AST Commercial Space Transportation

Go for launch

Part 450 Industry Workshop – Day 2

faa.gov/space

Federal Aviation Administration

Agenda

Time	Topic
10:00 AM	**Opening Remarks**
10:06 AM	**Hazard Control Strategies** § 450.108 Flight Abort
10:51 AM	Q&A
11:06 AM	**Hazard Control Strategies** § 450.109 Flight Hazard Analysis § 450.110 Physical Containment § 450.111 Wind Weighting
11:25 AM	Q&A
11:40 AM	**Lunch Break**
12:10 PM	**Flight Safety Analysis** § 450.113 Flight Safety Analysis Requirements—Scope. § 450.115 Flight Safety Analysis Methods.
12:50 PM	Q&A
1:00 PM	**Flight Safety Analysis** § 450.117 Trajectory Analysis for Normal Flight § 450.119 Trajectory Analysis for Malfunction Flight. § 450.121 Debris Analysis. § 450.123 Population Exposure Analysis.
1:55 PM	Break

Agenda

Time	Topic
2:05 PM	**Flight Safety Analysis** § 450.131 Probability of Failure Analysis § 450.133 Flight Hazard Area Analysis
2:35 PM	Q&A
2:50 PM	**Flight Safety Analysis** § 450.135 Debris Risk Analysis § 450.137 Far-field Overpressure Blast Effects Analysis. § 450.139 Toxic Hazards for Flight
3:25 PM	Q&A
3:40 PM	Break
3:50 PM	**Prescribed Hazard for Safety-Critical Hardware and Computing Systems** § 450.141 Computing Systems
4:10 PM	Q&A
4:25 PM	**End of Day 2**

Flight Abort

In the final rule, the FAA consolidates the requirements for flight abort in § 450.108 and revises the more prescriptive requirements from the proposal into a single performance-based regulation.

Pursuant to § 450.108(a), flight safety limits are only required in phases of flight in which flight abort is used as a hazard control strategy to meet the safety criteria of § 450.101.

§ 450.108 Flight Abort.

(a) *Applicability*. This section applies to the use of flight abort as a hazard control strategy for the flight, or phase of flight, of a launch or reentry vehicle to meet the public safety criteria of § 450.101.

Flight Safety System

§ 450.108 Flight Abort.

(b) *Flight Safety System.* An operator must use a flight safety system that:

§ 450.145: Highly reliable flight safety system

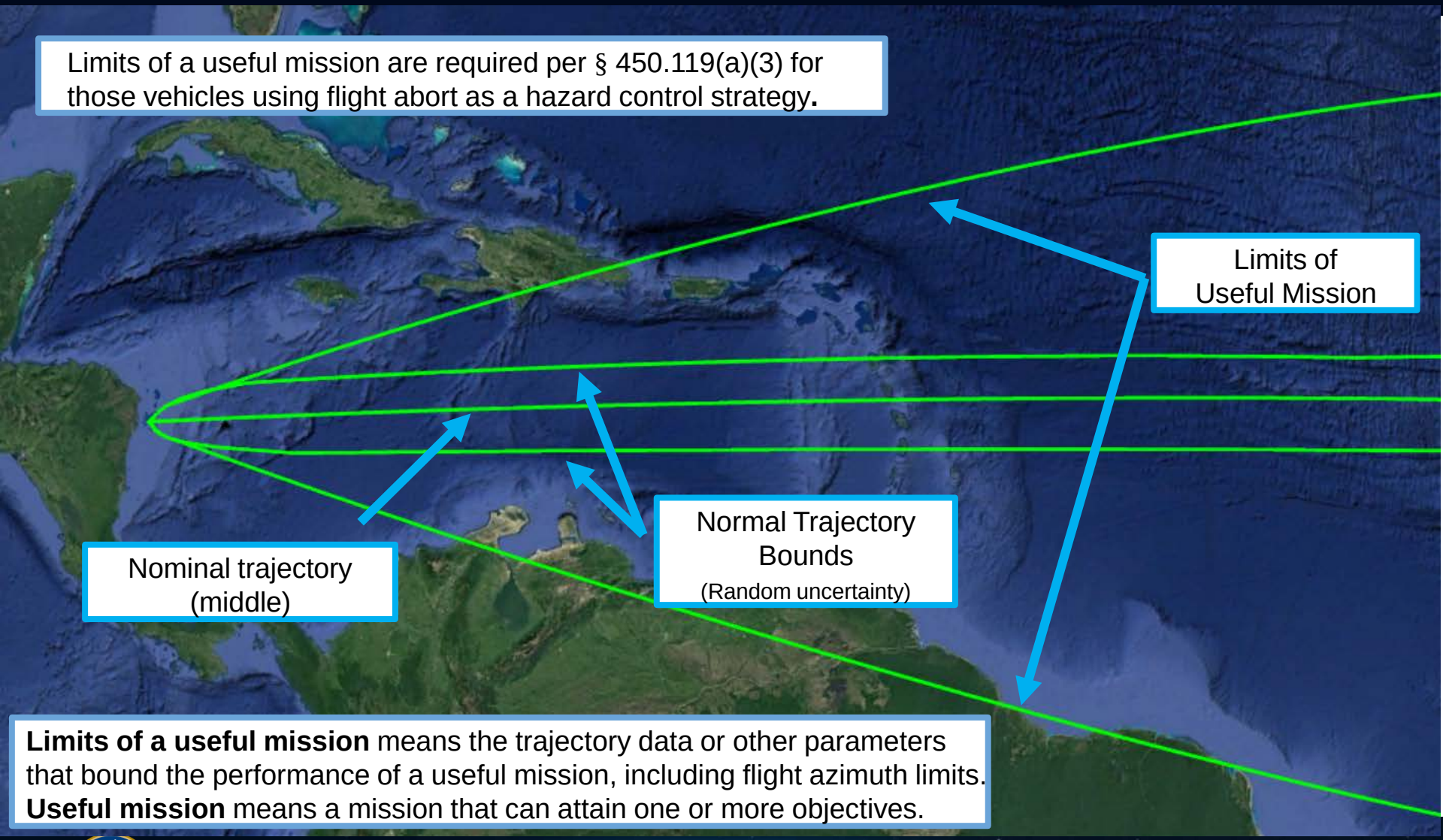
(1) Meets the requirements of § 450.145 if the consequence of any reasonably foreseeable failure mode in any significant period of flight is greater than 1×10^{-2} conditional expected casualties in uncontrolled areas; or

§ 450.143: Safety-critical system design, test, and documentation

(2) Meets the requirements of § 450.143 if the consequence of any reasonably foreseeable failure mode in any significant period of flight is between 1×10^{-2} and 1×10^{-3} conditional expected casualties for uncontrolled areas.

An example means of compliance for § 450.108(b)(1) is Range Commanders Council Standard (RCC) 319 19: *Flight Termination Systems Commonality Standard*

Limits of a Useful Mission



Flight Safety Limits Objectives

§ 450.101(a) and (b) include:

- Collective risk
- Individual risk
- Aircraft risk
- Risk to critical assets

For launch vehicles (a) and reentry vehicles (b).

§ 450.108 Flight Abort.

(c) *Flight Safety Limits Objectives.* An operator must determine and use flight safety limits that define when an operator must initiate flight abort for each of the following—

(1) To ensure compliance with the safety criteria of § 450.101(a) and (b);

Explanation and details on how to comply with § 450.108(c) will be included in AC 450.108-1 *Flight Abort Rule Development.* Planned issuance is Q1 2021.

Flight Safety Limits Objectives

§ 450.108(c)(2) as finalized acknowledges that debris impact is not the only risk contributor that must be accounted for in determining flight safety limits. For example, a release of toxic propellant following a debris impact may also contribute to risk. Therefore, in § 450.108(c)(2), an operator must determine and use flight safety limits to prevent continued flight from increasing risk once a vehicle can no longer achieve a useful mission. The FAA recognizes that a vehicle may deviate from the limits of a useful mission during a period when hazard containment through flight abort is not possible. In this case, the requirement is not to allow continued flight to increase risk, though some risk from either flight abort or continued flight may be unavoidable.

§ 450.108 Flight Abort.

(c) *Flight Safety Limits Objectives.* An operator must determine and use flight safety limits that define when an operator must initiate flight abort for each of the following—

(2) To prevent continued flight from increasing risk in uncontrolled areas if the vehicle is unable to achieve a useful mission;

Flight Safety Limits Objectives

A period of materially increased public exposure would include the beginning of a period when the vehicle will overfly a major landmass prior to orbital insertion. Overflight of large islands with substantial population may also constitute a period of materially increased public exposure, while overflight of islands with small populations or other areas of sparse population will not constitute a period of materially increased public exposure. 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 intended for orbit that cannot achieve a minimum safe orbit would require flight abort under § 450.108(c)(3).

A critical vehicle parameter is a parameter that demonstrates the vehicle is capable of completing safe flight through the upcoming phase of flight for which population is exposed to hazardous debris effects from reasonably foreseeable failure modes.

§ 450.108 Flight Abort.

(c) *Flight Safety Limits Objectives.* An operator must determine and use flight safety limits that define when an operator must initiate flight abort for each of the following—

(3) 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;

Flight Safety Limits Objectives

The purpose of § 450.108(c)(4) is to ensure that, when an operator cannot develop flight safety limits that prevent hazards from affecting uncontrolled areas, the failure modes that result in deviations from the planned trajectory will not result in a high consequence event if the vehicle is unable to achieve a useful mission. This scenario can arise when some public exposure must be accepted to allow useful vehicles to continue during a phase of flight when flight abort is still used as a hazard control strategy.

This situation frequently occurs, for example, on northeasterly missions launched from the Eastern Range that are permitted to overfly some portions of Nova Scotia and Newfoundland on trajectories within the limits of a useful mission. If the vehicle fails after the overflight has begun and reaches flight safety limits protecting more westerly portions of the uncontrolled areas from flight outside the limits of a useful mission, the consequence from flight abort must meet the criteria in § 450.108(c)(4).

§ 450.108 Flight Abort.

(c) *Flight Safety Limits Objectives.* An operator must determine and use flight safety limits that define when an operator must initiate flight abort for each of the following—

(4) 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; and

Flight Safety Limits Objectives

For example, if a roll rate of a particular magnitude would preclude ground-based flight abort commands from being received by the vehicle, a flight safety limit should be developed that triggers flight abort before the roll rate reaches this value.

§ 450.108 Flight Abort.

(c) *Flight Safety Limits Objectives.* An operator must determine and use flight safety limits that define when an operator must initiate flight abort for each of the following—

(5) 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.

Flight Safety Limits Objectives

A CE_C analysis is not required if an FSS that complies with § 450.145 provides hazard containment. Hazard containment is a means of achieving the goals of § 450.108(c)(2) and (c)(4) because, if an operator provides for hazard containment, continued flight will not increase risk in uncontrolled areas and hazard containment would prevent conditional expected casualties greater than 1×10^{-2} in uncontrolled areas.

This strategy is not an option when hazard containment is not possible during a phase of flight when flight abort must be used as a hazard control strategy. For example, if an area of overflight occurs on the nominal trajectory during a phase of flight when flight abort is still used as a hazard control strategy, an operator cannot claim containment during this phase and must meet § 450.108(c)(2) and (c)(4).

§ 450.108 Flight Abort.

(c) *Flight Safety Limits Objectives.* An operator must determine and use flight safety limits that define when an operator must initiate flight abort for each of the following—

(6) In lieu of paragraph (c)(2) and (c)(4), 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.

An example means of compliance for § 450.108(c)(6) is *Legacy Regulations: § 417.213(a),(b), and (d).*

Flight Safety Limits Constraints

Direct debris impacts are not the only hazards posed by vehicle failures. For example, an intact impact of a vehicle may lead to a blast wave or release of toxic propellant, both of which must be considered when developing flight safety limits. Hazard generation and transport are factors that apply to all hazards, unlike factors that only apply to determining debris impact dispersions. Hazard generation refers to the process by which a vehicle becomes a hazard, and transport is how the hazard moves from the source to an exposed person or asset. Simply accounting for potential contributions to debris impact dispersions would not encompass all hazards, though debris impact dispersions also need to be accounted for under § 450.108(d)(2).

§ 450.108 Flight Abort.

(d) *Flight safety limits constraints*. An operator must determine flight safety limits that—

(1) 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;

(2) Account for physics of hazard generation and transport including uncertainty;

Explanation and details on how to comply with § 450.108(d) will be included in AC 450.108-1 *Flight Abort Rule Development.* Planned issuance is Q1 2021.

Flight Safety Limits Constraints

Data is valid when it is of sufficient quality to be used to make flight abort decisions. Data used to make flight abort decisions can be missing or invalid for a number of reasons, but resulting from an unplanned event, such as disruption or loss of communication pathways with ground-based or onboard tracking sensors. Despite an operator's or launch site's best efforts, the potential to lose track data is a contingency for which operators must plan.

Data loss flight times, or green numbers, are an example of a flight safety limit that may be used when data necessary to evaluate the flight abort rules is lost.

§ 450.108 Flight Abort.

(d) *Flight safety limits constraints*. An operator must determine flight safety limits that—

(3) Account for the potential to lose valid data necessary to evaluate the flight abort rules;

Flight Safety Limits Constraints

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. 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.

§ 450.108 Flight Abort.

(d) *Flight safety limits constraints*. An operator must determine flight safety limits that—

(4) Account for the time delay, including uncertainties, between the violation of a flight abort rule and the time when the flight safety system is expected to activate;

Flight Safety Limits Constraints

To comply with § 450.108(d)(5), first, the FSS must be assumed to have a reliability of one, meaning it is presumed to function without error. The risk evaluations using an FSS reliability of one ensure that the criteria are met if the FSS functions as intended. This requirement is important because an FSS failure should not be relied upon to make flight safety limits compliant with risk requirements. The decision to implement a flight abort is a deliberate safety intervention. The FAA wants to be sure that the public is safe given any deliberate safety intervention. Second, the risk evaluations must consider the predicted reliability of the FSS. Predicted reliability of the FSS is important because even low probabilities of FSS failures can have significant impacts on risk.

§ 450.108 Flight Abort.

(d) *Flight safety limits constraints*. An operator must determine flight safety limits that—

(5) Account in individual, collective, and conditional risk evaluations both for proper functioning of the flight safety system and failure of the flight safety system;

Flight Safety Limits Constraints

Two methods of demonstrating that flight abort does not increase risk in uncontrolled areas compared to continued flight are:

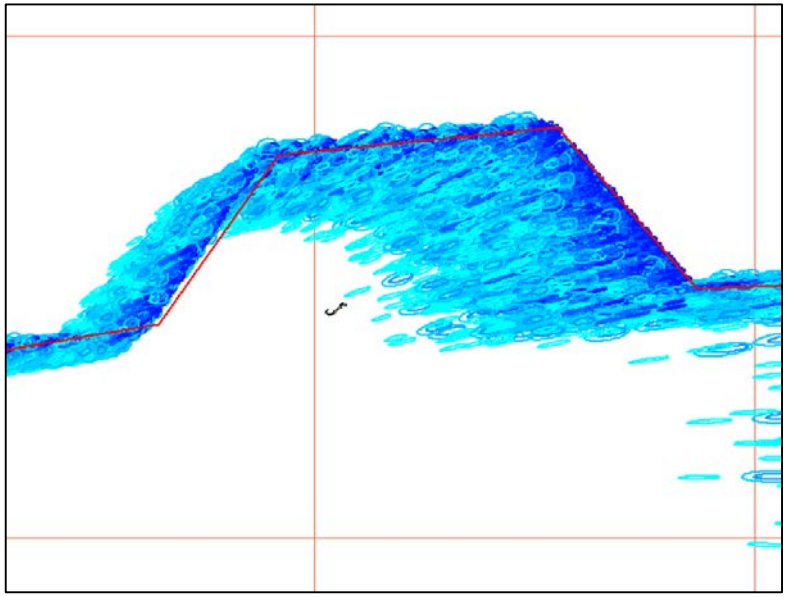
1. Inspect debris footprints from flight abort to confirm that they do not affect uncontrolled areas. This works best when inert debris footprints capture the hazard extent.
2. Perform numerical analysis showing that the risk from each abort case is not larger than the risk from no abort.

In the example shown, the margin between Bermuda and the debris footprints resulting from flight abort is minimal and could be improved with modifications to the flight safety limits.

§ 450.108 Flight Abort.

(d) *Flight safety limits constraints*. An operator must determine flight safety limits that—

(6) Are designed to avoid flight abort that results in increased collective risk to the public in uncontrolled areas, compared to continued flight; and



Flight Safety Limits Constraints

Sections 450.108(c)(3) and 450.108(d)(7) in the final rule allow vehicles within the limits of a useful mission to enter a period of materially increased public exposure in uncontrolled areas, provided the trajectory meets the collective risk requirement.

§ 450.108 Flight Abort.

(d) *Flight safety limits constraints*. An operator must determine flight safety limits that—

(7) Ensure that 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).

End of Flight Abort

The term key flight safety event in the context of part 450 includes events that could compromise any safety-critical system, or otherwise increase the risk from high consequence events, such as events that subject a safety-critical system to environments at or near the maximum predicted environment.

§ 450.108 Flight Abort.

(e) *End of flight abort*. 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 the following conditions are met for the remainder of flight:

(1) Flight abort would not materially decrease the risk from a high consequence event; and

(2) There are no key flight safety events.

Flight Abort Rules

The phrase "under all reasonably foreseeable conditions" in § 450.108(f)(1) acknowledges that some conditions that prevent vehicle data from being available to evaluate flight abort rules might be unforeseeable and therefore unpreventable through planning and design.

Section 450.108(f)(2)(ii) is the flight abort rule used in conjunction with § 450.108(c)(5).

§ 450.108 Flight Abort.

(f) *Flight abort rules.* For each launch or reentry, an operator must establish and observe flight abort rules that govern the conduct of the launch or reentry as follows.

(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.

(2) The flight safety system must abort flight:

(i) When valid, real-time data indicate the vehicle has violated any flight safety limit developed in accordance with this section

(ii) When the vehicle state approaches identified conditions that are anticipated to compromise the capability of the flight safety system and further flight has the potential to violate a flight safety limit; and

(iii) In accordance with methods used to satisfy (d)(3) of this section, if tracking data is invalid and further flight has the potential to violate a flight safety limit.

