FAA | AST Commercial Space Transportation

Flight Safety Analysis (FSA) Workshop #2 - AST

Federal Aviation Administration

May 30, 2024

Introduction & Questions

The purpose of this workshop is to provide the international community insight into FAA Flight Safety Analysis requirements under Title 14 of the Code of Federal Regulations (14 CFR) § 450

Three Sections:

Day 1: May 28, 2024

- Safety Criteria under Part 450

Day 2: May 30, 2024

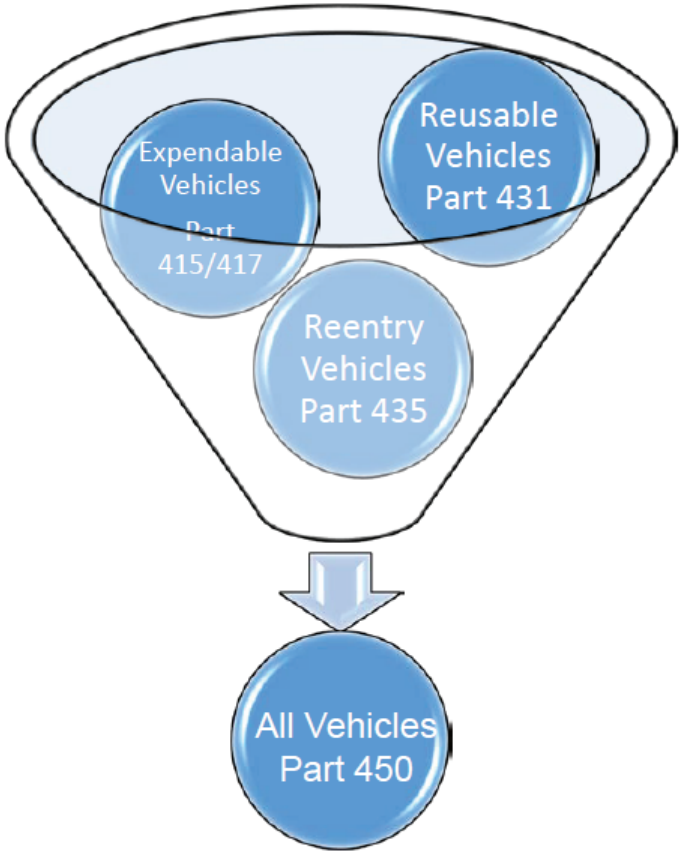
- Overview of FSA sections 450.108 to 450.137
- Explanation of § 450.115(c) elements

- **Q&A Session will be held after each section.**
  - Participants should use the Q&A function to ask questions.
  - We will answer as many questions as time allows.
  - Any unanswered questions will be answered after the workshop in a written Q&A document or at a future FSA Office Hours.

Section 2: Overview of FSA sections 450.108 to 450.137

Part 450

- Part 450
  - Consolidates multiple regulatory regimes into one set of requirements for all vehicle types
  - Performance-based requirements utilizing flexible means of compliance
  - Single license may authorize operations at multiple sites
- Shift from a focus on products to a focus on methods
  - Flexibility in the approaches and level of effort for an analysis
    - If methodology approaches and the applicant's process are still valid a license modification would not be necessary for a new flight azimuth or a new launch site
      - ➢ Process accounts for any updates to the analysis as result of variable inputs
        - ✓ Probability of failure
        - ✓ Wind profiles
        - ✓ Exposed population
        - ✓ Variable flight rules, etc.



450.35(a) Compliance (1 of 2)

For the purpose of § 450.35(a), the FAA has identified six types of acceptable MOCs

- **Type 1 – A current Advisory Circular**
  - Must be followed precisely; some Advisory Circulars provide guidance and include options so an applicant would need to tailor for their use (and becomes type 5 below)

- **Type 2 – A standard that has been accepted by the FAA**
  - FAA Accepted Means of Compliance that are publicly available are maintained on the FAA website at: https://www.faa.gov/space/streamlinedlicensingprocess/part-450-means-compliance-table/
  - Must be followed precisely, otherwise an applicant would need to tailor for their use (and becomes type 5 below)

- **Type 3 – Services provided by an *approved* federal entity (e.g. SLD-45)**
  - In accordance with § 450.45(b), the 'FAA will accept any safety-related launch or reentry service or property provided by a Federal launch or reentry site or other Federal entity by contract, as long as the FAA determines that the launch or reentry services or property provided satisfy this part'
  - Applicant is responsible for complying with requirements not provided by the federal entity
    - No entity performs all of FSA, for example

450.35(a) Compliance (2 of 2)

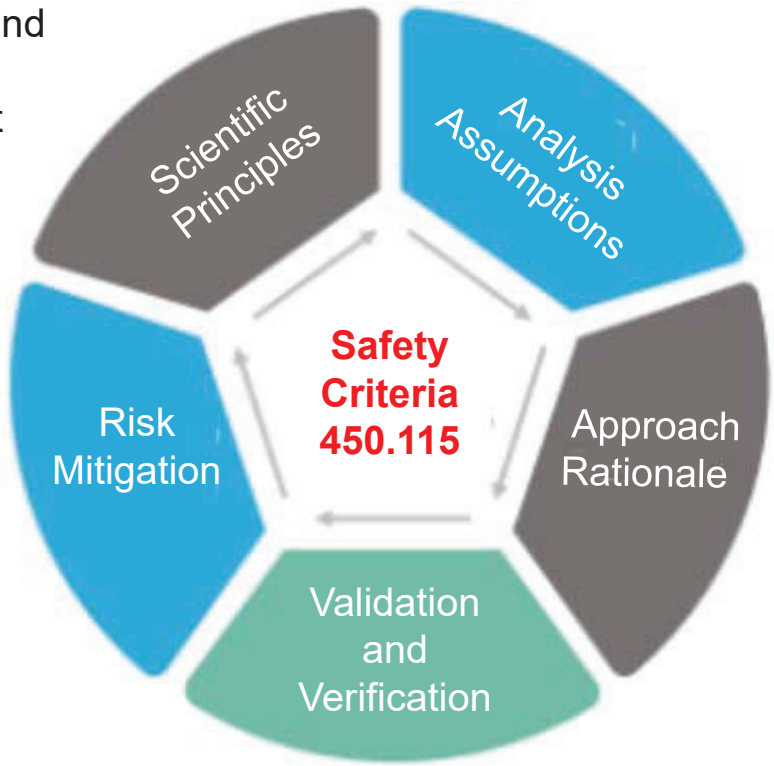
- **Type 4 – A Safety Element Approval (SEA), § 450.39**
  - An SEA can include “vehicle, safety system, process, service, or personnel”
  - An SEA has an approved scope - extent to which it satisfies requirement(s) and scenarios for which it applies
  - There are not yet any SEAs for part 450 FSA requirements
- **Type 5 – FAA approved applicant-specific descriptions of methods**
  - Can be a tailored version of Type 1 or 2
  - Usually takes weeks to months for iteration between applicant and AST to get to compliance
- **Type 6 – Actual mission data being used as representative**
  - Restrictive to the mission profile and conditions analyzed
  - Evaluation would occur via an independent safety analysis and the FAA may require additional products for this purpose per 450.45(e)(7)
- **FAA determines:**
  - If an applicant can legitimately use a previously accepted MOC based on consistency with all the conditions relevant to the previously accepted MOC
  - If the current application demonstrates a method that exactly follows an accepted MOC

FSA Methodology – What is an FSA Methodology?

