
FAA
Commercial Space Transportation
faa.gov/space
Flight Abort Hazard Control Strategy
§ 450.108
ASA-210

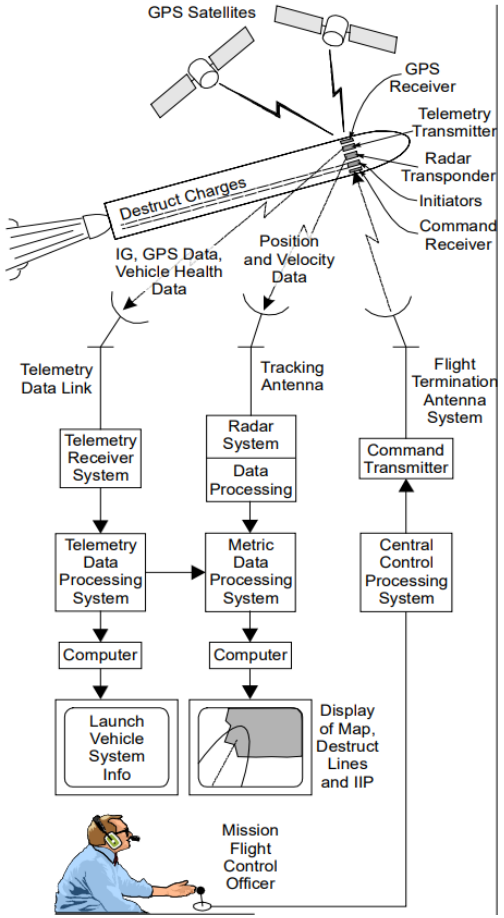
Flight Abort

- Means the process to limit or restrict the hazards to public health and safety and the safety of property presented by a launch vehicle or re-entry vehicle, including any payload, while in flight by initiating and accomplishing a controlled ending to vehicle flight.

- Is typically necessary in orbital launches given the relatively high probability of failure for ELVs, compared to certified aircraft and the potential for a high consequence event given a failure

- Per 450.101(c), an operator sufficiently protects against a high consequence event by:
  - **using flight abort in accordance with § 450.108**
  - demonstrating that CEC is below a certain threshold without any FSS
  - demonstrating sufficient vehicle reliability

- Main Purpose is to
  - prevent **high consequence** events as a result of launch/re-entry vehicle failures
  - ensure that each operation satisfies the public risk criteria



Metric for Consequence

FAA has accepted CEC metric for the consequence as an appropriate means to assess the need for prudent mitigations (such as flight abort) of risks to public safety and the safety of property.

- Both traditional and conditional risk metrics to evaluate the level of rigor required for safety analyses and hazard control strategies, including flight abort and flight hazard analyses.
  - **EC** factors in the probability of occurrence for each reasonably foreseeable dangerous event
  - **CEC** determines the expected casualties assuming the dangerous event will occur
    - Free from the large uncertainties typically associated with the failure probabilities for launch or reentry operations
    - Better quantifies the consequences of an event and is embedded in quantitative risk analysis

CEC threshold of .01:

- DOD/NASA/FAA use quantity-distance limits originally designed to limit conditional individual risk of fatality to 0.01 from inert debris fragment impacts (propelled by accidental explosions)
- USAF/NASA explosive safety standards do not permit public buildings at closer distances than where hazardous debris impacts corresponding to a consequence limit of no more than 0.01 conditional risk of fatality
- The average ground consequence from a general aviation crash is 0.01 conditional expected fatality

CEC is the metric to determine:

1. The need for flight abort with a reliable FSS as a hazard control strategy
2. The reliability standards for any required FSS
3. When to initiate a flight abort

Protection Against a High Consequence Event

Per 450.101(c), an operator sufficiently protects against a high consequence event by:

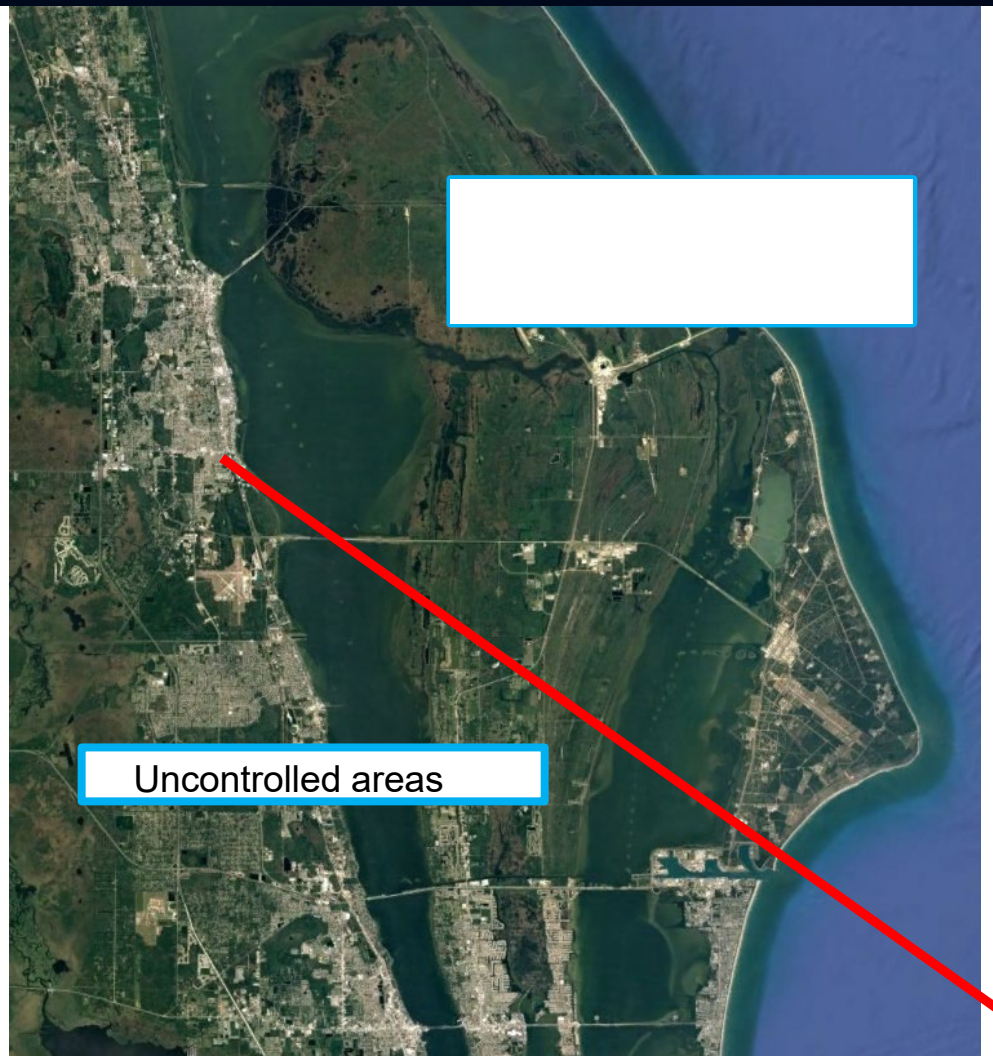
(1) using flight abort in accordance with § 450.108
(2) demonstrating that CEC is below a certain threshold without any FSS, or
(3) demonstrating sufficient vehicle reliability

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

§ 450.108(a), addresses applicability
§ 450.108(b), addresses flight safety system reliability
§ 450.108(c), addresses flight safety limits objectives
§ 450.108(d), addresses flight safety limits constraints
§ 450.108(e), addresses end of flight abort
§ 450.108(f), addresses flight abort rules
§ 450.108(g), addresses application requirements

Uncontrolled Areas

- Some flight abort requirements in 450.108 only apply to “uncontrolled areas”.
- Section 401.7 defines “uncontrolled area”:
  - *“An area of land not controlled by a launch or reentry operator, a launch or reentry site operator, an adjacent site operator, or other entity by agreement.”*
- Operators have more discretion over when flight abort is necessary to protect the public in controlled areas.
- Operators should describe how the controlled area is determined in their 450.108 methodology. AC 450.101-1B has guidance on this.



§ 450.108(a) Applicability

- § 450.101(c) allows for three distinct approaches to providing high consequence event protection:
  - § 450.101(c)(1): *use of flight abort as a hazard control strategy in accordance with § 450.108*
    - This is the subject of the remainder of this workshop
    - In practice, a § 450.108 hazard control strategy is used by operators who cannot demonstrate compliance to this section via (c)(2) or (c)(3).
    - § 450.108(a) is a tieback to § 450.101: ***"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 safety criteria of § 450.101."***
  - § 450.101(c)(2): *ensuring that the consequence of any reasonably foreseeable failure during any significant period of flight is no greater than 1 x 10^{-3} conditional expected casualties*
    - Period of flight would be significant if it is long enough for a mitigation, such as flight abort, to decrease the public risks or consequences materially from any reasonably foreseeable failure mode
  - § 450.101(c)(3): *sufficient demonstrated reliability*
    - The FAA would find certain FSAs not applicable if empirical data sufficiently showed that the demonstrated reliability and estimated public risks of the system are equivalent to general aviation aircraft during a given phase of flight
      - Aircraft-like controllable phases of flight, such as the captive carry phase or for phases with non-rocket powered or glide phases previously authorized under an airworthiness certificate
      - Guidance on demonstrated reliability as a means of compliance is available in AC 450.101-1B

§ 450.108(b) Flight safety system reliability

- FSS required by § 450.108(b)(1) must comply with § 450.145 when the consequence of any reasonably foreseeable failure mode in any significant period of flight is greater than 1x10-2 CEC in uncontrolled areas
  - § 450.145: Highly reliable FSS of design reliability of 0.999 at 95 percent confidence
  - If applicant elects to use a highly reliable FSS, CEC analysis for the purposes of determining FSS reliability under § 450.108(b)(2) is not required, but all other CEC requirements in § 450.108 still apply

- FSS required by § 450.108(b)(2) must comply only with § 450.143 rather than meeting the additional requirements in § 450.145 when the consequence of any reasonably foreseeable failure mode in any significant period of flight is between 1x10-2 and 1x10-3 CEC in uncontrolled areas
  - § 450.143: fault tolerant, fail safe, damage-tolerant, designed such that no fault can lead to increased risk to the public, tested at conditions beyond predicted operating environments, free of defects, free of integration and workmanship errors.

