety mitigation however, if the vehicle has deviated from normal flight and propellant has not been dispersed. The determination of how long to allow a vehicle to continue to fly in this situation is then based on when a vehicle was expected to complete the overflight. If it has not completed overflight within the time that was within the range of a useful mission, then the vehicle can be presumed to have failed during this time. Since the vehicle's position may have significant uncertainty, it is not known whether continued flight will reduce risk relative to flight abort in a given situation. However, when abort reduces consequences (e.g. casualty area), as it normally does, the average risk of all data loss scenarios is reduced by taking abort action.

Note: In order to determine the acceptable duration of data loss, if the overflight resulted in materially increased exposure, an operator should use the conditional limit regions developed per paragraph 13.9 of this AC. In this case, the duration of acceptable data loss while a vehicle is inside a conditional limit region should be equal to the maximum expected time of exiting the region minus the current flight time, plus a few seconds of buffer, unless this is shorter than the values determined in the paragraphs below. If the overflight of uncontrolled populated areas does not materially increase exposure, then regions equivalent to the conditional limit regions should be determined in order to determine the duration of acceptable data loss.

13.13.4 Durations When Data Loss Occurs on Unintended Trajectory.

When data is lost after a vehicle has departed the normal envelope but remains within the limits of a useful mission, the analysis should take into account that the vehicle could now reach flight safety limits more quickly than if it were within the nominal envelope. An applicant should choose to use either a simple approach or to perform an analysis to determine data loss times as a function of location. The simple approach is to set the data loss duration to be the duration over which signal reacquisition is expected take place if it is lost (normally one second or less). The more complex approach expands on the baseline method described above. In this case, regions are defined at progressively further distances from the normal trajectory envelope, out to the boundary. Each failure trajectory is then analyzed for when it exits each region, as illustrated in Figure 13-11. For each region, the trajectories are then grouped by the time they exit the region. For each group, the minimum duration is the maximum allowable duration of data loss for that region for that time interval. In the region closest to the boundary, the duration is the signal reacquisition time.

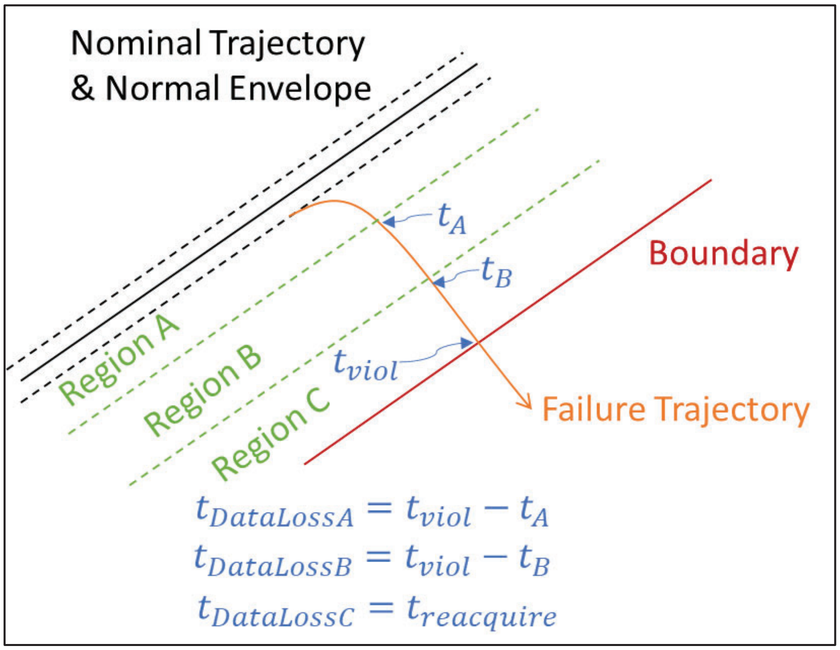


Figure 13-11: Data Loss Calculation for Unintended Flight Regions

13.13.5 Durations When Envelopes Are Not Known

For systems that do not have the capability to determine if the vehicle is within the normal envelope or the limits of a useful mission when data is lost, additional consideration is needed. In this case, the locations of the flight safety limits and populated areas are important. Because the vehicle could be anywhere inside the flight safety limits when data is lost, the duration of allowed data limits should be the minimum time from the vehicle could travel from a limit to populated area, as illustrated in Figure 13-12. In order to obtain reasonable data loss durations, the flight safety limits may need to be adjusted to provide more standoff from populated areas.