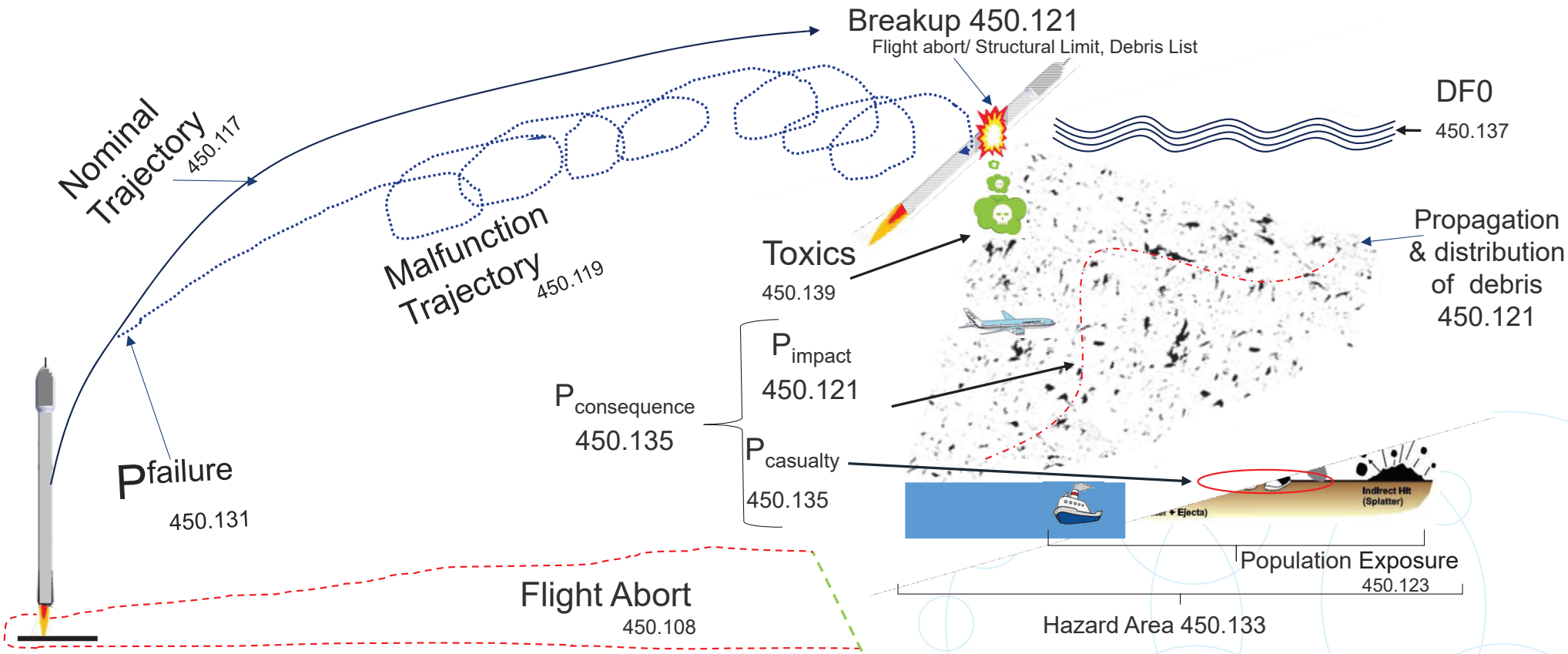
- An FSA methodology refers to the systematic, planned, structural and repeatable operating procedure an applicant performs to achieve a level of fidelity in flight safety analysis sufficient to demonstrate that any risk to the public satisfies the safety criteria of § 450.101, and should include:
  - Input data development and scientific principles
  - Analysis assumptions and justifications
  - Rationale of the proposed approach
  - Validation and verification of results
  - Risk mitigation development

- Refer to in the regulation as "description of the methods" use to demonstrate compliance with the FSA sub-analysis
  - Typically preceded by constraints and objectives
  - Typically followed by data requirements

- FSA methodology should address each of the requirements of 450.115(c) over the lifecycle of the proposed license activity



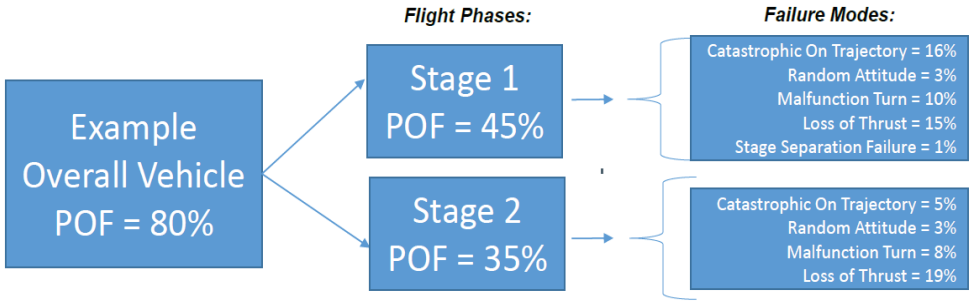
Components of FSA

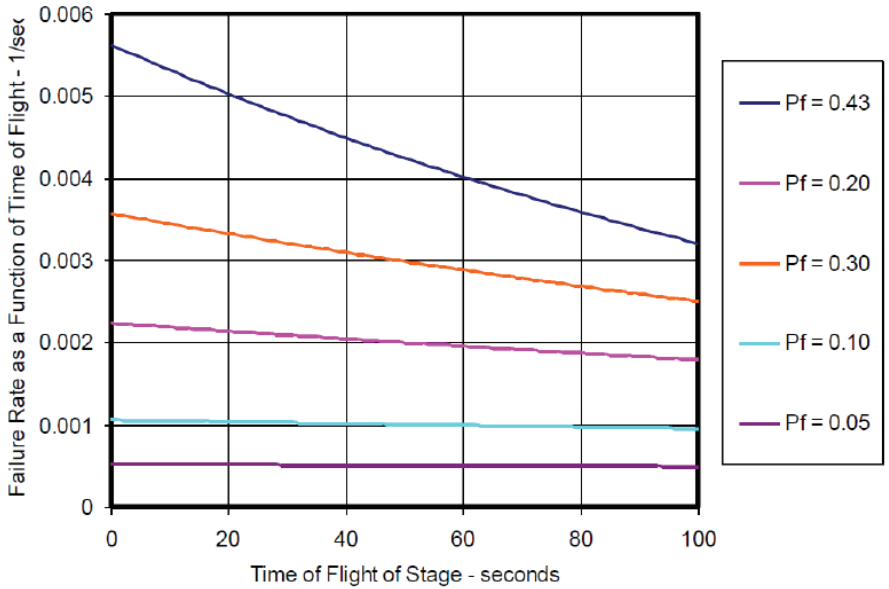


Federal Aviation Administration

450.131 (Probability of Failure)

- 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
- POF must be distributed across flight phases and failure modes
- Treats POF for first two flights differently than subsequent flights. Historical data shows that manufacturer experience makes a big difference.
- 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.