§ 450.119(a)(3) Limits of a Useful Mission

- When flight abort is used as a hazard control strategy, a flight safety analysis must include a trajectory analysis that establishes trajectory data or parameters that describe the limits of a useful mission.
- Limits of a useful mission (LUM) are used to determine when the focus changes from achieving the mission objectives to safely aborting the flight.
- Per 14 CFR 401.7, “Limits of a useful mission” means the trajectory data or other parameters that bound the performance of a useful mission, including flight azimuth limits.
  - Useful mission means a mission that can attain one or more objectives (14 CFR 401.7).
  - The operator decides what is a useful mission and establishes the limits of a useful mission.
  - As stated in 450.119(a)(3), the FAA does not consider the collection of data related to a failure to be a useful mission.

§ 450.108(c) Flight safety limits objectives

- § 450.108(c)(1) requires that operators determine and use flight safety limits that define when an operator must initiate flight abort to ensure compliance with the safety criteria of § 450.101(a) and (b);
  - Specifies the relevant subparagraphs in § 450.101 to which this requirement applies
    - § 450.101(a) and (b) address thresholds for collective risk, individual risk, aircraft risk and critical assets for launch and reentry operations respectively.
    - § 450.101(c) [protection against high consequence events] can be met through use of flight abort as a hazard control strategy, and § 450.101(d) [disposal criteria], (e) [protection of people and assets on orbit], and (f) [notification of planned events] are not relevant to flight abort.

- § 450.108(c)(2) requires that operators determine and use flight safety limits that define when an operator must initiate flight abort to prevent continued flight from increasing risk in uncontrolled areas if the vehicle is unable to achieve a useful mission.
  - AC 450.108-1 states that flight safety limits should consider risks of casualty from any hazard, including debris, toxic release, or explosions, including far-field blast overpressure (FFBO) effects. This is consistent with § 450.115(b)(2).
  - AC 450.108-1 includes guidance on specific flight safety limits including fixed/moving IIP lines, azimuth limits, minimum/maximum limits.
  - Flight safety limits must be placed to ensure the lower-risk strategy is used, per § 450.108(d)(6), whether aborting flight once the vehicle has departed from the limits of a useful mission or allowing the flight to continue, at least until a location is reached where abort would reduce the risk.

§ 450.108(c) Flight safety limits objectives (cont)

- 450.108(c)(3) requires that an operator must determine and use flight safety limits that define when an operator must initiate flight abort 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.
- Similar approach to a gate analysis under 417
  - Primary purpose of gates is to establish safe locations and conditions to abort the flight prior to the vehicle entering a region or condition where it may endanger populated or other protected areas if flight were to continue.
  - For example, the beginning of a period when the vehicle will overfly a major landmass prior to orbital insertion (*e.g.,* Europe, Africa, or South America) or the overflight of large islands with substantial population
- Consequence (CEC >1e-02) may be used to determine if an exposed area should be considered an area of materially increased public exposure
- As described in AC 450.108-1, 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. Examples include:
  - Tank pressure that is higher than the normal operating range and could lead to a rupture
  - Acceleration that is too low and would result in a vehicle failing to reach orbit

§ 450.108(c) flight safety limits objectives (cont)

- 450.108(c)(4) requires that an operator must determine and use flight safety limits that define when an operator must initiate flight abort to prevent conditional expected casualties greater than 1e-02 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 initiating in any significant period of flight
  - Purpose 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.
  - Applies in cases of flight abort and in cases where the vehicle is outside the limits of a useful mission. These cases are combined to compute the CEC.
  - Vehicle failures within the limits of a useful mission are excluded because flight abort cannot prevent a failure from affecting uncontrolled areas that must be exposed to allow a vehicle on a useful mission to continue flight
    - Includes failures from unplanned turn from the nominal trajectory while overflying uncontrolled areas and breaks up aerodynamically before exiting the limits of a useful mission
  - Under § 450.108(c)(4), flight safety limits must not allow CEC greater than 1e-02 unless the consequence resulted from a vehicle within the limits of a useful mission
    - Consequence from on-trajectory failure (OT) or loss of thrust (LOT) could not be mitigated by flight abort without aborting a vehicle on a useful mission
- Flight safety limits must be designed to meet the EC and CEC requirements as described in § 450.108(c)(1) and (c)(4), respectively

§ 450.108(c) Flight safety limits objectives (cont)

- **450.108(c)(5) requires that an operator must determine and use flight safety limits that define when an operator must initiate flight abort to prevent the vehicle state from reaching identified conditions that are anticipated to compromise the capability of the FSS if further flight has the potential to violate a flight safety limit**
  - 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(c)(6) states that, in lieu of meeting § 450.108(c)(2) and § 450.108(c)(4), an operator must determine and use flight safety limits that define when an operator may initiate flight abort to prevent debris capable of causing a casualty due to any hazard from affecting uncontrolled areas using an FSS that complies with § 450.145.**
  - This is to clarify that CEC analysis is not required if an FSS that complies with § 450.145 provides hazard containment
    - 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 1e-02 in uncontrolled areas
  - As stated in the Part 450 Final Rule (85 FR 79566), FAA found that it was unnecessarily restrictive to require designated impact limit lines to bound the area where debris with a ballistic coefficient of three pounds per square foot or more were allowed to impact if the FSS functions properly
    - As evidenced by the need for the FAA to grant waivers to allow innovative missions to proceed safely, such as return of boosters to the launch site
    - However, if an operator satisfies the current requirements in § 417.213, it would meet the requirement in § 450.108(c)(6)

§ 450.108(d) Flight safety limits constraints

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

- 450.108(d)(2) requires that flight safety limits account for the physics of hazard generation and transport including uncertainty.
  - Hazard generation refers to the process by which a vehicle becomes a hazard
    - Direct debris impacts are not the only hazards posed by vehicle failures
      - Example, intact impact of a vehicle may lead to a blast wave or release of toxic propellant, both of which should be considered when developing flight safety limits
  - Transport is how the hazard moves from the source to an exposed person or asset
    - Factors like winds, imparted velocities, uncertainty in mass properties, terrain characteristics should be accounted for when developing flight safety limits.

§ 450.108(d) Flight safety limits constraints (cont)

- § 450.108(d)(3) requires an operator to account for the potential to lose valid data necessary to evaluate the flight abort rules
  - The loss of valid data does not absolve the operator from attempting to meet the flight safety limits requirements in § 450.108(c) and (d)
  - Applicant must determine when flight abort is required if track data used to evaluate the flight abort rules is lost
    - Example: If a vehicle is able to reach a flight safety limit when track data is lost, then a countdown begins that would indicate, upon reaching zero, that a flight safety limit may have been reached and thus command to abort
  - Data loss flight times would not be necessary in phases of flight when an FSS is not required or when a flight safety limit can not be reached

- § 450.108(d)(4) requires that flight safety limits account for the time delay, including uncertainties, between the violation of a flight abort rule and the time when the FSS is expected to activate
  - Time delays are important in a flight safety limits analysis because the decision to abort flight must be made in time to achieve the flight safety limits objectives
    - 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 and properly sampled

§ 450.108(d) Flight safety limits constraints (cont)

- § 450.108(d)(5) requires an operator to determine flight safety limits that account for individual, collective, and conditional risk evaluations both for proper functioning of the FSS and failure of the FSS.
  - The risks from a failed abort must be considered in evaluation of § 450.101(a) and (b) and §450.108(c)(4)
  - Outcomes of malfunction flight where the FSS fails should be included in the residual risk, with a conditional probability of one minus the reliability of the FSS
  - An operator would not be required to perform a conditional risk evaluation if it follows §450.108(c)(6) [containment], because § 450.108(c)(4) [CEC when activating flight abort or CEC outside limits of a useful mission] would not apply
  - Applicant should still assess the collective and individual risk from a failure of the flight safety system

- § 450.108(d)(6) requires that flight safety limits be designed to avoid flight abort that results in increased collective risk to the public in uncontrolled areas, compared to continued flight.
  - Common-sense requirement that taking abort action should not present a higher risk to the public than not taking abort action
  - Best practice is that flight safety limits analysis would minimize all foreseeable consequences, not just those to people on the ground or to the extent necessary to meet the public safety criteria
    - Identify the location for flight safety limits not where an abort would still result in meeting the consequence criteria, but at a location that minimizes the consequence
    - It may not be possible to evaluate every possible location of flight safety limits, but it is possible to evaluate for each malfunction trajectory whether the risks from aborting are equal to or less than the risks from not aborting at all.

