U.S. Department
of Transportation
Federal Aviation
Administration

Advisory Circular

Subject: Probability of Failure Analysis

Date: D R A F T

AC No: 450.131-1

Initiated By: AST-1

This Advisory Circular (AC) provides guidance and an example means of compliance for performing a probability of failure analysis in accordance with Title 14 of the Code of Federal Regulations (14 CFR) 450.131. A flight safety analysis that accounts for vehicle failure probability is required for launch or reentry in accordance with § 450.113(a). This AC assists with performing a probability of failure analysis in accordance with § 450.131, obtaining a Part 450 license, and operating in compliance with the related regulations.

The Federal Aviation Administration (FAA) considers this AC an accepted means of compliance for complying with the regulatory requirements of § 450.131.

This is a guidance document. Its content is not legally binding in its own right and will not be relied upon by the Department as a separate basis for affirmative enforcement action or other administrative penalty. Conformity with the guidance document is voluntary only. Nonconformity will not affect rights and obligations under existing statutes and regulations.

If you have suggestions for improving this AC, you may use the Advisory Circular Feedback Form at the end of this AC.

Executive Director, Office of Operational Safety
Commercial Space Transportation

Contents

Paragraph **Page**

Figures

Contents (continued)

Paragraph **Page**

Tables

1 PURPOSE.

This AC provides guidance and an example means of compliance for performing a probability of failure analysis in accordance with Title 14 of the Code of Federal Regulations (14 CFR) § 450.131. Such an analysis is required under most circumstances for all phases of flight. This AC is intended to assist prospective applicants and operators in performing a probability of failure analysis in compliance with § 450.131.

1.1 Regulatory Scope.

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, in accordance with § 450.115(a). In accordance with § 450.131(a), 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.

1.2 Level of Imperatives.

Chapter 7 of this AC presents one, but not the only, acceptable means of compliance with the associated regulatory requirements. The FAA will consider other means of compliance that an applicant may elect to present. In addition, an operator may tailor the provisions of the presented means of compliance to meet its unique needs, provided the changes are accepted as a means of compliance by FAA. Throughout Chapter 7, the word "must" characterizes statements that directly follow from regulatory text and therefore reflect regulatory mandates. The word "should" describes a requirement if electing to use this means of compliance; variation from these requirements is possible, but must be justified and accepted by FAA as an alternative means of compliance. The word "may" describes variations or alternatives allowed within the accepted means of compliance.

2 APPLICABILITY.

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

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

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

3 APPLICABLE REGULATIONS AND RELATED DOCUMENTS.

3.1 Applicable United States Code (U.S.C.) Statute.

Title 51 National and Commercial Space Programs, U.S.C. Subtitle V, Chapter 509. *Commercial Space Launch Activities*.

3.2 Related FAA Commercial Space Transportation Regulations.

The following 14 CFR regulations must be accounted for when showing compliance with 14 CFR 450.131, *Probability Failure Analysis*. The full text of these regulations can be downloaded from http://www.ecfr.gov. A paper copy can be ordered from the Government Printing Office, Superintendent of Documents, Attn: New Orders, P.O. Box 371954, Pittsburgh, PA, 15250-7954.

- Section 1.1, *General definitions*.
- Section 401.7, *Definitions*.
- Section 450.101, *Safety criteria.*
- Section 450.103, *System safety program*.
- Section 450.107, *Hazard control strategies.*
- Section 450.109, *Flight hazard analysis.*
- Section 450.113, *Flight safety analysis requirements – scope*.
- Section 450.115, *Flight safety analysis methods.*
- Section 450.117, *Trajectory analysis for normal flight*.
- Section 450.119, *Trajectory analysis for malfunction flight*.
- Section 450.135, *Debris risk analysis*.
- Section 450.137, *Far-field overpressure blast effects analysis*.
- Section 450.139, *Toxic hazards for flight*.
- Section 450.173, *Mishap plan – reporting, response, and investigation requirements*.
- Section 450.213, *Pre-flight reporting*.
- Section 450.215, *Post-flight reporting*.

3.3 **Related FAA Advisory Circulars.**

The following FAA Advisory Circulars are the most relevant to this AC. They are available through the FAA website, https://www.faa.gov/space/legislationregulationguidance/commercial-space-advisory-circulars-acs/commercial-space.

- AC 450.101-1B, *High Consequence Event Protection*, dated April 9, 2024.
- AC 450.107-1, *Hazard Control Strategies Determination,* dated July 27, 2021.
- AC 450.109-1, *Flight Hazard Analysis*, dated August 5, 2021.
- AC 450.115-2, *Describing Flight Safety Analysis Methods*, dated September 20, 2024.
- AC 450.173-1, *Part 450 Mishap Plan – Reporting, Response, and Investigation Requirements*, dated August 12, 2021.

3.4 **References.**

1. Guarro, S.; P. Wilde., and E. Tomei, *Launch and Reentry Vehicle Probability of Failure Analysis Methodology for Evaluation of Public Risk in Commercial Human Spaceflight*, Proceedings of 13th International Association for the Advancement of Space Safety (IAASS) Conference, Prague, Czech Republic, October 8 to 10, 2024.
2. Modarres, M., Kaminskiy, M.P., and Krivtsov, V., *Reliability Engineering and Risk Analysis: A Practical Guide, Second Edition (2nd ed.)*. CRC Press (2009).
3. Titulaer, S., *Probability of Failure Analysis for New Launch Vehicles*, Proceedings of 13th IAASS Conference, Prague, Czech Republic, October 8 - 10, 2024.
4. Manning, C., "Technology Readiness Levels," NASA, September 27, 2023. https://www.nasa.gov/directorates/somd/space-communications-navigation-program/technology-readiness-levels/.
5. Pfitzer, T., and M. Stroud, *System Safety Metrics Method for Space Launch Systems*, A-P-T Research, Inc, Doc. No. CDSP-FL004-18-00401, October 16, 2018. https://www.faa.gov/media/95516.
6. Federal Aviation Administration, *Guide to Probability of Failure Analysis for New Expendable Launch Vehicles*. Guide to Probability of Failure Analysis for New Expendable Launch Vehicles.
7. OSD Manufacturing Technology Program, *Manufacturing Readiness Level (MRL) Deskbook*, May 2011. https://www.dodmrl.com/MRL_Deskbook_V2.pdf.

4 DEFINITION OF TERMS.

For this AC, the following terms and definitions are used:

4.1 Conditional Failure Rate

A conditional failure rate is the probability per unit time that a failure will occur at a given time, assuming success prior to that time.

4.2 Conditional Probability of Failure

Conditional probability of failure refers to the probability of a failure occurring during a flight phase, flight stage, or flight event, given that all preceding flight phases, flight stages, and flight events have been successfully completed.

4.3 Failure Initiation

Failure initiation is the event of a subsystem beginning to perform off-nominally that results in a vehicle failure.

4.4 Failure Manifestation

Failure manifestation is the characterization of a failure at the vehicle level, such as structural failure or trajectory deviation.

4.5 Failure Mode

A failure mode is a unique combination of three elements: the initiating system/subsystem of the failure, the resulting manifestation of the failure, and the flight event where the failure occurs.

4.6 Failure Response Mode

A failure response mode is a group of failure modes that result in a homogenous distribution of trajectories, prior to consideration of mitigations or hazard control strategies. Failure response modes are modelled to comply with § 450.119 requirements.

4.7 Observed Failure Rate

An observed failure rate is the ratio of failures to attempts in a defined period of flight divided by the duration of the period.

4.8 Observed Probability of Failure

Observed or unconditional probability of failure refers to the probability of a failure occurring during a flight phase, flight stage, or flight event, given the initiation of an operation.

4.9 Phase of Flight

A period of flight between two milestones in the vehicle flight sequence, which is not necessarily a set period of time, where the probability of failure distribution for each reasonably foreseeable failure mode is homogeneous.

4.10 **Similar Flight**

Flight of a vehicle developed and launched or reentered in similar circumstances in the context of § 450.131(a)(1).

4.11 **Similar Vehicle or Vehicle Stage**

Vehicles or vehicle stages that were developed and launched or reentered under similar circumstances in the context of § 450.131(a)(1).

4.12 **Subject Flight**

The flight that the probability of failure applies to.

4.13 **Subject Vehicle or Vehicle Stage**

The vehicle or vehicle stage that undertakes or is part of the subject flight.

4.14 **Uncertainty**

The absence of perfectly detailed knowledge. Uncertainty includes incertitude (the exact value is unknown) and variability (the value is changing). Uncertainty may also include other forms such as vagueness, ambiguity, and fuzziness (in the sense of border-line cases).

4.15 **Vehicle Response**

Vehicle response is the characterization of the behavior of a given vehicle. This is generally either a type of breakup or a type of trajectory deviation.

5 ACRONYMS.

AC – Advisory Circular

AST – FAA's Office of Commercial Space

CCSFS – Cape Canaveral Space Force Station

CFR – Code of Federal Regulations

CSV – Comma Separated Values

CSWG – Common Standards Working Group

FAA – Federal Aviation Administration

FM – Failure Mode

FRM – Failure Response Mode

FSS – Flight Safety System

FTAR – Failure Time and Rate Data File

GNC – Guidance, Navigation, and Control

IAASS – International Association for the Advancement of Space Safety

IIP – Instantaneous Impact Point

LEO – low Earth orbit

MOC – Means of Compliance

MFCO – Mission Flight Control Officer

NASA – National Aeronautics and Space Administration

POF – Probability of Failure

SMC – Space and Missile Systems Center Standard

SRB – Solid Rocket Booster

SV – State Vector

U.S. – United States

USC – United States Code

VSFB – Vandenberg Space Force Base

6 EXPLANATION OF THE REGULATIONS.

6.1 Explanation of § 450.131(a) General.

Part 450.131(a) states that "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."

6.1.1 For Each Hazard.

The phrase "for each hazard" should be interpreted as each potential cause of failure, as defined in § 450.131(b), relevant to the flight safety analysis, including the debris risk analysis (§ 450.135), the far-field overpressure blast effects analysis (§ 450.137), and toxic hazards for flight (§ 450.139) as applicable to a given mission or group of missions.

6.1.2 Phase of Flight.

A phase of flight refers to a period of flight between two milestones in the vehicle flight sequence where the probability of failure distribution for each reasonably foreseeable failure mode is homogeneous, as described in detail in paragraph 6.1 of AC 450.101-1B. Here, a failure probability distribution is considered homogeneous if there are no discontinuities and the failure probability distribution is defined by a single mathematical function (e.g., a linear, exponential, or uniform distribution). Each phase of flight within the scope of the flight safety analysis, as defined by § 450.113, should be accounted for in the probability of failure analysis.

In order to define the phases of flight for the flight safety analysis, the operator should perform a decomposition of the mission or missions into a sequence of flight events for which conditional failure probabilities are to be estimated from applicable flight history data. A flight event is an occurrence identified by a set of objective conditions during launch or reentry. Flight events can be subdivided or combined to form phases of flight.

Phases of flight can be divided into two types:

- **Discrete:** A discrete phase of flight is a short duration event and usually contains a key flight safety event.
    - **Example**: Stage separation
- **Continuous:** A continuous phase of flight is longer than a discrete phase of flight and should not contain any key flight safety event.[1]
    - **Example:** Stage burn

[1] A key flight safety event is a flight activity that has an increased likelihood of causing a failure compared with the portions of flight that come before or after it, such as a staging, engine cutoff or reignition, payload fairing separation, etc., described in further detail in paragraph 6.1 of AC 450.101-1B.

In decomposing a mission into phases of flight, the resulting collection of phases of flight must be mutually exclusive and at the same time cover the full duration of the flight within the scope of the flight safety analysis defined in § 450.113(a). At the most basic level, the flight event decomposition coincides with the phases of flight decomposition (each phase of flight is mapped to exactly one flight event). However, a higher fidelity POF analysis may divide a phase of flight into parallel events.

Example: Given a vehicle with a core and two strap-on boosters, a phase of flight may contain a period in which both the core and the strap-on boosters are providing thrust. In this case, the phase of flight can be divided into three events: one event for each burn of the strap-on boosters and one for the burn of the core booster. The POF analysis would then define a homogenous probability of failure distribution for each reasonably foreseeable failure mode during the burn of the strap-on boosters and then separately during the burn of the core booster.

Typical flight events for launch vehicles include:

- stage burn
- stage separation
- engine ignition or restart
- payload fairing separation
- Guidance, Navigation, and Control (GNC) events

For a launch vehicle with reusable boosters, typical flight events include:

- boostback burn
- freefall
- entry burn
- glide
- landing burn

Typical flight events for reentry vehicles include:

- deorbit burn
- separation
- reentry
- service module jettison

Depending on the level of fidelity of the analysis, the reentry event may be further subdivided into events based on the environments experienced during reentry (change in heating, change in pressure, etc.).

Decomposition of a flight should implement the following:

- Timespans of events should account "for each…phase of flight" per § 450.131(a), which should be interpreted as covering the full timespan of the flight that is within the scope of § 450.113.[2]
- Each key safety event should have its own corresponding flight event.
- A flight event's failure rate can be characterized by a single rate function.[3]
- A contingency flight may include different key flight safety events, and thus a different decomposition than the nominal flight(s). For an abort contingency specifically, the key flight safety events and decomposition may change from the nominal flight after the abort.

Generally, a flight decomposition resulting in more events can lead to a higher level of fidelity analysis. However, it is important to note that estimating the failure probability of each event may become more challenging due to sparser data being available. Therefore, it is necessary to strike a balance between the number of events used and the accuracy of the estimation. The level of fidelity should be consistent with the POF methodology and the available supporting data, and rationale for the level of fidelity must be identified per § 450.115(c)(3). The flight history data of vehicles developed and launched or reentered in similar circumstances and/or the subject vehicle should be considered, as described further in paragraphs 6.2 and 6.3 of this AC, and may be used directly to develop the POF. Historically, probabilistic risk assessment or other bottoms up approaches have also been used as inputs, specifically into POF allocations. These approaches may be utilized if the POF analysis is demonstrated to be consistent with historical data described in § 450.131(a)(1) and (2).

An applicant's probability of failure methodology submitted in accordance with § 450.131(f)(1) may include the specific flight decomposition itself or may be more broadly scoped to describe how the decomposition will be completed for each mission type. For the latter, the methodology may describe the process that the operator uses to identify all key flight safety events at a consistent resolution for a given mission type, followed by the process used to identify flight events and phases of flight. If the operator chooses the more broadly scoped methodology, the key flight safety events and flight decomposition would become items that FAA may inspect for compliance after a license is issued.

6.1.3 Vehicle Failure Probability.

Vehicle failure probability, or probability of failure, should be interpreted as the likelihood that a launch or reentry vehicle has a failure during flight within the scope of the flight safety analysis per § 450.113 for any reason, including a payload event. Failure is further explained in paragraph 6.4 of this AC.

