

# **DRAFT FAA GUIDELINES ON PROBABILITY OF FAILURE ANALYSIS FOR NEW EXPENDABLE LAUNCH VEHICLES**

## **1. Introduction**

The purpose of these guidelines is to facilitate valid probability of failure analyses for new expendable launch vehicles (ELVs)<sup>1</sup>. A valid probability of failure analysis is essential to public safety for launches that employ risk management, or a combination of hazard isolation and risk management. Risk is a measure that accounts for both the probability of occurrence (in this case, the occurrence is a failure of a launch vehicle) and the consequence of a hazard to a population or installation. Mathematically, risk is the product of the probability of occurrence and the consequences of a hazard. A probability of failure analysis for an ELV produces an estimate of the probability of occurrence of a hazardous event. Therefore, a probability of failure analysis is an essential element of any launch risk analysis, such as the debris risk analysis required by § 415.35(a). In general, a launch risk analysis allocates the probability of occurrence to flight times and failure modes. However, these guidelines do not currently address allocation of the probability of occurrence.

Recognizing the central importance of probability of failure estimates to launch risk analyses, the FAA and Air Force, through the Common Standards Working Group (CSWG), devoted substantial resources to develop guidelines that include a performance standard for launch vehicle failure probability analysis, common acceptable methodologies for determining failure probabilities for new launch vehicles, and definitions of key terms. A performance standard permits a launch operator to continue to employ alternative, potentially innovative methodologies so long as they satisfy the performance standard. Current practice at the Federal launch ranges includes multiple methodologies to determine the probability of failure for launch vehicles because there is more than one way to establish an acceptable estimate of the probability of failure. In addition, the FAA here presents

specific methodology guidelines that define an acceptable method, but not necessarily the only method, to demonstrate compliance with the performance standard. The methods recommended here are also intended to illustrate an acceptable level of fidelity for new ELV probability of failure analyses.

The FAA and the Air Force, through the CSWG, have found that these guidelines are consistent with practice at the Federal ranges, and represent a major improvement over the rigid method proposed in the FAA's Licensing and Safety Requirements for Launch, Notice of Proposed Rulemaking, the October 2000 NPRM [Fed. Reg., Vol.65, No.207, Oct. 25, 2000, pp 63922 to 64123]. The October 2000 NPRM proposed to assign a fixed failure probability of 0.31 for the first 15 flights of a launch vehicle and a failure probability of 0.10 for the next fifteen flights. For a launch vehicle with 30 or more flights, the October 2000 NPRM proposed that a launch operator "use the empirical failure probability determined from the actual flight history." Given the set of practical constraints underlying an assessment of expendable launch vehicle failure probabilities, these guidelines provide a more flexible approach that is technically valid, and is responsive to the current needs of the ELV industry. These draft guidelines are intended to provide a commonly accepted framework for probability of failure analyses. As such, these guidelines should be useful to anyone who performs or evaluates launch risk analyses for new ELVs, including Federal range safety personnel and launch operators.

## **2. Performance Standard**

The FAA uses the following performance standard and definitions to evaluate any probability of failure analysis for an expendable launch vehicle.

(a) Performance standard. All flight safety analyses for a launch, regardless of hazard or phase of flight, should account for launch vehicle failure probability in a consistent manner. A launch

---

<sup>1</sup> A formal definition of "new launch vehicles" does not exist. An integrated vehicle design with no or limited flight experience is generally considered new. The FAA will determine the applicability of these guidelines on a case-by-case

vehicle failure probability estimate should use accurate data, scientific principles, and a method that is statistically and probabilistically valid. For a launch vehicle with fewer than two flights, a failure probability estimate should account for the outcomes of all previous launches of vehicles developed and launched in similar circumstances. For a launch vehicle with two or more flights, a launch vehicle failure probability estimate should account for the outcomes of all previous flights of the subject vehicle in a valid manner. The outcomes of all previous flights of the subject vehicle should include all the in-flight failures and successes that occur from liftoff until after the last exercise of control over the launch vehicle. For a launch vehicle with two or more flights, the estimate should also account for changes in the vehicle configuration, the integration and processing of the vehicle, and other factors that affect the launch vehicle development or production.