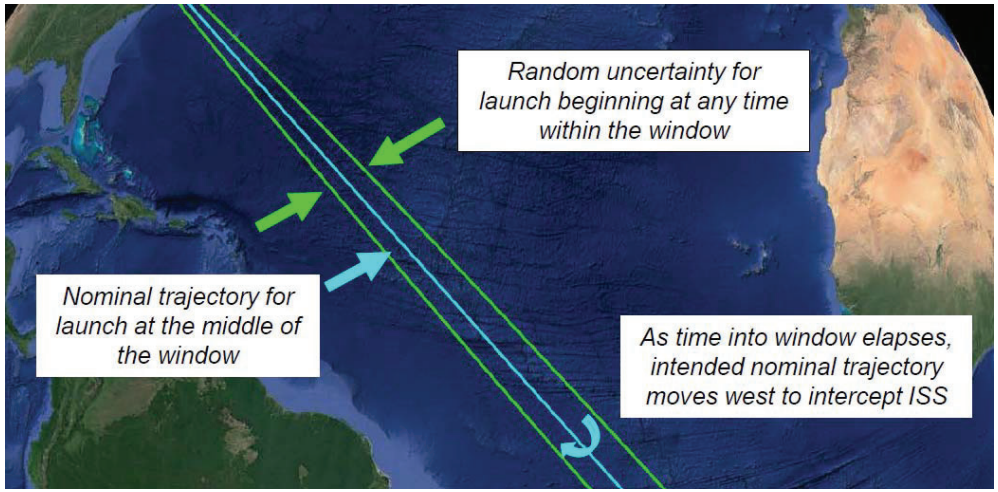


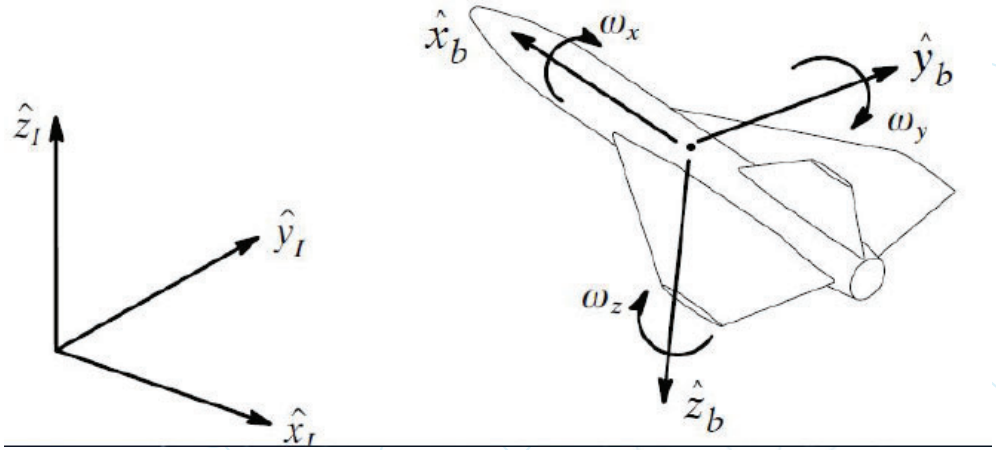


Federal Aviation Administration

450.117 Trajectory Analysis for Normal Flight

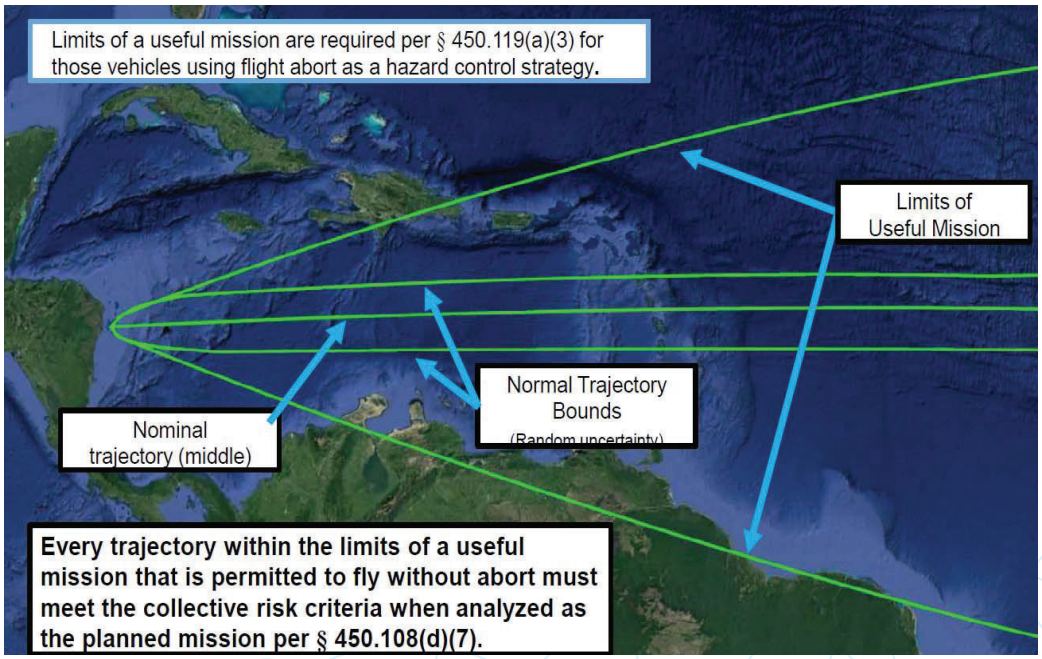
- § 450.117 specifies the constraints and objectives of analyses sufficient to characterize the trajectory of the vehicle during normal flight
- Requires besides a nominal trajectory, two sets of Normal trajectories: Variability and Uncertainty
- Variability trajectories are those characterized by conditions unknown prior to initiation of flight
- Uncertainty trajectories are characterized by parameters with significant influence that affect cross-range and downrange IIP locations
- Must be constructed using six degrees of freedom
  - includes comprehensive sets of aerodynamic and mass properties.
- Must account for atmospheric conditions that have an effect on the trajectory, including atmospheric profiles that are no less severe than the worst conditions