[2] A probability of one must be used for any planned debris hazards or impacts per § 450.133(a)(6).
[3] This applies even if the failure rate is zero, for example, during an upper stage coast between separation from the booster and ignition for a given failure mode. See additional detail in paragraph 6.6.5 of this AC.

6.1.4 Consistent.

"Consistent" in this context should be interpreted as in agreement. "Consistent" across hazards and phases of flight does not necessarily mean that the exact same probability of failure needs to be used for a given phase or hazard, but that the probability of failure used should be within the defined uncertainty such that conservatism can be implemented when needed to meet § 450.101(g). The § 450.101(g) requirement states that the analysis must produce results consistent with or more conservative than the results available from previous mishaps, tests, or other valid benchmarks. Therefore, an operator may vary the probability of failure within statistical confidence limits for the same event in different contexts to bias an analysis towards a conservative outcome.

Example: An operator is proposing to launch a two-stage launch vehicle from both Cape Canaveral Space Force Station (CCSFS) and Vandenberg Space Force Base (VSFB). In this case, due to a lack of fidelity, the best-available data indicates the mean conditional probability of a failure during first stage and second stages of flight are both 50%, with plus or minus 10% uncertainty at a minimal level of confidence (e.g., lower and upper bound confidence limits at 40% and 60% based on the binomial distribution). Given the fact that the public exposure to hazardous debris effects for launches from VSFB is relatively high during stage one, and the opposite is true for launches from CCSFS, a consistent and reasonably conservative probability of failure analysis that meets § 450.101(g) would use a 60%–40% split in the conditional probability of failure during stage one and stage two flight for launches from VSFB, but a 40%–60% split in the conditional probability of failure during stage one and stage two flight for launches from CCSFS.

This reasoning could also be applied to varying the probability for different hazards at the same launch site to bias the analysis towards a conservative outcome (debris analysis versus toxics analysis, for instance).

6.2 **Explanation of § 450.131(a)(1) Fewer Than Two Flights.**

Section 450.131(a)(1) states that "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."

6.2.1 Vehicle or Vehicle Stage With Fewer Than Two Flights.

An operator should consider the number of flights of its subject vehicle or vehicle stage.[4] See paragraph 6.5 of this AC for an explanation of what constitutes flight for a launch or reentry vehicle. In the context of § 450.131(a)(1), "vehicle" should be interpreted as the set of individual vehicles sharing the same design, rather than the individual build of a given vehicle (and likewise for "vehicle stage"). If an operator's subject vehicle or vehicle stage has zero or one flight only, then § 450.131(a)(1) is applicable.

[4] FAA's preferred method for a probability of failure analysis is to develop the probability of failure either by stage or by phase, rather than at the top-down vehicle level. A launch vehicle may have multiple stages to consider, while a reentry vehicle would not have separate stages but separate phases to be analyzed.

When determining whether § 450.131(a)(1) or § 450.131(a)(2) applies, it is important to determine which subject vehicle history is relevant, since vehicles often evolve over time or have different configurations. Significant upgrades/configuration changes to a vehicle may make past flight history inapplicable or less relevant.[5] Examples of significant upgrades include Falcon 1 vs Falcon 9 v1.0 vs Falcon 9 v1.1, as well as Atlas V vs. Atlas I and II. However, relatively minor changes, such as changing joint designs or refining guidance algorithms, should not reduce the relevance of past flights or make them inapplicable to flight history. Likewise, fixes in response to mishaps and anomalies are generally considered typical evolution of a vehicle and in most cases, should not reduce the relevance of past flights. However, it's possible that a reduced weighting factor may be applied to flight history if there is sufficient evidence to demonstrate the effectiveness of corrective actions.

Examples of changes that are considered significant enough to render subject vehicle flight history inapplicable or given less weight are:

- An entirely new or significantly upgraded stage, including:
  - Meaningful changes in the size of the structure.
  - Changes in the structural design (such as from pressure-stabilized to inherently stable).
  - Changes to the type of propulsion system (such as rocket powered only to rocket and scramjet).
  - Significant changes to the type or design of control system (such as thrust only to thrust plus control surfaces, or piloted control to autonomous control, or significant change in size of aerosurfaces).
  - Design changes that result in significant vehicle performance increases
  - Significant changes to material properties of safety-critical components (such as heat shielding).
- A new vehicle developer.
- A vehicle built up of stages and a guidance system used on previous versions of vehicles developed by the operator but not flown as an integrated vehicle.

6.2.2 Account for the Outcome.

Accounting for outcomes should be interpreted as "scoring" the flight history for use in the POF analysis. An operator should define a methodology for scoring, which in this context means determining the outcome (success, failure, or partial failure). Scoring can occur at different levels, such as by flight, stage, phase, or event (see description of these in paragraph 6.1.2). If a failure occurs, scoring also includes determination of the failure mode or failure response mode.[6]

[5] An operator may decrease the relevance of past flight history, or in other words adjust the degree of similarity to the subject vehicle, by applying weighting factors. Typically weighting factors are values from 0 to 1, where 0 is not at all similar to the subject vehicle and 1 is weighted as equivalent to the subject vehicle.

[6] Failure scoring should be done at the failure mode level, but if there is not enough information to determine the failure mode, then the scoring may be done at the failure response mode level.

Notes for determining phase/event of scoring:

- If a single failure occurs during concurrent events, the failure should only be scored for the relevant event; other concurrent events should receive no score.

  Example: If a payload fairing failure occurs during a stage burn, an operator would not score a failure in both the payload fairing and stage burn events; the stage burn phase should not receive a score in this case.

- It is less common, but it is possible to have two independent failures, either concurrently or non-concurrently. In this case, both events should be scored as a failure.

  Example: If both an engine fails to ignite, leading to no thrust during stage 2 burn phase, and an independent guidance system failure occurs during the second burn of a booster flyback, then each phase should be scored as a full failure.

- If a phase of flight does not begin due to an earlier failure, that phase should receive no score (zero successes or failures).

  Example: If the vehicle is lost due to a catastrophic explosion shortly after takeoff during stage 1 burn, then stage 1 burn should be scored as a full failure, and all subsequent phases should receive no score.

- Partial failures may be scored in multiple phases to account for the influence of a failure on the POF estimate if the failure had the potential to occur in a different phase. When scoring partial failures, the scoring should also include the number of observations in that phase (i.e. number of partial failures plus number of partial successes). A partial success should be scored if the vehicle successfully completed the phase, and zero success should be scored if the vehicle did not successfully complete the phase.

  Example: If a booster was lost after flyback and landing due to a stage 1 fuel leak, and there is potential to have lost the booster due to the fuel leak during two previous burns, then half a failure and half a success may be assigned to each of the two previous burns. This scoring accounts for the potential to lose the vehicle during the burn phases while not actually losing the vehicle until after landing.

6.2.3 Previous Flights.

Refer to paragraph 6.5 of this AC for explanation of previous flights.

6.2.4 Developed and Launched or Reentered in Similar Circumstances.

The phrase “developed and launched or reentered in similar circumstances” is intended to acknowledge the potential influence of how a vehicle is developed and operated on the true probability of failure. For brevity, the term “similar vehicles” is used for the vehicles developed and launched or reentered in similar circumstances as the subject vehicle, and the term “similar flights” is used for the flights of such vehicles. For a subject vehicle with no or little flight history, the POF estimate should be consistent

with the flight histories of similar vehicles. An accepted method to determine similar flights is:

1. Define the criteria to be considered for determining the set of similar vehicles, and then similar flights of those vehicles, to create an initial set of historical data. See paragraph 6.2.5 of this AC for criteria considerations.
2. Define how the phases of similar flights will be assessed. Similar flights should have flight decomposition defined in a similar manner to the subject vehicle, as described in paragraph 6.1.2 of this AC so that outcomes can be applied to the correct phases of flight.
3. Define how the outcomes of similar flights will be assessed (paragraph 6.2.2 of this AC). This may be defined separately from how outcomes of the subject vehicle are defined since less data is likely available. For similar flights, operators should use the best available data. Data obtained from public sources often does not have the same level of detail and root causes that the operator would have about their own subject vehicle. Assumptions and justifications should be provided for any missing information on failure modes and event timing.
4. Determine whether the criteria selected in step 1 above is meaningful. One way to determine whether the criteria selected in step 1 is meaningful is to test for statistical significance, as described in paragraph 6.2.5.4 of this AC.
5. Finalize set of similar flights. This may include weighting the flights by similarity to the subject vehicle. Weighting should account for uncertainty in the similarity, such as reducing weighting when there is little public information on a prior operation to make a similarity assessment.

Note that the process above may be applied to each phase of flight; each phase of flight of the subject vehicle may have a different set of similar flights.

Example: A winged reentry vehicle may have similar flights that include capsules for the high load regimes and exclude capsules for the glide phases of flight based on the similarity criteria used for each phase.

6.2.5 Similarity Criteria.

When deciding what constitutes similar operations, or the degree of similarity, the main factors that have major influence are 1) vehicle characteristics, 2) reliability approach, and 3) organizational processes, as discussed below.

6.2.5.1 **Vehicle Characteristics.**

6.2.5.1.1 Vehicle Configuration.

Vehicle configuration should consider types of propellants, the use of boosters, control system type, heat shielding type, etc. However, it may be appropriate to use data from a similar subsystem even if it is on a different type of vehicle.

6.2.5.1.2 Vehicle History.

History should consider both the history of the vehicle[7] (the vehicle "model") and of the particular vehicle hardware item for reusable vehicles. The number of successes and failures are both relevant. For example, a vehicle with a history of high rate of failures should be considered more similar to others with a high rate. Recent history may be more relevant than the early history when a vehicle was in a pre-operational phase. The number of prior flights of a vehicle item for reusable vehicles is also likely relevant. For example, the failure probability of first flights of vehicles has been higher than later flights because design defects, process deficiencies, and manufacturing defects are more likely to manifest. On the other hand, "flight leaders" may have a higher failure probability due to exposing wear out issues.[8]

6.2.5.1.3 Technological Maturity.

Technological maturity should consider the degree to which the technology on the vehicle has been successfully demonstrated on prior operations. Unlike vehicle history, this is not specific to the vehicle system, but the general level to which subsystems on the vehicle have a heritage from past vehicles. Operators may assess technological maturity of similar vehicles using Technological Readiness Levels (Reference 4). Similarly, operators may assess manufacturing capability using Manufacturing Readiness Levels Reference (7).

6.2.5.2 Reliability Approach.

Reliability of the vehicle is a key factor in the likelihood of failure. Risk elimination and mitigation measures, per § 450.109(b), are an essential means of reducing the likelihood of functional failures and thus obtaining higher reliability of a vehicle. These measures often aim to achieve a certain reliability, but the actual (real-world) reliability is typically far lower, at least until a system is very mature. Moreover, vehicles that are developed and launched or reentered using a "fail fast, fail forward" approach generally demonstrate a higher failure rate during initial flights than vehicles that employ a more traditional approach historically used by U.S. Government programs, where the developer attempts to address weaknesses prior to launch.

[7] History of the vehicle in this context means history of the type of vehicle itself (e.g., all history of the Electron vehicle). As discussed in footnote 5, the relevance of past vehicle history may be adjusted for similarity to the subject vehicle with weighting factors (e.g., the relevance of Falcon 9 v1.0 to Falcon 9 v1.1).

[8] The failure rate over time of reused hardware has historically followed a bathtub curve, as described further in Section 3.1.2 of Reference 2, where 1) the first region exhibits a decreasing failure rate due to early failures, 2) the middle region exhibits a constant failure rate due to random failures, and 3) the last region exhibits an increasing failure rate due to wear-out failures.

To address reliability, the level of rigor of the risk elimination and mitigation measures applied to other operations should be considered as a factor in similarity. Level of rigor for these measures include granularity of hazard analysis, thoroughness of evaluation of environments and uncertainty, extensiveness of verification and validation, etc. However, since a thorough analysis of past vehicle systems is not likely possible, operators should use available information that could inform the rigor, such as:

- Verification and validation evidence, which may be either direct (documentation, media) or indirect (requirements of the customer).
- Standards to which the vehicle systems have been certified (e.g. Space and Missile Systems Center Standard SMC-S-016, NASA Human Spaceflight Standards).
- Value of the payloads (e.g. "demonstration only" operations, high-value satellites, humans).
- The extent to which an independent organization has assessed mission assurance.
- Available records of hazard analysis (such as probabilistic risk assessments).
- Design standards used (for instance, factors of safety used in designing a system).

6.2.5.3 **Organizational Processes.**

6.2.5.3.1 System Safety Program Maturity.

A major factor in determining similar vehicles and similar flights is the maturity of the system safety program. Generally, developers with immature system safety programs (i.e. the minimum needed to meet system safety requirements) will have a higher likelihood of failure. Aspects of the system safety program that should be considered are:

- the completeness, independence, and authority of system safety organization,
- traceability documentation,
- audit practices,
- whether practice is consistent with current standards,
- the extent of training,
- how often personnel changes take place, and
- safety culture.

As with the discussion of reliability approaches above, a thorough analysis of past organizations may be difficult due to limited insight, but evidence, such as procurement information and/or requirements imposed by customers, regulations, or launch sites can be informative. Another acceptable method to assess system safety program maturity is described in Reference 5.

6.2.5.3.2 Developer Experience.

The experience levels of the developers of the selected similar vehicles may be considered with respect to the experience level of the subject vehicle's developer. Examples of criteria used previously to evaluate developer experience include:

- Experienced launch developers correspond to developers who have produced at least one vehicle with a demonstrated POF less than or equal to 33% (Reference 6).
- Brand new launch developers correspond to developers who have no previous experience and are using a new rocket engine.

The experience considered relevant should be of a similar scale of vehicle using similar technologies. For example, launch vehicle experience should not apply to reentry vehicle development (other examples include amateur rocket experience versus orbital vehicles, pad launch experience versus air launches, etc.).

6.2.5.4 **Statistical Significance.**

After criteria to identify similar flights are identified, an operator should evaluate if the criteria are statistically meaningful. Criteria should be based on logical reasoning (for example, there is no logical reason to separate flight ordinals 4, 8, 12, 16, etc. from all other flight ordinals).

One way to determine if a set of criteria is meaningful in determining similar vehicles and similar flights is to demonstrate statistical significance when being used in the dataset through a Bayesian uncertainty analysis.[9] A common approach to determine when datasets are distinct is to examining distributions using a Beta distribution[10] with a Jeffreys prior. In this approach, the parameters (α, β) of the Beta distribution are given by:

$$\alpha = r + 0.5$$
$$\beta = s + 0.5$$

Where s is the number of successes and r is the number of failures. This is related to the conditional probability of failure as $P_{cond} = \frac{r}{r+s}$. Plots of the beta distributions can be examined to determine if a set of criteria is

[9] For more discussion on the use of a Bayesian approach in POF analysis, see Reference 1.
[10] For more on beta distributions, see, for example, https://bookdown.org/pbaumgartner/bayesian-fun/05-beta-distribution.html.

significant. The methodology should have a quantifiable threshold for statistical significance of the criteria.