(b) Definitions.

**Flight.** For probability of failure analysis purposes, flight begins when a launch vehicle normally or inadvertently lifts off from a launch platform.

**Liftoff.** Liftoff occurs when there is any motion of the launch vehicle with respect to the launch platform. The term liftoff is most often used in the context of motion with respect to a fixed asset, such as a launch pad or sea platform, but here liftoff also includes separation from a carrier aircraft. For other types of launch platforms the determination of liftoff will be on a case-by-case basis, and may need to consider the threat to the general public prior to separation of the launch vehicle, such as when a balloon-launching craft is airborne.

**In-Flight Failure.** An in-flight failure occurs when a launch 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 during the mission or any future mission. A launch

---

basis. These guidelines do not necessarily apply to an integrated vehicle design with extensive flight experience.

accident<sup>2</sup> constitutes a failure. A launch incident<sup>3</sup> should be evaluated to determine if the anomalous condition exhibits the potential for a stage or its debris to impact the Earth or reenter the atmosphere during the mission or any future mission.

### **3.0 Methodology Guidelines**

#### **3.1 Overview**

The following guidelines describe sample methods that satisfy the FAA's performance standard for ELVs for the ascent phase of flight<sup>4</sup>. The FAA will accept an alternative estimate of a launch vehicle failure probability if a launch operator provides a clear and convincing demonstration that the proposed alternative provides an equivalent level of fidelity to the methods described in the following paragraphs.

#### **3.2 Vehicle Design With Less Than Two Flights Completed**

(a) For a launch vehicle with fewer than two flights completed, the analysis should use a baseline value<sup>5</sup> for the launch vehicle failure probability estimate equal to the upper limit of the 60% two-sided confidence limits of the binomial distribution for the outcomes of all previous flights of vehicles developed and launched in similar circumstances<sup>6</sup>.

(b) For a launch vehicle with fewer than two flights completed, the FAA may adjust the failure probability estimate away from the baseline value to account for the level of experience demonstrated by the launch operator and other factors that affect the probability of failure.

---

<sup>2</sup> In 14 CFR § 401.5, the FAA defines a launch accident as (1) A fatality or serious injury (as defined by 49 CFR 830.2) to any person who is not associated with the flight; (2) any damage to exceed \$25,000 to property not associated with the flight that is not located at the launch site or designated recovery area; (3) an unplanned event occurring during the flight of a launch vehicle resulting in the known impact of a launch vehicle, its payload or any component thereof: (a) for an expendable launch vehicle (ELV) outside designated impact limit lines; and (b) for a reusable launch vehicle (RLV), outside designated landing site.

<sup>3</sup> In 14 CFR § 401.5, the FAA defines a launch incident as an unplanned event occurring during flight of a launch vehicle, other than a launch accident, involving a malfunction of a flight safety system or safety critical system or failure of the licensee's safety organization, design, or operations.

<sup>4</sup> In this context the ascent phase of flight is from liftoff through orbital insertion, including each planned impact, for an orbital launch, and through final impact for a suborbital launch.

<sup>5</sup> A baseline value is the estimated launch vehicle failure probability for the first two flights unless adjustments away from the baseline value are justified to account for particular circumstances.

### 3.3 Vehicle Design With at Least Two Flights Completed

(a) For a launch vehicle with at least two flights completed, the analysis should use the reference value<sup>7</sup> for the launch vehicle failure probability of Table A based on the outcomes of all previous flights of the subject vehicle.

(i) Values listed on the far left of Table A apply when no launch failures were experienced. Values on the far right apply when only launch failures are experienced. Values in between apply to flight histories that include both failures and successes<sup>8</sup>.