450.119 Trajectory Analysis for Malfunction Flight

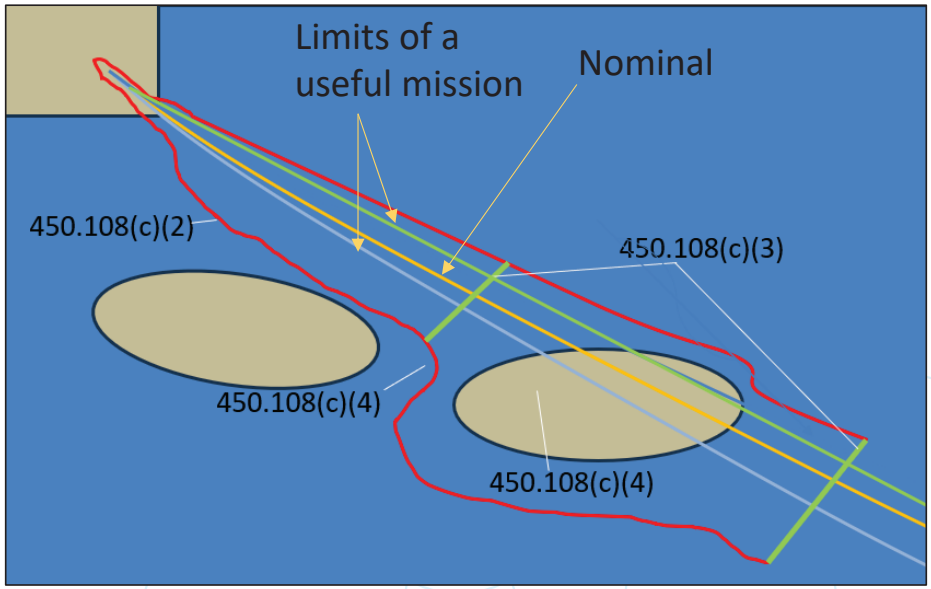
- A malfunction trajectory analysis is necessary to determine how far a vehicle can deviate from normal flight
- Must account for each cause of a malfunction flight, including software and hardware failures. A foreseeable failure is one that results from a functional hazard analysis (6 DOF modeling not required)
  - Random attitude, malfunction turn, incorrect azimuth, loss of thrust, on trajectory failure, degraded thrust
- Accounts for parameters with a significant influence on a vehicle's flight behavior until the time each malfunction trajectory will terminate due to vehicle breakup, ground impact, or orbital insertion
- Limits of a useful mission may be defined by some failures that still result in meeting objectives



Federal Aviation Administration

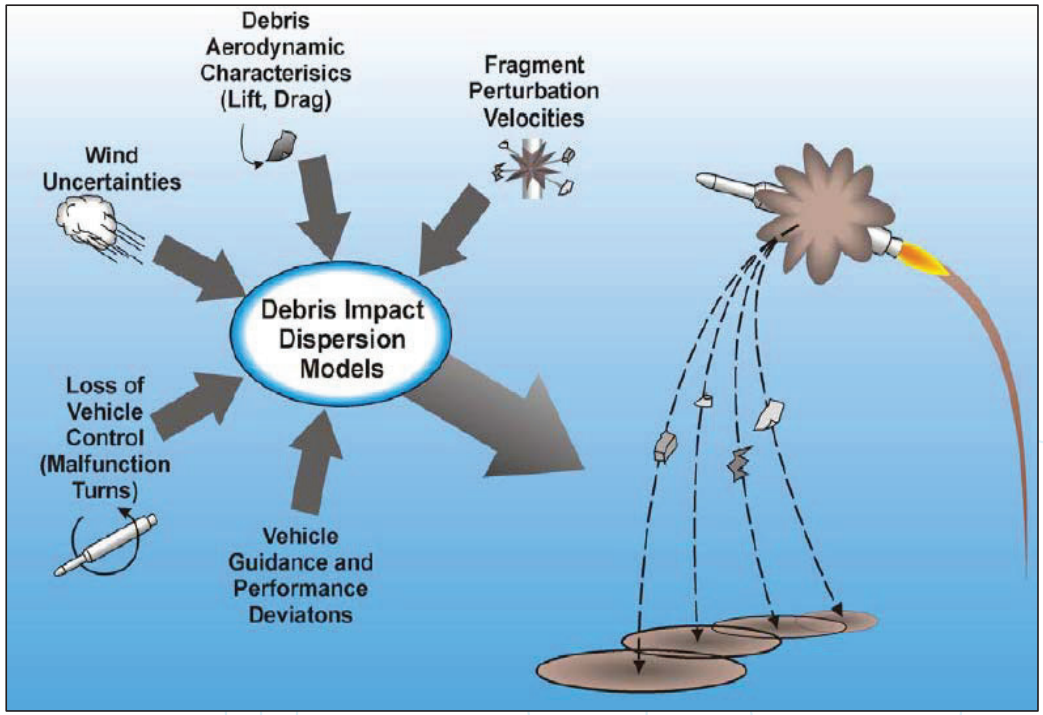
450.108 (Flight Abort)

- This section applies to the use of flight abort as a hazard control to meet the public safety criteria of § 450.101
- Key points:
  - Highly reliable flight safety system if CEc>1E-02
  - Safety-critical system if 1e-03<CEc>1e-02
  - Initiate abort to comply with safety criteria
  - Prevent continue flight from increasing risk, c(2)
  - Prevent vehicle from entering a period of materially increased public exposure if critical parameters indicate inability to complete flight within the limits of a useful mission, c(3)
  - 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, c(4)
  - Account the potential to lose valid data necessary to evaluate the flight abort rules



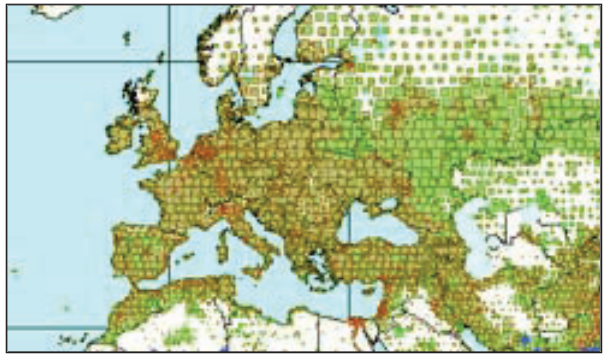
450.121 (Debris Analysis)