Example: Figure 1 shows POF distribution of the first two flights of new vehicles by new operators ("NN") in blue, based on the data provided in Table 1. The NN group was categorized further three different ways (high, medium, and low) using a beta distribution, depending on different combinations of whether each operator has ever built a rocket previously and if the subject vehicle used a brand-new rocket engine.

Table 1: Example of using distributions to identify statistically significant categorizations

	NN (All)	High NN	Medium NN	Low NN
Failures (*r*)	19	10	4	5
Successes (s)	48	4	23	21
Conditional POF (P_{cond})	28%	71%	15%	19%
alpha (α)	19.5	10.5	4.5	5.5
beta (*β*)	48.5	4.5	23.5	21.5

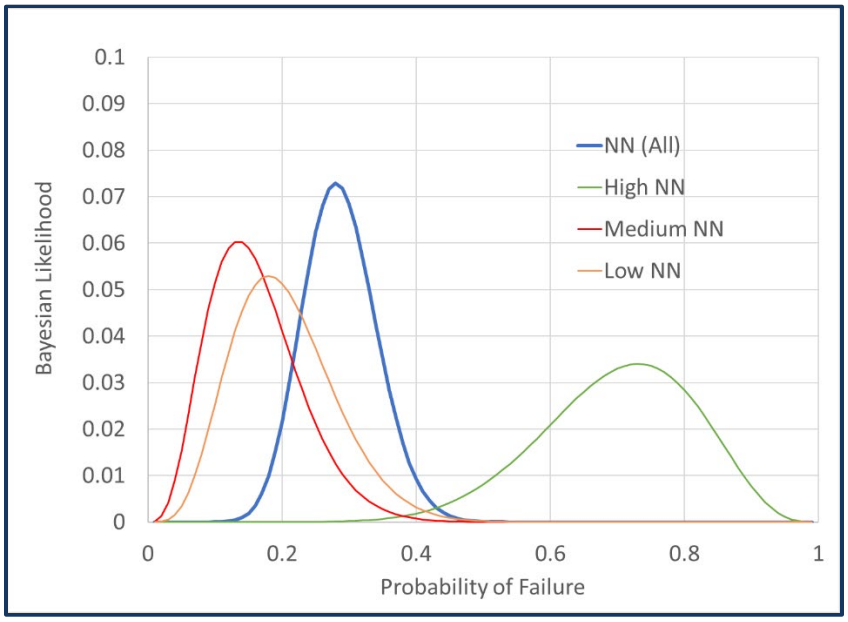

Figure 1: Example of using distributions to identify statistically significant categorizations

Figure 1 shows that "High NN" has very little overlap with other groups, demonstrating statistically distinct results. "Medium NN" and "Low NN" have significant overlap, illustrating they do not demonstrate distinct enough results to define their own categorizations.

Additional information and examples related to developing similarity criteria based on statistical significance may be found in Reference 3.[11]

6.3 **Explanation of § 450.131(a)(2) Two or More Flights.**

Section 450.131(a)(2) states that "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."

6.3.1 Vehicle or Vehicle Stage With Two or More Flights.

An operator should consider the number of flights of its subject vehicle or vehicle stage. See paragraph 6.5 of this AC for an explanation of what constitutes flight for a launch or reentry vehicle. In the context of § 450.131(a)(2) as with § 450.131(a)(1), "vehicle" should be interpreted as the set of individual vehicles sharing the same design, rather than the individual build of a given vehicle (and likewise for "vehicle stage"). If an operator's subject vehicle or vehicle stage has two or more flights, then § 450.131(a)(2) is required.[12] However, as discussed further in paragraph 6.3.4 of this AC, in most cases an operator should also account for § 450.131(a)(1) in addition to § 450.131(a)(2).

6.3.2 Account for the Outcomes.

Refer to paragraph 6.2.2 for explanation of accounting for outcomes of flight history in general. For accounting for outcomes of the subject vehicle or vehicle stage, operators should provide the scoring in the appropriate mishap reporting[13] or post-flight reporting.[14] The operator should clearly identify any failures that occurred (described further in paragraph 6.4 of this AC), describe how the data is categorized within predefined flight decomposition and data classification rules, and identify any exceptions to predefined rules. If a failure of the subject vehicle does not fit into defined decomposition and classification rules, the methodology may require an update.

Note that explicit scoring in the post-flight reporting is only necessary if a mishap or anomaly has occurred; the POF methodology may note that if all planned events occur nominally, the event will be scored as a success by default.

6.3.3 Previous Flights.

Refer to paragraph 6.5 of this AC for explanation of previous flights.

[11] Although the FAA cannot verify the accuracy of an external data source, Reference 3 also includes SpaceX's launch history database.
[12] This statement is true even if the first two flights have failure outcomes. Refer to paragraph 6.3.4 of this AC for consideration of recent failure frequency.
[13] Per § 450.173.
[14] Per § 450.215.

6.3.4 Statistically Valid Manner.

An operator's methodology must account for the outcomes of all previous flights of the subject vehicle or vehicle stage in a statistically valid manner. **For an explanation of valid statistical methods, refer to AC 450.115-2, paragraphs 7.1.2 and 8.2.3**. For a POF analysis, an operator should perform the following in order to account for outcomes in a statistically valid manner:

1. Clearly define the data collection and categorization rules of post-flight data reviews per § 450.103(d).[15]
2. Score all subject vehicle flights in post-flight data reviews on an ongoing basis for updated and reliable statistics.
3. Analyze the historical data to produce a predicted probability of failure for the subject operation, accounting for uncertainty per § 450.115(b)(1).

Except in the case where similar flights are demonstrably different than those of the subject vehicle (as described further in the first bullet below), an operator should continue to include previous flights of similar vehicles per § 450.131(a)(1).[16] Using only the subject vehicle data typically results in small data sets, so uncertainty is large. A common approach to combining similar vehicle data and subject vehicle history is a Bayesian update approach.

The predicted POF should not normally be lower than the failure frequency of the subject vehicle. There are some instances where the methodology could be reevaluated:

- An operator may remove historical data of similar flights if the failure probability of the subject vehicle is demonstrably different from that of the set of "similar vehicles." This can only be demonstrated after the subject vehicle has accumulated significant flight history. The operator should test for statistical significance, as described in paragraph 6.2.5.4 of this AC, of the subject vehicle outcomes against the historical data of similar flights as a part of the POF methodology to assess the validity of the historical data.
- An operator should have criteria to determine when POF methodology should be reevaluated to ensure compliance with § 450.101(g) which states "The method must produce results consistent with or more conservative than the results available from previous mishaps…" Generally, an operator's consideration of the most recent failures may provide a measure of recent failure frequency. This frequency should be within a methodology's predicted failure frequency, accounting for uncertainty. This criteria check should be completed as a part of the post-flight data review required per § 450.103(d).
    - If the subject vehicle experiences a failure that meets the definition of § 450.131(b), the following equation may be used to determine if the POF methodology should be reevaluated:

[15] At a minimum, the data must be collected and categorized at the same level of fidelity as the flight decomposition; however, higher fidelity data tracking may provide additional insights in the future and is encouraged.
[16] For this reason, the binomial "Christmas tree" approach from A417.25(b)(5)(iii) is not a preferred method, since it doesn't take into account prior information related to the vehicle or operator.

$$N_{prev} < \frac{1}{1.5 \times P_F}$$

Where N_{prev} is the difference between flight ordinals of the two most recent failures and P_F is the conditional probability of failure predicted for the most recent failure. The equation considers the two most recent failures to check if the actual outcomes are aligned with the methodology, with the 1.5 factor added for uncertainty. If the condition in the equation above is true, then the method should be reevaluated. This should apply at the flight, stage, phase, and event levels. Partial failures as applied to this equation will be addressed in a future revision of this AC.

Example: A simple two stage vehicle is decomposed into stage 1 and stage 2 phases. The vehicle has stage 1 failures on flights 3 and 40 and a stage 2 failure on flight 10. Flight 40 P_F is 5% for stage 1 and 3% for stage 2 (8% total vehicle P_F).

For stage 1:

$$N_{prev} = 40 - 3 = 37$$

$$\frac{1}{1.5 \times P_F} = \frac{1}{1.5 \times 5\%} = 13.3$$

For the whole vehicle:

$$N_{prev} = 40 - 10 = 30$$

$$\frac{1}{1.5 \times P_F} = \frac{1}{1.5 \times 8\%} = 8.3$$

For both stage 1 and the whole vehicle, N_{prev} is greater than $\frac{1}{1.5 \times P_F}$ so the methodology would not need to be reevaluated.

Some examples of aspects of the methodology that could be reevaluated include, but are not limited to, redefining criteria used to determine "similar circumstances" per § 450.131(a)(1), adjusting weighting factors, adjusting allocation, etc. The scope and result of method reevaluation is not meant to be prescriptive, as the criteria is meant to be used as a "checkpoint" during post-flight data review to see if method updates are warranted.

6.3.5 Account for Data.

Accounting for data on any mishap and anomaly should be interpreted such that an operator should consider any mishaps and anomalies of the subject vehicle and provide "scoring" of any mishaps or anomalies that may be considered failures or partial failures for use in the POF analysis. See paragraph 6.2.2 for more on scoring, paragraph 6.3.6 for mishaps, paragraph 6.3.7 for anomalies, and paragraph 6.4 for what constitutes a failure that should be scored.

6.3.6 Mishap.

Mishap is defined in § 401.7, using nine different criteria for consideration. Some of these criteria can help the operator determine if a failure has occurred. If a mishap of the subject vehicle results in any of the following criteria from the definition of mishap in § 401.7, then it should be considered a failure[17]:

> *(7) Unplanned permanent loss of a launch or reentry vehicle during licensed activity or permitted activity;*
>
> *(8) The impact of hazardous debris outside the planned landing site or designated hazard area; or*
>
> *(9) Failure to complete a launch or reentry as planned as reported in § 450.213(b).*

These criteria are described in further detail in AC 450.173-1, paragraph 5.6, subparagraphs (7), (8), and (9). Reference that AC for additional explanation on the mishap criteria listed for these events that constitute a mishap.

It is possible that the other event criteria, found in subparagraphs (1), (2), (3), (4), (5), and (6) of that paragraph *may* occur as the result of a failure, but they also may occur due to a cause other than a failure. See paragraph 5.6 of AC 450.173-1 for additional explanation on the mishap criteria outlined in subparagraphs (1) through (6).

6.3.7 Anomaly.

Per § 401.7, an anomaly is "any condition during licensed or permitted activity that deviates from what is standard, normal, or expected, during the verification or operation of a system, subsystem, process, facility, or supported equipment."

Section 450.103(d)(3) requires a post-flight data review to "identify any anomaly that may impact any flight hazard analysis, flight safety analysis, or safety-critical system, or is otherwise material to public safety". Section 450.103(d)(4) requires addressing these anomalies, including updates to the flight safety analysis, prior to the next flight. A POF methodology should describe how anomalies will be accounted for in the POF analysis, including any criteria used to determine the types of anomalies of the subject vehicle that will be tracked as failures or partial failures as discussed in paragraph 6.4.3.

[17] Note that a test-induced damage exception per § 450.175 should not be considered a mishap nor an observed failure/success.

6.4 Explanation of § 450.131(b) Failure.

Part 450.131(b) states that "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."

6.4.1 Failure.

The definition of failure provided in § 450.131(b) should be used to determine outcomes of previous flights of the subject vehicle and/or similar vehicles as required by § 450.131(a). A failure from a public safety perspective is not synonymous with a mission failure. On the one hand, a flight may successfully accomplish its objectives, but an object or debris outside of the planned envelope is a hazard to the public. On the other hand, a payload that fails to function may be a mission failure, but all objects could follow their expected trajectories through orbital insertion.

The paragraphs below provide an expanded discussion of the definition of failure from a public safety perspective. In general, a full failure should be counted when:

- A vehicle does not complete any phase of normal flight.
- A vehicle stage or its debris travels outside the normal trajectory envelope.
- A vehicle stage or its debris impacts land or water outside of planned impact regions.
- An anomalous condition produces unexpected and potentially hazardous debris.
- An anomalous condition exhibits the potential for the vehicle to fail in any of the ways described above during the mission or any future mission of similar vehicle capability.

6.4.2 When a Vehicle Does Not Complete Any Phase of Normal Flight.

A phase of flight is described in paragraph 6.1.2 of this AC and normal flight is defined in § 401.7. If a vehicle does not complete a phase of normal flight within the normal flight times as characterized in § 450.117, it should be interpreted such that the vehicle has not achieved the milestone that defines the end of a phase.[18]

A POF methodology should define how the failure will fit within the flight decomposition, as described in paragraph 6.1.2 of this AC. In some situations, a failure initiation may occur earlier than the failure manifestation at a vehicle level (refer to Chapter 4 of this AC for definitions of failure initiation and failure manifestation). In these situations, it can be difficult to assess when the failure "occurred" – i.e. which phase of flight a failure should be counted.

[18] One exception to this may be if the vehicle is following a contingency flight plan that is characterized as a normal trajectory, such as a captive carry flight scrubbing the drop of the rocket and returning to land following a planned flight path.

Note: A failure manifestation at the vehicle level occurs when the vehicle loses structural integrity or exceeds the bounds of the applicable normal uncertainty (incertitude) trajectory set in position, velocity, orientation, or angular velocity as function of flight time. See paragraph 6.4.6 of this AC for more discussion of outside normal uncertainty.

If the failure initiation and failure manifestation occurred in the same phase, it should be scored in that phase.

Example: On a two-stage launch vehicle, if the first stage burn has an anomaly that leads to the first stage flying outside of the normal trajectory envelope (see paragraph 6.4.6 of this AC) during its burn, then the failure should be scored during the first stage burn.

If a failure initiates in a phase but it does not manifest at the vehicle level until a later phase, then the operator should consider the specific circumstances of the failure and the information available.

Case 1: If a failure initiates in a phase and causes the vehicle to deviate in the same phase, but the vehicle continuously proceeds through a milestone before the failure manifests, and there are no vehicle configuration changes, then the failure should be counted in the phase where the failure initiated:

Example: A launch vehicle flight has phases delineated by dynamic pressure criteria (e.g. a high-Q phase). A guidance failure initiates before this phase begins, but the vehicle is still inside the normal trajectory envelope when the high-Q phase begins. The failure would be counted as occurring in the prior phase.