§ 450.108(d) Flight safety limits constraints (cont)

- § 450.108(d)(7) requires an operator to ensure any trajectory within the limits of a useful mission that is permitted to fly without abort would meet the collective risk criteria of § 450.101(a)(1) or (b)(1) when analyzed as if it were the planned mission in accordance with § 450.213(b)(2).
  - Requirement allows a non-normal flight to continue if the mission does not pose an unacceptable conditional risk given the present trajectory
    - Example: Incorrect azimuth, degraded thrust that may be included in the limits of useful mission
  - If trajectory does not meet collective, then applicant should implement an abort before the point in flight where the collective risk criteria would be exceeded
  - Applicant is not required to evaluate every possible trajectory within the limits
    - May include the edges of the limits and those identified, by inspection or analysis, that overfly population centers that could result in risks exceeding the criterion
  - DFO and toxic risks are often not relevant for this analysis and nominal values can be used because those effects are more significant early in flight when the envelope of trajectories is small
    - It is most important for examining debris risks when limits of a useful mission are significantly different than normal trajectories
  - At a minimum, account for the collective risk due to planned hazardous debris as well as the potential for on-trajectory failure modes
    - The total failure probability may be allocated to each on-trajectory failure mode; operator should provide evidence why the included failure mode(s) provide conservative results.
    - An operator may distribute the total failure probability across just the on-trajectory failure modes
    - All on-trajectory and off-trajectory failures modes may be considered, retaining their allocations with respect to the mission timeline and relative likelihoods.
  - The allocation with respect to time should be adjusted to correspond correctly to the events of the trajectories chosen to evaluate

§ 450.108(e) End of flight abort

- § 450.108(e) states that a flight does not need to be aborted to protect against high consequence events in uncontrolled areas beginning immediately after critical vehicle parameters are validated, if the vehicle is able to achieve a useful mission and (1) Flight abort would not materially decrease the risk from a high consequence event, and (2) there are no key flight safety events for the remainder of flight.
  - Identifies conditions that, if met, demonstrate a high consequence event is sufficiently mitigated
    - As stated in the Part 450 Final Rule, the FAA finds that meeting the requirements in § 450.108(e) demonstrates sufficient protection against the probability of high consequence events, even though the CEC may exceed the 1e-03 or 1e-02 thresholds during the subject phase of flight
  - Relieves the operator from the requirement to use flight abort in certain situations in which high consequence events are possible but would not be effectively mitigated by an FSS
    - Performing a comparison of the CEC and EC in uncontrolled areas with and without flight abort from each reasonably foreseeable failure mode in any significant period of flight during the subject phase of flight. If flight abort would not reduce the CEC and EC associated with each failure mode materially, then the requirement condition is met
    - Common example of this is when the FSS is safed before downrange overflight because flight abort would not materially decrease risk during the overflight
  - A key flight safety event means a permitted flight activity that has an increased probability of causing a launch accident compared with other portions of flight
    - Engine ignition/shutoff, open-loop to close-loop guidance transition, significant configuration change, max Q-alpha

§ 450.108(f) Flight abort rules

- § 450.108(f)(1) requires that vehicle data required to evaluate flight abort rules must be available to the FSS under all reasonably foreseeable conditions during normal and malfunctioning flight.
  - It is important that applicant identify potential flight safety limit types, based on system capabilities
  - Verify that the system can support the rules, if the abort decision is not on the vehicle, then the communication of an abort signal to the vehicle must be ensured
    - Each rule should be validated following a testing plan to ensure that their implementation within software or incorporation with hardware systems is functional
    - For telemetry data, the ability of the ground station to receive the data, including geometry considerations and atmospheric and plume attenuation effects should be accounted for
    - Ensure that the uncertainty in the measurements does not pose an unacceptable possibility of rule violation for an acceptable useful mission

- § 450.108(f)(2)(i) requires that the FSS must abort flight when valid, real-time data indicate the vehicle has violated any flight safety limit developed pursuant to 450.108
  - Define when a flight abort must be initiated in terms of real time tracking parameters to achieve objectives

§ 450.108(f) flight abort rules (cont)

- § 450.108(f)(2)(ii) requires that the FSS must abort flight when the vehicle state approaches identified conditions that are anticipated to compromise the capability of the FSS and further flight has the potential to violate a flight safety limit
  - This requirement is used in conjunction with the flight safety limits objective in § 450.108(c)(5) [initiate flight abort when reaching an environment may lead to FSS failure]
  - Not limited to just system safety analysis to determine which failure modes can compromise the capability of the FSS.
    - FSS survivability analysis or a link analysis for a command destruct architecture may identify conditions anticipated to compromise the capability of the FSS

- § 450.108(f)(2)(iii) requires that the FSS must abort flight in accordance with methods used to satisfy § 450.108(d)(3) if tracking data is invalid and further flight has the potential to violate a flight safety limit.
  - For example, incorporate data loss flight times to abort flight at the first possible violation of a flight safety limit, or earlier, if valid tracking data is insufficient for evaluating a minimum set of flight abort rules required to maintain compliance with proposed § 450.101.
  - This is the implementation of the flight safety limit developed to meet the constraint in § 450.108(d)(3)

§ 450.108(g) Application Requirements

(1) A description of the methods used to demonstrate compliance with paragraph (c) of this section, including descriptions of how each analysis constraint in paragraph (d) of this section is satisfied in accordance with § 450.115 ***[Next few slides]***

(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) of this section 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.

450.108 (g)(1) Description of method used to demonstrate compliance

450.115 (c)(1) Scientific Principles and Statistical Methods

- **Examples of flight abort related scientific principles and statistical methods that may be documented in the operator's description of method:**
- **Flight Rule generation – Fixed vs moving termination limits**
  - Convex polygon "hull" algorithms, determination of activation parameters and other quantitative criteria
- **Flight Rule detection – Present position vs Instantaneous impact point**
  - Statistical modeling approach to account for position and velocity uncertainty
  - Propagation method, vacuum/drag corrected propagation of IIPs
- **Time delay analysis – mean and uncertainty distribution for the elapsed time of FTS response**
  - MFCO reaction time, premature separation system, detonation delay, thrust termination, AFSS persistence
    - Gaussian distribution, general probability density function, cumulative distribution function
- **FTS induced breakup hazardous debris – Breakup mechanism for a liquid vs solid motor**
  - Debris characteristics due to design and placement of the particular detonation system.
  - Accounting for energetic effects of fuel remaining, ullage, pressure chamber, geometry of solid fuel, aerodynamics
- **Propagation of debris/Distribution of impacts – all fragments capable of causing a casualty**
  - Vacuum propagator accounting for all foreseeable forces that can influence any debris impact
  - Probability density distribution of debris impacts at 97% confidence
    - Statistics/thresholds used to expand hazard area surrounding fragment impacts where casualty is possible to account for roll of an inert fragment or the blast wave from an explosive fragment
    - Method use to demonstrate debris containment (or not)
  - Assessing risk, including CEC

450.108 (g)(1) Description of method used to demonstrate compliance

450.115 (c)(2) All assumptions and their justifications

- **Many assumptions go into modeling approximations, impact conditions, flight rule derivation, human/software & hardware response. Examples:**
  - Determine buffers, MFCO reaction time, wind effects
  - Failure modes that can potentially violate a flight safety limit
  - Determining trajectories that compose the limits of a useful mission
  - Satisfying 450.108(d)(7) when treating any trajectory within LUM as the planned mission
    - Failures accounted for, POF distribution
  - Debris propagation, assessing residual risk
  - Compute durations of acceptable data loss, satisfying § 450.108(d)(3)
  - Debris generation after FTS action
    - FTS detonation (structural limit, crack propagation, fuel mixing, breakup delays)
    - Residual thrust and vehicle response after thrust termination
      - Vehicle self breakup, intact impact

- **All assumptions and their justifications must be documented in the operator description of method, in accordance with § 450.115(c). Below is an example of what acceptable operator documentation could look like:**

Assumption	Justification
5 second response time from the moment violation occurs to MFCO sending functions	Typical reaction time use in range safety analysis for command missions
OT and LOT failures sufficient to validate LUMs against 450.101 safety criteria. Mission POF distributed proportionally between failure modes.	Based on launch history, OT and LOT are the most likely failure modes. Conservative to distribute all POF onto these failure modes.
Capping maximum green number to a certain value	Unlikely that lost track will recover after a given time
Downrange weather data will be based on the Global Gridded Upper Atmosphere Statistics (GGUAS) weather database for the intended launch month	Best available weather data for launch operations. Consistent with current analysis approach for launches from federal ranges.