Application Requirements

The FAA clarifies that an applicant will need only to submit flight safety limits for a representative mission in its application. Pursuant to § 450.213(c), flight abort products must be submitted for each mission no less than 30 days before flight unless the Administrator agrees to a different time frame in accordance with § 404.15 in the license.

(g) *Application requirements.* An applicant must submit in its application the following:

(1) A description of the methods used to demonstrate compliance with § 450.108(c), including descriptions of how each analysis constraint in § 450.108(d) is satisfied in accordance with § 450.115.

(2) A description of how each flight safety limit and flight abort rule is evaluated and implemented during vehicle flight, including the quantitative criteria that will be used, a description of any critical parameters, and how the values required in paragraphs (c)(3) and (e) are identified;

(3) A graphic depiction or series of depictions of flight safety limits for a representative mission together with the launch or landing point, all uncontrolled area boundaries, the nominal trajectory, extents of normal flight, and limits of a useful mission trajectories, with all trajectories in the same projection as each of the flight safety limits; and

(4) A description of the vehicle data that will be available to evaluate flight abort rules under all reasonably foreseeable conditions during normal and malfunctioning flight.

Q&A

Flight Hazard Analysis

Pursuant to 450.109(b), A flight hazard analysis must identify, describe, and analyze all reasonably foreseeable hazards to public safety resulting from the flight of a launch or reentry vehicle, mitigate hazards as appropriate, and validate and verify the hazard mitigations.

§ 450.109 Flight Hazard Analysis.

(a) *Applicability.* This section applies to the use of a flight hazard analysis as a hazard control strategy to derive hazard controls for the flight, or phase of flight, of a launch or reentry vehicle. Hazards associated with computing systems and software are further addressed in § 450.141.

Explanation and details on how to comply with § 450.109 will be included in AC 450.109-1 "Flight Hazard Analysis" Planned issuance is Q1 2021.

Flight Hazard Analysis

Flight hazard analysis is the traditional safety approach for reusable launch vehicles, and is the most flexible hazard control strategy because an operator derives specific hazard controls unique to its launch or reentry vehicle system and operations concept. Flight hazard analysis is mandated as a hazard control strategy if the other three hazard control strategies cannot mitigate the safety hazards sufficient to meet the safety criteria of § 450.101.

§ 450.109 Flight Hazard Analysis.

(b) *Analysis.* A flight hazard analysis must identify, describe, and analyze all reasonably foreseeable hazards to public safety resulting from the flight of a launch or reentry vehicle. Each flight hazard analysis must—

(1) Identify all reasonably foreseeable hazards, and the corresponding failure mode for each hazard, associated with the launch or reentry system relevant to public safety, including those resulting from:

(i) Vehicle operation, including staging and release; (ii) System, subsystem, and component failures or faults; (iii) Software operations; (iv) Environmental conditions; (v) Human factors; (vi) Design inadequacies; (vii) Procedure deficiencies; (viii) Functional and physical interfaces between subsystems, including any vehicle payload; (ix) Reuse of components or systems; and (x) Interactions of any of the above.

(2) Assess each hazard's likelihood and severity.

(3) Ensure that the likelihood of any hazardous condition that may cause death or serious injury to the public is extremely remote.

(4) Identify and describe the risk elimination and mitigation measures required to satisfy paragraph (b)(3) of this section.

(5) Document that the risk elimination and mitigation measures achieve the risk levels of paragraph (b)(3) of this section through validation and verification. Verification includes:

(i) Analysis; (ii) Test; (iii) Demonstration; or (iv) Inspection.

Flight Hazard Analysis

§ 450.109 Flight Hazard Analysis.

(c) *New Hazards.* An operator must establish and document the criteria and techniques for identifying new hazards throughout the lifecycle of the launch or reentry system.

(d) *Completeness Prior to Flight.* For every launch or reentry, the flight hazard analysis must be complete and all hazards must be mitigated to an acceptable level in accordance with paragraph (b)(3) of this section.

(e) *Updates.* An operator must continually update the flight hazard analysis throughout the lifecycle of the launch or reentry system.

(f) *Application requirements*. An applicant must submit in its application the following:

(1) Flight hazard analysis products of paragraphs (b)(1) through (5) of this section, including data that verifies the risk elimination and mitigation measures resulting from the applicant's flight hazard analyses required by paragraph (b)(5) of this section; and

(2) The criteria and techniques for identifying new hazards throughout the lifecycle of the launch or reentry system as required by paragraph (c) of this section.

Flight Hazard Analysis

Flight Hazard Analysis

Top-Level System [TBD]	Next-Level System [TBD]	Subsystem	Component(s) / Item(s)	Functional Failure ID(s)	Failure Description and End Effect	Possible Cause(s)	Subsystem-Level								System/Mission-Level[1]							
							Risk Before Mitigation Measures			Risk Elimination / Mitigation Measures	Risk After Mitigation Measures			Verification Evidence	Hazard to Public[1]	Risk Elimination / Mitigation Measures[1]	Risk After Mitigation Measures[1]			Verification Evidence[1]		
							L	S	R		L	S	R				L	S	R			
		Avionics	Main Computer	TBD	Main computer [Function TBD] during [Mission Phase(s) TBD] fails [Failure TBD], possibly resulting in loss of vehicle control, break-up, or [End Effect TBD]	C1 – Board Failure C2 – Electro-Static Discharge (ESD) C3 – Foreign Object Debris (FOD) C4, and so on…	Initial or no data	TBD	TBD	C1.M1 – Specific to mitigation of board failure (design, test, manufacturing process, etc) C1.M2 – Specific to mitigation of C1 C1.M3, and so on…	TBD	TBD	TBD	C1.M1.V1 – Documented evidence specific to performed C1.M1 mitigation C1.M1.V2, and so on… C1.M2.V1, and so on… C1.M3.V1, and so on…	H1 – Off-nominal trajectory H2 – Abort Debris / Landing H3 – Reentry Debris H4, and so on…	H1.M1 - Specific to mitigation of H1 [Flight Safety System (FSS), operational restrictions, clear areas, etc…] H1.M2, and so on…	TBD	TBD	TBD	H1.M1.V1 – Documented evidence specific to H1.M1 mitigation H1.M1.V2, and so on… H1.M2.V1, and so on…
										C2.M1 – Specific to mitigation of ESD (design, test, manufacturing process, etc) C2.M2 - Specific to mitigation of C2 C2.M3, and so on…				C2.M1.V1 – Documented evidence specific to performed C2.M1 mitigation C2.M1.V2, and so on… C2.M2.V1, and so on… C2.M3.V1, and so on…		H2.M1 - Specific to mitigation of H2 [deorbit criteria, contingencies, established clear areas for NOTAM/NOTMAR, etc…] H2.M2, and so on…				H2.M1.V1 – Documented evidence specific to H2.M1 mitigation H2.M1.V2, and so on… H2.M2.V1, and so on…
										C3.M1 – Specific to mitigation of FOD (design, test, manufacturing process, etc) C3.M2 - Specific to mitigation of C3 C3.M3, and so on…				C3.M1.V1 – Documented evidence specific to performed C3.M1 mitigation C3.M1.V2, and so on… C3.M2.V1, and so on… C3.M3.V1, and so on…		H3.M1 - Specific to mitigation of H3 [abort criteria, mission rules, contingencies, established clear areas for NOTAM/NOTMAR, etc…] H3.M2, and so on…				H3.M1.V1 – Documented evidence specific to H3.M1 mitigation H3.M1.V2, and so on… H3.M2.V1, and so on…

Data from Functional Hazard Analysis

Via Fault Tree Analyses; FMEA/FMECA; HEA Subsystem Hazard Analysis, etc.

Identify/Verify mitigations to specific causes of functional failures at the subsystem/component level (e.g., design, manufacturing, etc.)

Identify/Verify specific system/mission mitigations for residual system safety risk of public safety hazards (e.g., FSS, ops restrictions, etc.)

↓Traceability↑

Physical Containment

In the final rule, FAA clarifies that the hazard area must be clear of the public and critical assets.

Explanation and details on how to comply with § 450.110 will be included in AC 450.110-1 "Physical Containment Flight Safety Analysis". Planned Issuance is Q2 2021.

§ 450.110 Physical Containment.

(a) *Applicability.* This section applies to the use of physical containment as a hazard control strategy for the flight, or phase of flight, of a launch or reentry vehicle to meet the public safety criteria of § 450.101(a), (b), and (c).

(b) *Containment*. To use physical containment as a hazard control strategy, an operator must—

(1) Develop the flight hazard area in accordance with § 450.133;

(2) Ensure that the launch vehicle does not have sufficient energy for any hazards associated with its flight to reach outside the flight hazard area;

(3) Ensure the hazard area is clear of the public and critical assets; and

(4) Apply other mitigation measures necessary to ensure no public or critical asset exposure to hazards, such as control of public access or wind placards.

Physical Containment

The physical containment hazard control strategy is designed to be a simple method of protecting public safety by launching within an area that is cleared of public and critical assets, and within an area that contains hazards based on the potential energy of the vehicle.

This hazard control strategy is appropriate for missions that have limited vehicle kinematic range and have tightly controlled airspace and access to the operational area.

§ 450.110 Physical Containment.

(c) *Application requirements.* An applicant must submit in its application the following:

(1) A demonstration that the launch vehicle does not have sufficient energy for any hazards associated with its flight to reach outside the flight hazard area developed in accordance with § 450.133; and

(2) A description of the methods used to ensure that flight hazard areas are cleared of the public and critical assets.

Wind Weighting

In the applicability section, the FAA specifies that an operator may use wind weighting as a hazard control strategy to meet the public safety criteria of § 450.101 to § 450.101(a), (b), and (c), which address launch risk criteria, reentry risk criteria, and high consequence event protection.

Explanation and details on how to comply with § 450.111 can be found in §§ 415.109(b)(2)(v), 417.125, 417.201(c), 417.233, and Appendix C to Part 417

§ 450.111 Wind Weighting.

(a) *Applicability.* This section applies to the use of wind weighting as a hazard control strategy for the flight of an unguided suborbital launch vehicle to meet the public safety criteria of § 450.101(a), (b), and (c).

(b) *Wind weighting safety system.* The flight of an unguided suborbital launch vehicle that uses a wind weighting safety system must meet the following:

(1) The launcher azimuth and elevation settings must be wind weighted to correct for the effects of wind conditions at the time of flight to provide impact locations that will ensure compliance with the safety criteria in § 450.101; and

(2) An operator must use launcher azimuth and elevation angle settings that ensures the rocket will not fly in an unintended direction accounting for uncertainties in vehicle and launcher design and manufacturing, and atmospheric uncertainties.

Wind Weighting

There is no requirement for an applicant to provide additional products that allow an independent analysis as requested by the Administrator because the requirement was redundant with § 450.45(e)(7)(ii).

This hazard control strategy is intended for the launch of unguided suborbital launch vehicles where wind weighting can be used to demonstrate that the population exposure is low enough to meet the requirements of § 450.111.

§ 450.111 Wind Weighting.

(c) *Analysis*. An operator must—

(1) Establish flight commit criteria and other flight safety rules that control the risk to the public from potential adverse effects resulting from normal and malfunctioning flight;

(2) Establish any wind constraints under which flight may occur; and

(3) Conduct a wind weighting analysis that establishes the launcher azimuth and elevation settings that correct for the windcocking and wind-drift effects on the unguided suborbital launch vehicle.

(d) *Stability.* An unguided suborbital launch vehicle, in all configurations, must be stable throughout each stage of powered flight.

(e) *Application requirements.* An applicant must submit in its application the following:

(1) A description of its wind weighting analysis methods, including its method and schedule of determining wind speed and wind direction for each altitude layer;

(2) A description of its wind weighting safety system including all equipment used to perform the wind weighting analysis; and

(3) A representative wind weighting analysis using actual or statistical winds for the launch area and samples of the output.

Q&A

AST Commercial Space Transportation

Go for launch

On Break

Next Session Starts at 12:10 PM EST

faa.gov/space

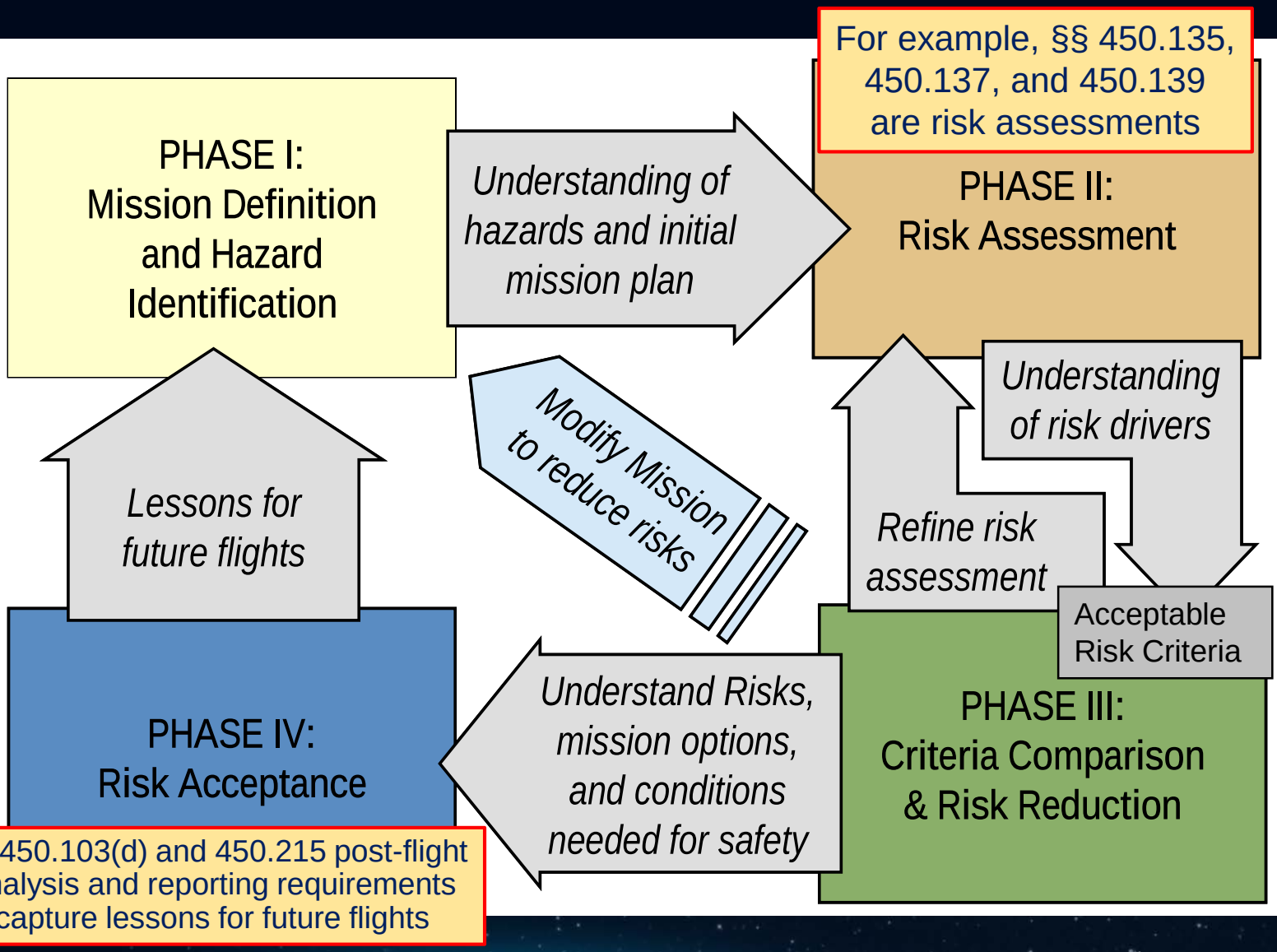
Federal Aviation Administration

Context for Flight Safety Analysis (FSA)

FSA is a key part of risk management.

Risk management is a systematic and logical process to identify hazards and control the risks they pose.