Case 2: If the initiating event of a failure occurs in one phase, but there is no potential effect on the performance of the vehicle until a later phase, then the failure should be counted where the failure began to manifest.

Example: A propellant leak develops in an upper stage during first stage flight. There is no effect on the first stage flight. This failure should be counted when the failure manifests, which may be in the upper stage ignition event (if ignition fails) or during the burn phase (if propellant runs out).

Case 3: If a failure initiates during a phase, had the potential to affect the performance of the vehicle during that phase, but did not manifest until a later phase, the failure should normally be allocated as an anomalous condition (see paragraph 6.4.3) to the initiating phase and a failure in the phase where it manifested. If anomalies are scored as partial failures, this would result in scoring the phase where it manifested as a partial failure also (the remainder of the full failure that was allocated to the initiating phase).

Example: On a reusable stage 1 booster with flyback, there is a propellant leak during the first stage burn that leads to the landing burn phase beginning but not completing. The scenario should be considered an anomalous condition in the first phase and a failure in the landing phase, since this captures where the hazard was generated (i.e. landing phase) and the potential for the failure to have manifested in first stage burn.

If a situation arises that does not clearly fit in these categories, operators are encouraged to discuss the approach with FAA.

It is important that allocation of failures to phases be consistent with the methodology used to characterize malfunction flight per § 450.119(c)(1). For case 1, it is critical that the malfunction flight simulation begin in the initiating phase and the malfunction continue through the following phase(s). The approach to handling case 3 requires careful consideration to ensure that each scenario is properly considered. If a vehicle can separate into two during flight, the situation where a failure initiates but then separation occurs should be considered in the malfunction trajectory analysis.

The level of fidelity of assigning failures to phases may be lower for flights of similar vehicles as compared to flights of the subject vehicle. When detailed failure information is not available, it is acceptable to score the failure in the phase where the failure manifested.

6.4.3 Anomalous Condition.

Derived from the definition of anomaly in § 401.7, an anomalous condition should be interpreted as any condition that deviates from what is standard, normal, or expected, during the verification or operation of a system, subsystem, process, facility, or support equipment. Per § 450.103(d)(3), an anomaly is required to be identified by an operator in the post-flight data review if the anomaly may impact any flight hazard analysis, flight safety analysis, or safety critical system, or is otherwise material to public safety. Operators should track anomalies that occur during licensed activity and categorize them by severity. The severity level of the anomaly should then be used to assign an outcome (success, failure, or partial failures).

6.4.4 Exhibits the Potential.

The definition of failure in § 450.131(b) includes the phrase "exhibits the potential" to account for situations where no hazard to the public occurred on a given operation, but it likely would have if the same anomaly occurred on another operation of the same vehicle. Examples include if a given anomalous condition would cause a failure on a mission of a different azimuth, on a mission with a heavier payload, at a different time in flight, etc. Similarly, if a failure manifests outside the scope of the flight safety analysis defined in § 450.113, the operator should consider if it exhibited the potential to fail at a different time in flight or on a different mission of similar capability.

Example: If an anomaly occurs after orbital insertion that would have likely caused a failure on a mission going to a different orbit, this should be counted as a failure.

6.4.5 For a Stage or Its Debris to Impact the Earth or Reenter the Atmosphere.

"For a stage or its debris" should be interpreted as referring to a vehicle's stage or a vehicle's debris, which should include an intact vehicle, vehicle fragments, any detached vehicle component whether intact or in fragments, payload, or planned jettison bodies. If a stage or its debris shows evidence of or exhibits the potential to travel outside of the normal trajectory envelope, even if it demises upon atmospheric reentry, then a failure has occurred. Similarly, if a stage or its debris shows evidence of or exhibits the potential to impact land or water outside any planned impact region as required by §§ 450.133(b)(1) and (c)(1), then a failure has occurred.

6.4.6 Outside the Normal Trajectory Envelope.

"Outside the normal trajectory envelope" should be interpreted as a deviation in present position, instantaneous impact point (IIP), and/or time[19] outside of the set of incertitude trajectories required by § 450.117(a)(2). This should be assessed at the beginning and end of each phase of flight. The POF methodology should specify the criteria for determining if the vehicle has traveled inside or outside of the normal trajectory envelope. An operator may use a factor of two of the 97% confidence of the three-dimensional spatial volume and of the time distribution. For example, if the trajectory IIP incertitude has been characterized by a bivariate normal distribution at each milestone, and if the actual IIP is outside twice the 97% confidence ellipse of that distribution, then it is a failure.

Note: Unexpected debris has no normal trajectory envelope, so unplanned events that produce hazardous debris are also generally considered failures.[20]

6.4.7 During the Mission or Any Future Mission of Similar Vehicle Capability.

"During the mission" should be interpreted as during launch or reentry, including any phase of flight within the scope of the flight safety analysis, as defined by § 450.113. Future missions of similar vehicle capability should be interpreted as missions that may take place at a later time with similar objectives (reentry, orbital, or suborbital, for instance).

The requirement states that anomalous conditions could occur either during the mission or any future mission of similar vehicle capability to count as a failure.

Example: An orbital launch vehicle substantially underperforms outside of the normal trajectory envelope during a mission but still reaching its intended orbit because the payload is lighter than the maximum payload weight; this anomaly should be counted as a failure since the vehicle went outside the normal trajectory envelope, and a future mission with a heavier payload or targeting a different orbit has the potential to not achieve orbit and impact the Earth outside of hazard areas.

6.5 Explanation of § 450.131(c) Previous Flight.

Section 450.131(c)(1) defines "previous flight" for launch by stating that, for flight safety analysis purposes, the "flight of a launch vehicle begins at a time in which a launch vehicle lifts off from the surface of the Earth." Section 450.131(c)(2) defines "previous flight" for reentry by stating that, for flight safety analysis purposes, the "flight of a reentry vehicle or deorbiting upper stage begins at a time in which a vehicle attempts to initiate reentry."

6.5.1 Previous flight.

The definition of previous flight provided in § 450.131(c) should be used to determine applicable flights of the subject vehicle and/or similar vehicles as required by § 450.131(a).

[19] Time is important to consider because hazard areas are time based.

[20] Unplanned hazardous debris should be captured within a failure response mode; it may be negligible risk compared to catastrophic on-trajectory failure response mode.

Note: Applicable flights for the probability of failure analysis to consider may include flights conducted outside FAA licensed activity, such as amateur, permitted, U.S. government, or foreign launches, reentries, or flights.

6.5.2 Launch Vehicle.

Section 401.7 defines a launch vehicle as "a vehicle built to operate in, or place a payload in, outer space or a suborbital rocket."

6.5.3 Lifts Off from the Surface of the Earth.

Per § 401.7*,* liftoff "means any motion of the launch vehicle with intention to initiate flight." Liftoff occurs when the vehicle moves relative to the launch platform, whether the platform is on land or floating in a body of water. It should then be interpreted that:

- While consideration of ignition *prior* to lift-off is not required when determining applicable previous flights, a failure where ignition occurs and a vehicle topples over while still in contact with the pad should be taken into account in the probability of failure analysis.
- Captive carry phases of flight should be accounted for in the probability of failure analysis, unless the exception in § 450.113(b) applies to that phase of flight.

6.5.4 Reentry Vehicle.

Section 401.7 defines a reentry vehicle as "a vehicle designed to return from Earth orbit or outer space to Earth substantially intact. A reusable launch vehicle that is designed to return from Earth orbit or outer space to Earth substantially intact is a reentry vehicle."

6.5.5 Deorbiting upper stage.

A deorbiting upper stage should be interpreted as a stage of a vehicle that returns or attempts to return from Earth orbit to Earth in a controlled manner. This phrase is included to ensure that disposal, as defined in § 401.7, is also included in "previous flight" defined in § 450.131(c).

6.5.6 Time in Which a Vehicle Attempts to Initiate a Reentry.

The time in which a reentry vehicle or deorbiting upper stage attempts to initiate a reentry should be interpreted as the first time at which the reentry flight would fall within the scope of license per § 450.3(c).

It is noted in § 450.3(c) that the scope of a reentry license includes activities conducted in Earth orbit or outer space to determine reentry readiness, otherwise known as reentry readiness checks. The scope of the flight safety analysis, however, is defined differently and begins at the initiation of the deorbit itself, as described in § 450.113(a)(4). Failures that occur within the scope of reentry license but outside the scope of the flight safety analysis should still be accounted for in the POF analysis, as these failures could still meet the definition of § 450.131(b). A random reentry failure should also be accounted for in the POF analysis, even if it occurred outside the scope of the reentry license, since a random reentry meets the definition of § 450.131(b) failure, in that it exhibits the potential for a stage or its debris to impact the Earth.

6.6 **Explanation of § 450.131(d) Allocation**.

Part 450.131(d) states that "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."

6.6.1 Allocation.

In this context, "allocation" should be interpreted as the distribution of the probability of failure across flight phases and failure modes/failure response modes, as described further in paragraphs 6.6.2 and 6.6.3 of this AC.

6.6.2 Distributed Across Flight Phases.

The probability of failure should be allotted across all phases of flight within the scope of the flight safety analysis defined in § 450.113(a). "Phase of flight" is explained in paragraph 6.1.2. An operator should ensure distribution across flight phases by calculating the probability of failure at the flight phase, stage, or event levels.

6.6.3 Distributed Across Failure Modes.

6.6.3.1 **Failure Modes.**

The probability of failure should be allocated across failure modes applicable to the subject vehicle. In the context of § 450.131, failure modes are used to classify historical failures to determine the probabilities of the various ways a flight can malfunction. Failure modes should be linked to the functional hazard analysis, as described in AC 450.107-1. A failure mode consists of three elements: the initiating subsystem of the failure, the resulting manifestation of the failure (also known as the vehicle response), and the flight event where the failure manifests.

To illustrate, consider the following failure mode examples:

- Propulsion system failure (turbopump failure of only engine) leading to total loss of thrust during stage 2 burn.
- Guidance system failure (computer shutdown) leading to total loss of thrust during stage 2 burn.

- Propulsion system failure (only engine failed to ignite) leading to no thrust during initiation of stage 2.
- Flight safety system failure (data to Mission Flight Control Officer (MFCO) screen lost) leading to loss of thrust during stage 2 burn.

These demonstrate that simply labeling a failure mode as "loss of thrust" does not provide enough context when categorizing past failures, since multiple failure modes may have the same vehicle response. A loss of thrust vehicle response can be caused by an engine failure, guidance failure, or propellant exhaustion for instance. The initiating subsystem element is necessary when categorizing historical failures for the purpose of a POF analysis because what causes one type of failure on a past vehicle may cause a different type of failure on the subject vehicle. This becomes important when determining allocation to failure response modes, as discussed in paragraph 6.6.3.2 below.

An operator should determine what failure modes are reasonably foreseeable within each flight phase, stage, or event defined within the scope of the flight safety analysis.[21] Certain failure modes may always be present across the flight while others may only be foreseeable while certain hardware is in operation or certain environments are experienced.

Example: A failure mode associated with the flight computer will be foreseeable from the beginning to the end of the flight. However, a failure mode of a solid rocket strap-on booster is only foreseeable while that booster is burning or until it is jettisoned, depending on the failure mode itself.

The identification of failure modes should be consistent with the functional hazard analysis per § 450.107(b) and malfunction trajectory analysis per § 450.119:

- The functional hazard analysis identifies all failure modes that can occur within all defined flight phases.
- All failure modes identified across all flight phases should be modeled using appropriately defined failure response modes (described further below in paragraph 6.6.3.2) in a § 450.119 means of compliance.

It is noted that for vehicles that employ innovative/emergent designs and technologies, an operator may use techniques such as fault tree and event tree analyses if there is a lack of historical failure data for these types of systems as long as the analyses are designed with appropriate failure mode end states relevant to public safety. For more on how to meet § 450.131(d)(1) given a lack of historical data for a given failure mode, see paragraph 6.6.4 of this AC.

[21] For more on ensuring failure modes are consistent with historical data of similar flights and subject vehicle flights per § 450.131(d)(1) and (d)(2), refer to paragraphs 6.6.5-6.6.7 of this AC.

6.6.3.2 **Failure Response Modes.**

A failure response mode is a group of failure modes that result in a homogenous distribution of trajectories, prior to consideration of mitigations or hazard control strategies. While *failure modes* contain the specifics on the initiating subsystem, response, and timing, *failure response modes* are used to model the failure modes. The failure response modes determine the types of malfunction trajectories modeled per § 450.119.

It is important to note that the same failure on two different vehicles can result in different failure response modes.

Example: Loss of thrust due to an engine failure in a single engine stage may translate to a degraded thrust of a multi-engine vehicle (rather than loss of thrust).

Therefore, the functional hazard analysis should define a failure mode to failure response mode relationship for the subject vehicle. The process for determining the failure mode to failure response mode relationship using the functional hazard analysis should be described within the POF methodology. Typically, failure response modes are used to develop simulations of malfunction trajectories per § 450.119.

Examples of generic failure response modes developed from historical flight failure data are:

- For launch vehicles:
  - Erratic flight (external forces exceed control authority).
  - Fixed control force offset/malfunction turn (tumble/spiral/corkscrew).
- For reentry vehicles:
  - Tumbling, ballistic trajectory due to attitude control failure.
  - Shallow trajectory maintaining attitude control due to deorbit overburn.

The failure response modes listed above are examples only and not meant to be all-inclusive. The operator is responsible for performing an analysis of the subject vehicle to determine failure response modes that would reasonably be expected to occur.

6.6.4 Consistent.

As described in paragraph 6.1.4, "consistent" should be interpreted as in agreement.

One acceptable method for a consistent distribution is for the operator to compile the ratios of failures per failure mode[22] to total number of failures, including both datasets described in § 450.131(d)(1) and (d)(2). These ratios may then be used to assign failure mode allocations using Bayesian inference based on the Dirichlet-Multinomial distribution, similar to the way Bayesian inference is used to estimate failure

[22] Allocation may be distributed by failure mode or failure response mode. Allocation by failure mode is a higher fidelity method, but both options meet the intent of § 450.131(d)(1).

probability. This method is especially useful if there are zero past failures for some of the reasonably foreseeable failure response modes. Bayesian inference will give those failure modes non-zero estimates along with corresponding uncertainty estimates. The sum of all possible failure modes for each flight event, phase, or stage should be equal to 1.

However, "consistent with" means that operators may use allocation methods that do not directly use the data described in § 450.131(d)(1) and (d)(2) as inputs, such as the means of compliance shown in paragraph 7.1 or leveraging probabilistic risk assessments or flight hazard analyses data. In these methods, the allocation should be demonstrated to be in agreement with, or more conservative than, available previous flight data as described in § 450.131(d)(1) and (d)(2).