(ii) Reference values in Table A are shown in bold. The reference values are the midpoints between 60% two-sided confidence limits<sup>9</sup> of the binomial distribution. For the special cases of zero failures or all failures, the reference values are equal to the midpoints between the 80% one-sided confidence limit of the binomial distribution and zero or one, respectively.

(iii) Upper and lower confidence bounds in Table A are shown directly above and below each reference value. These confidence bounds are based on 60% two-sided confidence limits of the binomial distribution. For the special cases of zero failures or all failures, the upper and lower confidence bounds are equal to the 80% one-sided confidence limit and zero or one, respectively.

(b) The FAA may adjust the failure probability estimate to account for evidence obtained from the flight history of the vehicle, corrective actions taken in response to a failure of the vehicle, vehicle configuration, or other vehicle modifications that may affect reliability. The FAA may also adjust the failure probability estimate to account for the demonstrated quality of the engineering approach to

---

<sup>6</sup> During the pre-application consultation phase of the license process, the FAA plans to make data available on the outcomes of the first two flights of previous launches of new ELVs.

<sup>7</sup> A reference value is the estimated launch vehicle failure probability for greater than two flights unless adjustments away from the reference value are justified to account for particular circumstances.

<sup>8</sup> For example, a vehicle that experienced one failure in seven launches would have a reference value of 0.20: the bold value in the second column of the row for launch eight.

<sup>9</sup> If there are only two possible outcomes (success or failure) for a repeatable process that remains unchanged (i.e. Bernoulli trials), then there is a 40% chance that the actual probability of failure is outside the range specified by the 60% two-sided confidence limits in Table A. Specifically, there is a 20% chance that the actual probability of failure is above the range specified by the 60% two-sided confidence limits, and a 20% chance that the actual probability of failure is below the range specified by the 60% two-sided confidence limits.

launch vehicle processing, and associated hazard mitigation. The launch risk analysis should use a final failure probability estimate within the confidence limits of Table A.

(c) For a launch vehicle with at least two flights completed, the FAA will accept a Bayesian estimate based on a uniform prior distribution of one hypothetical failure in two hypothetical flights updated with the outcomes of all previous flights of the subject vehicle.

### **3.4 Summary**

For a vehicle with fewer than two flights, use a baseline value equal to the upper limit of the 60% two-sided confidence limits of the binomial distribution (shown above the bold values in Table A) for the outcomes of all previous flights of vehicles developed and launched in similar circumstances. During the pre-application consultation phase of the license process, the FAA will provide the current data on the outcomes of the first two flights of previous launches of new ELVs. For example, if the outcomes of all previous flights of vehicles developed and launched in similar circumstances was one failure in seven launches, then the baseline value would be 0.37: the value immediately above the bold value in the second column of the row labeled for launch number eight. The FAA may adjust the failure probability estimate away from the baseline value to account for the level of experience demonstrated by the launch operator and other factors that affect the probability of failure.

For a vehicle with two or more flights, the failure probability estimate should be based on Table A and the vehicle's flight history. For example, a vehicle that experienced one failure in seven launches would have a reference failure probability estimate of 0.20: the bold value in the second column of the row labeled for launch number eight. The reference probability estimate will be the final estimate input to any launch risk analysis unless the FAA has a reason to make an adjustment away from the reference value. The FAA may adjust the failure probability estimate to account for evidence obtained from the flight history of the vehicle, corrective actions taken in response to prior failures of the vehicle, vehicle configuration changes, other vehicle or processing modifications that

may affect reliability. The FAA may also adjust the failure probability estimate to account for the demonstrated quality of the engineering approach to launch vehicle processing, and associated hazard mitigation. In all cases, the launch risk analyses for flight should use a final failure probability estimate within the confidence limits of Table A.