Figure is taken from Range Commanders Council (RCC) 321-20



Roadmap for FSA sections in 450

A FSA consists of a set of quantitative analyses used to:

1. **Demonstrate compliance with the safety criteria in § 450.101**
2. **Determine flight hazard areas, and other mitigation measures**
3. **Determine flight commit criteria and flight abort rules (if necessary)**

§§ 450.113 and 450.115 contain the FSA scope and method requirements

§§ 450.117 through 450.139 fit in two categories of analyses:

Analyses to Develop Key Inputs to Quantitative Risk Analyses (QRAs)

1. Probability of failure analysis
2. Trajectory analysis for normal flight
3. Trajectory analysis for malfunction flight
4. Debris analysis
5. Population exposure analysis

QRAs to Demonstrate Compliance with § 450.101

A. Flight hazard area analysis

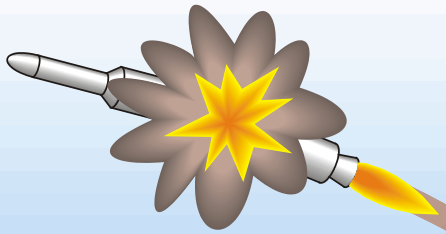
B. Debris risk analysis

C. Far-field overpressure blast effects analysis

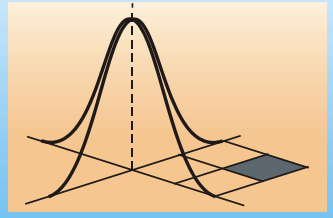
D. Toxic hazards for flight

Overview of Launch Debris Risk Analysis

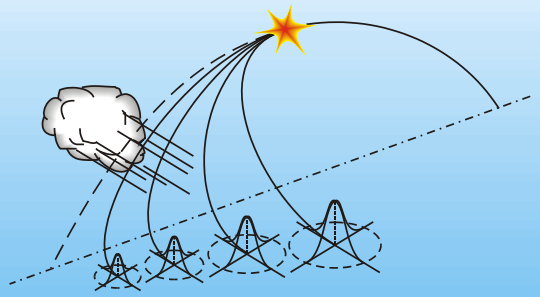
- Define Failure Modes
- Define Failure Rates for Each Mode
- Define Dynamics of Vehicle Dispersion for Each Mode at Each Failure Time
- Include Effects of Debris Velocity Perturbation, Wind, Lift, Drag Uncertainty, and Simulate Command Destruct Logic



Compute Impact Probability for Each Object on Each Population Center at Each Mode/Time



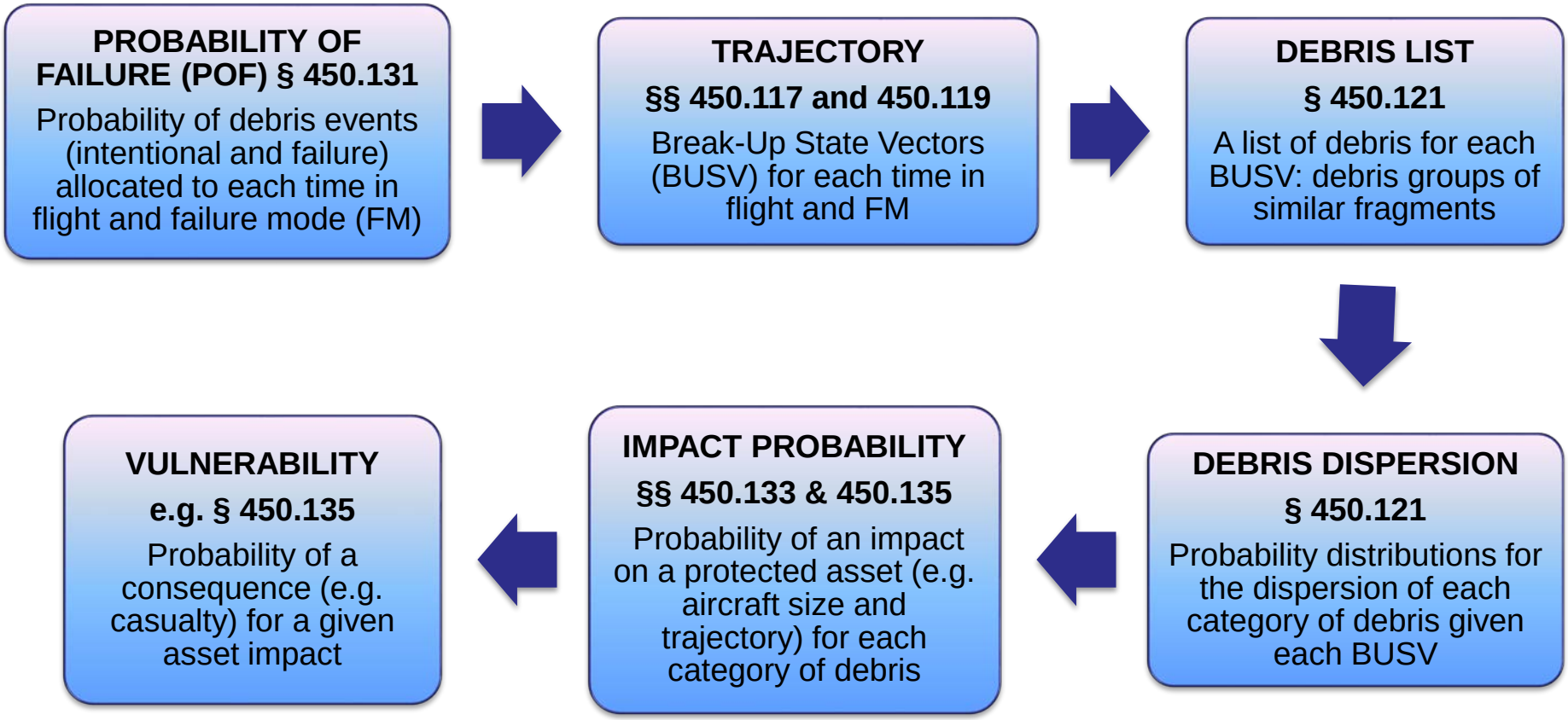
Develop Impact Probability Density Functions for Each Debris Item for Each Failure Mode for Each Time



Compute Casualty Expectation for Each Population Center for Each Object at Each Mode/Time

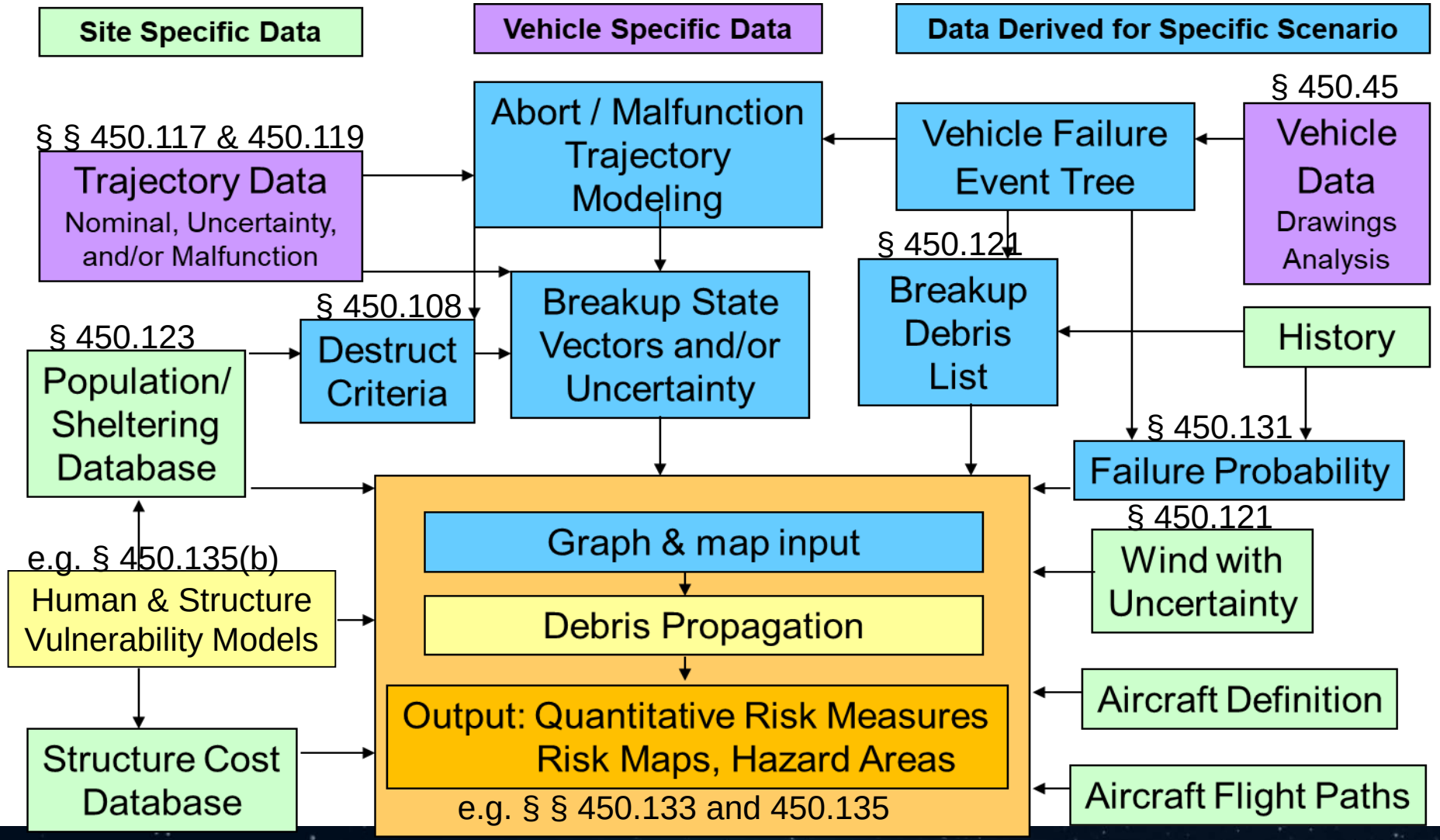
Combine Casualty Expectations and Impact Probabilities to Determine Risk

Key Elements of a FSA



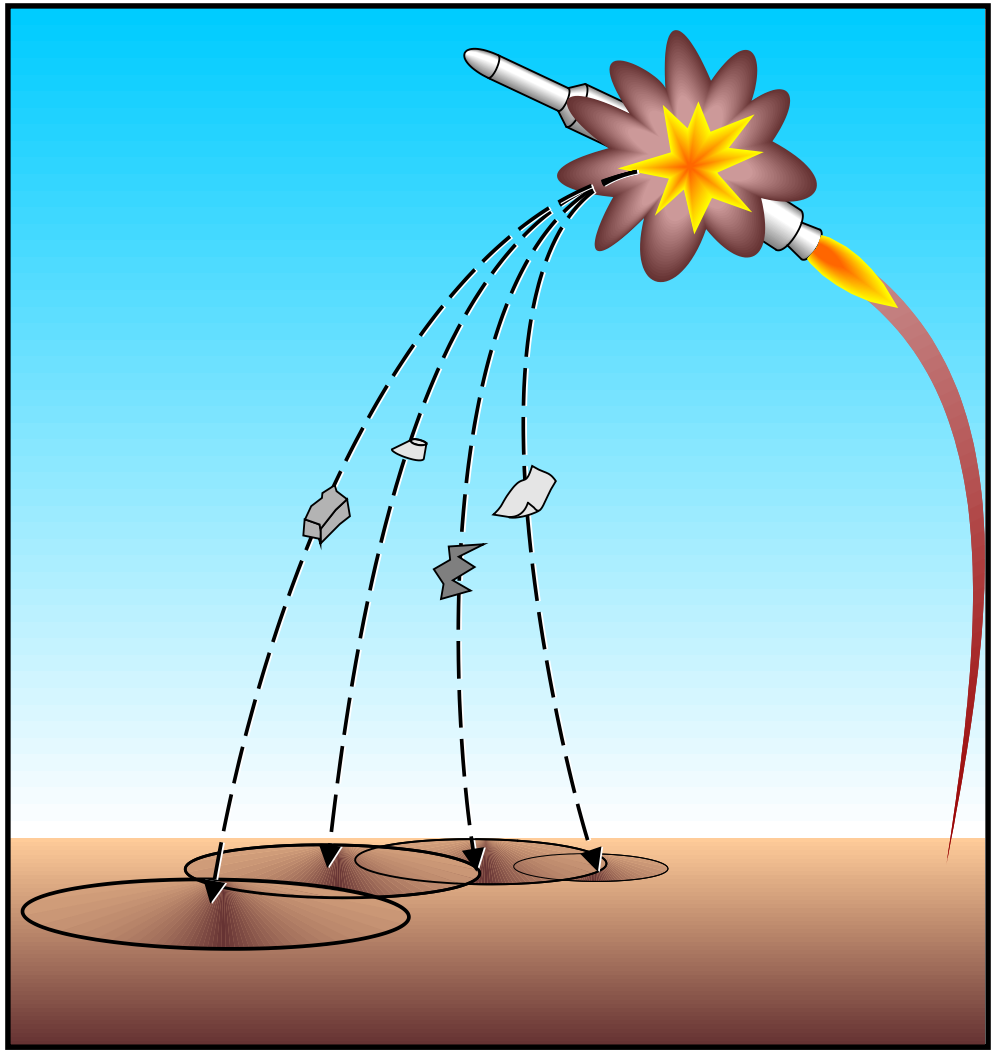
The last two (vulnerability and impact probability) and the criteria for aircraft protection, have aspects that are necessarily unique to aircraft hazard area analysis; all other sub-models are common with the ground risk analysis.

Overview of FSA Inputs and Outputs



Debris Footprint Concept

- The debris footprint is the statistical region defining the scatter of debris resulting from a breakup at a specific point in time and space.
- The footprint can be viewed as a statistical representation of an accident.



Debris Centerline and Ballistic Coefficient

Debris paths are computed based on Newton's laws of motion

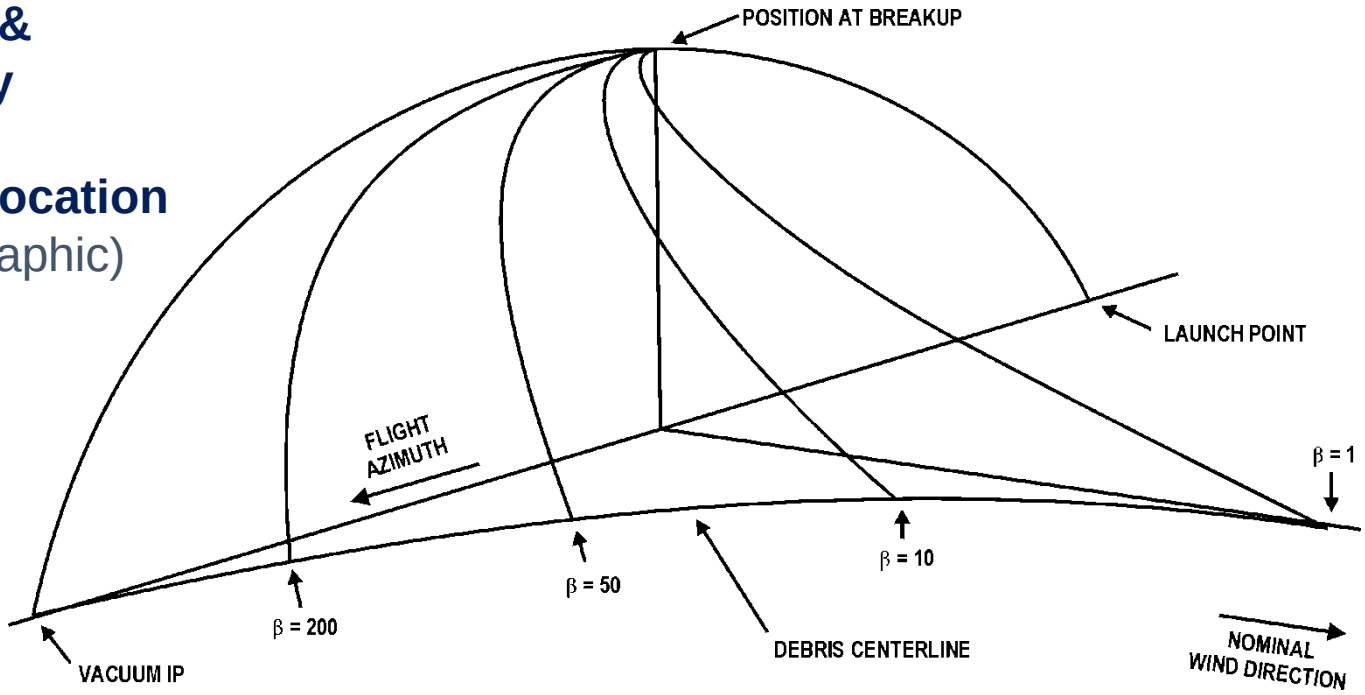
State vector (position, velocity) establishes initial conditions.

Ballistic coefficient & atmospheric density profile influence downrange impact location
(Lift ignored in this graphic)

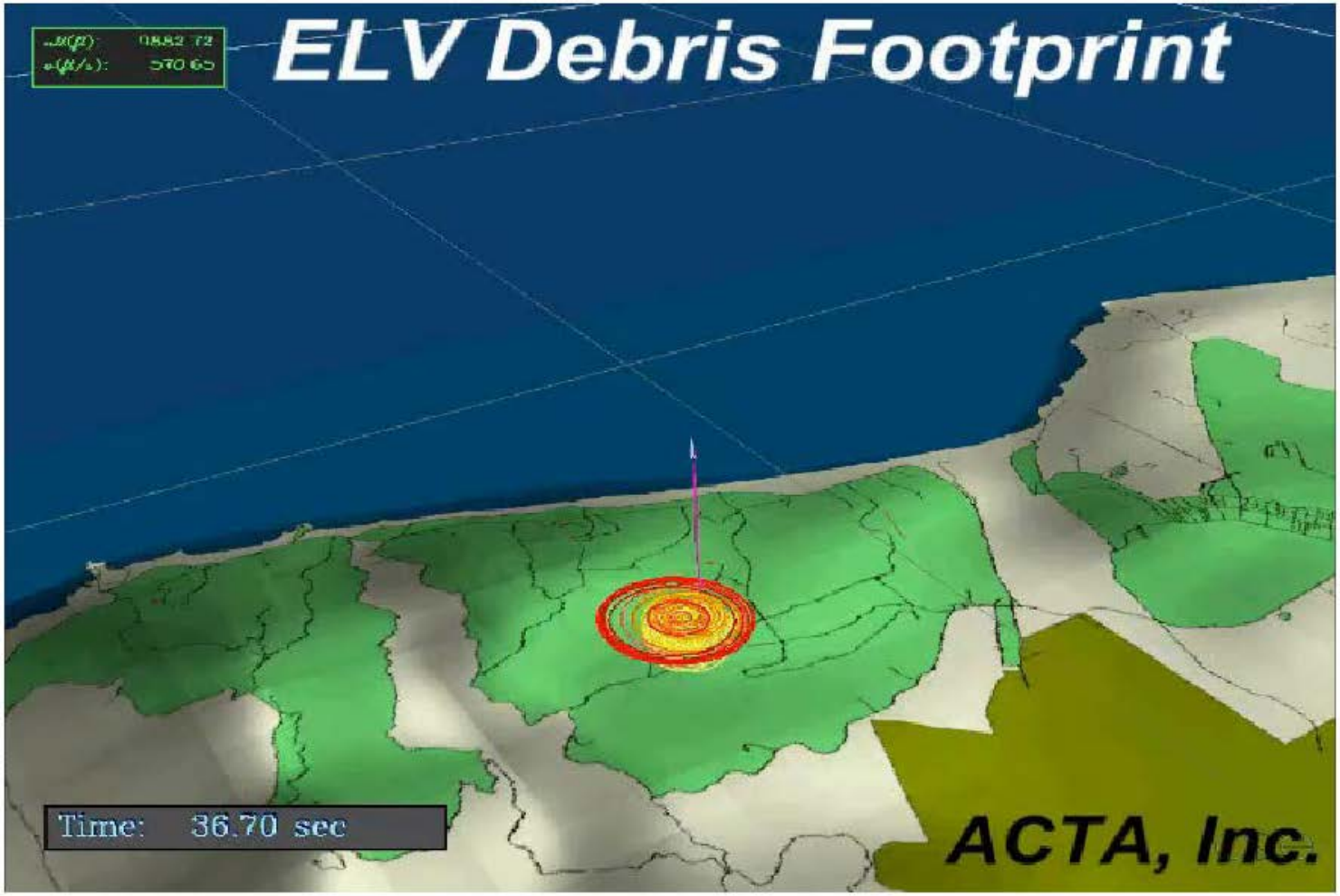
Ballistic coefficient: ratio of weight/drag