Operators may consider adjustments to allocation based on different factors such as evidence from flight history patterns, effectiveness of corrective actions taken in response to failures, and vehicle configuration changes that affect reliability. Such adjustments should be documented with technical justification and remain within statistically defensible uncertainty bounds.

6.6.5 The data available from all previous flights of vehicles developed and launched or reentered in similar circumstances.

In order to meet § 450.131(d)(1), the operator should collect the failure history of similar vehicles to be the basis of a failure mode allocation dataset. A top-level process for this is described in paragraph 6.2.4, with guidelines for similarity criteria described in paragraph 6.2.5. However, due to the limited availability of failure data, the criteria for "similar" may be less restrictive than used for calculating the POF by stage, event, or phase. The most important characteristic of similar circumstances in the context of § 450.131(d)(1) is that the failure mode experienced by a similar vehicle is a credible failure mode for the subject vehicle for each respective flight event.

Example: A turbo pump failure of a liquid propellant engine during stage 1 burn is a credible failure mode for other liquid propellant engine burn stages, but not applicable to a solid propellant motor burn stage.

Example: Catastrophic explosion of an engine during a coast phase is not reasonably foreseeable, resulting in a zero failure probability for this failure mode during the coast phases.

Next, the operator should convert the failure mode dataset into appropriate failure response modes relevant to the subject vehicle with the aid of the functional hazard analysis.

Note: Lack of detail may make it difficult to determine a failure mode for prior similar vehicle failures. The failures where there is insufficient data to make a reasonable categorization of the failure mode should be categorized directly by failure response mode if possible. If there is still not enough information to reasonably score the failure response mode, those similar vehicle failures may be ignored, as making an incorrect inference or guess will not add value to the allocation.

6.6.6 Data from previous flights of vehicles, stages, or components developed and launched, reentered, flown, or tested by the subject vehicle developer or operator.

To meet § 450.131(d)(2), an operator should collect the outcomes of previous flights of their subject vehicle, as described in paragraphs 6.3.2 and 6.3.3 of this AC, in addition to other relevant previous experience, as described in paragraph 6.6.7. The outcomes should include any anomalies accounted for in the POF analysis, as described further in paragraph 6.4.3. These outcomes should be added to the outcomes of similar vehicle data as described above in paragraph 6.6.5.

6.6.7 Previous Experience.

Previous experience by the subject vehicle developer or operator should be interpreted as past launches, reentries, and tests by the subject vehicle developer or operator. This allows the allocation across phases and failures to account for data from previous flights of vehicles, stages, or components by the subject vehicle developer or operator that did not qualify as launch or reentry operations, such as drop tests or glide flights. However, past tests may be considered inapplicable or given less weight, such as with the following cases:

- A test success should have a reduced weight applied if the test environment was less severe than in flight.
- A test failure may be considered inapplicable if the intent was to test to fail and the failure was consistent with pre-test analysis.
- A test failure with a vehicle/stage configuration that was subsequently modified to address that failure followed by additional tests or experience demonstrating the effectiveness of the corrective actions may have a reduced weight applied.

Relevant previous experience is described further in paragraphs 6.6.7.1 to 6.6.7.3 of this AC.

6.6.7.1 **Similar Vehicle, Stage, or Component Design Characteristics.**

Relevant previous experience of the subject vehicle developer or operator may be accounted for when determining probability of failure allocations. See paragraph 6.2.5.1 of this AC for considerations of past vehicles, stages, or component design characteristics that can also be applied to previous experience of the subject vehicle developer or operator. Previous experience may be significantly different enough such that it may be considered inapplicable or given less weight.

Example: When determining POF allocation of a solid propellant stage, previous liquid propellant stage history may be considered applicable if failures were unrelated to the propulsion system (e.g. a fairing failure). However, the liquid propellant history may be weighted less if the failure was related to the propulsion system.

6.6.7.2 **Similar Development and Integration Processes, Including the Extent of Integrated System Testing.**

See paragraph 6.2.5.2 of this AC for considerations of reliability that may also be applied to previous experience of the subject vehicle developer or operator, as a proxy for development and integration processes similarity. Previous experience may be significantly different enough such that it may be considered inapplicable or given less weight.

Example: If the subject vehicle operator's previous experience used the same verification and validation process, it may be weighed similarly to the subject vehicle when determining allocation.

6.6.7.3 **Similar Level of Experience of the Vehicle Operation and Development Team Members.**

See paragraph 6.2.5.3 of this AC for considerations of similar level of experience, including system safety program maturity and developer experience, that may also be applied to previous experience of the subject vehicle developer or operator. Previous experience may be significantly different enough such that it may be considered inapplicable or given less weight.

Example: If there has been significant staff turnover since previous experience, with new staff having little experience with new technology, previous experience may be weighed less when determining the POF allocation of the subject vehicle.

6.7 **Explanation of § 450.131(e) Observed vs Conditional Failure Rate.**

Part 450.131(e) states that "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."

6.7.1 Probability of Failure Allocation.

Refer to paragraph 6.6.1 of this AC for explanation of allocation of probability of failure.

6.7.2 Must Account for Significant Differences in the Observed Failure Rate and the Conditional Failure Rate.

A conditional failure rate should be interpreted as the probability per unit time that a failure will occur at a given time, assuming success prior to that time. An observed failure rate[23] should be interpreted as the ratio of failures to attempts in a defined period of flight divided by the duration of the period.

[23] In the context of the § 450.131 regulations, an observed failure rate is also known as an unconditional or absolute failure rate. Likewise, an observed POF is also known as an unconditional or absolute POF.

Accounting for significant differences in the observed and conditional failure rates should be interpreted such that when calculating the observed failure rate, the likelihood of success in previous phases should be included in the calculation,[24] as explained further in the equations below. In practice, this means observed failure rates will be lower than the conditional failure rates later in flight, since probabilities of early flight failures make it less probable that failures at later flight times will be observed. The difference between a conditional and observed failure rate is more significant with large failure probabilities; for relatively small probabilities, the observed and conditional failure rates are nearly the same.

6.7.2.1 **Rate Equations.**

Calculations for the observed and conditional failure rates begin with a dataset of scored outcomes, as described in paragraphs 6.2.2 and 6.3.2:

n_j is the number of successes plus number of failures of event *j*
r_j is the number of failures of event *j*

The mean conditional POF of event j ($P_{cond,j}$) is calculated by:

$$P_{cond,j} = \frac{r_j}{n_j}$$

To compute the observed POFs for a flight with no parallel events, P_{obs}, the probabilities of starting the current i^{th} event should be computed as follows:

$$P_{start,i} = \prod_{j=1}^{n-1}(1 - P_{cond,j})$$

where *n* is the sequence number of the current event. Thus, $P_{start,i}$ is the product of the probabilities of success, $1 - P_{cond,j}$, of all previous events. The observed failure probabilities are then given by:

$$P_{obs_i} = P_{cond,i} \times P_{start,i}$$

where $P_{cond,i}$ is the conditional POF for the i^{th} event.

For discrete events, the observed failure probability should be allocated to the state at which the event occurs in each normal trajectory simulation of the event as determined per § 450.117.

[24] "Previous phases" should apply to phases within the scope of the flight safety analysis per § 450.113(a) for a given launch or reentry license.

For a phase, stage, or event that has a non-trivial duration, the observed failure decreases with time to account for the probability that a failure occurs earlier within the phase, stage, or event. First, the constant conditional failure rate for event *i* is computed by[25]:

$$h_i = \frac{-\ln\left(1 - P_{cond,i}\right)}{T_i}$$

where T_i is the duration of the i^{th} event. This is the largest value of the observed failure rate, which occurs at the beginning of the initial phase (when $P_{start,i}$= 100%). The observed failure rate over the duration of the event is then given by:

$$f_i(t) = P_{start,i} \times h_i e^{-h_i(t-t_{0,i})}$$

where $t_{0,i}$ is the time at the beginning of the event and t is a value between the start and end event times $[t_{0,i}, t_{end,i}]$. The integral of $f_i(t)$ over the event's operating time is equal to $F_i(t)$, the cumulative failure probability, also known as the phase's observed POF, $P_{obs,i}$.

Note: The failure rate in a time interval that has a constant conditional rate may be approximated as linear with respect to time if the change in the observed failure rate over the interval is less than 10% of the rate at the end of the interval.

6.7.2.2 **Example**.

A simple two stage launch vehicle history is used to demonstrate the conditional and observed failure rate calculations described in paragraph 6.7.2.1, using the dataset in Table 2 below:

Table 2: Example two stage dataset

	Successes + Failures, *n*	Failures, *r*	Time Start (sec)	Time End (sec)	Duration, *T* (sec)
Stage 1	9	4	0	12	12
Stage 2	5	2	12	20	8

[25] See Reference 2 for equation derivation.

Using the above data, the conditional and observed probabilities of failure can be calculated for each event. Note that the probability of starting the initial event should be 100%. The calculations for stage 2 are demonstrated below:

$$P_{cond,s2} = \frac{r}{n} = \frac{2}{5} = 0.40$$

$$P_{start,s2} = \prod_{j=1}^{n-1}(1 - P_{cond,j}) = \left(1 - P_{cond,s1}\right) = \left(1 - \frac{4}{9}\right) = 0.56$$

$$P_{obs,s2} = P_{cond,s2} \times P_{start_{s2}} = 0.40 \times 0.56 = 0.22$$

The conditional failure rate can then be calculated as follows:

$$h_{s2} = \frac{-\ln\left(1 - P_{cond,s2}\right)}{T_{s2}} = \frac{-\ln(1 - 0.40)}{8} = 0.064$$

As a reminder, the observed failure rate is a nonlinear decreasing function over time. The beginning and end failure rates for stage 2 are calculated below for demonstration purposes:

$$f_{beginning,s2} = P_{start,s2} \times h_{s2} e^{-h_{s2}\left(t - t_{0,s2}\right)} = 0.56 \times 0.064 e^{-(0.064)(12-12)} = 0.035$$

$$f_{end,s2} = P_{start,s2} \times h_{s2} e^{-h_{s2}\left(t - t_{0,s2}\right)} = 0.56 \times 0.064 e^{-(0.064)(20-12)} = 0.021$$

For the example above, the final results per phase are provided in Table 3. Figure 2 shows a comparison plot of the conditional and total observed failure rates for stages 1 and 2.

Table 3: Example two stage failure rate results

	P_{cond}	P_{start}	P_{obs}	h	$f_{beginning}$	f_{end}
Stage 1	44%	100%	44%	0.049	0.049	0.027
Stage 2	40%	56%	22%	0.064	0.035	0.021

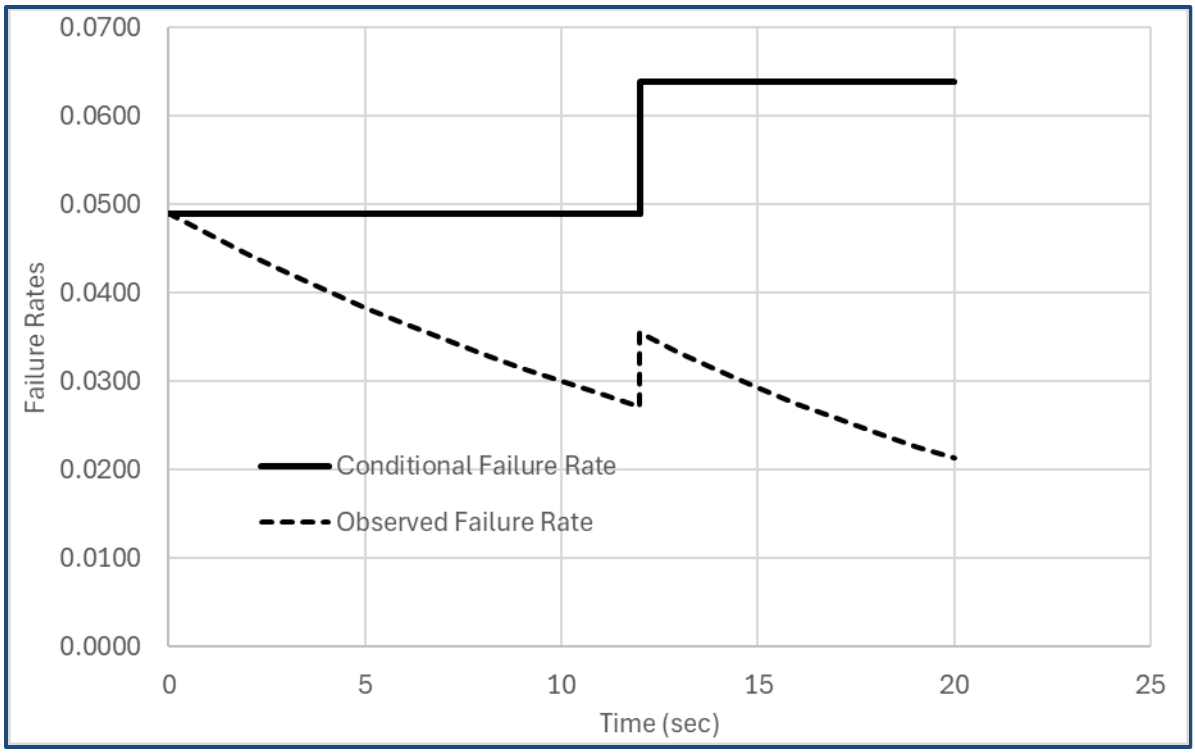

Figure 2: Example two stage failure rate results

6.7.3 Constant Conditional Failure Rate.

A constant conditional failure rate should be interpreted as a conditional failure rate, as explained in paragraph 6.7.2 of this AC, that is uniformly distributed over time, as shown in the example in paragraph 6.7.2.2 of this AC. A constant conditional failure rate is a reasonable assumption in the absence of better information. This is a particularly good assumption for steady state phases such as engine burns for long durations, excluding transient phases such as engine startup.

6.7.4 Each Phase of Flight.

Refer to paragraph 6.1.2 of this AC for explanation of phase of flight. To meet this part of § 450.131(e), both conditions below should be met:

Each flight phase within the scope of the flight safety analysis, as defined by § 450.113, should have a conditional failure rate defined.

- A constant conditional failure rate, as explained in paragraph 6.7.3 of this AC, should be used for each phase of flight, unless there is clear and convincing evidence otherwise, as described in paragraph 6.7.5.

6.7.5 Unless There Is Clear and Convincing Evidence of a Different Conditional Failure Rate for a Particular Vehicle, Stage, or Phase of Flight.

Clear and convincing evidence of a different conditional failure rate is intended to mean informed by underlying knowledge of the subject vehicle (or stage or phase of flight of the vehicle), including its performance and causes of failures that would best inform the rate function. However, if there is no knowledge of the vehicle or its stage/phase of flight that can better inform the conditional failure rate, then a constant conditional failure rate is required.