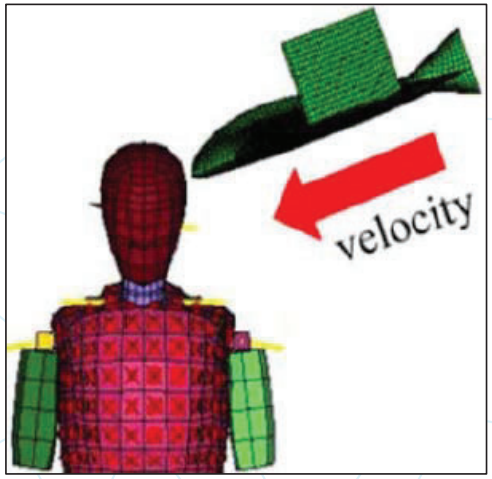
- A debris analysis must compute statistically valid debris impact probability distributions
- The propagation of debris from each predicted breakup location to impact must account for all foreseeable forces that can influence any debris impact location, and all foreseeable sources of impact dispersion.
- 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
- Account for all causes of breakup Flight Abort, structural breakup, impact



450.123 (Population Analysis)

- Hazards usually cannot be contained to unpopulated areas thus a population exposure analysis must also be performed, and its methodology described
- 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
  - This analysis must quantify locations of people relative to potential hazards and any sheltering (inside a structure)
  - Population database may have pretty good resolution for downrange population and overflight but is generally insufficient for identifying populations at specific locations
    - Special concern such as neighboring ops, launch pads & processing buildings, spectator areas, stadiums, cruise terminals, recreational areas (such as crowded beaches), launch viewing areas, vacation locations (e.g. parks, beaches, and hotels), seasonal events (e.g. harvest, fishing), schools airports and hospitals
- 450 allows operators to propose impact vulnerability models appropriate for the materials used in their operations



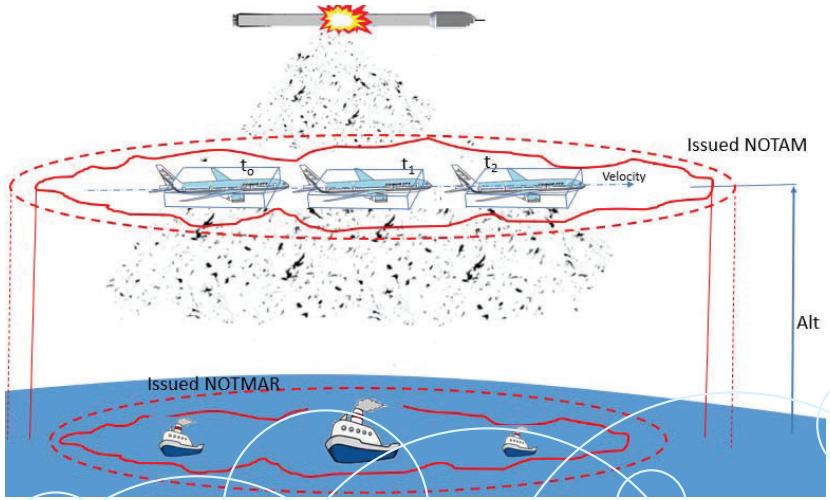


450.135, 450.137, 450.139 (Debris Risk Analysis, Far-field overpressure blast effects analysis, Toxic Hazards)

- Specifies the requirements for quantitative risk analyses to demonstrate that the risks to the public from debris, far-field overpressure, and toxic hazards are consistent with the safety criteria in § 450.101
- Can be conducted either prior to the day of the operation or during the countdown and must account for flight commit criteria if needed to ensure compliance with safety criteria
- Model the casualty area, and compute the predicted consequences of each reasonably foreseeable failure mode
- For 450.135 debris analysis must include all sources of impact dispersions and vulnerability of people including effects of building, vehicles, waterborne vessels, aircraft
  - Method to compute conditional collective casualty expectation for each failure mode , collective risk contribution, individual probability of casualty
- For 450.137 meteorological conditions are known to have a potentially substantial influence on the propagation and attenuation of blast waves
  - Methods used to compute the foreseeable explosive yield probability pairs, peak incident overpressures as a function of distance from the explosion, probability of window breakage and probability of casualty for a representative individual
- For 450.139 a 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, determine a toxic hazard area

450.133 (Flight Hazard Area Analysis)

- Methodology used for Flight hazard area analysis to ensure the risk to a protected entity (people, waterborne vessels, aircraft)
- Allows operators to reduce or otherwise optimize the size of the regions for warnings of potential hazardous debris resulting from normal flight events.
- 97 percent probability of containment, all hazardous debris resulting from normal flight events capable of causing a casualty
- Waterborne vessel hazard areas, i.e., Notices to Mariners (NOTMARs)
  - Contain probability of debris capable of causing a casualty impacting on or near a vessel would exceed 1e-5, or
  - Individual probability of casualty for any person on board a vessel would exceed 1e-06
- Land hazard areas in accordance with § 450.133(c)
  - a probability of casualty of 1e-05 or greater for neighboring operations personnel, and 1 1e-06 or greater for other members of the public,
- Airspace hazard volumes, i.e., Notices to Airmen (NOTAMs), to comply with § 450.133(d) requirements
  - probability of impact with debris capable of causing a casualty on an aircraft would exceed 1e-06



Federal Aviation Administration

Relevance of 450.115(a) & (b) & 450.101(g)

- 450.115(a) requires that an operator's FSA method account for all reasonable failures of safety-critical systems during nominal and non-nominal launch or reentry that could jeopardize public safety
- Sets standard of analysis scope
  - Identify, describe, and analyze all reasonably foreseeable hazards and hazardous event to public safety
    - Foreseeable means that the failure event is identifiable and derived from a functional hazard analysis

- 450.115(b) specifies the necessary fidelity and resolution of any FSA
  - Demonstrate risk satisfies 450.101
    - Accounting for all known sources of uncertainty
    - Identify the dominant source of each type of public risk
  - Include use of mitigations
  - Use accepted methodology per 450.35(a)(1)

- 450.101(g) notes that any analysis used to demonstrate compliance with 450.101 must use accurate data, and accepted scientific principles and the analysis must be statistically valid abd produce results consistent with or
- more conservative than the results available from previous mishaps, tests, or other valid benchmarks, such as
- higher-fidelity methods