450.108 (g)(1) Description of method used to demonstrate compliance

450.115 (c)(3) The rationale for the level for fidelity

- **§ 450.115(b)(1) requires the operator to account for all known sources of uncertainty in the flight safety analysis used to verify compliance with § 450.101(a)(1) or (b)(1).**
- **Sources of uncertainty should be considered when developing level of fidelity rationale to comply with § 450.115(c)(3)**
- **Examples of FSA levels of fidelity that may be relevant to § 450.108**
  - Placement of flight safety limits
    - High fidelity analysis may be necessary for launch area, overflight of population where there is an inability to contain debris or there is potential for high consequence events
    - Lower fidelity analysis may be used for over ocean exposed areas where analysis shows that the hazard footprint from flight abort would not reach uncontrolled areas
  - Structural capacity of the vehicle determining breakup at FTS action, breakup during free fall or Intact impact
    - High fidelity analysis may be necessary to demonstrate vehicle will breakup at FTS activation and/or during free fall
    - Alternatively risk results from all breakup scenarios (including intact impact) could be unioned for conservatism
  - Debris list
    - High fidelity (vehicle specific derived via FEA & CFD) may be necessary for areas of high consequence or significant risk exposure to the public or critical assets
    - Lower fidelity (such as “maximum risk” list from similar vehicles and flight termination system) may be acceptable for low population remote areas, or a set of different fragments types and aerodynamic characteristics to demonstrate containment
  - Propagation of hazardous debris
    - Atmospheric conditions and uncertainty considerations at time analysis is performed, validation at DOL
    - 3dof vs 6dof modeling (position & velocity vectors and debris orientation considerations)

450.108 (g)(1) Description of method used to demonstrate compliance

450.115 (c)(4) *The evidence for validation and verification per 450.101(g)*

- **Flight safety limits are often developed using the same codes as those used for trajectory and risk analyses**
  - Evidence of validation and verification may be documented V&V for commercial or Government software.
  - For codes developed by the applicant, comparisons to manual calculations, other codes, etc.

- **For automated flight safety system (AFSS) an applicant should present evidence of validation and verification of Mission Data Load (MDL) to demonstrate that the flight rules incorporated into the system behave as analyzed in the FSA**
  - Telemetry data, the ability of the ground station to receive the data, including geometry considerations and atmospheric and plume attenuation effects should be accounted for
  - Ensured that the uncertainty in the measurements does not pose an unacceptable possibility of rule violation for an acceptable useful mission
  - Validated following a testing plan to ensure that their implementation within software or incorporation with hardware systems is functional, verify that system can support the rules including validation of critical parameters.
    - Testing of software should be performed in accordance with AC 450.141-1
  - Verifying that limits are not increasing risk by inspection and/or numerical analysis (conditional risk)
    - Conditional risk for each trajectory should be equal to or less than allowing flight to continue

450.108 (g)(1) Description of method used to demonstrate compliance

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

- **Documented case of flight abort using flight safety limits developed using the applicant's methods that resulted in achieving the flight safety limits objectives**
  - These cases may be rare and of limited scope
- **Comparison of flight safety limits developed using the applicant's methods to those developed by an accepted Federal entity for the same or a similar mission.**
  - The extent to which this benchmark would be comparable to the intended operation would be relative to the similarity of the missions that the Federal entity and the applicant analyzed.
  - The applicant should explain how the comparison is a useful benchmark, as there may be many flight safety limit solutions that would meet 108(c) and (d).

450.108 (g)(1) Description of method used to demonstrate compliance

450.115 (c)(6) *The extent to which risk mitigations were accounted for in the analyses*

- **Examples of flight abort related risk mitigations that may be identified in the operator's description of method**
  - Accounting for the potential to lose valid data necessary to evaluate flight data rules
  - Redundant FTS design
    - Use of multiple receivers & sensors and other hardware/software
  - Use of less common flight safety limits
    - Prevention of intact impacts, fuel venting
    - Fixed minimum altitude
    - Azimuth limits
  - Restricting limits of a useful mission
  - Inclusion of risk from FTS failure
  - Use of generous buffers between debris footprints (resulting from FTS action) and populated uncontrolled & controlled areas

End of 450.108

Q&A

Advisory Circular 450.108-1

FAA
Commercial Space Transportation
faa.gov/space

AC 450.108-1 Overview

AC organization

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

Expanded discussion of two key terms

- Debris footprint
- Hazard footprint

} Useful constructs for developing abort rules

Explanation of statistical meaning of footprint

Chapter 13 – Means of Compliance

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

- A step-by-step approach that provides a method to achieve the requirements.
- May be applied to a single flight or a series of similar flights

    Some steps may apply for all flights of a vehicle

Chapter 13 – Means of Compliance (cont)

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

Chapter 13 – Means of Compliance (cont)

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

Chapter 13 – Means of Compliance (cont)

7. **Determine candidate quantitative parameters for flight safety limits**
   - This is a complicated step, AC 450.108-1 provides a defined process that operators can use for what has been a qualitative, approximate exercise
   - This section provides definitions for each type of limit and a process for developing the parameters for each
   - Normally a subset of limits are used
8. **Define conditional limits, if needed**
   - Conditional limits come in different types depending on the geometry of the exposed population to the mission
   - Two key steps:
     - Determining the conditional limit evaluation trigger(s)
     - Establishing the ranges for critical vehicle parameters

Chapter 13 – Means of Compliance (cont)

9. **Validate the system can support the rules**
   - For ground-based systems, verify that communication will be maintained
   - Ensure that uncertainty is not too large
   - Test implementation in software
10. **Verify risk reduction**
   - Confirm 450.108(d)(6) is satisfied, either by inspection or numerical analysis

Chapter 13 – Means of Compliance (cont)

11. **Assess residual risk**

    Perform flight safety analysis to ensure that E_C and CE_C criteria are satisfied

        P_C is managed by hazard areas

12. **Compute durations of acceptable data loss**

    This is complex, because many data loss scenarios are not connected to malfunction flight, but some have common-cause with malfunction

    Also complicated because the problem is a lack of knowledge – have to consider what the vehicle could be doing