Example: For a reentry vehicle, heat flux and dynamic load functions compared to breakup thresholds may be used as a higher fidelity means of computing failure rate functions.

6.8 **Explanation of § 450.131(f) Application Requirements**.

Part 450.131(f) contains the application requirements for the probability of failure analysis.

6.8.1 In Accordance With § 450.131(f)(1), an Operator Must Submit a Description of the Methods in Probability of Failure Analysis, in Accordance With § 450.115(c).

Per § 450.131(f)(1), an operator must submit a description of the methods used in probability of failure analysis, in accordance with § 450.115(c). The methodology should sufficiently describe how each part of §§ 450.131(a)-(e) are accounted for, in addition to §§ 450.115(c)(1)-(6). Sections 450.115(c)(1)-(6) may apply to multiple parts of the POF method. An operator should use the following resources when developing a description of the POF methods:

- **AC 450.115-2**. This advisory circular provides general guidance for documenting and submitting a description of a flight safety analysis methodology in accordance with § 450.115(c).
- **Thoroughness Checklist in Chapter 8**. Chapter 8 of this AC provides a guide to operators to ensure the level of detail of the POF method is adequate.

6.8.2 Representative Tabular Data and Graphs.

In accordance with § 450.131(f)(2), an operator must submit a representative set of tabular data and graphs of the predicted failure rate and cumulative failure probability for each reasonably foreseeable failure mode.[26] To meet this requirement, the operator should provide tables of the conditional failure rates by failure mode and cumulative observed POF by failure mode, as demonstrated by Table 4 and Table 5 of this AC. The operator should provide graphs of the observed failure rates by failure mode and cumulative observed POF by failure mode, as demonstrated by Figure 3 and Figure 4 below. The operator should also provide the total observed POF. All tabular data and graphs should cover all phases of flight within the scope of the flight safety analysis, as defined by § 450.113.

Table 4: Example Tabular Data, Conditional Failure Rates per FM

			FM1	FM2	FM3
Phase of Flight	**Start Time (sec)**	**End Time (sec)**	**Conditional Failure Rate (h_i)**	**Conditional Failure Rate (h_i)**	**Conditional Failure Rate (h_i)**
Stage 1	0	174	4.6E-4	1.1E-4	6.3E-4
Coast	174	181	0	0	0
Stage 2	181	580	3.7E-4	9.2E-5	4.9E-4

[26] An operator may provide table/graph results by either failure mode or failure response mode to meet § 450.131(f)(2). If providing by failure mode, the modes should be combined into failure response modes modeled per § 450.119.

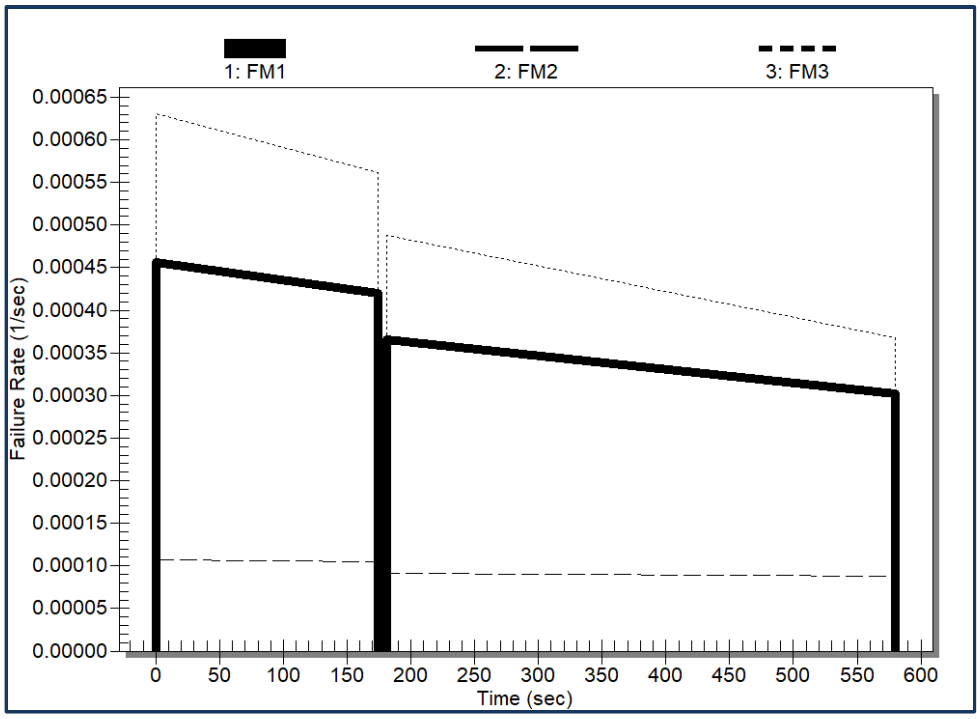

Figure 3: Representative Graph, Observed Failure Rates Per FM

Table 5: Representative Tabular Data, Cumulative Observed POF by FM and Total

			FM1	FM2	FM3	*Total*
Phase of Flight	**Start Time**	**End Time**	**Observed POF**	**Observed POF**	**Observed POF**	**Observed POF**
Stage 1	0	174	7.6E-02	1.8E-02	1.0E-01	2.0E-01
Coast	174	181	0	0	0	0
Stage 2	181	580	1.3E-01	3.6E-02	1.7E-01	3.4E-01
Cumulative Failure Probability			2.1E-01	5.4E-02	2.7E-01	**5.4E-01**

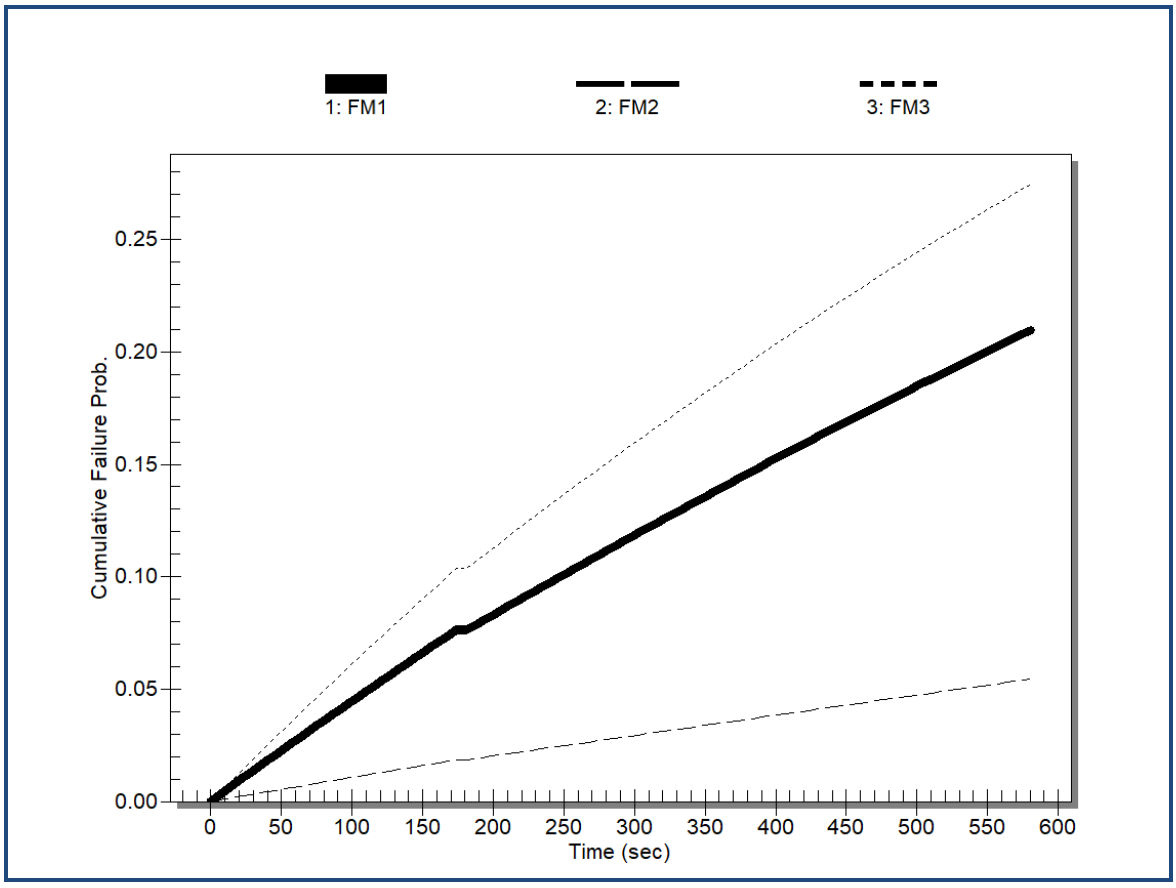

Figure 4: Representative Graph, Cumulative Observed POF by FM

Note: The ARCTOS Failure Time and Rate (FTAR) CSV file format is acceptable for submitting the § 450.131(f)(2) tabular data and graphs, as FAA has software to read and display it.

Per § 450.213(c), the representative set of tabular data and graphs described in § 450.131(f)(2) should be resubmitted per mission as a part of pre-flight reporting in the same format as the representative data, unless the licensee demonstrated during the application process that this data does not need to be updated to account for mission specific factors.

7 MEANS OF COMPLIANCE.

This chapter contains means of compliance (MOC) for different situations. Each MOC begins with a clear definition of the situation(s) to which it applies. Currently only one MOC is included; more are planned for future updates of this AC.

7.1 A Simplified POF Analysis for Reentry Capsule.

7.1.1 Purpose.

This MOC is provided to guide applicants in performing a simplified and conservative POF analysis for a class of reentry capsules. The method in this MOC approach requires minimal analysis effort because it does not require the use of historical flight data nor does it need justification of the reliability of the vehicle systems. An applicant may also use this method as an initial screening tool to determine whether a higher fidelity analysis or additional risk mitigation measures are necessary.

7.1.2 Scope.

This MOC is applicable to the reentry flights of a class of expendable or reusable reentry capsules with the following characteristics:

- The reentry is from low Earth orbit (LEO) to Earth's atmosphere.
- The reentry vehicle consists of a support bus and a reentry capsule. The bus and the capsule are designed to separate before entry into the atmosphere.
- The capsule is equipped with a parachute but is without aero-control surfaces or a reaction control system.
- The capsule has no other configuration changes (e.g. detachable heatshield) or key flight safety events.

It is the responsibility of the applicant to determine whether the method in this MOC is appropriate for its vehicle and mission. The applicant may be able to adopt the method with modifications subject to FAA approval.

7.1.3 Method Outline.

A POF Analysis based on this MOC includes the following steps:

1. Starting with the nominal trajectory, identify milestones and divide the reentry into flight phases. Together, the flight phases must cover the entire reentry mission within the scope of the flight safety analysis as defined by § 450.113(a)(4).
2. Identify all reasonably foreseeable failure response modes (FRMs) and map to the relevant flight phases. Note that this method assigns a failure probability of 1 directly to each failure response mode in each phase instead of allocating through the group of failure modes associated with the failure response mode.
3. For each failure response mode within each flight phase, calculate the conditional and observed failure rates assuming a conditional probability of failure of 1 for the failure mode based on an exponentially decaying observed failure rate function. The cumulative failure probabilities can then be calculated.

4. Create a representative set of tabular data and graphs of the predicted failure rates and cumulative failure probability, in accordance with § 450.131(f)(2).
5. Repeat steps 1-3 for each variability trajectory.

The method in this MOC produces a total probability of failure exceeding 100%. Firstly, the outcome of a phase has no bearing on the failure probability estimates of the phases that come after it. Additionally, the failure probability within a flight phase is over-allocated to its failure modes. These conservatisms are applied in lieu of conducting a higher-fidelity POF analysis and are justified from a regulatory perspective by the conservative estimates the method produces in accordance with § 450.101(g).

7.1.4 Method Details.

This paragraph goes over the steps outlined above in detail.

Step 1: Starting with the nominal trajectory, identify milestones and divide the reentry mission into flight phases, as described in paragraph 6.1.2 of this AC. In the absence of more specific data, FAA has determined it reasonable to use the generic milestones defined in Table 6.

Table 6: Definition of a Set of Generic Milestones

Milestone	Description
Deorbit burn start	Ignition of the deorbit propulsion system
Deorbit burn end	Shut off of the deorbit propulsion system
Capsule-bus separation	Separation of reentry capsule from its supporting bus
Entry interface	Point of atmospheric entry.
Start of main heating	Point before peak aerodynamic heating where the heating rate reaches 10% of its peak
End of main heating	Point after peak aerodynamic heating where the heating rate drops below 90% of its peak
Parachute deployment	Deployment of the landing parachute system
Touchdown	Capsule touchdown

The flight phases should be defined such that start and ends times from the trajectory can be clearly identified. Using the generic milestones in Table 6, the reentry mission is divided into the flight phases shown in Table 7.

Table 7: Definition of Reentry Flight Phases

ID	Flight Phase	Start	End
0	Deorbit Ignition	Discrete	
1	Deorbit Burn	Burn start	Burn end
2	Pre-Separation Exo-Atmospheric Coasting	Deorbit Burn end	Separation
3	Separation	Discrete	
4	Post-Separation Exo-Atmospheric Coasting	Separation	Entry interface (120 km altitude)
5	Upper Atmosphere Traversal	Entry interface (120 km altitude)	Start of main aerodynamic heating
6	Main Aerothermal Dynamic Loading	Start of main aerodynamic heating	End of main aerodynamic heating
7	Lower Atmosphere Traversal	End of main aerodynamic heating	Start of parachute deplolyment
8	Parachute Deployment	Start of parachute deployment	End of parachute deployment
9	Landing	End of parachute deployment	Capsule secured on the ground

Step 2. Table 8 of this AC lists the reasonably foreseeable failure response modes for this reentry vehicle[27]. It is the responsibility of the operator to ensure all reasonably foreseeable failure response modes are identified and consistent with the functional hazard analysis.

Table 8: Reentry Capsule Failure Response Modes

FRM ID	FRM	FRM Description
1	Random Reentry	Delayed random reentry because capsule is placed in a degraded orbit prior to IIP on the surface of the Earth
2	Incorrect start state vector (SV)	Uprange or downrange shift of impact point due to deorbit burn timing error
3	Ballistic tumble	Tumbling, ballistic trajectory
4	Underburn, stable fall	Shallow trajectory due to deorbit over burn
5	Overburn, stable fall	Steep trajectory due to deorbit under burn
6	Explosion	Engine explosion/overpressure burst
7	Uncontrolled intact fall	Combined capsule and service module fail to separate and fall as a single uncontrolled object
8	Aerodynamics error	Trajectory and landing point deviation due to incorrect aerodynamics
9	Aerothermal breakup	Aerothermal breakup due to loss of thermal-structural integrity
10	Aerodynamic breakup	Aerodynamic breakup due to loss of structural integrity
11	Ballistic fall, stable	Stable, ballistic fall of capsule
12	Partial parachute	Degraded parachute performance

[27] Note that planned events, such as a hardware jettison, are outside the scope of § 450.131, but a probability of one must be used for any planned debris hazards or impacts per § 450.133(a)(6).