Example of level of specificity

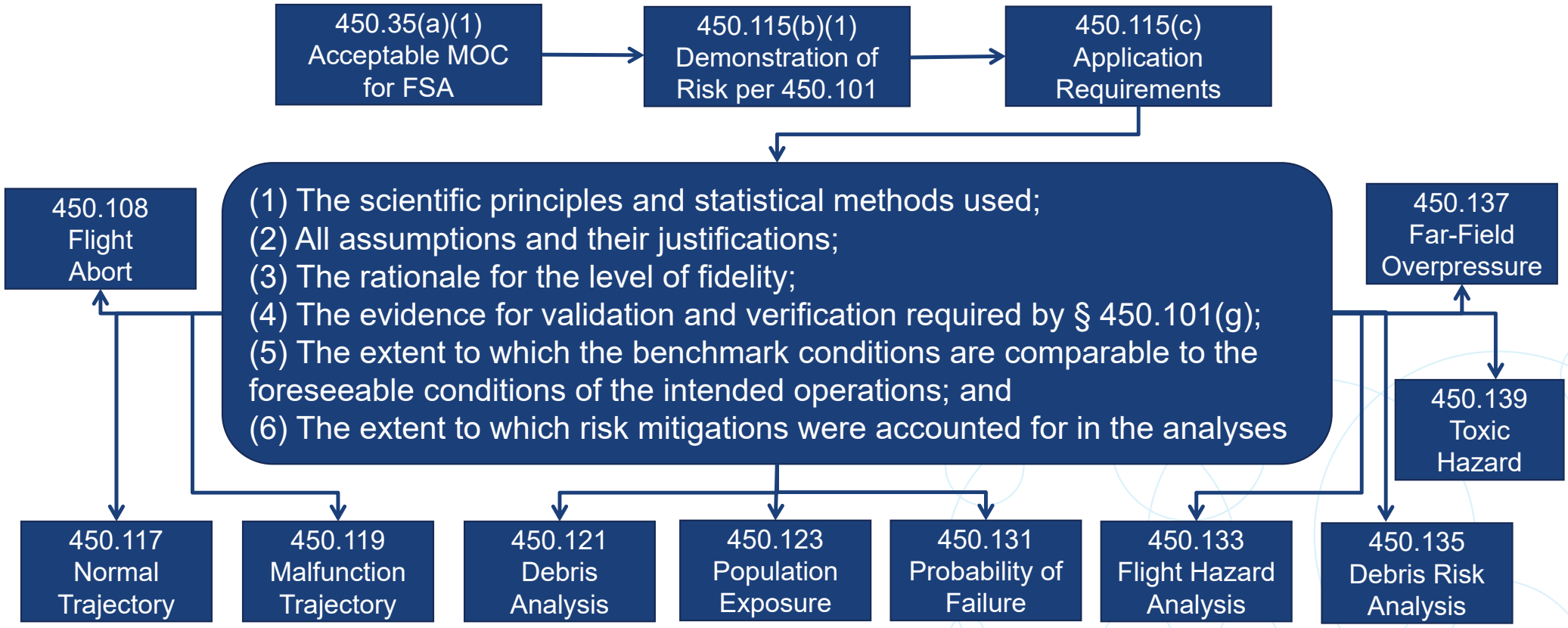
Unacceptable submission:
Debris impact locations are calculated using a 3DOF propagator that incorporates air density and wind using our in-house tool.

Acceptable submission:
Standard 3DOF computational simulation is used to compute trajectories for uncontrolled, unpowered objects. Input data are the initial position and velocity in ECI coordinates, the object's ballistic coefficient as a function of Mach number, and the specification of a 3-D atmospheric model (e.g. a Global Forecast System forecast). Equations of motion appropriate for a rotating Earth are used to determine the flight path of an object using a 3DOF simulation approach [ref 1]. The equations are integrated with respect to time using a Runge-Kutta method with the Adams-Bashforth predictor-corrector in ref 2 with an initial timestep of 1E-6s. Earth parameters through J2 are from WGS84 [ref 3]. Extraction and transformation of air density, speed of sound, and wind data are discussed in ref 4. The output is the trajectory (time, position, velocity) of the object in ECI coordinates from the initial state to impact with the Earth's surface at the interval of the integration steps.

1. Weiland*, Three and Six Degree of Freedom Trajectory Simulations, ch X*.
2. Press et al., *Numerical Recipes in C, 2nd Edition,* ch 16.
3. Department of Defense World Geodetic System 1984
4. XYZ Company, *Atmospheric Data Application Programmer's Interface Reference, version 6.1.*

This is an extremely brief version compared to some documentation we have seen on this topic.

Description of Methods per 450.115 (c) application requirement



FSA Methodology Overview

Content

- Address each element of the subject sub-analysis (e.g. constraints, objectives, and application requirements)
- Cover each element of 450.115(c) for each topic
- Describe the intended usage and limitations

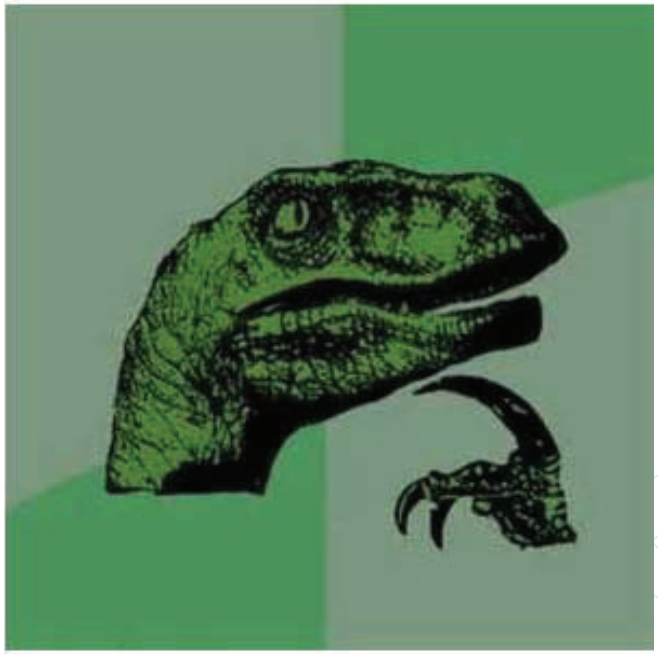
Rigor

- Logic is clearly described
- Based on generally accepted approaches
  - With specific references
- Mathematics are complete
- Evidence presented and analyzed

Depth/Definitiveness

- Verifiable: possible to reproduce consistent results and draw consistent conclusion using the same input data
- Inspectable: statements could be unambiguously supported by evidence upon request
- Repeatable: Two different engineers would not interpret in a meaningfully different way.

End of Overview of FSA sections 450.108 to 450.137



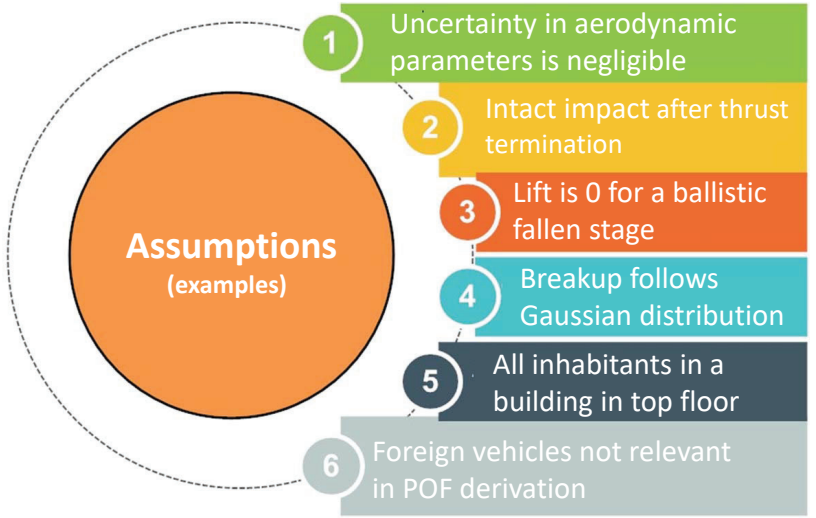
- Q&A

Section 3: Explanation of § 450.115(c) elements

Note: We have found that assumptions & justifications per § 450.115(c)(2) makes more sense to be discussed before scientific principles and statistical methods per § 450.115(c)(1).