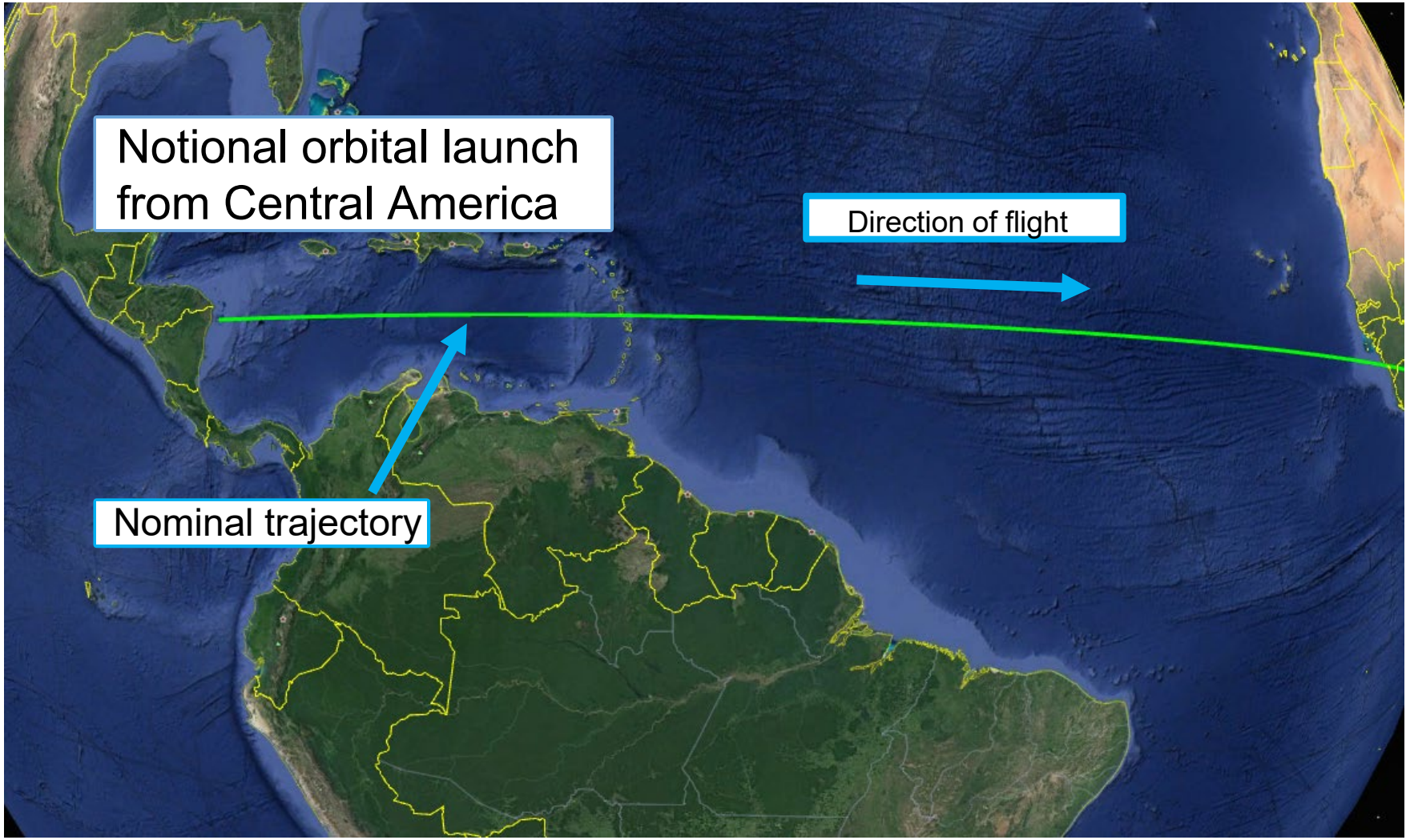
End of AC 450.108-1

Q&A

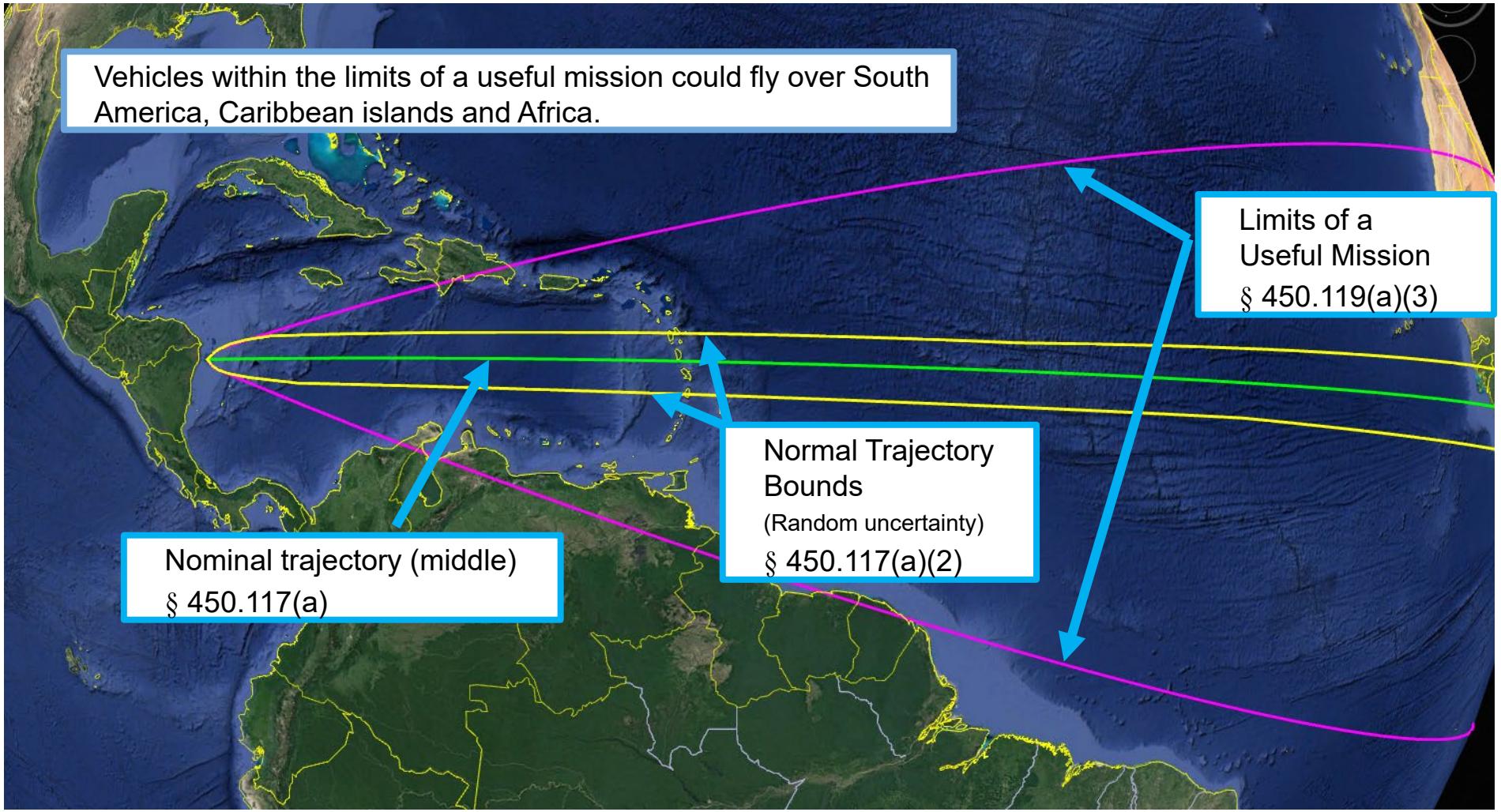
Example

FAA
Commercial Space Transportation
faa.gov/space

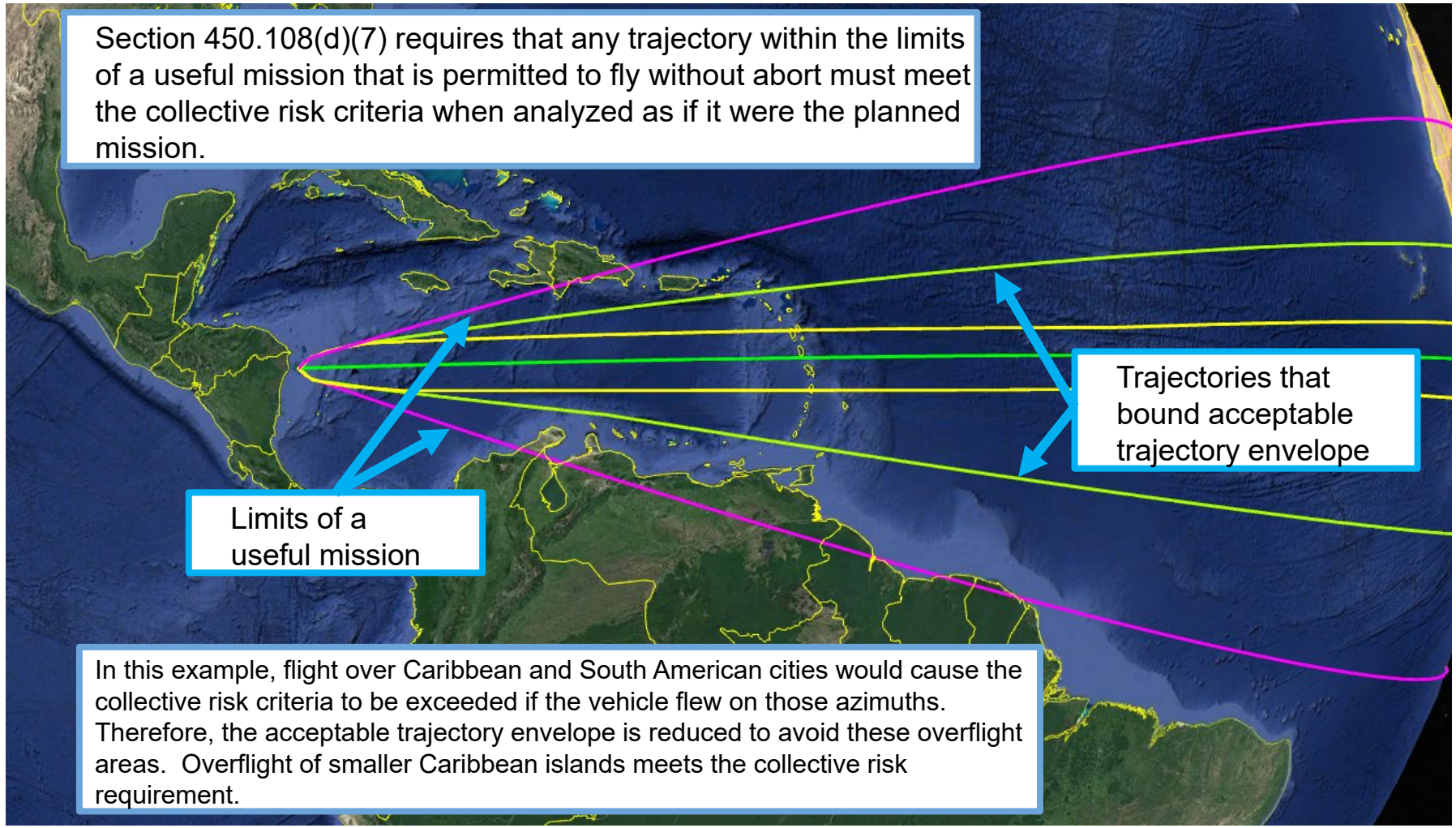
Example Mission Overview



Example Limits of a Useful Mission



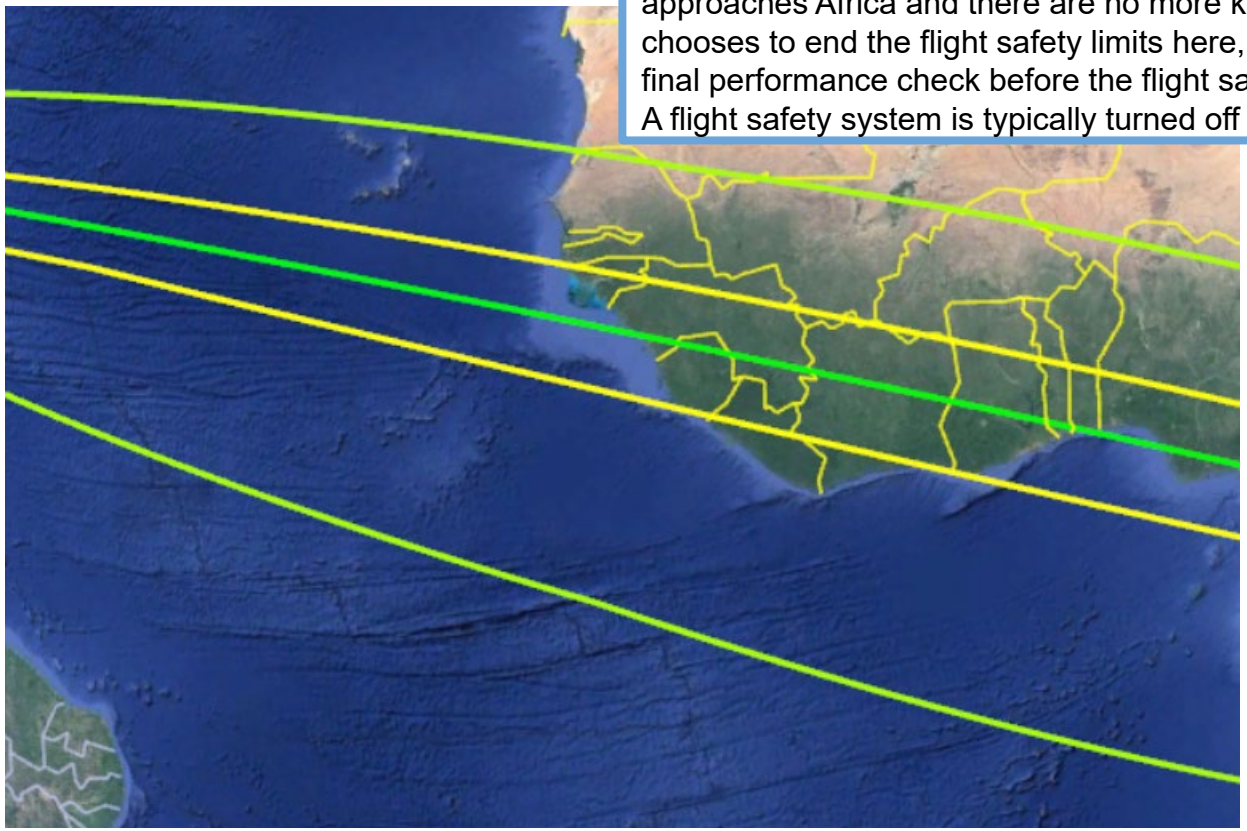
Acceptable Limits of a Useful Mission



End of Flight Abort

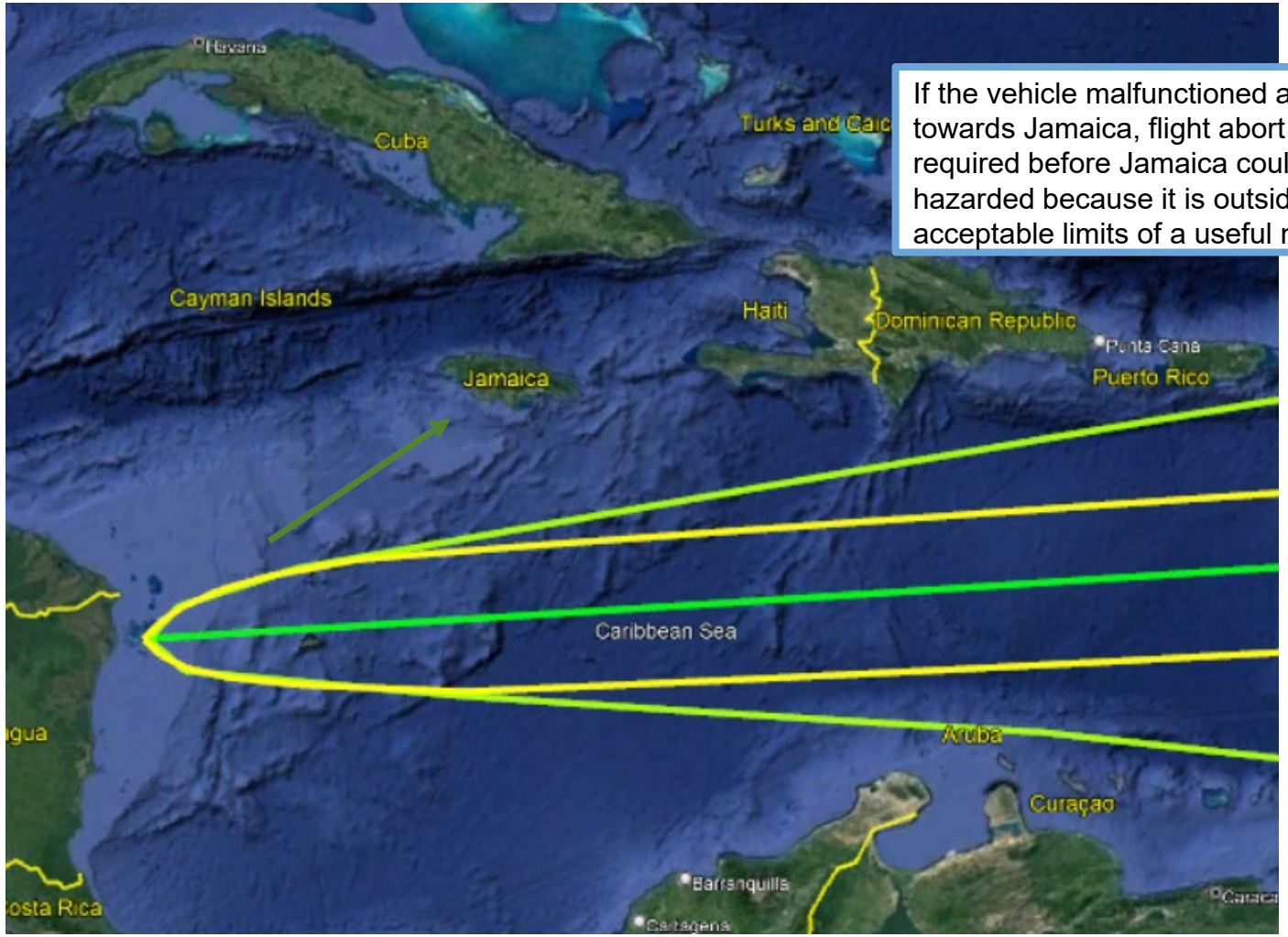
- Section 450.108(e) allows flight abort capability to be ended immediately after critical vehicle parameters are validated, if the vehicle is able to achieve a useful mission and the following conditions are met for the remainder of flight
  - Flight abort would not materially decrease the risk from a high consequence event; and
  - There are no key flight safety events

For example, there may be no benefit to flight abort during overflight downrange just before orbital insertion, as abort may not reduce the risk