Next, Table 9 maps the failure response modes to the phases of flight in which the failure response modes are credible:

Table 9: Mapping of failure response modes to flight phases

Phase ID	Flight Phase	1-Random Reentry	2-Incorrect start SV	3-Ballistic tumble	4-Underburn, stable fall	5-Overburn, stable fall	6-Explosion	7-Uncontrolled intact fall	8-Aerodynamics error	9-Aerothermal breakup	10-Aerodynamic breakup	11-Ballistic fall, stable	12-Partial Parachute
0	Deorbit Ignition		X										
1	Deorbit Burn	X		X	X	X	X						
2	Pre-Separation Exo-Atmospheric Coasting			X									
3	Separation			X				X	X				
4	Post-Separation Exo-Atmospheric Coasting			X									
5	Upper Atmosphere Traversal			X					X				
6	Main Aerothermal Dynamic Loading			X					X	X			
7	Lower Atmosphere Traversal			X					X		X		
8	Parachute Deployment										X	X	X
9	Landing											X	

Step 3. Determine the conditional failure rate per failure response mode within each flight phase, then calculate the observed failure rate and cumulative failure probabilities. A more common method is to use the standard constant conditional failure rate assumption, as required in § 450.131(e) unless there is clear and convincing evidence otherwise, together with the conditional failure probability to calculate the corresponding observed failure rate and failure probability function. However, with the assumption of a failure probability of 1, a constant failure rate is not mathematically possible. For this MOC, FAA has determined it reasonable to use the following equations for the conditional failure rate $h_C(t)$:

$$h_C(t) = \frac{C}{1 - e^{-C(T_E - t)}} \tag{1}$$

$$C = \frac{1}{(T_E - T_B)\sqrt{2}} \tag{2}$$

where T_B and T_E are the start and end times of the flight phase and C is a parameter that controls the rate of decay of the observed failure rate. An exponentially decaying observed failure rate $h_O(t)$ can then be calculated in the form of

$$h_O(t) = Ge^{-Ct} \ \ for \ \ T_B \le t \le T_E \tag{3}$$

$$G = \frac{C}{e^{-CT_B} - e^{-CT_E}} \tag{4}$$

where G is a parameter that constrains the probability of failure to 1.

With the observed failure rate determined, the corresponding observed failure probability P_{obs} for the failure mode can be calculated using the following equation:

$$F(t) = P_{obs} = 1 - \frac{e^{-Ct} - e^{-CT_E}}{e^{-CT_B} - e^{-CT_E}} \tag{5}$$

Note: For a failure response mode associated with a discrete flight phase, it is not necessary to calculate a failure rate.

Step 4. In accordance with § 450.131(f)(2), the applicant must submit a representative set of tabular data and graphs of the predicted failure rate and cumulative failure probability for each foreseeable failure response mode.

The tabular data for the failure rate is shown as the event times and the constant C. It applies to each failure mode present in a phase. This data allows the conditional failure rate to be computed for any time within the interval using equation (1) and the observed failure rate using equation (3). These equations are used to plot graphs of failure rate as a function of time along the nominal trajectory.

The cumulative failure "probability" per phase is equal the number of failure response modes since the cumulative failure probability is equal to 1 per failure response mode. The cumulative probability vs. time graph uses equation (5) multiplied by the number of modes in each phase, then added to the total probability at the beginning of the phase. So for a given phase, i:

$$P_{cum,i}(t) = N_{FRM,i}F_i(t) + P_{cum,i-1} \quad (6)$$

Where $N_{FRM,i}$ is the number of FRMs in the phase (see Table 9) and $F_i(t)$ is from equation (5).

Since the failure rate time histories for all failure response modes associated with a flight phase are identical (all failure response modes have the same time span and a failure probability of 1), they are represented by one line labeled by the flight phase.

Several invariant conditions can be used to catch potential numerical errors in the above calculations:

- ✓ The ratio between the last and first values of the observed failure rate in each phase should be close to $\exp\left(-1/\sqrt{2}\right) = 0.493$.
- ✓ The last value of the cumulative failure probability should be close to 1 in each phase.
- ✓ The time integration of the observed failure rate between any two time-points within the flight phase should be close to the difference between the cumulative failure probability values at the two time points.

Step 5. Repeat steps 1-3 for each variability trajectory. Note that it is not necessary to produce the representative tabular data and graphs as described in Step 4 for each of the variability trajectories in addition to the nominal trajectory, but the relevant POF data should be applied to its respective variability trajectory.

7.1.5 Example Dataset.

Table 10 provides an example timeline based on the generic milestones provided in Table 6. However, the flight times and altitudes of many of these milestones are mission dependent. It is the responsibility of the operator to ensure that the flight phase division is consistent with its reentry mission and make appropriate changes if more specific data is available. For example, the point of peak heating is dependent on the configuration and trajectory profile that may vary significantly from capsule to capsule and mission to mission and should be determined from the thermal loading and trajectory analyses for the specific mission.

Table 10: Example Reentry Timeline

Milestone	Time (s)
Deorbit burn start	0
Deorbit burn end	220
Capsule-bus separation	1400
Entry interface	2030
Start of main heating	2140
End of main heating	2200
Start of parachute deployment	2700
End of parachute deployment	2705
Touchdown	3360

Flight phases by time are then derived based on the generic milestones and example timeline, as shown in Table 11.

Table 11: Example Reentry Flight Phases by Time

ID	Flight Phase	Start (s)	End (s)
0	Deorbit Ignition	0	0
1	Deorbit Burn	0	220
2	Pre-Separation Exo-Atmospheric Coasting	220	1400
3	Separation	1400	1400
4	Post-Separation Exo-Atmospheric Coasting	1400	2030
5	Upper Atmosphere Traversal	2030	2140
6	Main Aerothermal Dynamic Loading	2140	2200
7	Lower Atmosphere Traversal	2200	2700
8	Parachute Deployment	2700	2705
9	Landing	2705	3360

Figure 5 shows the time histories of the observed failure rate by phase of flight:

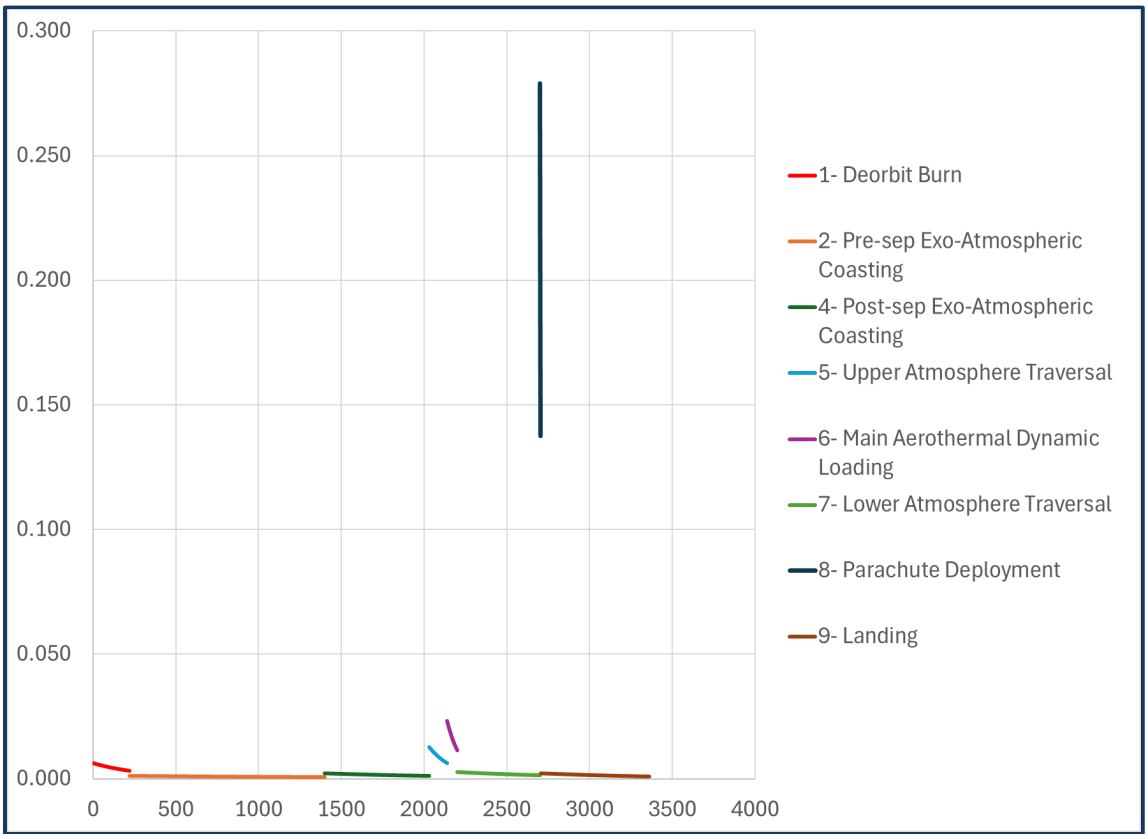

Figure 5: Reentry Flight Observed Failure Rates

Figure 6 shows the cumulative failure probabilities summed across flight phases and failure response modes.

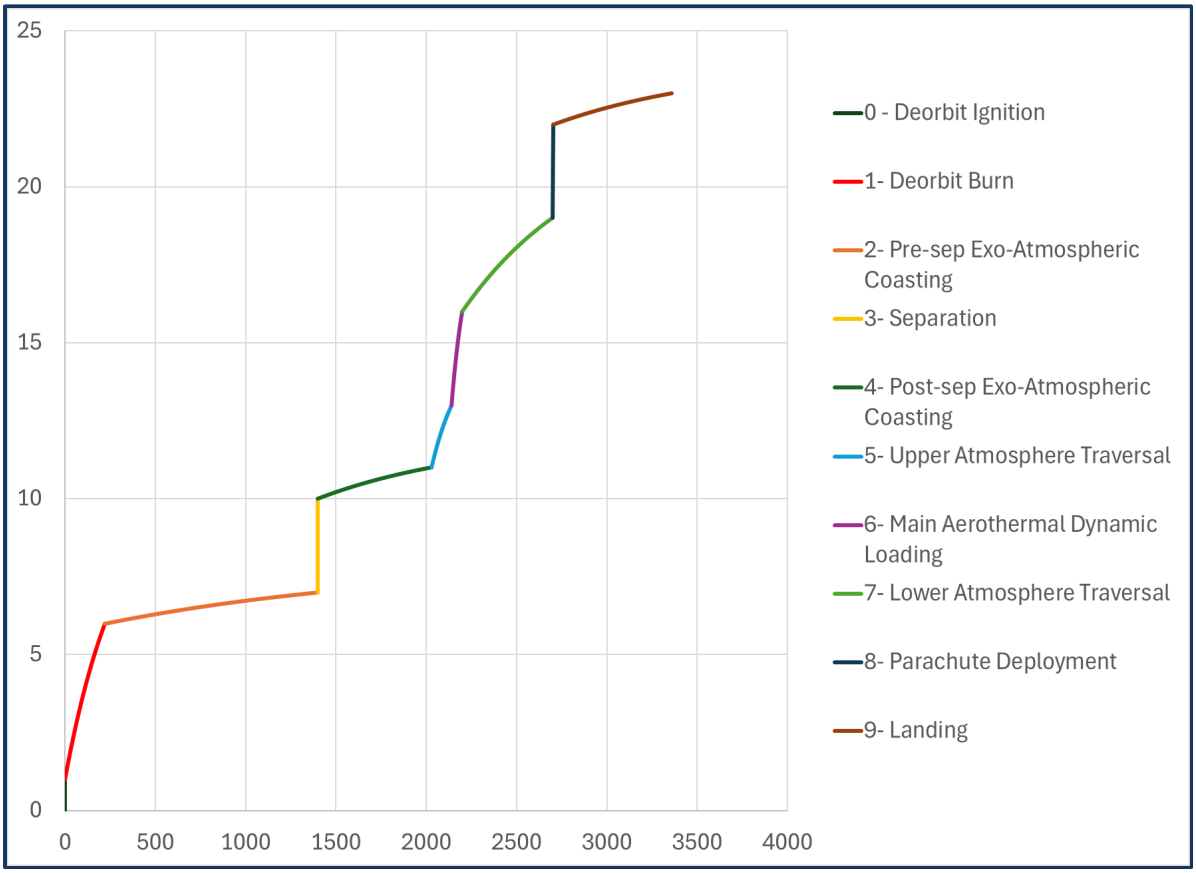

Figure 6: Cumulative Failure Probabilities Summed Across Flight Phases and Failure Response Modes

Table 12 of this AC lists the C value as well as the cumulative failure probability by phase ("intra-phase") and total cumulative failure probability for each flight phase ("inter-phase"). The intra-phase cumulative failure probability is the sum of the cumulative failure probabilities of all failure response modes at the end of the phase; the cumulation is reset at the beginning of each phase. The inter-phase cumulative failure probability is similar except that the cumulation is not reset across phases.

It is noted that the failure response modes of deorbit ignition and bus-capsule separation are discrete modes each with a failure probability of 1, and represented as vertical lines in Figure 6 of this AC.

Table 12: Cumulative Failure Probabilities

ID	Flight Phase	Start (s)	End (s)	C	Cumulative Pf per phase	Total Cumulative Pf
0	Deorbit Ignition	0	0	N/A	1	1
1	Deorbit Burn	0	220	3.21E-03	5	6
2	Pre-sep Exo-Atmospheric Coasting	220	1400	5.99E-04	1	7
3	Separation	1400	1400	N/A	3	10
4	Post-sep Exo-Atmospheric Coasting	1400	2030	1.12E-03	1	11
5	Upper Atmosphere Traversal	2030	2140	6.43E-03	2	13
6	Main Aerothermal Dynamic Loading	2140	2200	1.18E-02	3	16
7	Lower Atmosphere Traversal	2200	2700	1.41E-03	3	19
8	Parachute Deployment	2700	2705	1.41E-01	3	22
9	Landing	2705	3360	1.08E-03	1	23

7.1.6 Assumptions and Justifications.

Table 13 contains a list of MOC assumptions and justifications:

Table 13: Assumptions and Justifications

No.	Assumption	Justification
1	The probability of failure for each failure response mode for each flight phase is 1.	This is a conservative assumption for failure probability in accordance with § 450.101(g) since it is the maximum possible probability per failure mode per phase.
2	The observed failure rate can be expressed as an exponentially decaying function shown in equation (3) within a flight phase.	FAA has determined this is reasonable in the absence of other evidence.
3	The milestones defined in Table 6 are adequate for the class of reentry capsules targeted by this MOC.	The table covers the most common milestones for the class of reentry vehicles described in paragraph 7.1.2 of this AC. Warning is included for users to either adapt aspects of this MOC or use a different approach.
4	The milestone timeline given in Table 10 is adequate as an example for the class of capsules targeted by this MOC.	The table is included to provide concrete numerical values so plots of the failure rates and cumulative failure probabilities can be created. Warning is included for users to update the table using values specific to the subject mission.