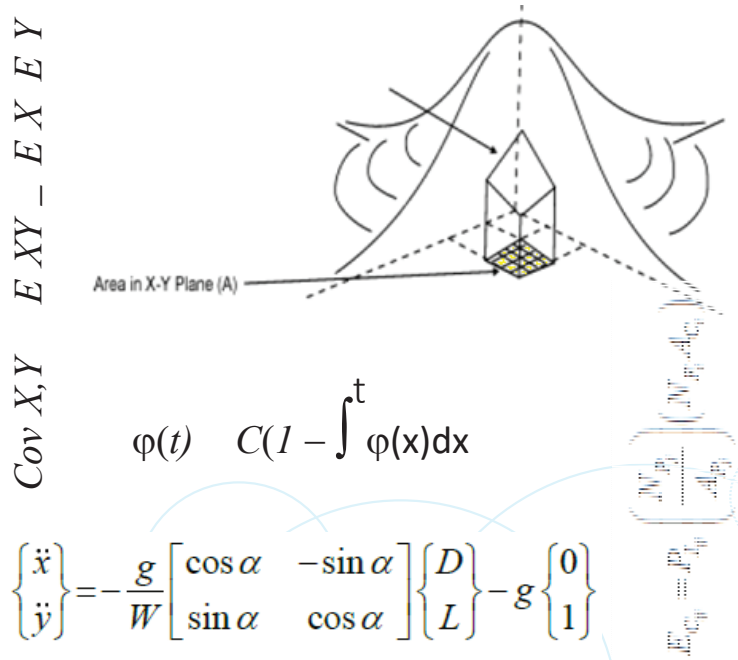
450.115(c)(2) All assumptions and their justifications

- Assumptions are things that are accepted as true or plausible and are often necessary to simplify problems and set limits to analysis
- There are three types of assumptions in a methodology:
  - The scope for which the methodology is intended to cover (and not cover)
    - Methods and procedures are allowed
  - The physical phenomena which are relevant to the modeling
    - Is it a rigid body code?
    - Assumptions about the physics included in the code that limit the applicability of the simulation?
  - Statistical selection and distributions
    - Normal distribution?
    - Uniformity?
- Assumptions should be stated clearly at relevant points within the narrative
  - Often helpful to summarize key assumptions and their justification in a matrix



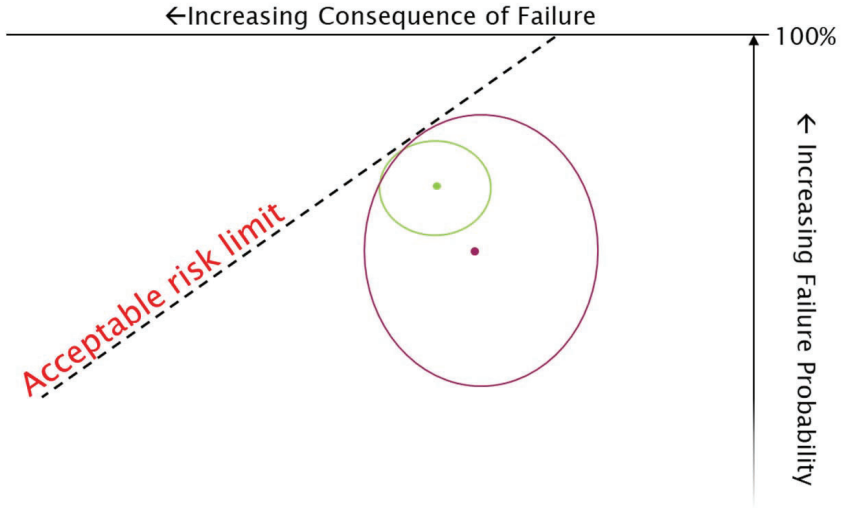
450.115(c)(1) Scientific Principles and Statistical Methods

- This discussion typically begins with an overview that describes integration of different elements of the modeling (sub-models)
  - Diagrams and flowcharts are often helpful, especially data flow diagrams
  - The link between the overview and the documentation of the elements should be clear
- Each sub-model should be based on established scientific principles, standard statistical methods, and/or empirical data
  - Scientific principles refer to knowledge based on the scientific method, such as that established in the fields of physics, chemistry, and engineering
  - A statistically valid analysis is the result of a sound application of mathematics and accounts for the uncertainty in any statistical inference due to sample size limits, the degree of applicability of data to a particular system, and the degree of homogeneity of the data.
- The depth of the detail should include equations and/or examples, but not algorithm implementation.
  - Standard mathematics (e.g. linear algebra, calculus) can be assumed
  - For off-the-shelf engineering software, provide references to technical manuals. AST may request applicants' assistance in obtaining them



450.115(c)(3) The rationale for the level of fidelity (1 of 2)

- Fidelity means the degree of exactness of the approach as compared to the real-world.
  - Per 450.115(b) the method needs to have sufficient fidelity to establish compliance with the safety criteria, considering uncertainty.
  - Fidelity is measured by bias (e.g. conservatism) and uncertainty



- Documentation should discuss
  - At the level of **each sub-model and input data**
  - Explanation of how this fidelity was found
    - Quantitative: Has data to support bias and uncertainty, such as by comparison to a higher fidelity model or data. This typically comes from models that have been simplified to run more quickly or require less analysis.
    - Qualitative: Bias/uncertainty which does not have supporting data within the analysis, but instead has an estimate based on outside knowledge or on engineering judgment, e.g. we have evidence that the prediction over-estimates the value 90% or 99% or X% of the time
  - How it affects the fidelity of the overall results the context of risk analysis

450.115(c)(3) The rationale for the level of fidelity (2 of 2)

- **Choice of fidelity is an operator decision: It is a cost-benefit analysis**
- Higher fidelity approaches are usually more costly
  - More work for applicant to develop
  - More work to develop input data
  - More effort for FAA to evaluate
    - True for even for a “simple” mission – there are more things to go awry with a more complex approach
- Lower fidelity approaches usually result in more operational restrictions
  - Lower-fidelity introduces assumptions that add conservatism into the answer
  - Restrictions include larger hazard areas, limited visitors, etc
    - The surroundings may make some restrictions not practical
- Note: one can compare the fidelity of two approaches, but there is no such thing as an absolute metric for fidelity.