$$\beta = \frac{W}{C_D A}$$

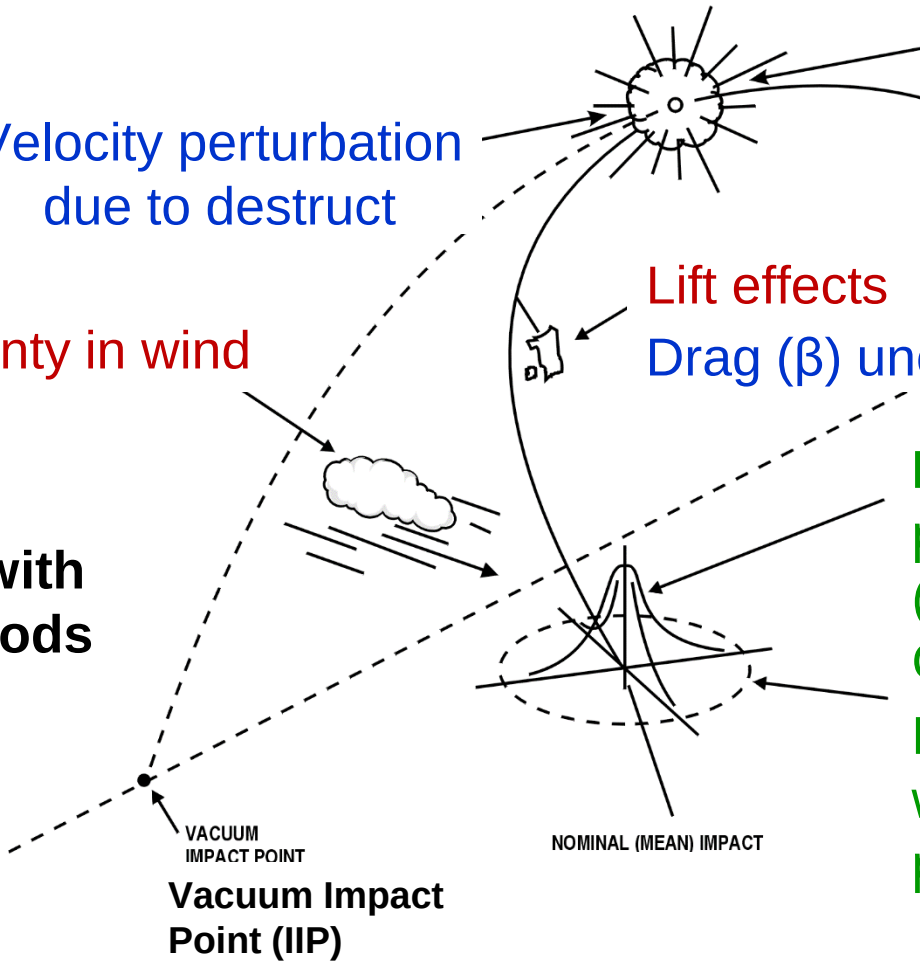
C_D may be a function of Mach number, shape, etc.



Wind effects: low β debris slows down rapidly due to high drag forces, then gets blown down wind (cross-range)


ELV Debris Footprint
Time: 36.70 sec
ACTA, Inc.

Contributions to Debris Dispersions



Uncertainty accounted for with statistical methods either Monte Carlo sampling or Analytical

Result: Impact probability distribution (often modeled as Gaussian)

Distribution shown with ellipses of equal probability

Flight Safety Analysis Requirements—Scope

An operator must perform and document a FSA for all phases of flight with scope of launch and reentry, unless otherwise agreed to by the FAA. The FAA may agree there is no need for an FSA for certain phases of flight based on demonstrated reliability for any vehicle. Conceivably, an operation could have an extensive and safe enough flight history to demonstrate compliance with the risk criteria in § 450.101(a) and (b) based on empirical data in lieu of the traditional risk analysis.

The L-1011 carrier vehicle used for Pegasus launches is an example of a carrier aircraft with enough empirical evidence to demonstrate compliance with the public risk criteria in § 450.101(a) or (b).

§ 450.113 Flight Safety Analysis Requirements—Scope.

(a) An operator must perform and document a flight safety analysis for all phases of flight, except as specified in paragraph (b), as follows —

(1) For orbital launch, from liftoff through orbital insertion, and through all component impacts or landings;

(2) For suborbital launch, from liftoff through all component impacts or landings;

(3) For disposal, from the initiation of the deorbit through final impact; and

(4) For reentry, from the initiation of the deorbit through all component impacts or landing.

(b) An operator is not required to perform and document a flight safety analysis for a phase of flight if agreed to by the Administrator based on demonstrated reliability. **An operator demonstrates reliability by using operational and flight history to show compliance with the risk criteria in § 450.101(a) and (b)**.

Flight Safety Analysis Methods

Section 450.115 specifies that the operator's analysis methods 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 health and safety, and the safety of property.

450 does not direct how an operator must identify the reasonably foreseeable events (e.g. failure modes), but § 450.103(b) does direct that a functional hazard analysis must be done.

An operator must comply with these foundational sections when performing any of the separate analyses that together comprise a FSA.

§ 450.115 Flight Safety Analysis Methods.

(a) *Scope of the analysis*. 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.

(b) *Level of fidelity of the analysis*. An operator's **flight safety analysis method must have a level of fidelity sufficient to**—

(1) Demonstrate that any risk to the public satisfies the public safety criteria of § 450.101, including the use of mitigations, **accounting for all known sources of uncertainty, using a means of compliance accepted by the Administrator**; and

(2) **Identify the dominant source of each type of public risk** with a criterion in § 450.101(a) or 450.101(b) in terms of phase of flight, source of hazard (such as toxic exposure, inert, or explosive debris), and failure mode.

Flight Safety Analysis Methods

Per § 450.115(c)(4), an applicant must identify the evidence for validation and verification required by § 450.101(g), which addresses the required accuracy and validity of data and scientific principles.

Rationale for the level of fidelity typically linked to requirements in § 450.115(b)(1) to account "for all known sources of uncertainty" and § 450.101(g) to produce results consistent with or more conservative than the results available from previous mishaps, tests, or other valid benchmarks, such as higher-fidelity methods.

§ 450.115 Flight Safety Analysis Methods.

(c) *Application requirements.* An applicant must submit a description of the flight safety analysis methodology, including identification of:

(1) The scientific principles and statistical methods used;

(2) All assumptions and their justifications;

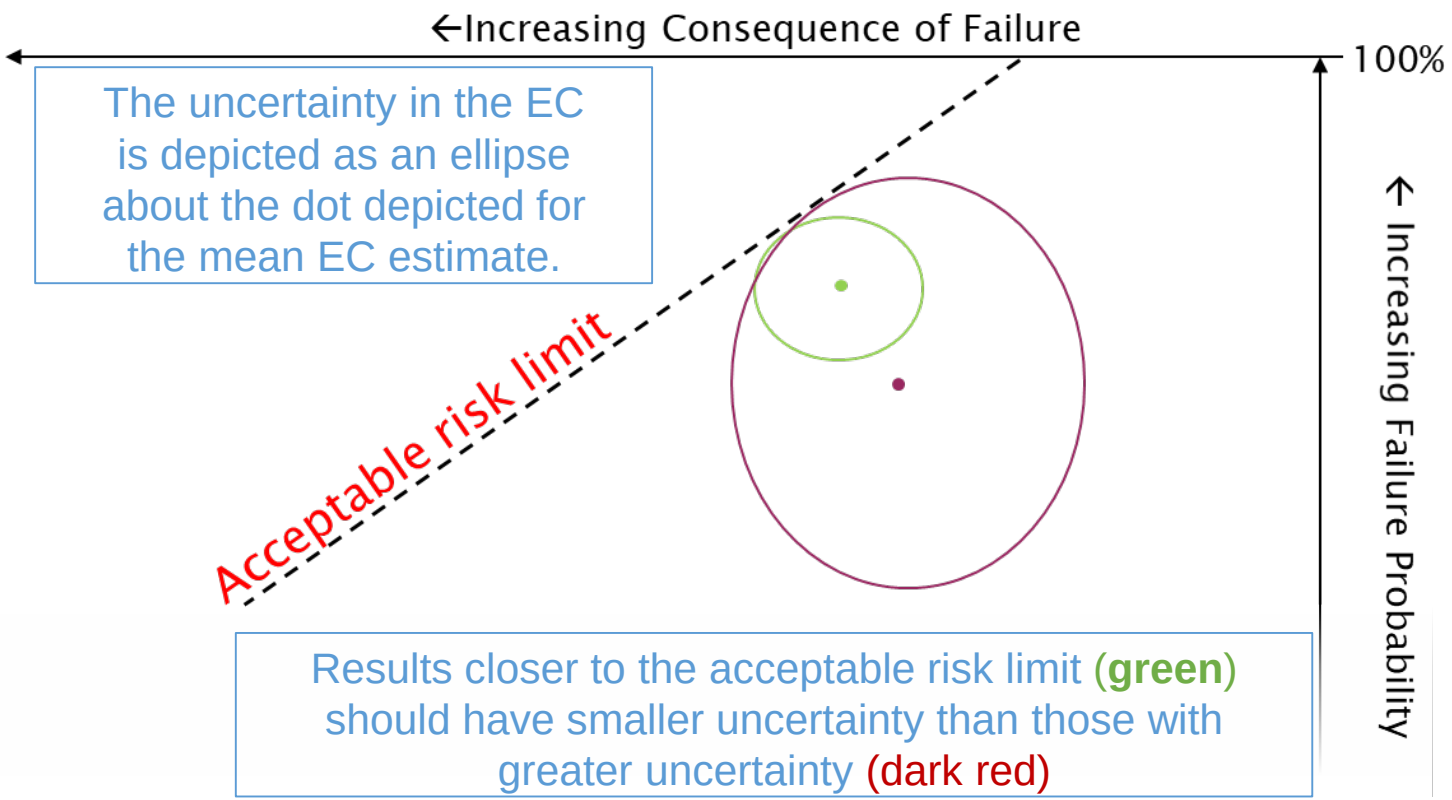
(3) **The rationale for the level of fidelity**;

(4) The evidence for validation and verification required by § 450.101(g);

(5) The extent to which the benchmark conditions are comparable to the foreseeable conditions of the intended operations; and

(6) The extent to which risk mitigations were accounted for in the analyses.

Flight Safety Analysis Methods



The uncertainty in the EC is depicted as an ellipse about the dot depicted for the mean EC estimate.

Results closer to the acceptable risk limit (**green**) should have smaller uncertainty than those with greater uncertainty (dark red)

Explanation and details on how to comply with § 450.115 are included in AC 450.115-1 "High Fidelity Flight Safety Analysis " and AC 450.115-2 "Medium Fidelity Flight Safety Analysis."

Methods that consistently use conservative failure probability estimates produce results with the dot (EC point estimate) at the top edge of the ellipse.

Methods that make conservative consequence estimates (casualty area and population) produce results with the dot (EC point estimate) at the left edge of the ellipse.

Q&A

Trajectory Analysis

Per § 401.7, **nominal** means, in reference to launch vehicle performance, trajectory, or stage impact point, a launch vehicle flight where all vehicle aerodynamic parameters are as expected, *all vehicle internal and external systems perform exactly as planned*, and there are no external perturbing influences other than atmospheric drag and gravity.

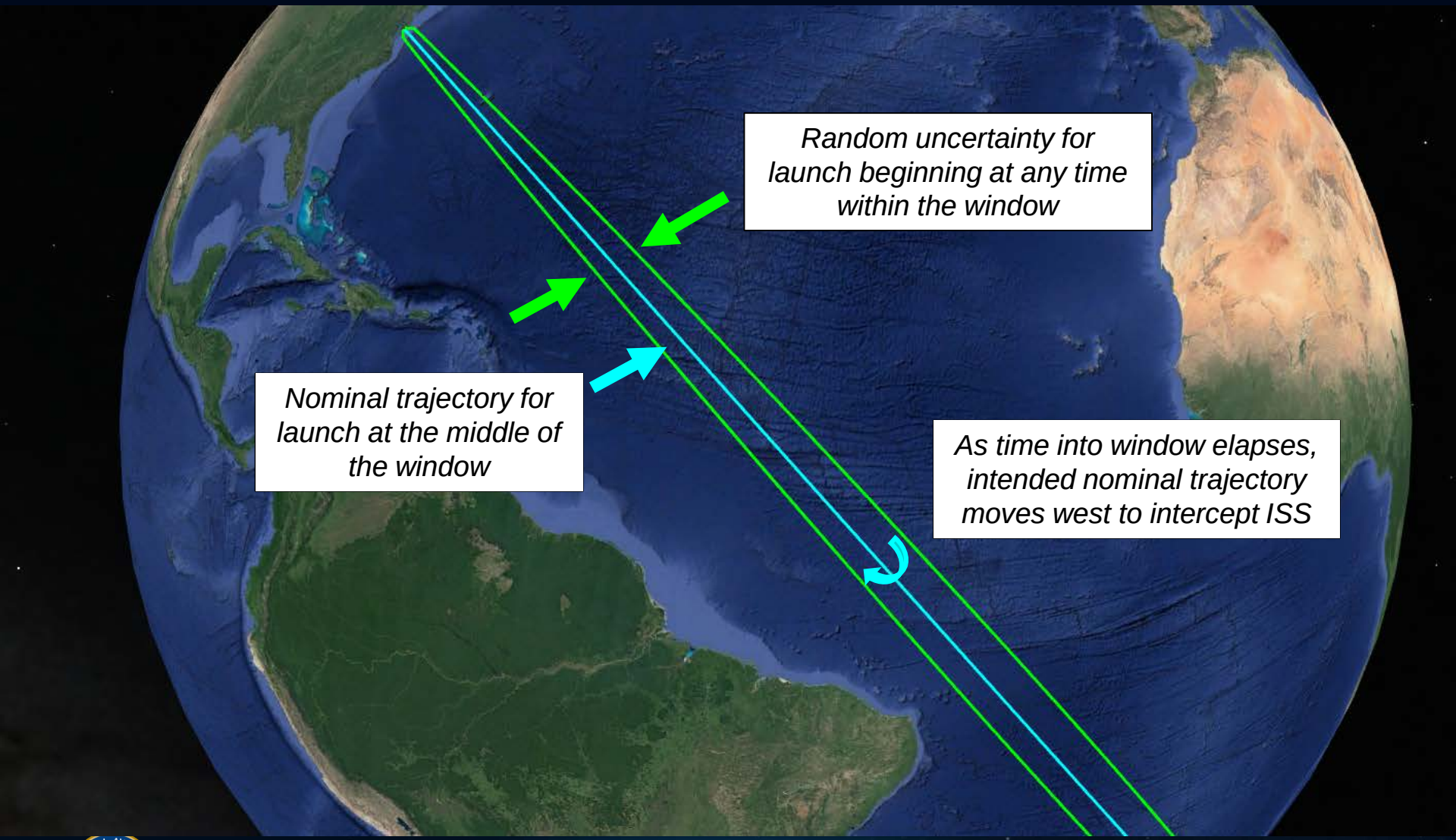
Per § 401.7, **normal flight** is the flight of a properly performing vehicle whose real-time vacuum instantaneous impact point *does not deviate from the nominal vacuum instantaneous impact point by more than the sum of the wind effects and the three-sigma guidance and performance deviations* in the uprange, downrange, left-crossrange, or right-crossrange directions.

- *Variability* describes how the intended trajectory could vary due to conditions known prior to initiation of flight. One example of variability is for ISS missions, where as the launch time into the window elapses, the trajectory must be adjusted to achieve intercept with the ISS. (See illustration on next slide)
- *Uncertainty* is how the actual trajectory could differ from the intended trajectory due to random uncertainties in all parameters with a significant influence on the vehicle's behavior throughout normal flight. This uncertainty accounts for motor performance, weather conditions, thrust offsets, etc.

Per § 401.7, **normal trajectory** means a trajectory that describes normal flight.

A **malfunction trajectory** represents a vehicle's deviation capability in the event of a malfunction during flight. This deviation from normal flight is referred to as **malfunction flight**.

Variability vs Random Uncertainty



Trajectory Analysis for Normal Flight

§ 450.117 specifies the constraints and objectives of analyses sufficient to characterize the trajectory of the vehicle during normal flight.

Generally, the FAA considers "a significant influence" to include any parametric uncertainties within three-sigma that affect the cross-range IIP location or downrange IIP rate by at least one percent because the IIP location and rate is often a convenient surrogate for the potential impact locations of hazardous debris. One percent is a typical threshold value used in RCC 321-20 Standard and Supplement. Thus, the final rule does not intend for applicants to characterize the influence of all random uncertainties or variability, but only those with a significant influence on the potential impact locations for hazardous debris.

§ 450.117 Trajectory Analysis for Normal Flight.

(a) *General*. A flight safety analysis must include a trajectory analysis that establishes, for any phase of flight within the scope as provided by § 450.113(a), the limits of a launch or reentry vehicle's normal flight as defined by the nominal trajectory, and the following sets of trajectories sufficient to characterize variability and uncertainty during normal flight:

(1) A set of trajectories to characterize variability. This set must describe how the intended trajectory could vary due to conditions known prior to initiation of flight; and

(2) A set of trajectories to characterize uncertainty. This set must describe how the actual trajectory could differ from the intended trajectory due to random uncertainties in all parameters with a significant influence on the vehicle's behavior throughout normal flight.

Trajectory Analysis for Normal Flight

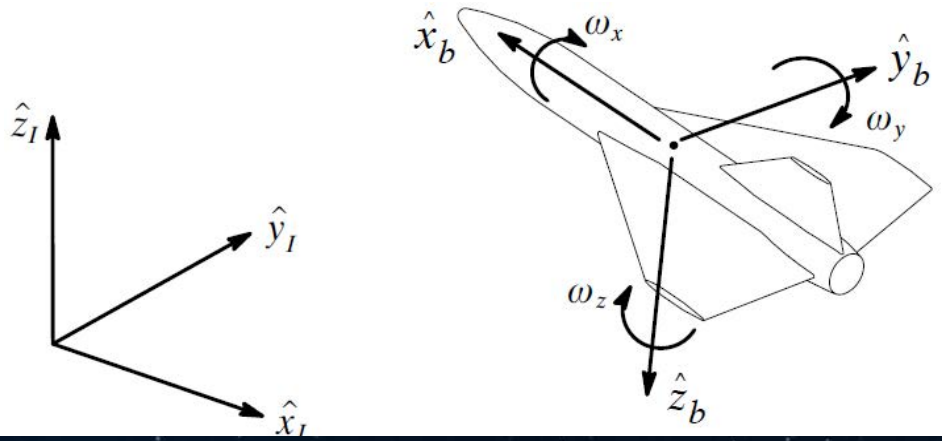
§ 450.117(b) means that normal flight trajectory analyses must account for position, velocity, and orientation of the vehicle because both linear (translational) and rotational motion can affect the public risks.