from a malfunction. A “key flight safety event” means a flight activity that has an increased probability of causing a failure compared with other portions of flight.
In this example, the second stage is near the end of its burn when the IIP approaches Africa and there are no more key flight safety events. The operator chooses to end the flight safety limits here, and the vehicle will pass through a final performance check before the flight safety limits end just prior to overflight. A flight safety system is typically turned off after the end of flight abort capability.



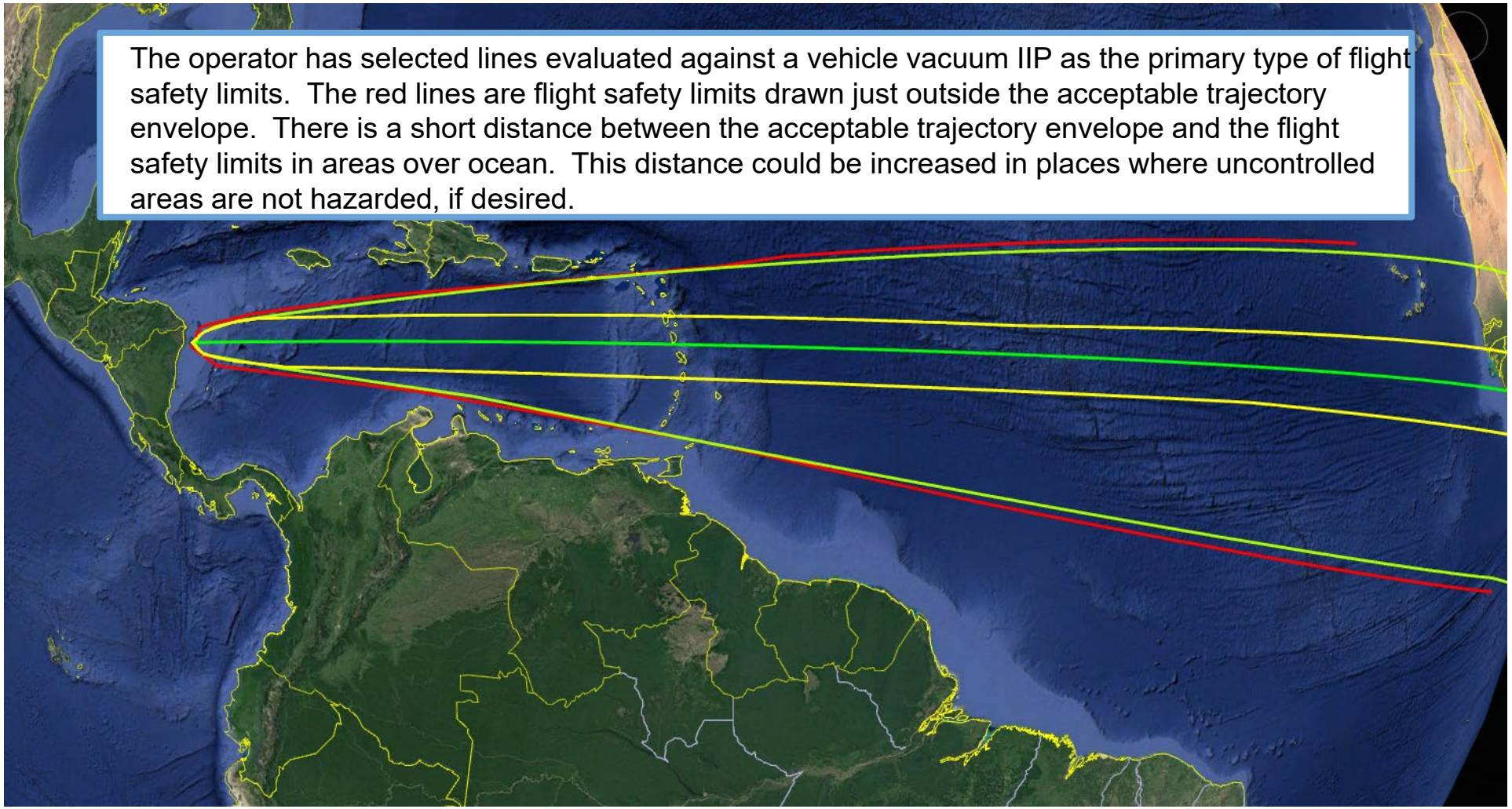
Abort to Protect Against Increased Risk

- Section 450.108(c)(2) requires that flight abort be initiated to prevent continued flight from increasing risk in uncontrolled areas if the vehicle is unable to achieve a useful mission
- This is a very important regulation and drives the placement of many flight safety limits