7.1.7 Compliance Matrix.

The table below lists statements of compliance:

Table 14: Compliance Matrix

450 Section	Regulatory Text	Compliance Statement
§ 450.131(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.	This method assumes a failure probability of 1 for each failure response mode within each flight phase – the maximum value possible. The sum of the failure probabilities of the mutually exclusive failure response modes in a flight phase can be greater than 1, and the failure probability of the failure response modes in a flight phase are independent of the failure of any proceeding phases, all of which contribute to an estimate that is more conservative than that from a standard probability of failure analysis.
§ 450.131(a)(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.	This method provides a more conservative estimate than directly using outcomes of similar flights as data inputs, which is in accordance with § 450.101(g).
§ 450.131(a)(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.	This method provides a more conservative estimate than directly using outcomes of the subject vehicle flights as data inputs, which is in accordance with § 450.101(g).

450 Section	Regulatory Text	Compliance Statement
§ 450.131(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.	This method provides a more conservative estimate than directly using failure outcomes as data inputs, which is in accordance with § 450.101(g). Failure response modes are identified and listed in Table 8 of this AC.
§ 450.131(c)	Previous flight. For flight safety analysis purposes—	See subsections of § 450.131(c) described in rows below.
§ 450.131(c)(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	N/A
§450.131(c)(2)	The flight of a reentry vehicle or deorbiting upper stage begins at a time in which a vehicle attempts to initiate a reentry.	This method provides a more conservative estimate than directly using previous flights of similar vehicles and/or subject vehicle flights as data inputs, which is in accordance with § 450.101(g).
§ 450.131(d)	*Allocation.* The vehicle failure probability estimate must be distributed across flight phases and failure modes. The distribution must be consistent with—	Each phase of flight within the scope of § 450.113 is accounted for in this method, along with all reasonably foreseeable failure response modes.
§ 450.131(d)(1)	The data available from all previous flights of vehicles developed and launched or reentered in similar circumstances; and	This method provides a more conservative estimate than directly using the data available from all previous flights of similar vehicles as data inputs, which is in accordance with § 450.101(g).

450 Section	Regulatory Text	Compliance Statement
§ 450.131(d)(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—	This method provides a more conservative estimate than directly using the data from previous flights as listed in this requirement as data inputs, which is in accordance with § 450.101(g).
§ 450.131(d)(2)(i)	Vehicle, stage, or component design characteristics;	See § 450.131(d)(2) compliance statement.
§ 450.131(d)(2)(ii)	Development and integration processes, including the extent of integrated system testing; and	See § 450.131(d)(2) compliance statement.
§ 450.131(d)(2)(iii)	Level of experience of the vehicle operation and development team members.	See § 450.131(d)(2) compliance statement.
§ 450.131(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.	Due to the conservative assumption of a failure probability of 1 for all failure response modes, a constant conditional failure rate is no longer appropriate. The FAA has determined it reasonable to use equation (1) to calculate the constant conditional failure rate and equation (3) for the observed failure rate.
§ 450.131(f)	Application requirements. An applicant must submit:	See subsections below.
§ 450.131(f)(1)	A description of the methods used in probability of failure analysis, in accordance with § 450.115(c); and	Paragraphs 7.1.3 and 7.1.4 of this AC provide description of the methods. Compliance with § 450.115(c) is described in subsequent responses, below.

450 Section	Regulatory Text	Compliance Statement
§ 450.131(f)(2)	A representative set of tabular data and graphs of the predicted failure rate and cumulative failure probability for each foreseeable failure mode.	See paragraph 7.1.5 of this AC.
§ 450.115(c)	Application requirements. An applicant must submit a description of the flight safety analysis methodology, including identification of:	See subsections of § 450.115(c) in the rows that follow.
§ 450.115(c)(1)	The scientific principles and statistical methods used;	See paragraphs 7.1.2 through 7.1.4 of this AC.
§ 450.115(c)(2)	All assumptions and their justifications;	See Table 13 of this AC.
§ 450.115(c)(3)	The rationale for the level of fidelity;	This is a simple conservative method intended for low-risk reentry missions or used as a screening tool. It trades conservatism for ease of use.
§ 450.115(c)(4)	The evidence for validation and verification required by § 450.101(g);	Invariant conditions were used to check numerical errors, as described in paragraph 7.1.4.
§ 450.115(c)(5)	The extent to which the benchmark conditions are comparable to the foreseeable conditions of the intended operations; and	The use of a failure probability of 1 for all failure response modes is more conservative than what can be foreseen of the intended operations.
§ 450.115(c)(6)	The extent to which risk mitigations were accounted for in the analyses.	See Table 13, assumption #1 of this AC.

8 THOROUGHNESS CHECKLIST.

Table 15 through Table 22 of this AC are checklists that an operator should use to aid in creating a complete methodology. The checklists are intended to provide a quick yes/no answer to address if the content is present, regardless of technical merit or depth of the material. The "Yes/No" column of each checklist may be used by the operator for this purpose. FAA review of an application will flow more quickly if all checklist items are clearly identifiable in an application. Note that the checklists are to be used as a guide only, as different means of compliance may not require every checklist item.

8.1 Scope and Data Requirements.

Table 15 defines prerequisite information for the operator to assess the scope and completeness of the methodology to be presented. Each checklist item contains a brief additional discussion on the type of information expected by the FAA.

Table 15: Background Checklist

Checklist Item		Discussion	Yes/No
Does the method define the scope of applicability? [§ 450.115(a)]	Flights this method is applicable [§ 450.131(a)(1) and § 450.131(a)(2)]	Sometimes different methods are appropriate during test/development and operational phases of a vehicle. The method should provide clear criteria for applicability.	
	Phases of flight method is applicable [§ 450.131(d)]	A method is usually only appropriate for a type of operation (e.g. launch or reentry) and may only be appropriate for certain types of events, such as a burn phase.	
	Configurations of the vehicle method is applicable [§ 450.131(d)(2)(i)]	Normally a method has assumptions about the configuration of the vehicle, such as having a certain number of stages or no additional boosters (e.g. SRBs).	
	Does it handle changes to the operations program, hardware, flight profiles, etc.?	A method should be clear about whether it handles significant modifications to a vehicle design, makes assumption about the operational plan (e.g. differences between crewed and uncrewed operation), or is constrained to certain flight areas (such as not hazarding uncontrolled areas).	

Checklist Item		Discussion	Yes/No
	Expendable versus reuse of vehicle/hardware?	If a method is for reusable systems, it should describe what aspects of the analysis consider reusability.	
Does the method define data requirements for performing the analysis?	Basic vehicle design	Description of number of stages, propellant types, jettison hardware, recoverable hardware, etc. and its implications in the analysis.	
	Event sequencing	Description of how event sequencing per operation will be determined and utilized in the POF analysis.	
	Event timing	Description of how event timing per operation will be determined and utilized in the POF analysis.	

8.2 **Definitions**.

Table 16 of this AC outlines a list of definitions applied to the methodology. These terms are utilized in § 450.131. However, the methodology should specify how they are applied within the methodology and applied to the subject vehicle.

Table 16: Definitions Applied in the Application

Checklist Item		Section Reference	Yes/No
Does the method include a description of how the following definitions are used in the method?	Similar circumstances • Should include multiple aspects of the vehicle design and development	6.2	
	Failure • Should include post-flight reporting § 450.215(b)(1) and § 450.173(e)(2) scoring process	0	
	Previous flights of the subject vehicle • Should include considerations for changes in configuration of vehicle and components.	6.5	

8.3 **Flight Data**.

Table 17 of this AC defines a list of common data products that may be produced and data processes to build prerequisite datasets for computations. While there is no requirement for how the task is performed, a common solution is to construct a database that is designed to store the data in a complete, accurate, and up-to-date manner to produce valid query results for an analysis. The checklist is built around the assumption of a database or similar solution with the three main categories of the checklist being equivalent to a database's design ("data parameterization"), database's data load ("data load"), and database query logic/capabilities ("data selection"). Each item in the checklist must have their assumptions and justifications logically stated to satisfy § 450.115(c)(2).

Table 17: Flight Data Checklist

The following topics should include all 3 elements for each: Assumptions, justifications, and logic		Yes/No
Does the method include a description of data parameterization?	Categorization of flight phases / events	
	Categorization of vehicles	
	Categorization of flights	
	Categorization of failure modes	
	Categorization of outcomes	
Does the method include a description of data loading?	Criteria for defining comprehensiveness of historical data	
	Maintenance (updates for new flights)	
	Criteria for defining accuracy of data/reliability of data sources	
Does the method include a description of data selection?	Query for similarity ("Vehicles developed and operated under similar circumstances") parameters	
	Query of outcomes by flight phase / event	
	Query of outcomes by failure mode	

8.4 **Calculations.**

Table 18 of this AC defines a common list of calculations performed assuming availability of prerequisite data. Each item in the checklist must have their assumptions and justifications logically stated, including all mathematics, to satisfy § 450.115(c)(2). The column "Section Reference(s)" refers to sections of this document where more information can be found.

Table 18: Calculations Checklist

The following topics should include all 4 elements for each: Assumptions, justifications, logic, and mathematics		Section Reference(s)	Yes/No
Does the method include the following descriptions related to vehicle analysis?	Flight event/phase decomposition, including sequence and dependencies	6.1.2	
	Failure mode identification for each event/phase	6.6.3	
	Relationship to functional hazard analysis	6.6.3	
Does the method include the following descriptions of data analysis calculations?	Application of similar flight history	6.2	
	Application of subject vehicle/stage flight history	6.3	
	Incorporation of uncertainty § 450.115(b)(2)	0	
Does the method include the following descriptions related to allocation?	Allocation of probability by failure mode	6.6	
	Allocation of probability of by event / phases	6.6	
Does the method include the following descriptions of rate calculations?	Calculation of conditional failure rates	6.7.2, 6.7.3	
	Justification for conditional rate selection	6.7.3, 0	
	Observed failure rate calculations given conditional rates accounting for probabilities of past events	6.7.2	

8.5 **Outputs**.

Table 19 of this AC lists the expected outputs defined within the method. The intent is to know the content of what is transmitted between analyses (from POF analysis into respective risk analyses) and to understand the format the applicant will be submitting in compliance with § 450.131(f)(2).

Table 19: Outputs

Checklist Item		Yes/No
Does the method define the outputs?	Is there a format output definition for failure rates defined for each subsequent FSA analysis use case (§§ 450.133, 450.135, 450.137, 450.139)?	
	Is there a format output definition for failure rates defined for tabular and graphs for predicted failure rate and cumulative for compliance with § 450.131(f)(2)?	

8.6 **Section 450.115(c)(4)-(6)**.

Table 15 through Table 19 help to ensure § 450.115(c)(1) and (2) are thoroughly addressed. Table 20 through Table 22 define § 450.115(c)(3) to (6) requirements needed to assess a methodology. The discussion columns provide brief guidance on these aspects as applied to the probability of failure methodology. Refer to chapters 7 and 8 of AC 450.115-2, for detailed explanation and standard of sufficiency for § 450.115(c).

Table 20: Section 450.115(c)(3),(5), and (6) Checklist

Is there a discussion of:	Discussion	Yes/No
The level of fidelity of the analysis?	The level of fidelity (bias and uncertainty) should be assessed. Sensitivity studies on the effects of different parameter selections should be performed to demonstrate performance of the model. Sensitivity studies may also include consequences of hypothetical failures. The fidelity should consider allocation with respect to phases and to failure modes.	
The benchmarks used to demonstrate the validity of results?	Benchmarks should include: • Comparison of how the method performs under different conditions, such as applied to flight history of other historical vehicles. • A description of the ongoing check for validity of the method during the § 450.103(d) post-flight data review, including criteria for determining when the POF method should be reevaluated to ensure compliance with § 450.101(g) (as described in section 0).	
Risk mitigations that are accounted for in the analysis?	Common risk mitigations that are applicable to probability of failure analysis include evidence for reliability of the vehicle safety-critical elements and conservative choices in the POF analysis itself, such as selection of data and parameter selection.	

As a part of § 450.115(c)(4), processes should be validated by the operator to confirm validity of their results.

Table 21 of this AC lists process validation checks that an operator should use for probability of failure analysis.

Table 21: Review Process Validation

Is there a description of process validation of:	Discussion	Yes/No
Historical flight data collection, updates, and accessibility?	There should be a description of how the applicant will confirm that the historical flight data used in analysis is valid. This starts with validation of collection process, including updates, to be comprehensive and correctly categorized. This also includes validation that appropriate data is correctly applied in the analysis.	
Vehicle analysis for flight events, phases, and failure modes?	Given a definition of how the vehicle will be broken into flight events, phases, and failure modes, the process should identify all required elements of the decomposition of the vehicle without any remaining phases or failure modes unaccounted for.	

Also in accordance with § 450.115(c)(4), Table 22 defines a checklist for all software used in probability of failure analysis to confirm that there is an adequate description of all software used and each piece of software's verification and validation (V&V) has been performed, and configuration control has been employed. When spreadsheets are used, there should be evidence of V&V of the implementation of the formulas used in the spreadsheet, rather than the spreadsheet program itself (such as Excel)[28].

Table 22: Software Checklist

Is there evidence of verification and validation for all the software tools used to implement the method?	Verification, Yes/No	Validation, Yes/No	Configuration Control, Yes/No
Software tool 1			
Software tool 2			

[28] See AC 450.115-2, sections 7.4.4 and 7.4.6 for further description of spreadsheet validation and verification.

OMB Control Number: 2120-0746
Expiration Date: 12/31/2027

Advisory Circular Feedback Form

If you find an error in this AC, have recommendations for improving it, or have suggestions for new items/subjects to be added, you may let us know by (1) emailing this form to 9-AST-ASZ210-Directives@faa.gov, or (2) faxing it to (202) 267-5450.

Subject:_____ Date: _____

Please mark all appropriate line items:

☐ An error (procedural or typographical) has been noted in paragraph _____on page _____.

☐ Recommend paragraph _____ on page be changed as follows:

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

☐ Other comments:

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

Submitted by: _____ Date: _____