The FAA recognizes that wind is the primary atmospheric consideration for most vehicles, but, for some (non-traditional) vehicles, other atmospheric parameters such as density, humidity, or temperature may affect trajectory and be part of the flight commit criteria. The final rule expressly refers to all atmospheric conditions in § 450.117(c).

§ 450.117 Trajectory Analysis for Normal Flight.

(b) *Trajectory model.* A final trajectory analysis must use a six-degree of freedom trajectory model to satisfy the requirements of paragraph (a) of this section.

(c) *Atmospheric effects.* A trajectory analysis must account for atmospheric conditions that have an effect on the trajectory, including atmospheric profiles that are no less severe than the worst conditions under which flight might be attempted, and for uncertainty in the atmospheric conditions.



Trajectory Analysis for Normal Flight

Quantitative input data used to model the vehicle's normal flight in six degrees of freedom includes comprehensive sets of aerodynamic and mass properties.

Explanation and details on how to comply with these requirements will be included in Advisory Circular 450.117-1, "Trajectory Analysis." Planned issuance is Q2 2021.

§ 450.117 Trajectory Analysis for Normal Flight

(d) *Application requirements*. An applicant must submit the following:

(1) A description of the methods used to characterize the vehicle's flight behavior throughout normal flight, in accordance with § 450.115(c).

(2) The quantitative input data, **including uncertainties**, used to model the vehicle's normal flight in six degrees of freedom.

(3) The worst atmospheric conditions under which flight might be attempted, and a description of how the operator will evaluate the atmospheric conditions and uncertainty in the atmospheric conditions prior to initiating the operation;

(4) Representative normal flight trajectory analysis outputs, including the position velocity, and orientation for each second of flight for—

(i) The nominal trajectory;

(ii) A set of trajectories that characterize variability in the intended trajectory based on conditions known prior to initiation of flight; and

(iii) A set of trajectories that characterize how the actual trajectory could differ from the intended trajectory due to random uncertainties.

Trajectory Analysis for Malfunction Flight

A malfunction trajectory analysis is necessary to determine how far a vehicle can deviate from normal flight. This analysis helps determine potential impact points in the case of a malfunction and is therefore a vital input for the analyses needed to demonstrate compliance with risk criteria.

An example of a means compliance for § 450.119 will be included in Advisory Circular 450.117-1, "Trajectory Analysis." Planned issuance is Q2 2021.

§ 450.119 Trajectory Analysis for Malfunction Flight.

(a) *General.* A flight safety analysis must include a trajectory analysis that establishes—

(1) The vehicle's deviation capability in the event of a malfunction during flight,

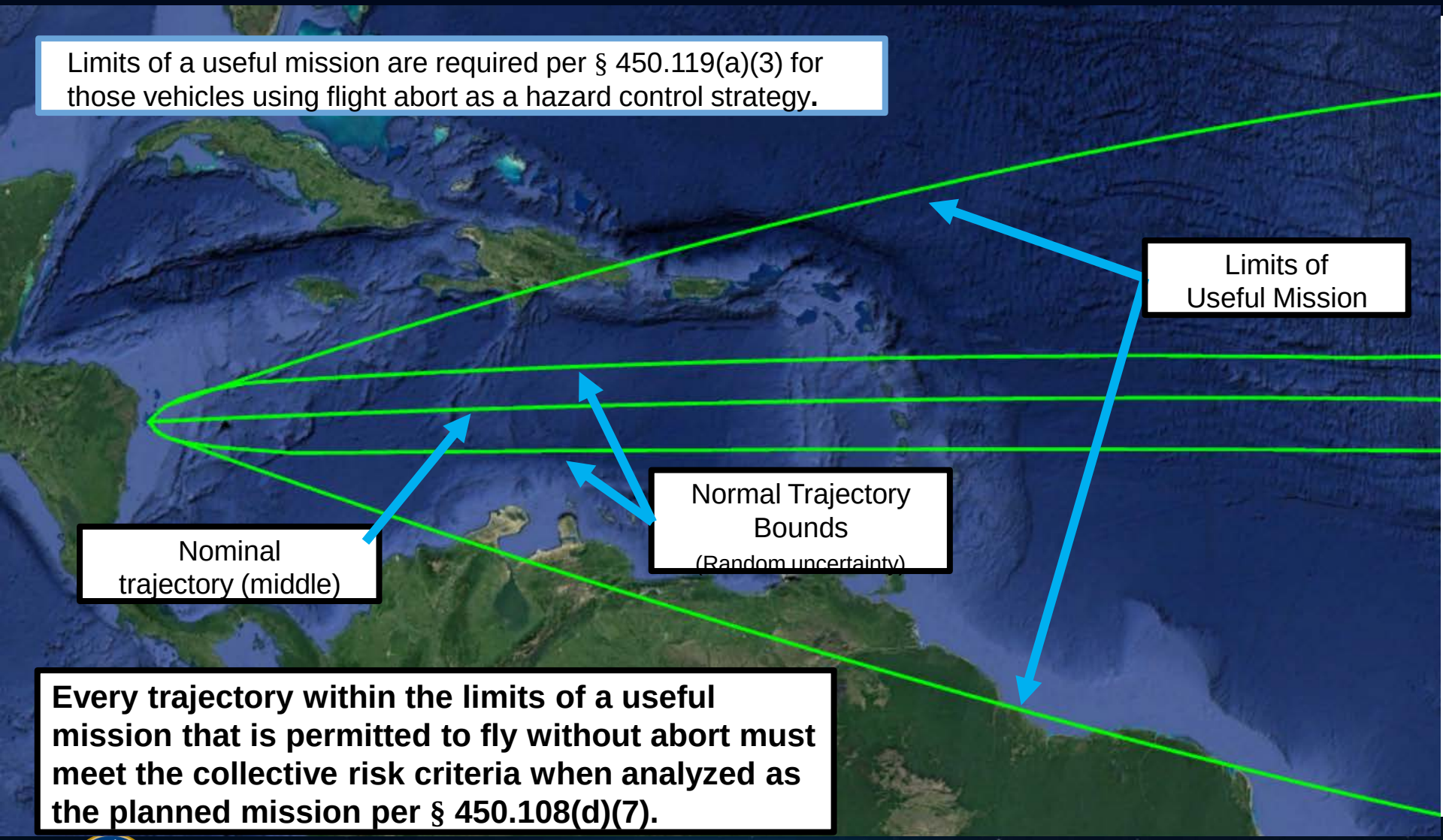
(2) The trajectory dispersion resulting from reasonably foreseeable malfunctions, and

(3) For vehicles using flight abort as a hazard control strategy under § 450.108, **trajectory data or parameters that describe the limits of a useful mission**. The FAA does not consider the collection of data related to a failure to be a useful mission.

(See illustration on next slide)

Limits of a Useful Mission

Limits of a useful mission are required per § 450.119(a)(3) for those vehicles using flight abort as a hazard control strategy.



Every trajectory within the limits of a useful mission that is permitted to fly without abort must meet the collective risk criteria when analyzed as the planned mission per § 450.108(d)(7).

Trajectory Analysis for Malfunction Flight

Malfunction trajectory analysis must account for each cause of a malfunction flight, including software and hardware failures. For each cause of a malfunction trajectory, the analysis is required to characterize the foreseeable trajectories resulting from a malfunction.

§ 450.119(b)(2) intentionally excludes termination due to flight abort so that this analysis will produce complete trajectory data (i.e. data to be able to account for flight abort action and inaction in risk analyses).

§ 450.119 Trajectory Analysis for Malfunction Flight.

(b) *Analysis Constraints*. A malfunction trajectory analysis must account for each cause of a malfunction flight, including software and hardware failures, for every period of normal flight. The analysis for each type of malfunction must have sufficient temporal and spatial resolution to establish flight safety limits, if any, and individual risk contours that are smooth and continuous. The analysis must account for—

(1) The relative probability of occurrence of each malfunction;

(2) **The probability distribution of position and velocity of the vehicle when each malfunction trajectory will terminate due to vehicle breakup, ground impact, or orbital insertion along with the cause of termination and the state of the vehicle**;

(3) The parameters with a significant influence on a vehicle's flight behavior from the time a malfunction begins to cause a flight deviation until the time each malfunction trajectory will terminate due to vehicle breakup, ground impact, or orbital insertion; and

(4) The potential for failure of the flight safety system, if any.

Trajectory Analysis for Malfunction Flight

§ 450.119(c)(3)(iii) is flexible in its application compared to the NPRM because, although it still requires a quantitative description, the regulation permits something other than the statistical distribution

§ 450.119 Trajectory Analysis for Malfunction Flight.

(c) *Application Requirements.* An applicant must submit—

(1) A description of the methodology used to characterize the vehicle's flight behavior throughout malfunction flight, in accordance with § 450.115(c).

(2) A description of the methodology used to determine the limits of a useful mission, in accordance with § 450.115(c).

(3) A description of the input data used to characterize the vehicle's malfunction flight behavior, including:

(i) A list of each cause of malfunction flight considered;

(ii) A list of each type of malfunction flight for which malfunction flight behavior was characterized; and

(iii) A quantitative description of the parameters, including uncertainties, with a significant influence on the vehicle's malfunction behavior for each type of malfunction flight characterized.

(4) Representative malfunction flight trajectory analysis outputs, including the position and velocity as a function of flight time for—

(i) Each set of trajectories that characterizes a type of malfunction flight;

(ii) The probability of each set of trajectories that characterizes a type of malfunction flight; and

(iii) A set of trajectories that characterizes the limits of a useful mission as described in paragraph (a)(3) of this section.

Debris Analysis

In the updated regulation, parts (a) and (b) are very similar to current § 417.211 requirements.

But (c) goes into more detail about the propagation of debris using statistically valid methods.

§ 450.121 Debris Analysis.

(a) *General*. A flight safety analysis must include an analysis characterizing the **hazardous debris** generated from normal and malfunctioning vehicle flight as a function of vehicle flight sequence.

(b*) Vehicle impact and breakup analysis*. A debris analysis must account for:

(1) Each reasonably foreseeable cause of vehicle breakup and intact impact,

(2) Vehicle structural characteristics and materials, and

(3) Energetic effects during break-up or at impact.

Per §401.7, **hazardous debris means** any object or substance capable of causing a casualty or loss of functionality to a critical asset. Hazardous debris includes inert debris and explosive debris such as an intact vehicle, vehicle fragments, any detached vehicle component whether intact or in fragments, payload, and any planned jettison bodies

Debris Analysis

(c) *Propagation of debris*. A debris analysis must compute statistically valid debris impact probability distributions. The propagation of debris from each predicted breakup location to impact must account for—

(1) All foreseeable forces that can influence any debris impact location; and

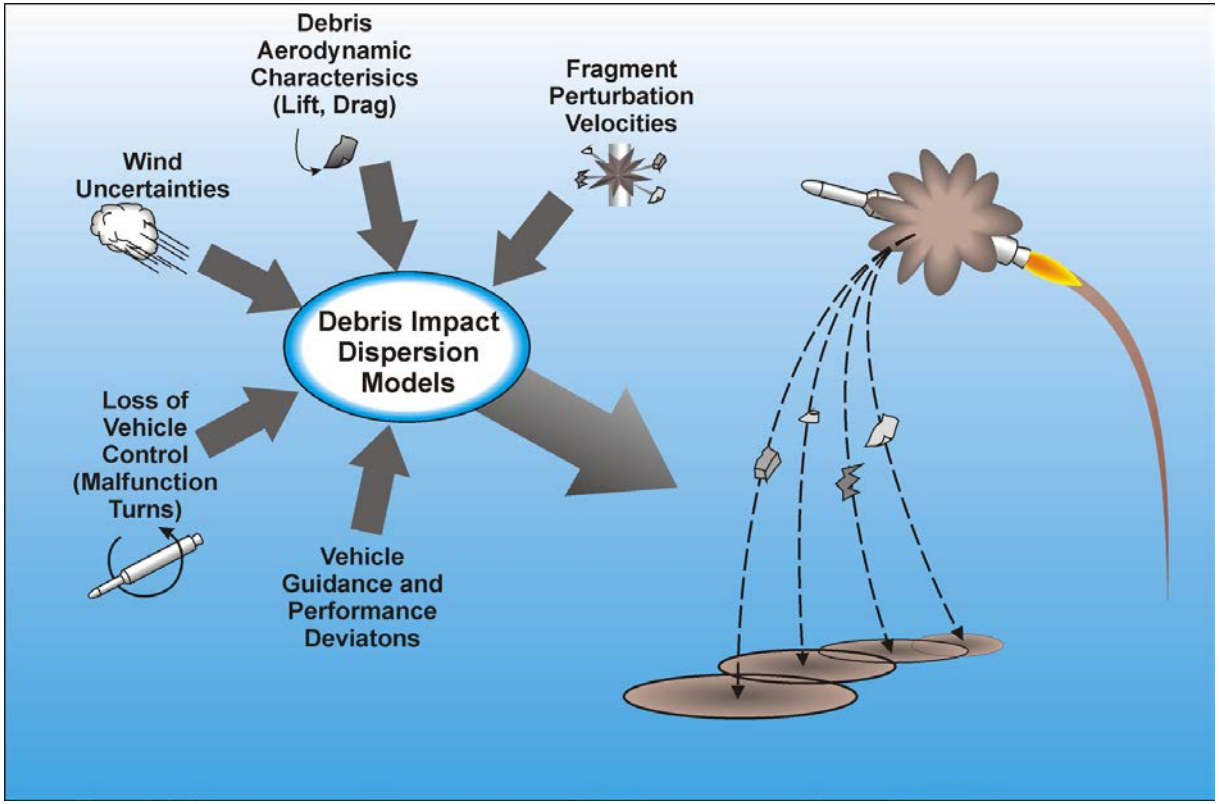
(2) All foreseeable sources of impact dispersion, including, at a minimum:

(i) The uncertainties in **atmospheric conditions**;

(ii) Debris **aerodynamic parameters**, including uncertainties;

(iii) **Pre-breakup position and velocity**, including uncertainties; and

(iv) **Breakup-imparted velocities**, including uncertainties.



Explanation and details on how to comply with these requirements will be included will be included in AC 450.115-1 “High Fidelity Flight Safety Analysis “ and AC 450.115-2 “Medium Fidelity Flight Safety Analysis.”

Debris Analysis

A debris analysis must compute statistically valid debris impact probability distributions. The propagation of debris from each predicted breakup location to impact must account for all foreseeable forces that can influence any debris impact location, and all foreseeable sources of impact dispersion. The FAA notes that a quantitative description of the physical, aerodynamic, and harmful characteristics of hazardous debris is a prerequisite to compute statistically valid debris impact probability distributions and to quantify the risks to the public.

§ 450.121 Debris Analysis.
(d) *Application requirements.* An applicant must submit:

(1) A description of all scenarios that can lead to hazardous debris;

(2) A description of the methods used to perform the vehicle impact and breakup analysis, in accordance with § 450.115(c);

(3) A description of the methods used to compute debris impact distributions, in accordance with § 450.115(c);

(4) A description of the atmospheric data used as input to the debris analysis; and

(5) A quantitative description of the physical, aerodynamic, and harmful characteristics of hazardous debris.

Shuttle Challenger Breaks-up and SRB flies intact

Accounting for Population Exposure

Space flight poses risk to the public

- Debris usually cannot be contained to unpopulated areas
- Debris can cause injuries

To quantify risk, locations of people relative to potential debris impacts must be modeled

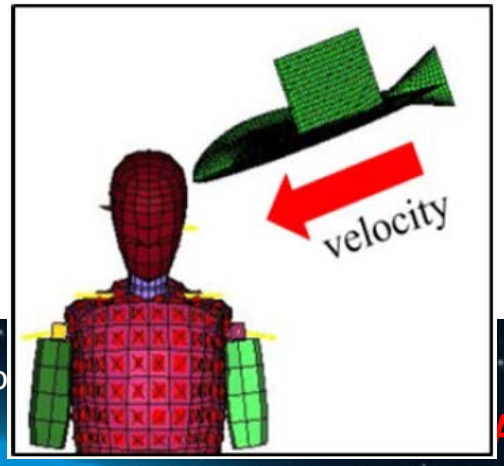
- Model, not data, because there is uncertainty

People are differentially affected if they are inside a building or outside (this is called "sheltering")

- Quantitative model of the vulnerability of people
- Model of the structural response of buildings to debris

450 allows operators to propose impact vulnerability models appropriate for the materials used in their operations.

For example, recent research and development sponsored by the FAA demonstrates that the threshold kinetic energy capable of causing a casualty from a collision with a rigid object is substantially lower than for a collision with an object made of certain composite materials (such as a small UAS).



Population Exposure Analysis

A population exposure analysis must also be used to provide input to other public risk analyses to address toxic hazards and far-field overpressure blast effects, if any.

An exposure model provides critical input data on the geographical location of people and critical assets at various times when the launch or reentry operation could occur

The standard of "significant" means that the scope of the population exposure analysis is bounded by what is necessary to demonstrate compliance with the risk criteria in § 450.101(a) and (b), consistent with the scope requirements set in §§ 450.113 and 450.115.

§ 450.123 Population Exposure Analysis.

(a) *General.* A flight safety analysis must account for the distribution of people for the entire region where there is a significant probability of impact of hazardous debris.