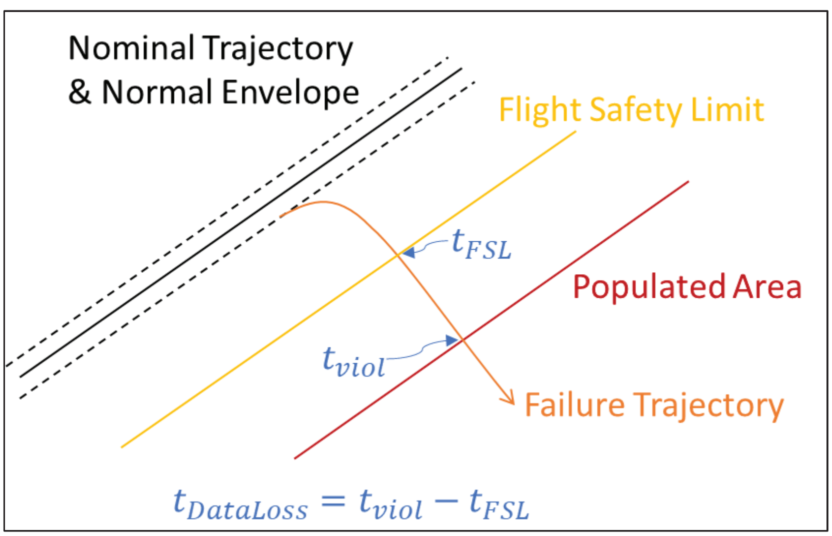


Figure 13-12: Data Loss Calculation when Envelopes Are Not Known

13.13.6 Extending the Durations.

There are certain situations where an appropriate risk reduction strategy is to have longer durations of acceptable data loss. Both of these require more extensive risk analysis to demonstrate that risk criteria are met and the lowest risk approach has been chosen.

13.13.6.1 The first occurs due to the distribution of the exposed public. One situation is when there is significant risk to the public within the limits of a useful mission, but then a large region with little to no population. In this case, since the abort location is not known when there is data loss, it is likely higher risk to abort inside the region of a useful mission than to have the vehicle potentially fly further and abort in an area with little to no population.

13.13.6.2 It may be possible in some scenarios to extend the data loss durations based on assessment of the trajectories that are first to produce areas of predicted casualty, rather than the trajectories that are first to reach flight safety limits or the limits of useful mission. This is a more exhaustive analysis, but would result in longer durations.

14 APPLICATION REQUIREMENTS.

14.1 Document Compliance with Flight Safety Limits Objectives and Constraints.

In order to comply with § 450.108(g)(1), a description of the methods used to comply with § 450.108(c) is required, to include descriptions of how each analysis constraint in § 450.108(d) is satisfied in accordance with § 450.115. Chapter 13 of this AC provides a template for a means of compliance for this. The applicant should indicate which paragraphs from chapter 13 of this AC were used with no modifications, and where deviations were made. Where deviations were made, the applicant should describe the process used with at least the level of detail contained in chapter 13 of this AC. Specific examples for a representative mission should be provided to demonstrate compliance.

14.2 Document each Flight Safety Limit and Flight Abort Rule.

For § 450.108(g)(2), the applicant should provide a list of flight safety limits and abort rules, and associated quantitative criteria and critical parameters. Each limit should define the parameters that are obtained from sensors, and the actual parameters that are evaluated. For example, sensors commonly provide position and velocity in three components in an Earth-centered inertial frame in metric units. An actual evaluation might be that the vacuum impact point (VacIP) on the surface of the earth is contained in a polygon defined by a series of geodetic vertices connected by great circles. References for the algorithms used to translate from the sensor data to VacIP and for the polygon evaluation should then be provided. This qualifies as a full description of the evaluation and implementation of that particular flight safety limit. A similar precise specification for other limits should also be provided.