Analogy

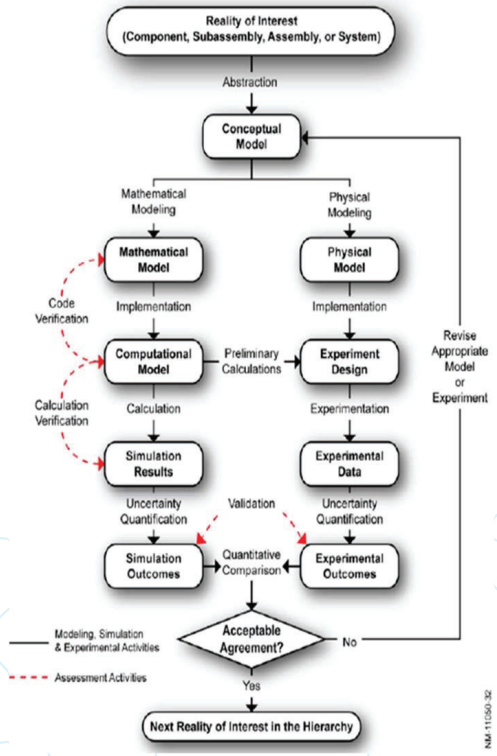
A hand saw can do everything a circular saw can do

With a hand saw it’s hard to get a significant injury while using it. But it’s slow and tedious.

A circular saw is a lot more costly to build (including safety features and testing) and needs more caution when using, even for a simple cut.

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

- **Process V&V:** Ensure that the structural and operating procedure achieves a level of fidelity that is sufficient to be used for risk analysis, includes:
  - A record of traceability from the input data's source through all aspects of its transmission, storage, and processing to its final form
  - Configuration Management that is applied over the process or product's life cycle to provide visibility into and to control changes to performance and to functionality and physical characteristic and include a well-controlled process for improving modeling based on flight experience like a Post-Flight Data Review
  - Includes computing system safety items that meet the definition of ‘‘safety-critical’’ in § 401.7
- **Modeling and Simulation (M&S) V&V:** Have we built the software right? Have we built the right software?
  - V&V of the Mathematical model that includes mathematical equations, boundary values, initial conditions, and modeling data needed to describe the conceptual model which is implemented into a computational/simulation model (code)
  - The rigor of V&V depends on the level of criticality of the model (typically IV&V is not necessary)
- **User qualification V&V:** ensures proper use of the process and/or M&S to reproduce the function or action of the product/service/system
- Operator qualifications and recertification
  - Qualifications & experience assessments of the people developing, testing, & using key elements related to the process or M&S, including, maintenance, operation, results analysis, training, and error reporting
  - Intended to identify personnel who are likely to perform the process successfully
  - Define roles and responsibilities
  - Description of the minimum requirements
- Includes safety-critical personnel qualifications (§ 450.149), especially those that perform countdown activities
- DoDI 5000.61 provides a good overview of V&V for modeling and simulation.
- NASA-STD-7009A and NASA-HDBK-7009A provides good description of accepted modeling and simulation practices
  - Link: NASA HANDBOOK FOR MODELS AND SIMULATIONS: AN IMPLEMENTATION GUIDE FOR NASA-STD-7009 | Standards



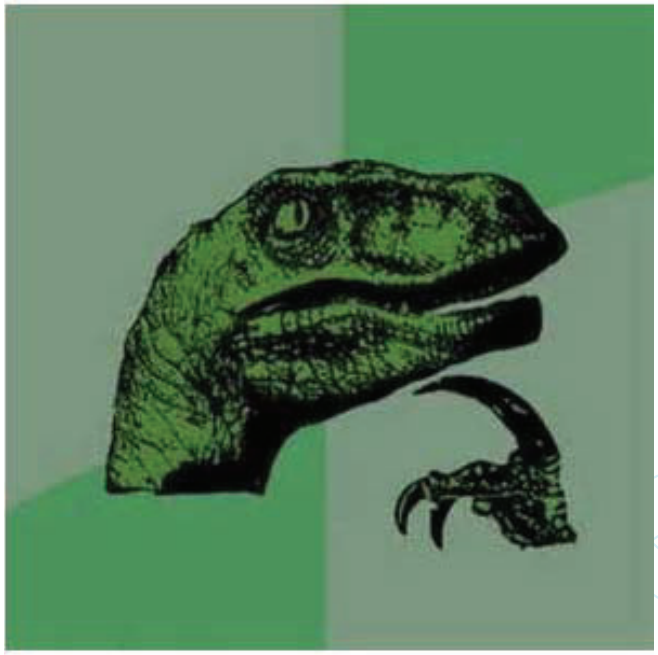
450.115(c)(5) *The extent to which the benchmark conditions are comparable to the foreseeable conditions of the intended operations*

- A benchmark is an independent ‘ good’ or acceptable standard against which comparison can be made to check that a product, service or system fulfils intended purpose
- Describe situations where the modeling approach has been compared to empirical data and/or other modeling approaches
  - Provides context and is a critical element of an analysis to identify best practices
  - Can help to identify issues and improvements in process and technical development of Sofware
- Conditions should be compared to the intended scope of the methodology, discussing the regimes where the model is closer to and further from the benchmarks
  - Benchmark should run in parallel with the methodology, bringing in standards and best practices from elsewhere, while the methodology preserves knowledge generated within the organization
  - If inappropriate benchmark are used the analyst may end up making erroneous conclusions
- No amount of benchmarking is sufficient to verify accuracy
  - Benchmarks increase confidence but cannot alone determine correctness
- Regulation includes “extent to which” is used as the FAA acknowledges that there could be cases that are so unique that relevant benchmarks are unavailable
  - Applicants are still expected to address and provide some reasoning to the extent to which benchmarks were used relying on the best available data.
  - In the lack of a benchmark an applicant may discuss the level of conservatism included in their approximations.

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

- This describes how mitigations (e.g. flight safety system, hazard areas, launch commit criteria) are incorporated in the flight safety analysis process and methods
- Mitigations include those described in the functional hazard analysis (FHA)
  - Mitigations include redundancy of the design and conservatism used in the analysis
  - The FHA mitigations should be correlated to FSA elements
- FSA produces mitigations (e.g. flight safety limits, hazard areas) which are used in downstream analyses
  - Arguably these are the most important products of the FSA
- Regulation includes “extent to which”, as the FAA acknowledges that there could be cases that are so unique that relevant mitigations are unavailable or applicable
  - Applicants are still expected to address and provide some reasoning to the extent to which risk mitigations were used relying on the best available data

End of Explanation of § 450.115(c) elements and Day 2



- Q&A