(b) *Constraints.* The exposure analysis must—

(1) Characterize the distribution of people both geographically and temporally;

(2) Account for the distribution of people among structures and vehicle types;

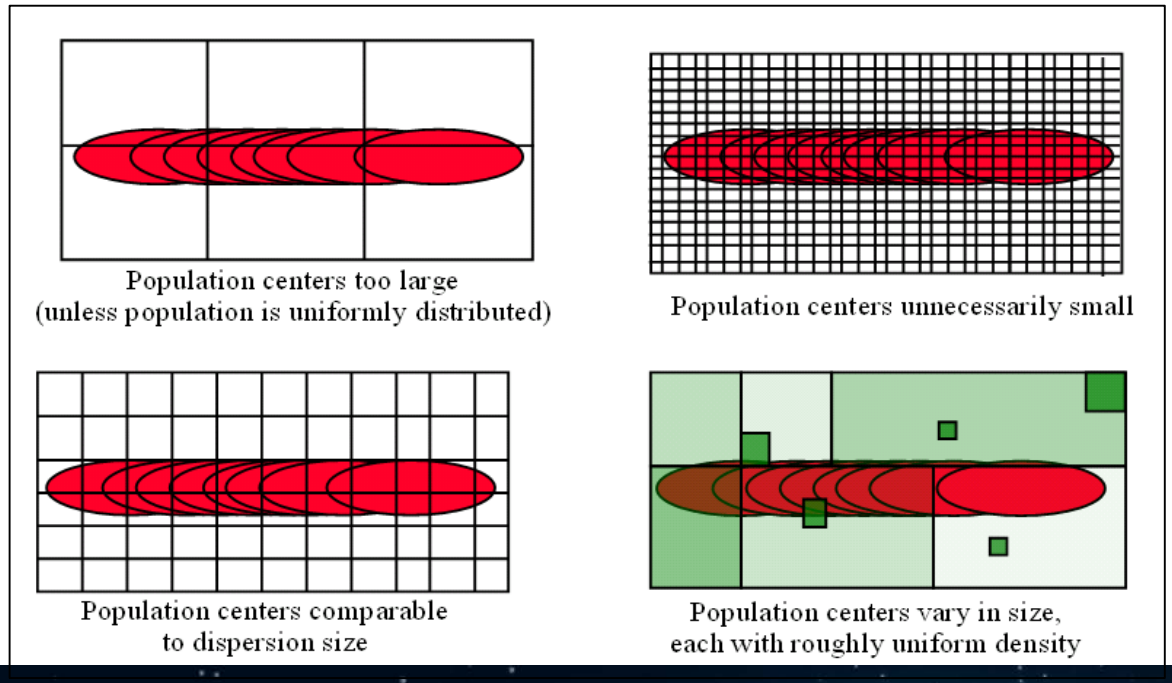
(3) Use reliable, accurate, and timely source data; and

(4) Account for vulnerability of people to hazardous debris effects.

Explanation and details on how to comply with these requirements will be included in "450.123-1, Population Exposure". Planned issuance is Q3 2021.

Population Exposure Analysis

The population exposure analysis must also be used to provide input to other public risk analyses to address toxic hazards and far-field overpressure blast effects, if any. The FAA specifies that the complete population exposure data must be in tabular form



§ 450.123 Population Exposure Analysis.

(c) *Application Requirements*. An applicant must submit:

(1) A description of the methods used to develop the exposure input data in accordance with § 450.115(c), and

(2) Complete population exposure data, in tabular form.

AST Commercial Space Transportation

Go for launch

On Break

Next Session Starts at 2:05 PM EST

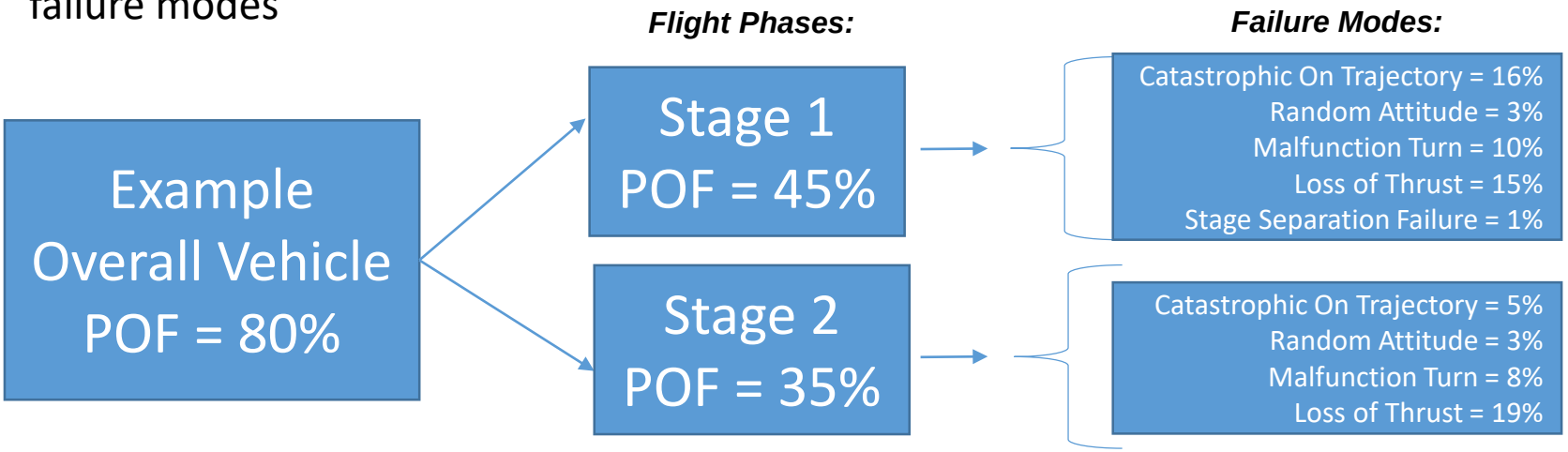
faa.gov/space

Federal Aviation Administration

Probability of Failure Analysis

Background:

- The purpose of a probability of failure (POF) analysis is to characterize the likelihood of hazard generating events that could constitute a threat to people or property
- Two approaches:
  - Top Down: Starting with an overall vehicle or stage POF
  - Bottom Up: Starting as low as individual components, with the overall vehicle POF calculated "upward"
- In either approach, the overall vehicle POF must be distributed across flight phases and failure modes



Probability of Failure Analysis

§ 450.131 codifies performance-based regulations consistent with current practices

Treats POF for first two flights differently than subsequent flights. Historical data shows that manufacturer experience makes a big difference.

Explanation and details on how to comply with these requirements will be included in AC 450.131-1 “Probability Of Failure”. Planned Issuance is Q2 2021.

§ 450.131 Probability of Failure Analysis.

(a) *General*. For each hazard and phase of flight, a flight safety analysis for a launch or reentry must account for vehicle failure probability. The probability of failure must be consistent for all hazards and phases of flight.

(1) For a vehicle or vehicle stage **with fewer than two flights**, the failure probability estimate **must account for the outcome of all previous flights of vehicles developed and launched or reentered in similar circumstances**.

(2) For a vehicle or vehicle stage with **two or more flights,** vehicle failure probability estimates **must account for the outcomes of all previous flights of the vehicle or vehicle stage in a statistically valid manner**. The outcomes of all previous flights of the vehicle or vehicle stage must account for data on any mishap and anomaly.

Probability of Failure Analysis

The probability of failure (POF) must be consistent for all hazards and phases of flight.

The POF should be reasonably conservative.

Here, “consistent” does not mean that the operator can’t vary the POF within a given uncertainty for the same event in different contexts (e.g. stage 1 vs stage 2, or debris vs toxic analysis), in order to be conservative in each case.

§ 450.131 Probability of Failure Analysis.

(a) *General*. For each hazard and phase of flight, a flight safety analysis for a launch or reentry must account for vehicle failure probability. The **probability of failure must be consistent for all hazards and phases of flight**.

(1) For a vehicle or vehicle stage with fewer than two flights, the failure probability estimate must account for the outcome of all previous flights of vehicles developed and launched or reentered in similar circumstances.

(2) For a vehicle or vehicle stage with two or more flights, vehicle failure probability estimates must account for the outcomes of all previous flights of the vehicle or vehicle stage in a statistically valid manner. The outcomes of all previous flights of the vehicle or vehicle stage must account for data on any mishap and anomaly.

Probability of Failure Analysis

For the purposes of § 450.131(c)(1) and (c)(2), a previous flight may include flights conducted outside FAA licensed activity, such as amateur, permitted, U.S. government, or foreign launches, reentries, or flights. A previous flight may also include FAA-licensed activity, such as a static fire anomaly, if the outcome exhibited the potential for a stage or its debris to impact the Earth or reenter the atmosphere outside the normal trajectory envelope during the mission or any future mission of similar vehicle capability.

§ 450.131 Probability of Failure Analysis.

(b) *Failure.* For flight safety analysis purposes, a failure occurs when a vehicle does not complete any phase of normal flight or when any anomalous condition exhibits the potential for a stage or its debris to impact the Earth or reenter the atmosphere outside the normal trajectory envelope during the mission or any future mission of similar vehicle capability.

(c) *Previous flight.* For flight safety analysis purposes—

(1) The flight of a launch vehicle begins at a time in which a launch vehicle lifts off from the surface of the Earth; and

(2) The flight of a reentry vehicle or deorbiting upper stage begins at a time in which a vehicle attempts to initiate a reentry.

Probability of Failure Analysis

A POF analysis must account for the POF during all phases of flight to ensure public safety, including captive carry, unless the exception in § **450.113(b)** applies to that phase.

§ 450.113(b): An operator is not required to perform and document a flight safety analysis for a phase of flight if agreed to by the Administrator based on demonstrated reliability. An operator demonstrates reliability by using operational and flight history to show compliance with the risk criteria in § 450.101(a) and (b).

§ 450.131 Probability of Failure Analysis.

(b) *Failure.* For flight safety analysis purposes, a failure occurs when a vehicle does not complete any phase of normal flight or when any anomalous condition exhibits the potential for a stage or its debris to impact the Earth or reenter the atmosphere outside the normal trajectory envelope during the mission or any future mission of similar vehicle capability.

(c) *Previous flight.* For flight safety analysis purposes—

(1) The flight of a launch vehicle begins at a time in which a launch vehicle lifts off from the surface of the Earth; and

(2) The flight of a reentry vehicle or deorbiting upper stage begins at a time in which a vehicle attempts to initiate a reentry.

Probability of Failure Analysis

A vehicle probability of failure must be distributed across flight times and vehicle response modes.

POF allocation requirements were not specified in 431/415/417.

§ 450.131(d) requirements are consistent with current practices.

§ 450.131(d) requirements focus on the data that must be used and results of the POF analysis, not methods.

§ 450.131 Probability of Failure Analysis.

(d) *Allocation*. The vehicle failure probability estimate must be distributed across flight phases and failure modes. **The distribution must be consistent with**—

(1) The **data available from all previous flights of vehicles developed and launched or reentered in similar circumstances**; and

(2) **Data from previous flights of vehicles**, stages, or components developed and launched, reentered, flown, or tested **by the subject vehicle developer or operator**. Such data **may include previous experience involving similar**—

(i) Vehicle, stage, or component design characteristics;

(ii) Development and integration processes, including the extent of integrated system testing; and

(iii) Level of experience of the vehicle operation and development team members.

Probability of Failure Analysis

The conditional POF assumes the condition that all prior events were successfully completed.

The observed POF accounts for the probability of success for the prior event.

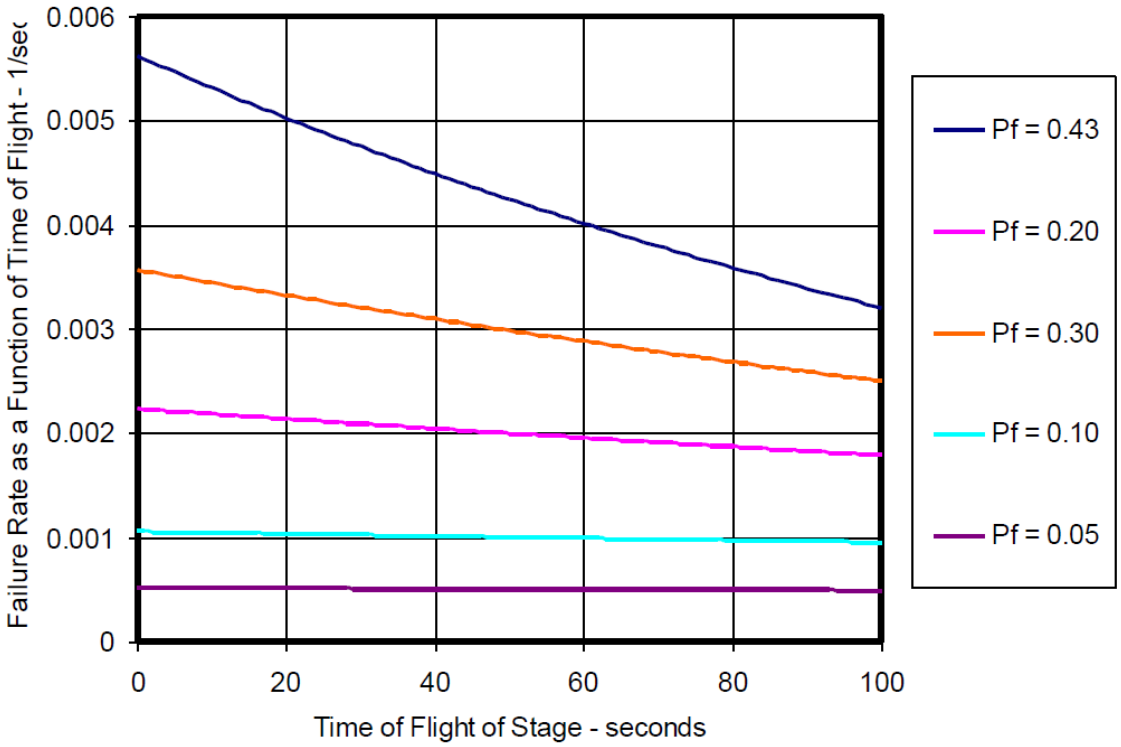
If the overall vehicle or stage POF is below 10%, there generally isn't a significant difference between observed and conditional failure rates.

§ 450.131 Probability of Failure Analysis.

(e) *Observed vs. conditional failure rate.* Probability of failure allocation must account for significant differences in the observed failure rate and the conditional failure rate. A probability of failure analysis must use a constant conditional failure rate for each phase of flight, unless there is clear and convincing evidence of a different conditional failure rate for a particular vehicle, stage, or phase of flight.

Probability of Failure Analysis

- Below illustrates the effect of total POF on the observed failure rate is significant for stages with high failure probabilities:
- For the high failure probabilities, the effect front-loads the POF; a failure is less likely towards the end of the burn because of the likelihood that a failure already occurred earlier in the burn



Probability of Failure Analysis

Section 450.131(f)(1) requires methods used in POF be in accordance with § 450.115(c) because that section sets out the application requirements for all FSA methodologies.

§ 450.131 Probability of Failure Analysis.

(f) *Application requirements*. An applicant must submit:

(1) A description of the methods used in probability of failure analysis, in accordance with § 450.115(c); and

(2) A representative set of tabular data and graphs of the predicted failure rate and cumulative failure probability for each foreseeable failure mode.

More Background Material: *Guide to Probability of Failure Analysis for New Expendable Launch Vehicles*, FAA/AST, November 2005 and "*Probability of Failure Analysis Standards and Guidelines for Expendable Launch Vehicles*" 2013

Flight Hazard Area Analysis

This part specifies requirements for a flight hazard area analysis, including requirements specific to waterborne vessel hazard areas, land hazard areas, and airspace hazard volumes.

Explanation and details on how to comply with these requirements will be included will be included in AC 450.115-1 “High Fidelity Flight Safety Analysis “, AC 450.115-2 “Medium Fidelity Flight Safety Analysis.” and AC 450.133-1 “Airspace and Waterborne Vessel Hazard Areas.”

§ 450.133(a)(6) rationale: planned debris impact should be safe assuming they occur; safety should not be contingent on a failure.

§ 450.133 Flight Hazard Area Analysis.

(a) *General.* A flight safety analysis must include a flight hazard area analysis that identifies any region of **land, sea, or air** that must be surveyed, publicized, controlled, or evacuated in order to control the risk to the public. The analysis must account for, at a minimum—

(1) The regions of land, sea, and air potentially exposed to hazardous debris generated during normal flight events and all reasonably foreseeable failure modes;

(2) Any hazard controls implemented to control risk from any hazard;

(3) The limits of a launch or reentry vehicle’s normal flight, including—

(i) Atmospheric conditions that are no less severe than the worst atmospheric conditions under which flight might be attempted; and

(ii) Uncertainty in the atmospheric conditions;

(4) All hazardous debris;

(5) Sources of debris dispersion in accordance with § 450.121(c); and

(6) **A probability of one for any planned debris hazards or planned impacts**.

More Background Material: RCC 321-20 Supplement (Available for Public Release)

Flight Hazard Area Analysis

Per §401.7, hazardous debris means any object or substance capable of causing a casualty or loss of functionality to a critical asset. Hazardous debris includes inert debris and explosive debris such as an intact vehicle, vehicle fragments, any detached vehicle component whether intact or in fragments, payload, and any planned jettison bodies. (Therefore, includes toxic substances)

§ 450.121(c) describes FSA requirements for propagation of debris.

§ 450.133 Flight Hazard Area Analysis.

(a) *General.* A flight safety analysis must include a flight hazard area analysis that identifies any region of land, sea, or air that must be surveyed, publicized, controlled, or evacuated in order to control the risk to the public. **The analysis must account for, at a minimum**—

(1) The regions of land, sea, and air potentially exposed to hazardous debris generated during normal flight events and all reasonably foreseeable failure modes;

(2) Any hazard controls implemented to control risk from any hazard;

(3) The limits of a launch or reentry vehicle's normal flight, including—

(i) Atmospheric conditions that are no less severe than the worst atmospheric conditions under which flight might be attempted; and

(ii) Uncertainty in the atmospheric conditions;

(4) **All hazardous debris**;

(5) **Sources of debris dispersion** in accordance with § 450.121(c); and

(6) A probability of one for any planned debris hazards or planned impacts.

Flight Hazard Area Analysis

§ 450.133(b)(1), (c)(1), and (d)(1) align FAA regulations with practices at Federal launch/reentry sites by allowing operators to reduce or otherwise optimize the size of the regions for warnings of potential hazardous debris resulting from normal flight events.

97% containment is a change from Part 417's 3-sigma containment.

§ 450.133 Flight Hazard Area Analysis.