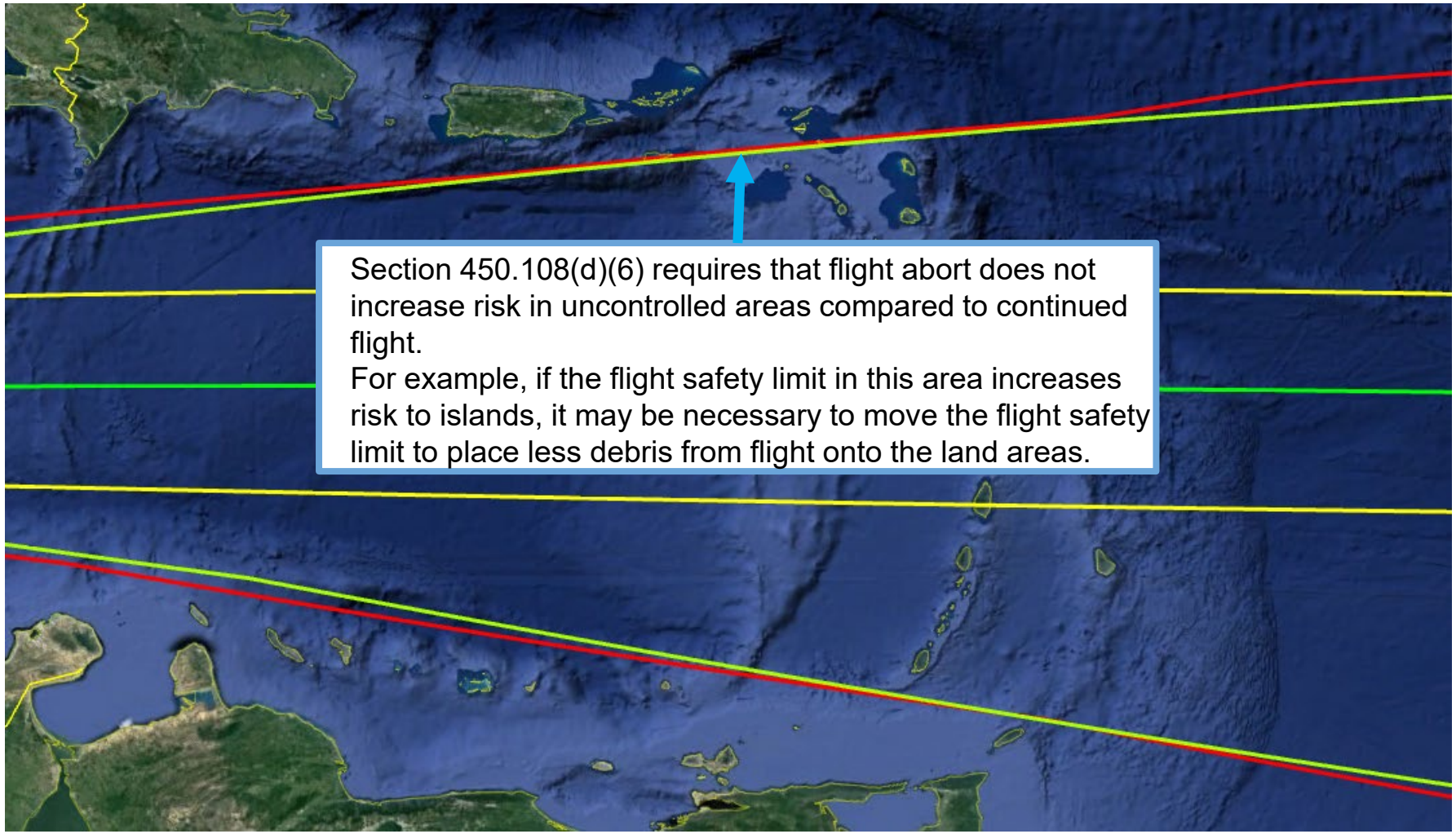


If the vehicle malfunctioned and flew towards Jamaica, flight abort would be required before Jamaica could be hazarded because it is outside the acceptable limits of a useful mission.