14.3 Document Critical Parameters.

Likewise, for § 450.108(g)(2), the list of critical parameters used to evaluate a vehicle prior to entering a period of increased exposure, corresponding to § 450.108(c)(3), or ending flight abort, corresponding to § 450.108(e), must be provided, along with identification of how these ranges of values are identified. This identification should include the rationale for why each parameter is helpful for assessing the vehicle, and indicate if parameters described in this AC for this purpose were not selected and why. The description should provide evidence for how these ranges of values are identified. An example analysis of the determination of the expected range of critical parameters should be provided to demonstrate compliance. This should be based on a representative mission, including corresponding data and graphics to clearly illustrate the range of parameters.

14.4 Graphic Depiction of Flight Safety Limits.

For § 450.108(g)(3), the applicant must provide graphical depiction(s) of flight safety limits with relevant context as specified in that requirement. This must be provided as part of the application for a representative mission and should be consistent with the submission of trajectory data in § 450.117(d)(4). There must be a graphical depiction in the projection of each flight safety limit. For example, IIP-based limits should be shown on a map that shows the vertices of the limits and the segments between them. The segments should be shown as they are actually evaluated (great circles, straight lines on a particular projection, etc.). This map should include uncontrolled areas that are relevant, as well as the IIP traces of the nominal trajectory, extents of normal flight and limits of a useful mission.

- A Cartesian plot should be used for many other parameters where the limit is defined by two variables. For example, to depict a range vs. altitude limit, a plot with axes of range and altitude in the units of the evaluation should be provided. It is not possible to show uncontrolled areas on this projection, but the launch point, the nominal trajectory, and the extent of normal trajectories and the limits of useful mission must be shown. An applicant may show both maximum and minimum limits on the same set of depictions.
- Usually depictions at different scales are necessary to show the limits in sufficient detail—all vertices of limits should be visually identifiable on at least one depiction. Labels of the vertices or a corresponding data table for each limit should be provided as well.

14.5 **Document Vehicle Data**.

For § 450.108(g)(4), a description of the vehicle data that will be available to evaluate flight rules under all reasonably foreseeable conditions during normal and malfunctioning flight must be provided. These correspond to the sensor data discussed above to comply with § 450.108(g)(2), but in addition the conditions under which the data are available to the flight safety system must be specified. This is particularly important for ground-based flight safety systems where data may be available for only portions of flight.

OMB Control Number: 2120-0746
(Expiration Date: 08/31/2021)

Advisory Circular Feedback Form

Paperwork Reduction Act Burden Statement: A federal agency may not conduct or sponsor, and a person is not required to respond to, nor shall a person be subject to a penalty for failure to comply with a collection of information subject to the requirements of the Paperwork Reduction Act unless that collection of information displays a currently valid OMB Control Number. The OMB Control Number for this information collection is 2120-0746. Public reporting for this collection of information is estimated to be approximately 5 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. All responses to this collection of information are voluntary to obtain or retain benefits per 14 CFR 77. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to: Information Collection Clearance Officer, Federal Aviation Administration, 10101 Hillwood Parkway, Fort Worth, TX 76177-1524.

If you find an error in this AC, have recommendations for improving it, or have suggestions for new items/subjects to be added, you may let us know by (1) emailing this form to ASTApplications@faa.gov, or (2) faxing it to (202) 267-5450.

Subject: (insert AC title/number here) Date: Click here to enter text.

Please check all appropriate line items:

☐ An error (procedural or typographical) has been noted in paragraph Click here to enter text. on page Click here to enter text..

☐ Recommend paragraph Click here to enter text. on page Click here to enter text. be changed as follows:

Click here to enter text.

☐ In a future change to this AC, please cover the following subject:
(Briefly describe what you want added.)

Click here to enter text.

☐ Other comments:

Click here to enter text.

☐ I would like to discuss the above. Please contact me.

Submitted by: ________________________________ Date: __________________________