(b) *Waterborne vessel hazard areas*. The flight hazard area analysis for waterborne vessels must determine the areas and durations for regions of water—

(1) That are necessary to contain, with 97 percent probability of containment, all debris resulting from normal flight events capable of causing a casualty to persons on waterborne vessels;

(2) That are necessary to contain either where the probability of debris capable of causing a casualty impacting on or near a vessel would exceed 1×10^{-5}, accounting for all relevant hazards, or where the individual probability of casualty for any person on board a vessel would exceed the individual risk criteria in § 450.101(a)(2) or (b)(2); and

(3) Where reduced vessel traffic is necessary to meet the collective risk criteria in § 450.101(a)(1) or (b)(1).

(c) *Land hazard areas*. The flight hazard area analysis for land must determine the durations and areas regions of land—

(1) That are necessary to contain, with 97 percent probability of containment, all debris resulting from normal flight events capable of causing a casualty to any person on land;

(2) Where the individual probability of casualty for any person on land would exceed the individual risk criteria in § 450.101(a)(2) or (b)(2); and

(3) Where reduced population is necessary to meet the collective risk criteria in § 450.101(a)(1) or (b)(1).

Flight Hazard Area Analysis

§ 450.133(b)(2), (c)(2) and (d)(2) use probability of impact contours or probability of casualty contours to meet the risk requirements in § 450.101 for sea, land, and air.

Note again that people on waterborne vessels are now included in collective and individual risk calculations. However, operators may still use the part 417 approach and use the 1E-5 probability of impact contour for ships.

§ 450.133 Flight Hazard Area Analysis.

(b) *Waterborne vessel hazard areas*. The flight hazard area analysis for waterborne vessels must determine the areas and durations for regions of water—

(1) That are necessary to contain, with 97 percent probability of containment, all debris resulting from normal flight events capable of causing a casualty to persons on waterborne vessels;

(2) That are necessary to contain either where the probability of debris capable of causing a casualty impacting on or near a vessel would exceed 1×10^{-5}, accounting for all relevant hazards, or where the individual probability of casualty for any person on board a vessel would exceed the individual risk criteria in § 450.101(a)(2) or (b)(2); and

(3) Where reduced vessel traffic is necessary to meet the collective risk criteria in § 450.101(a)(1) or (b)(1).

(c) *Land hazard areas*. The flight hazard area analysis for land must determine the durations and areas regions of land—

(1) That are necessary to contain, with 97 percent probability of containment, all debris resulting from normal flight events capable of causing a casualty to any person on land;

(2) Where the individual probability of casualty for any person on land would exceed the individual risk criteria in § 450.101(a)(2) or (b)(2); and

(3) Where reduced population is necessary to meet the collective risk criteria in § 450.101(a)(1) or (b)(1).

Flight Hazard Area Analysis

The flight hazard area analysis for airspace only needs to account for reasonably expected air traffic in a given region. A specific altitude isn't stated in the regulation in order to keep it performance based, and account for operations in different regions

§ 450.133 Flight Hazard Area Analysis.

(d) *Airspace hazard volumes*. The flight hazard area analysis for airspace must determine the durations and volumes for regions of air to be submitted to the FAA for approval—

(1) That are necessary to contain, with 97 percent probability of containment, all debris resulting from normal flight events capable of causing a casualty to persons on an aircraft; and

(2) Where the probability of impact on an aircraft would exceed the aircraft risk criterion in § 450.101(a)(3) or (b)(3).

Explanation and details on how to comply with these requirements will be included will be included in AC 450.133-1 Airspace and Waterborne Vessel Hazard Areas. Planned issuance is Q2 2021.

Flight Hazard Area Analysis

§ 450.133 Flight Hazard Area Analysis.

(e) *Application requirements.* An applicant must submit:

(1) **A description of the methodology to be used in the flight hazard area analysis in accordance with § 450.115(c)**, including:

(i) Classes of waterborne vessel and vulnerability criteria employed; and

(ii) Classes of aircraft and vulnerability criteria employed.

(2) Tabular data and graphs of the results of the flight hazard area analysis, including:

(i) Geographical coordinates of all hazard areas that are representative of those to be published, in accordance with § 450.161, prior to any proposed operation;

(ii) Representative 97 percent probability of containment contours for all debris resulting from normal flight events capable of causing a casualty for all locations specified in paragraph (a);

(iii) Representative individual probability of casualty contours for all locations specified in paragraph (a), including tabular data and graphs showing the hypothetical location of any member of the public that could be exposed to a probability of casualty of 1×10^{-5} or greater for neighboring operations personnel, and 1×10^{-6} or greater for other members of the public, given all foreseeable conditions within the flight commit criteria;

(iv) If applicable, representative 1×10^{-5} and 1×10^{-6} probability of impact contours for all debris capable of causing a casualty to persons on a waterborne vessel regardless of location; and

(v) Representative 1×10^{-6} and 1×10^{-7} probability of impact contours for all debris capable of causing a casualty to persons on an aircraft regardless of location.

450.115(c) describe the FSA methodology application requirements

2 sets of contours for waterborne vessels and aircraft are necessary to demonstrate computational resolution and fidelity

Q&A

Debris Risk Analysis

A debris risk analysis must demonstrate compliance with § 450.101.

This analysis can be conducted either prior to the day of the operation or during the countdown.

Any valid debris risk analysis must account for "flight commit criteria and flight abort rules" if such controls are necessary to ensure compliance with the criteria in § 450.101.

Since the debris risk analysis is typically used to identify flight commit criteria and flight abort rules, such as wind constraints, this analysis may be iterative.

§ 450.135 Debris Risk Analysis.

(a) *General*: A flight safety analysis must include a debris risk analysis that demonstrates compliance with safety criteria in § 450.101, either—

(1) Prior to the day of the operation, accounting for all foreseeable conditions within the flight commit criteria; or

(2) During the countdown using the best available input data, including flight commit criteria and flight abort rules.

Example of a means of compliance for § 450.135 can be found in AC 450.115-1 "High Fidelity Flight Safety Analysis " and AC 450.115-2 "Medium Fidelity Flight Safety Analysis."

Debris Risk Analysis

Per § 450.121(c) the debris analysis must compute statistically valid debris impact probability distributions of all hazardous debris, which are key inputs here.

Driven significantly by trajectory dispersion

"Hazardous debris" in § 450.135(b)(3) includes all hazard sources, such as the potential for any toxic or explosive energy releases

§ 450.135 Debris Risk Analysis.

(b) *Casualty area and consequence analysis.* A debris risk analysis must model the casualty area, and compute the predicted consequences of each **reasonably foreseeable failure mode** in any significant period of flight in terms of conditional expected casualties.

The casualty area and consequence analysis must account for—

(1) All relevant debris fragment characteristics and the characteristics of a representative person exposed to any potential debris hazard;

(2) **Statistically-valid debris impact probability distributions**;

(3) **Any impact or effects of hazardous debris**; and

(4) The vulnerability of people to debris impact or effects, including:

(i) **Effects of buildings, ground vehicles, waterborne vessel, and aircraft upon the vulnerability of any occupants**;

(ii) Effect of atmospheric conditions on debris impact and effects;

(iii) Impact speed and angle, accounting for motion of impacted vehicles;

(iv) Uncertainty in input data, such as fragment impact parameters; and

(v) Uncertainty in modeling methodology.

Reasonably Foreseeable Failure Modes

Reasonably foreseeable failure modes may include:

- **On-trajectory explosion**
- **Low thrust / Loss of thrust**
- **Malfunction Turn** Failure - Representative of a TVC hardware failure; describes a condition where the vehicle experiences a thrust vector that is offset from the planned vector alignment with the vehicle body causing the vehicle to enter a turn that deviates from the normal trajectory
- **Random Attitude** Failure - Representative of a GNC System failure, leading the vehicle to assume an alternate trajectory in a controlled fashion and then zero out the rotation forces and fly the new heading to end of powered flight, breakup in atmosphere, or ground impact
  - The GNC system may have been improperly programmed, resulting in an "**Incorrect Azimuth**" failure beginning at T-0
  - The normal trajectory flight fails to execute the pitch-over maneuver to begin turning the vehicle into the downrange direction, resulting in a "**Straight-Up**" failure (for ground launch vehicles)
- **Other relevant failures**

Insufficient thrust to achieve intended trajectory

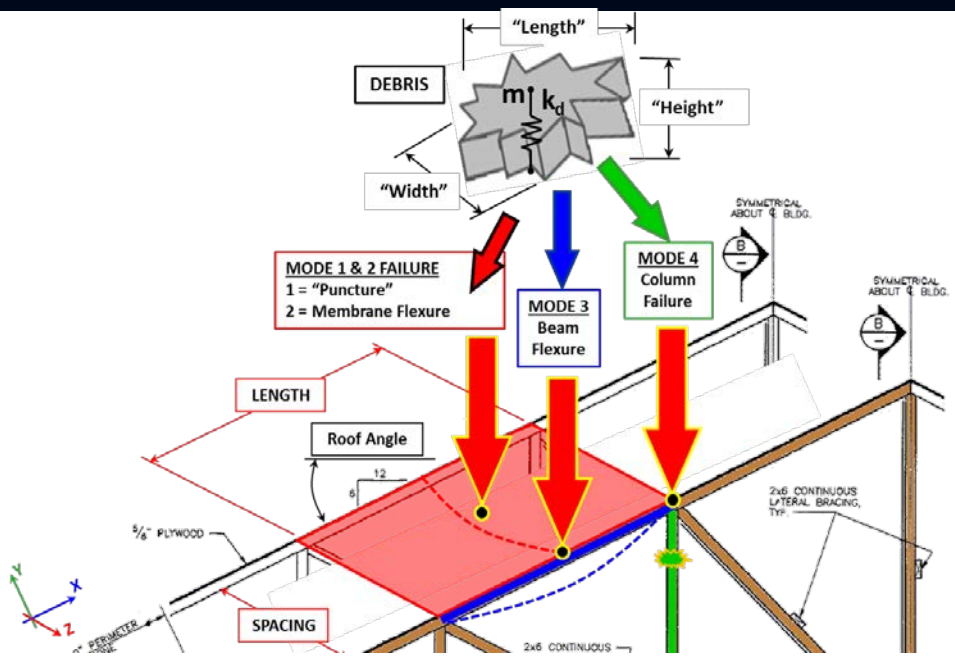
A vehicle knows where it's trying to go, but cannot get there

A vehicle assumes an incorrect guidance target and stabilizes in that direction

A vehicle flies the 'nominal' trajectory in the wrong direction

A Vehicle fails to execute the pitch-over maneuver

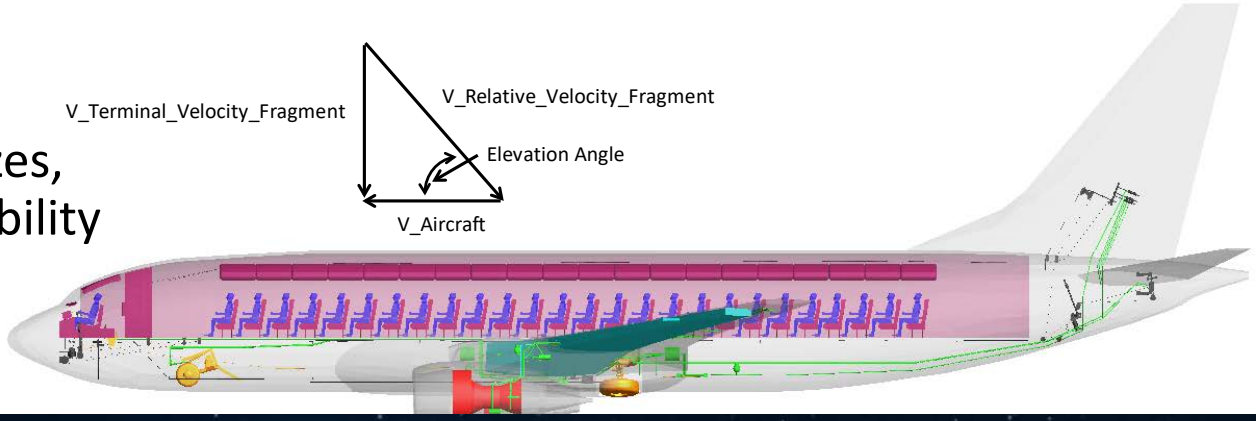
Examples of Important Vulnerability Factors



- **Safety models range from thresholds to probabilistic**

- Variety of roof types affects vulnerability to inert impacts
- Variety of wall and window types affects vulnerability to explosive debris impacts

- Variety of aircraft types, sizes, and speeds affects vulnerability to inert impact



Debris Risk Analysis

§ 450.135(c)(1) requires an operator to describe how they will account for the conditions immediately prior to enabling the operation, such as the final trajectory, atmospheric conditions, and the exposure of people.

(Because the risk criteria must be met given the conditions at the time the operation is initiated per § 450.101(a) and (b)

§ 401.7, **effective casualty area means** the aggregate casualty area of each piece of debris created by a vehicle failure at a particular point on its trajectory.

In reality, the probability of casualty decreases with the distance from say an explosive impact.

The effective casualty area is a modeling construct: the area within which 100 percent of the population are assumed to be a casualty, and outside of which 100 percent of the population are assumed not to be hurt.

§ 450.135 Debris Risk Analysis.

(c) *Application requirements.* An applicant must submit:

- (1) A description of the methods used to demonstrate compliance with the safety criteria in § 450.101, in accordance with § 450.115(c), including **a description of how the operator will account for the conditions immediately prior to enabling the flight of a launch vehicle or the reentry of a reentry vehicle**, such as the final trajectory, atmospheric conditions, and the exposure of people;
- (2) A description of the atmospheric data used as input to the debris risk analysis;
- (3) The effective unsheltered casualty area for all fragment classes, assuming a representative impact vector;
- (4) **The effective casualty area** for all fragment classes for a representative type of building, ground vehicle, waterborne vessel, and aircraft, assuming a representative impact vector;

Debris Risk Analysis

Worst foreseeable conditions means those conditions that produce the highest individual, collective, and conditional risks under which the operator would initiate the operation.

§ 450.135 Debris Risk Analysis.

(c) *Application requirements.* An applicant must submit:

...

(5) **Collective and individual debris risk analysis outputs under representative conditions and the worst foreseeable conditions**, including:

(i) **Total collective casualty expectation** for the proposed operation;

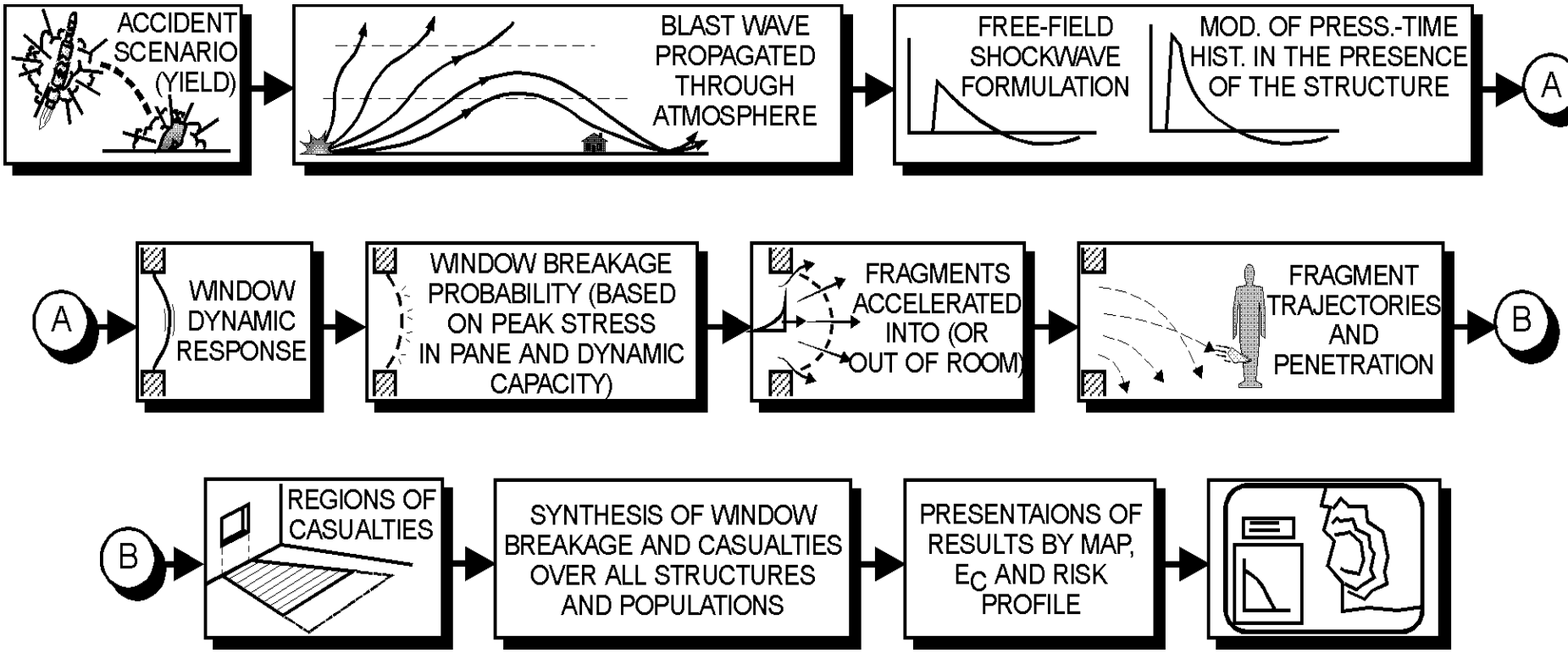
(ii) A list of the **collective risk contribution for at least the top ten population centers** and all centers with collective risk exceeding 1 percent of the collective risk criteria in § 450.101(a)(1) or (b)(1);

(iii) A list of the **maximum individual probability of casualty for the top ten population centers** and all centers that exceed 10 percent of the individual risk criteria in § 450.101(a)(2) or (b)(2); and

(iv) A list of the **conditional collective casualty expectation for each failure mode** for each significant period of flight under representative conditions and the **worst foreseeable conditions**.

Overview of Far-Field Overpressure Risk Analysis

Courtesy of ACTA



Far-field Overpressure Blast Effects Analysis

This analysis can be conducted either prior to the day of the operation or during the countdown.

An ANSI standard provides an easy means to establish no further analysis is necessary based on the max. yield, distance to nearby populations.

Meteorological conditions are known to have a potentially substantial influence on the propagation and attenuation of blast waves with peak incident overpressures at or below 1.0 psi.

Example of a means of compliance for § 450.137 can be found in AC 450.137-1 "Distance Focusing Overpressure Risk Analysis". Planned issuance is Q3 2021.