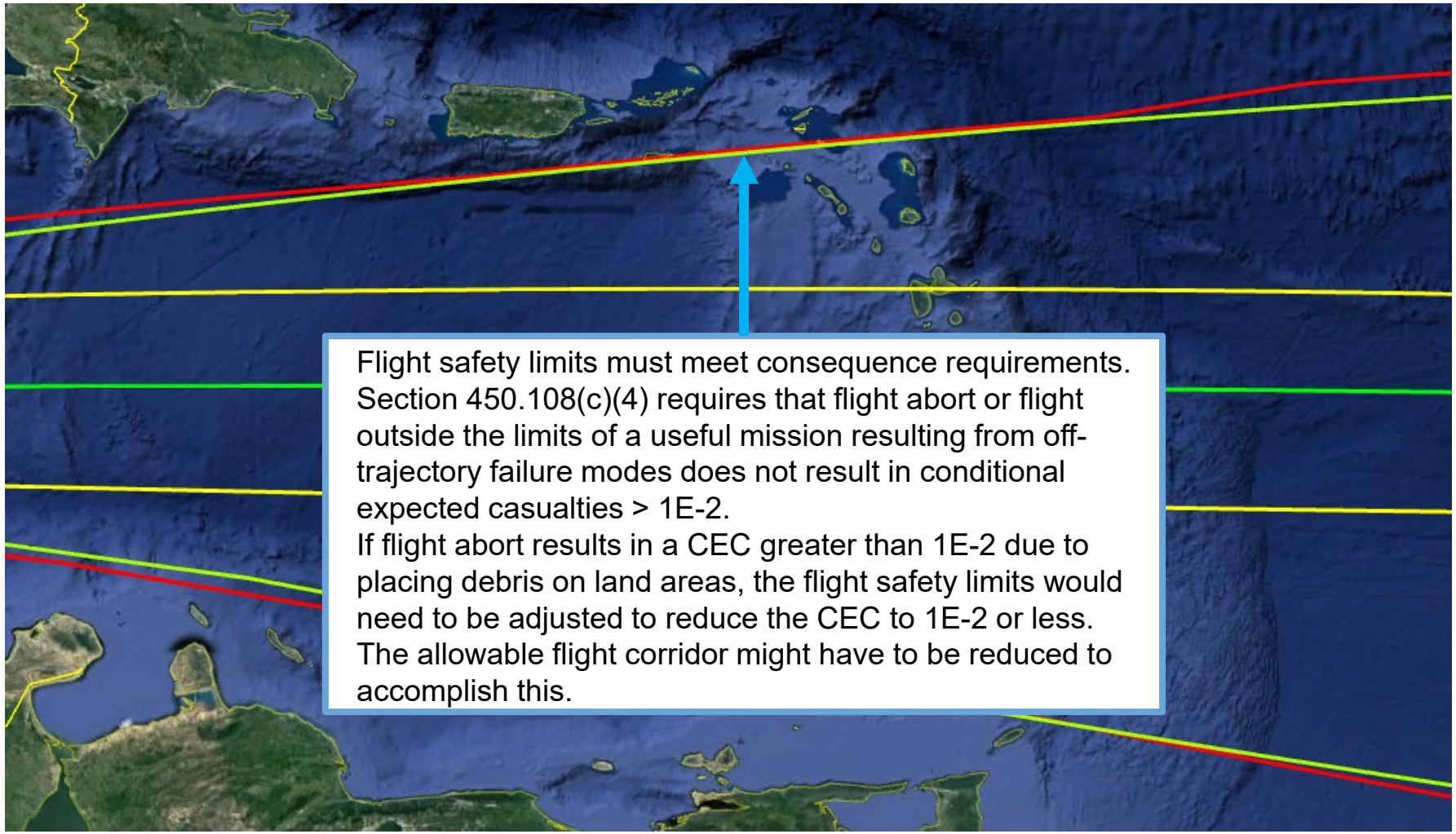
Example Flight Safety Limits



Abort Must Not Increase Risk



Consequence From Flight Abort

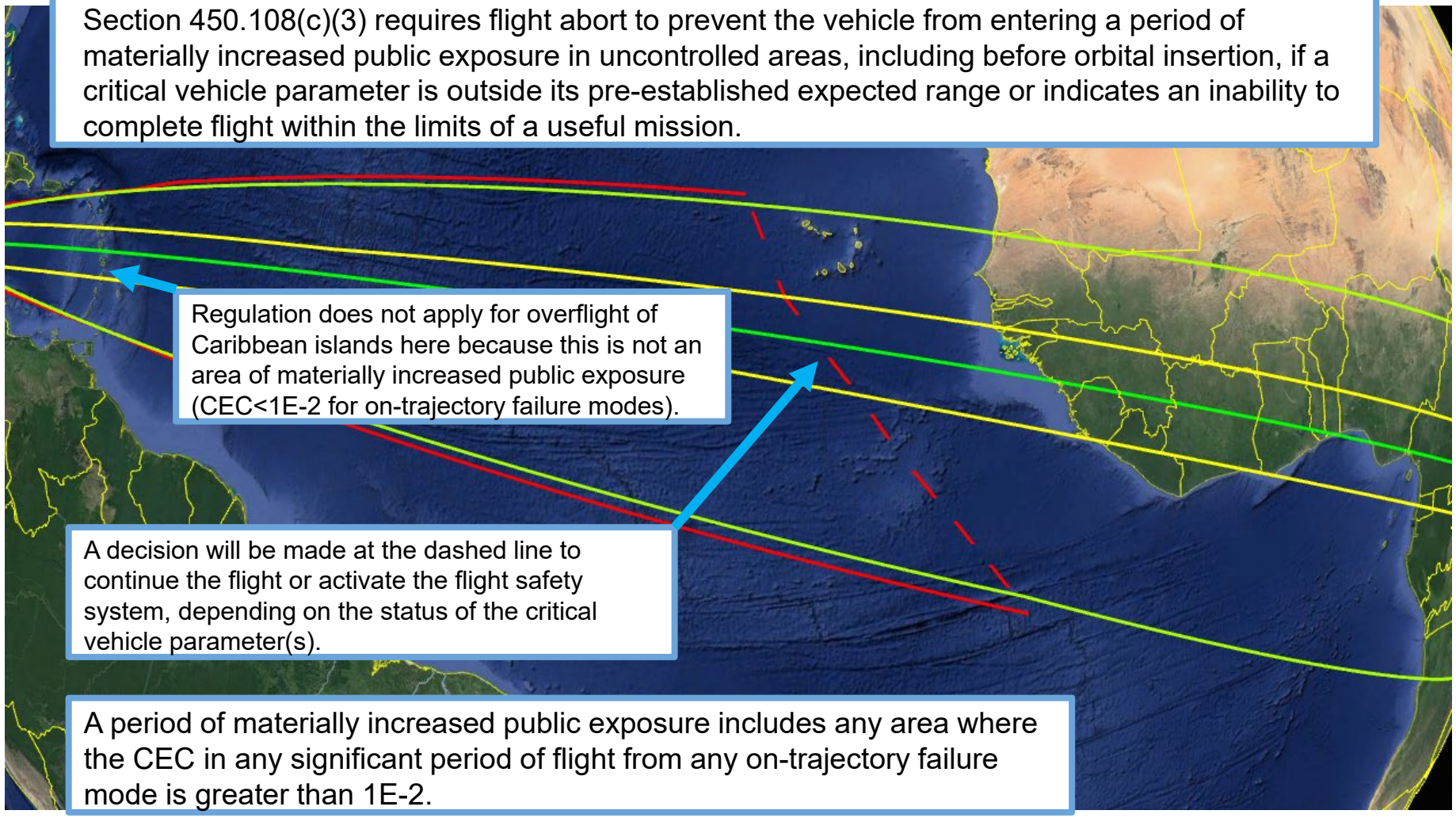


Flight safety limits must meet consequence requirements. Section 450.108(c)(4) requires that flight abort or flight outside the limits of a useful mission resulting from off-trajectory failure modes does not result in conditional expected casualties > 1E-2.

If flight abort results in a CEC greater than 1E-2 due to placing debris on land areas, the flight safety limits would need to be adjusted to reduce the CEC to 1E-2 or less. The allowable flight corridor might have to be reduced to accomplish this.

Check Vehicle Parameters Before Planned Overflight

Section 450.108(c)(3) requires flight abort 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.



Potentially Abort to Reduce Risk When Track is Lost

- Section 450.108(d)(3) requires that flight safety limits must account for the potential to lose valid data necessary to evaluate the flight abort rules
- Two potential strategies are:
  - Data loss flight times, where flight abort is initiated after a timer counts down. The timer is based on the shortest time to reach a flight safety limit after track is lost
  - Limiting the extent of the hazard location by initiating flight abort shortly after loss of track. Reducing the uncertainty of the hazard location helps with emergency response
- Acceptable data loss durations may be extended to avoid abort if it would endanger the public, or if periods of time where no data is reasonably expected are possible
- Planning for loss of track can include many considerations depending on the mission, so the regulation does not require a particular approach

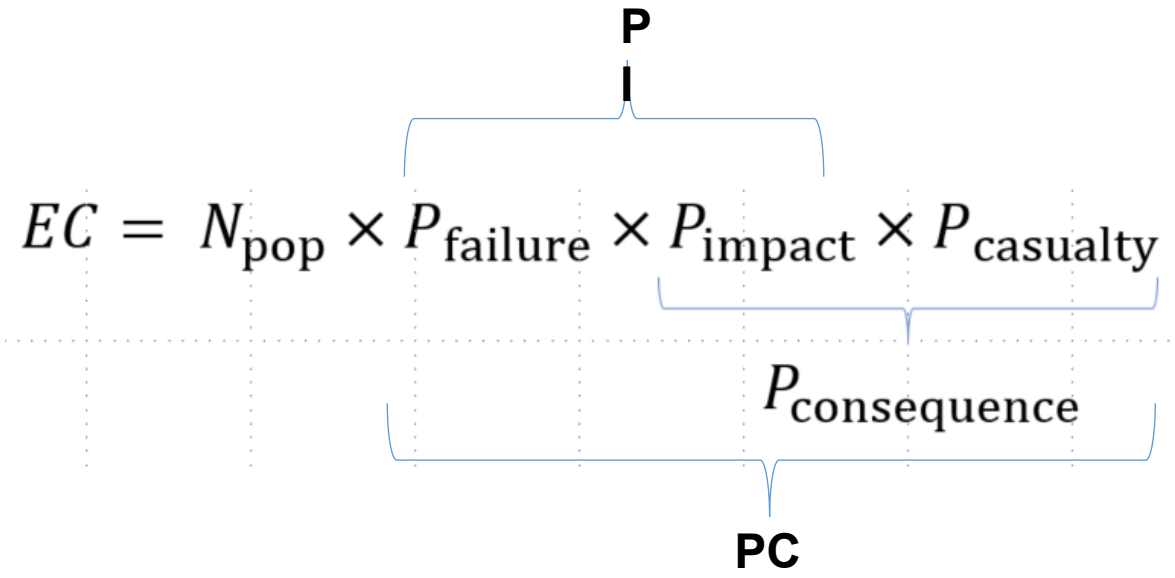
End of Example

Q&A

450.101 FSA Safety Criteria

Safety Criteria (450.101)		
Affected Population	**450.101(a/b)(1) Collective Risk (EC)**	**450.101(a/b)(2) Individual Risk (PC)**
Public (Excludes NOPS, People on Aircraf)	1.00E-04	1.00E-06
Neighboring Ops (NOPS)	2.00E-04	1.00E-05
Launch Essential	N/A	N/A
Affected Population	**450.101(a/b)(3) Aircraft (PI)**	**Note**: impact with debris capable of causing casualty
People on Aircraft	1.00E-06	
Hazard type	**450.101(a/b)(4) Critical Assets (PI)**	**450.101(a/b)(4) Critical Payloa (PI)**
probability of loss of functionality (derbris impact)	**1 × 10-3**	1 × 10-4
Affected Population	**450.101(c) protect against high consequence events**	
People on uncontrolled areas (land only)	1) using flight abort in accordance with § 450.108 2) demonstrating that CEC is no greater than 1e-3, or 3) demonstrating sufficient vehicle reliability	

Safety Criteria Metrics



$$CEc = N_{pop} X\ P_{consequence}$$

$p_{Consequence}$ is the *probability of consequence* and depends on the probability that hazardous debris impacts at or near the population center, and the probability that the impact results in a casualty

$$P_I = \sum (P_{failure} * P_{impact})$$

where:
P_I = Probability of Impact for the Cell,
Pf=Probability of failure for the event
P_i = Probability of impact accounting for number fragments impacting area and dispersion pattern

$$P_C = \sum \left(P_I * \frac{A_{cas}}{A_{cell}} \right); \quad P_{casualty} = \frac{A_{cas}}{A_{cell}}$$

where:
P_C = Probability of casualty
P_I = Probability of Impact for the Cell,
A_{cas} = Fragment Casualty Area including shelter effects, and
A_{cell} = Cell Area

$$E_C = \sum (P_C * N)$$

where:
N is the number of people in one grid cell
P_C is the probability of casualty
And, when N=1, $E_C = P_C$