§ 450.137 Far-field Overpressure Blast Effects Analysis.

(a) *General:* The far-field overpressure blast effect analysis must demonstrate compliance with public safety criteria in § 450.101, either—

(1) Prior to the day of the operation, accounting for all foreseeable conditions within the flight commit criteria; or

(2) During the countdown using the best available input data, including flight commit criteria and flight abort rules.

(b) *Analysis constraints.* The analysis must account for—

(1) The explosive capability of the vehicle and hazardous debris at impact and at altitude;

(2) The potential influence of meteorological conditions and terrain characteristics; and

(3) The potential for broken windows due to peak incident overpressures below 1.0 psi and related casualties based on the characteristics of exposed windows and the population's susceptibility to injury, with considerations including, at a minimum, shelter types, window types, and the time of day of the proposed operation.

Far-field Overpressure Blast Effects Analysis

§ 450.137 Far-field Overpressure Blast Effects Analysis.

(c) *Application requirements*. An applicant must submit a description of the far-field overpressure analysis, including all assumptions and justifications for the assumptions, analysis methods, input data, and results. At a minimum, the application must include:

(1) A description of the **population centers, terrain, building types, and window characteristics** used as input to the far-field overpressure analysis;

(2) A description of **the methods used to compute the foreseeable explosive yield probability pairs**, and the complete set of yield-probability pairs, used as input to the far-field overpressure analysis;

(3) A description of **the methods used to compute peak incident overpressures as a function of distance from the explosion and prevailing meteorological conditions**, including sample calculations for a representative range of the foreseeable meteorological conditions, yields, and population center locations;

(4) A description of the **methods used to compute the probability of window breakage**, including tabular data and graphs for the probability of breakage as a function of the peak incident overpressure for a representative range of window types, building types, and yields accounted for;

(5) A description of the **methods used to compute the probability of casualty for a representative individual**, including tabular data and graphs for the probability of casualty, as a function of location relative to the window and the peak incident overpressure for a representative range of window types, building types, and yields accounted for;

(6) Tabular data and graphs showing the hypothetical location of any member of the public that could be exposed to a probability of casualty of 1×10^{-5} or greater for neighboring operations personnel, and 1×10^{-6} or greater for other members of the public, given foreseeable conditions;

(7) The **maximum expected casualties that could result from far-field overpressure hazards given foreseeable conditions**; and

(8) A **description of the meteorological measurements used as input to any real-time far-field overpressure analysis**.

Toxic Hazards for Flight

In the final rule, the FAA clarifies that operators are not required to perform a toxic release hazard analysis for kerosene-based fuels unless directed by the Administrator.

Example of a means of compliance for § 450.139 can be found in AC 450.139-1 "Toxic Release Hazards Analysis". Planned issuance is Q3 2021.

§ 450.139 Toxic Hazards for Flight.

(a) *Applicability.*

(1) Except as specified in paragraph (a)(2), this section applies to any launch or reentry vehicle, including all vehicle components and payloads, that use toxic propellants or other toxic chemicals.

(2) No toxic release hazard analysis is required for kerosene-based fuels, unless the Administrator determines that an analysis is required to protect public safety.

Toxic Hazards for Flight

§ 450.139(b) requires an operator to conduct a toxic release hazard analysis and manage the risk of casualties from exposure to toxic release either through containing hazards in accordance with § 450.139(d) or by performing a toxic risk assessment, under § 450.139(e), that protects the public consistent with the safety criteria in § 450.101.

Toxic hazard area means a region on the Earth's surface where toxic concentrations and durations may be greater than accepted toxic thresholds for acute casualty, in the event of a worst case release or maximum credible release scenario during launch or reentry.

§ 450.139 Toxic Hazards for Flight

(b) *General*. An operator must—

(1) Conduct a toxic release hazard analysis in accordance with paragraph (c) of this section;

(2) Manage the risk of casualties that could arise from the exposure to toxic release through one of the following means:

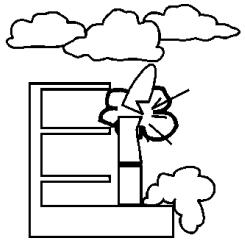
(i) Contain hazards caused by toxic release in accordance with paragraph (d) of this section; or

(ii) Perform a toxic risk assessment, in accordance with paragraph (e) of this section, that protects the public in compliance with the safety criteria of § 450.101, including toxic release hazards.

(3) Establish flight commit criteria based on the results of its toxic release hazard analysis and toxic containment or toxic risk assessment for any necessary evacuation of the public from any toxic hazard area.

Toxic Hazards for Flight

Overview of Toxic Risk Analysis

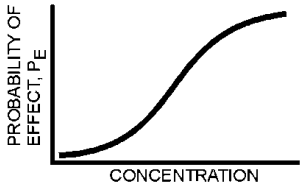


- NOMINAL LAUNCH OR ACCIDENT
- MET CONDITIONS

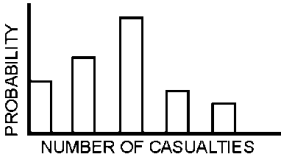
FORMATION AND DISPERSION OF TOXIC CLOUD

CONCENTRATIONS VS. TIME AT RECEPTORS

EXPOSURE-RESPONSE FUNCTIONS



- SUSCEPTIBILITY SUB-POPULATIONS
- SEVERITY LEVELS

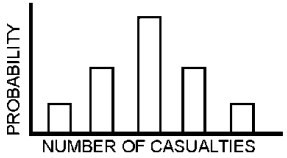


DISTRIBUTION OF NUMBER OF CASUALTIES, GIVEN P_E FOR:

- EACH RECEPTOR
- EACH POPULATION GROUP
- EACH SEVERITY LEVEL

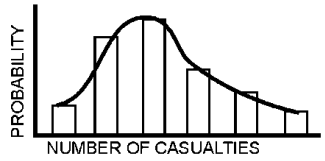
BINOMIAL DISTRIBUTION OR APPROXIMATE BY NORMAL OR POISSON DISTRIBUTION

GENERATE DISTRIBUTION OVER ALL RECEPTORS FOR EACH SCENARIO



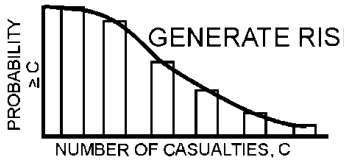
- EACH POPULATION GROUP/ SEVERITY LEVEL
- OVERALL

AGGREGATE OVER THE SCENARIOS TO OBTAIN DISTRIBUTION OF NUMBER OF CASUALTIES FOR THE MISSION



- EACH POPULATION GROUP/ SEVERITY LEVEL
- OVERALL

GENERATE RISK PROFILE



- EACH POPULATION GROUP/ SEVERITY LEVEL
- OVERALL

Toxic Hazards for Flight

§ 450.139(c) set forth the requirements for toxic release hazard analysis.

§ 450.139 Toxic Hazards for Flight

(c) *Toxic release hazard analysis.* A toxic release hazard analysis must—

(1) Account for any toxic release that could occur during nominal or non-nominal flight;

(2) Include a worst-case release scenario analysis or a maximum-credible release scenario analysis for each process that involves a toxic propellant or other chemical;

(3) Determine if toxic release can occur based on an evaluation of the chemical compositions and quantities of propellants, other chemicals, vehicle materials, and projected combustion products, and the possible toxic release scenarios;

(4) Account for both normal combustion products and any unreacted propellants and phase change or chemical derivatives of released substances; and

(5) Account for any operational constraints and emergency procedures that provide protection from toxic release.

Toxic Hazards for Flight

§ 450.139(d) requires an operator to manage the risk of casualty from the exposure to toxic release either by evacuating, or being prepared to evacuate, the public from a toxic hazard area, or by employing meteorological constraints. In either scenario—evacuation or employment of meteorological constraints—the operator would be required to ensure that the public will not be within a toxic area in the event of a worst-case or maximum credible release scenario.

§ 450.139 Toxic Hazards for Flight

(d) *Toxic containment*. An operator using toxic containment must manage the risk of any casualty from the exposure to toxic release either by—

(1) Evacuating, or being prepared to evacuate, the public from any toxic hazard area in the event of a worst-case release or maximum-credible release scenario; or

(2) Employing meteorological constraints to limit an operation to times during which prevailing winds and other conditions ensure that any member of the public would not be exposed to toxic concentrations and durations greater than accepted toxic thresholds for acute casualty in the event of a worst-case release or maximum-credible release scenario.

Toxic Hazards for Flight

§ 450.139 Toxic Hazards for Flight

(e) *Toxic risk assessment.* An operator using toxic risk assessment must establish flight commit criteria that demonstrate compliance with the safety criteria of § 450.101. A toxic risk assessment must—

The toxic risk assessment must account for: airborne concentration and duration thresholds of toxic propellants or other chemicals; physical phenomena expected to influence any toxic concentration and duration.

(1) Account for airborne concentration and duration thresholds of toxic propellants or other chemicals. For any toxic propellant, other chemicals, or combustion product, an operator must use airborne toxic concentration and duration thresholds identified in a means of compliance accepted by the Administrator;

(2) Account for physical phenomena expected to influence any toxic concentration and duration in the area surrounding the potential release site;

(3) Determine a toxic hazard area for the launch or reentry, surrounding the potential release site for each toxic propellant or other chemical based on the amount and toxicity of the propellant or other chemical, the exposure duration, and the meteorological conditions involved;

(4) Account for all members of the public who may be exposed to the toxic release, including all members of the public on land and on any waterborne vessels, populated offshore structures, and aircraft that are not operated in direct support of the launch or reentry; and

(5) Account for any risk mitigation measures applied in the risk assessment.

Toxic Hazards for Flight

§ 450.139 Toxic Hazards for Flight

(f) *Application requirements*. An applicant must submit:

(1) The identity of toxic propellant, chemical, or combustion products or derivatives in the possible toxic release;
(2) The applicant's selected airborne toxic concentration and duration thresholds;
(3) The meteorological conditions for the atmospheric transport and buoyant cloud rise of any toxic release from its source to downwind receptor locations;
(4) Characterization of the terrain, as input for modeling the atmospheric transport of a toxic release from its source to downwind receptor locations;
(5) The identity of the toxic dispersion model used, and any other input data;
(6) Representative results of an applicant's toxic dispersion modeling to predict concentrations and durations at selected downwind receptor locations, to determine the toxic hazard area for a released quantity of the toxic substance;
(7) A toxic release hazard analysis in accordance with paragraph (c) of this section:
  (i) A description of the failure modes and associated relative probabilities for potential toxic release scenarios used in the risk evaluation; and
  (ii) The methodology and representative results of an applicant's determination of the worst-case or maximum-credible quantity of any toxic release that might occur during the flight of a vehicle

Example means of compliance for § 450.139(e)(1) are Acute Exposure Guideline Level 2 (AEGL-2), Emergency Response Planning Guidelines Level 2 (ERPG-2), or Short-term Public Emergency Guidance Level (SPEGL)

Toxic Hazards for Flight

§ 450.139 Toxic Hazards for Flight

(f) *Application requirements*. An applicant must submit:

(8) In accordance with § 450.139 (b)(2),

(i) A toxic containment in accordance with paragraph (d) of this section, identify the evacuation plans or meteorological constraints and associated launch commit criteria needed to ensure that the public will not be within a toxic hazard area in the even of a worst-case release or maximum-credible release scenario; or

(ii) A toxic risk assessment in accordance with paragraph (e) of this section:

(1) A demonstration that the safety criteria in § 450.101 will be met;

(2) The population characteristics in receptor locations that are identified by toxic dispersion modeling as toxic hazard areas;

(3) A description of any risk mitigations applied in the toxic risk assessment; and

(4) A description of the population exposure input data used in accordance with § 450.123.

Q&A

AST Commercial Space Transportation

Go for launch

On Break

Next Session Starts at 3:50 PM EST

faa.gov/space

Federal Aviation Administration

Prescribed Hazard for Safety-Critical Hardware and Computing Systems

Objectives of 450.141

To produce understanding of computing systems and how to make them safe

- Each requirement is designed to drive understanding of an aspect of safe software
- Together, the requirements produce the minimum level of understanding necessary to know that computing systems are safe for the public

To fit with a wide range of development processes

- Each requirement is an integral goal of any safe development process
- Requirements are technology-independent

To work constructively with system safety

- Requirements build on the foundation laid by system safety analyses
- Requirements establish confidence in safe computing system behaviors
- Requirements facilitate understanding of human-computer and computer-hardware interfaces

Definitions

- **Computing system safety item**: Any software or data that implements a capability that, by intended operation, unintended operation, or non-operation, can present a hazard to the public. A computing system safety item often contains several software functions assembled to meet a group of related requirements (e.g. an autonomous flight safety system (AFSS) or GPS)).
- **Degree of control**: A computing system safety item's importance in the causal chain for a hazard, in either causing or preventing the hazard.
- **Level of criticality**: Means the combination of a computing system safety item's importance in the causal chain for a given hazard, which is commensurate to its degree of control, and the severity of that hazard.
- **Safety requirement**: A computing system requirement or software requirement defined for a computing system safety item that specifies an attribute or function that presents, prevents, or is otherwise involved in a hazard to the public.

Context and Structure

Computing system safety "executes" as a subroutine of system safety

- § 450.141 is applicable when software or computing systems are found to present or prevent a hazard to the public
- Derives appropriate risk controls for software and computing systems
- Outputs can be incorporated into system safety analyses

Rule structure:

- § 450.141 (a) identifies computing system safety items, the hazards presented by them, and their degrees of control over those hazards
  - What's important for safety and how important is it?
- § 450.141 (b) identifies, verifies, and validates safety requirements for computing system safety items
  - What does each item need to do to be safe?
- § 450.141 (c) defines development process expectations to limit risk
  - What processes introduce or limit risks?
- § 450.141 (d) lists application data requirements
  - What do I need to submit for a license?

Means of Compliance

AC 450.141-1 has two means of compliance:

1. Tailoring RCC 319-19 or later
   - Recommended for licenses where FSS contains all computing system safety items or operations at federal ranges
   - Tailored version must be tailored during pre-application consultation and included in the application
2. Direct compliance

Safety element approvals and 450.141

- AFSS is a safety element well-suited to use in multiple licensed systems
- Safety element approval may be sought for:
  - Computing system safety items (all parts of 141)
  - Computing system safety processes (for 450.141(b) safety requirement evaluation processes or 450.141(c) development process requirements)

Computing Systems

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

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

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

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

§ 450.141 Computing Systems.

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

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

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

450.141(a) In Practice

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

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

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

- Applicant and FAA should agree on the list of computing system safety items

450.141(a) In Practice

Criticality assessments for each computing system safety item by:

- Severity
- Degree of control

Two potential consequence methods:

1. Public safety consequence categories adapted from MIL-STD-882E
2. Functional Hazard Analysis consequence categories from 450.107 and 109

Five potential degree of control methods:

1. Assume all computing system safety items have highest degree of control
2. RCC 319-19 software categories (safety-critical, support-critical, non-critical)
3. MIL-STD-882E software control categories
4. NASA-GB-8719.13 software control categories
5. Fault tolerance

Computing Systems

Section 450.141(b) requires an operator to develop safety requirements for each computing system safety item.

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

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

§ 450.141 Computing Systems.

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

(1) Identify and evaluate safety requirements for each computing system safety item;

(2) Ensure the safety requirements are complete and correct;

(3) Implement each safety requirement; and

(4) Verify and validate the implementation of each safety requirement by using a method appropriate for the level of criticality of the computing system safety item. For each computing system safety item that is safety critical under § 401.7, verification and validation must include testing by a test team independent of the development division or organization.

450.141(b) In Practice

Computing system safety items implement safety requirements

- Identify safety requirements for each computing system safety item
  - Safety requirements are a subset of software or system requirements
- Validate the safety requirements (complete and correct)
  - Should check that the safety requirements are consistent with the system's safety requirements
  - Should check that the safety requirements fully specify all needed safety functionality
- Implement the safety requirements
  - As normal for computing system requirements
- Verify and validate the implementation of safety requirements
  - Includes IV&V for safety-critical computing system safety items

Computing Systems

The final rule calls for a development "process," rather than a "plan," that achieves the same objectives as a development plan but affords applicants greater flexibility to structure their processes. Operators need not employ a separate development process for each computing system safety item. The development process for each computing system safety item must be appropriate to the level of criticality of the computing system safety item and must satisfy the criteria listed in § 450.141(c), at a minimum

§ 450.141 Computing Systems.

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

(1) Responsibilities for each task associated with a computing system safety item;

(2) Processes for internal review and approval—including review that evaluates the implementation of all safety requirements—such that no person approves that person's own work;

(3) Processes to ensure development personnel are trained, qualified, and capable of performing their role;

(4) Processes that trace requirements to verification and validation evidence;

(5) Processes for configuration management that specify the content of each released version of a computing system safety item;

(6) Processes for testing that verify and validate all safety requirements to the extent required by paragraph (b)(4);

(7) Reuse policies that verify and validate the safety requirements for reused computing system safety items; and

(8) Third-party product use policies that verify and validate the safety requirements for any third-party product.

450.141(c) In Practice

Performance requirements for development processes

- Assignments of responsibility for development tasks, usually by position or title
- Review processes, typically for requirements vetting, implementation, and testing
- Training and qualification process for personnel in safety-related development roles
- Process for tracing requirements to verification and validation evidence
  - Should link each requirement to V&V thereof, enabling verification of a complete safety requirement set
- Configuration management to specify version content per computing system safety item
  - See also 450.103(c)
- Testing process rigor proportional to criticality, with IV&V for safety-critical computing system safety items
- Reuse policy
  - Should define evaluation and testing processes
- Third-party policy
  - Should define acceptance, evaluation, and testing processes

Computing Systems

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

These application requirements need not be met in separate documents.

§ 450.141 Computing Systems.

(d) *Application Requirements*. An applicant must:

(1) Identify and describe all computing system safety items involved in the proposed operations;

(2) Provide the safety requirements for each computing system safety item;

(3) Provide documentation of the development processes that meets § 450.141(c);

(4) Provide evidence of the execution of the appropriate development process for each computing system safety item; and

(5) Provide evidence of the implementation of each safety requirement.

450.141(d) In Practice

Requires documentation of (a-c)

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

Q&A

AST Commercial Space Transportation

Go for launch

End of Day 2

faa.gov/space

Federal Aviation Administration