## **4. Discussion**

The following discussion provides information that may be useful when using these guidelines, including discussion of the definitions of key terms, the rationale for these guidelines, and other clarifications. This section also summarizes two independent assessments obtained prior to publication of these draft guidelines.

### **4.1 Discussion of the Definitions**

An in-flight failure occurs when a launch 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 during the ascent phase of the mission or any future mission. For probability of failure analysis purposes, flight begins at a time in which a launch vehicle normally or inadvertently lifts off from a launch platform. Liftoff occurs when there is any motion of the launch vehicle with respect to the launch platform. The FAA has an existing regulation (§401.5) that defines the end of flight: “For purposes of an ELV launch, flight ends after the licensee’s last exercise of control over its launch vehicle.” Therefore, when using these guidelines, the “flight” history of a subject vehicle should include all the in-flight failures and successes that occur from liftoff until after the licensee’s last exercise of control. An in-flight failure includes those cases where the failure occurs after the launch vehicle achieves an orbit, but occurs in a stage that also operates prior to achieving orbit and hence the failure, had it occurred earlier in flight, could have been a hazard to the public. An in-flight failure may also include those cases where the failure occurs after the launch vehicle achieves an orbit, but occurs in a stage that could also operate prior to achieving an orbit during a future mission.

Initially, the FAA, in consultation with the CSWG, considered defining flight from the beginning of engine ignition to account for failures that resulted in liftoff or toppled the vehicle. However, there are times where a pre-planned engine shutdown can occur that precludes liftoff but remains within the confines of planned, or normal, mission behavior. These types of occurrences would obviously not be considered an in-flight failure. As a result, liftoff better serves to define the

beginning of flight, although there have been instances where anomalies in the final moments of a countdown have resulted in destruction of a vehicle. There are pre-flight anomalies that should be accounted for by launch risk analyses even though liftoff did not occur. For example, if an anomaly occurred without liftoff, and had the potential to affect public safety, then it should be accounted for by a risk analyses as an on-pad failure. However, such on-pad failures without liftoff should not be included in the “flight” history of a subject vehicle.

## **4.2 Discussion of the Performance Standard**

Current practice promotes risk management as a means of protecting the public from a wide range of potential hazards during launch. Specifically, proposed §417.107(b) of the SNPRM published July 30, 2002 [see Federal Register, Vol. 67, No. 146 page 49495] would define acceptable risk levels for impacting inert and impacting explosive debris, for toxic release (exposure to rocket propellant effluent), and for far field blast overpressure. The FAA’s performance standard specifies that all flight safety analyses for a launch, regardless of hazard or phase of flight, should account for launch vehicle failure probability in a consistent manner.

Key elements of an acceptable failure probability analysis include accurate data, scientific principles, and a method that is statistically and probabilistically valid. Accurate data in this context means completeness, exactness, and fidelity to the maximum extent possible. In this context, the FAA uses “scientific principles” to refer to knowledge, based on the scientific method, such as that established in the fields of physics, chemistry, and engineering<sup>10</sup>. A probability of failure estimate that is statistically and probabilistically valid should at least be the result of a sound application of mathematics. A sound application of mathematics uses correct premises and makes only conclusions that are properly derived from the premises. The principles of probability are a mathematical theory concerned with the analysis of random events. For example, in the mathematical theory of probability,

---

<sup>10</sup> A failure probability analysis based on non-scientific principles, such as astrology, would not be consistent with this guideline.

the probability of an event should satisfy Kolmogorov's axioms<sup>11</sup>. Probability is a mathematical basis for prediction of the ratio of outcomes that would produce a given event to the total number of outcomes. Statistics refers to a branch of mathematics dealing with the collection, analysis, interpretation, and presentation of numerical data. A valid statistical analysis should account for the uncertainty in a statistical inference due to sample size limits, the degree of applicability of data to a particular system, and the degree of homogeneity of the data.

For a launch vehicle with fewer than two flights, the standard specifies that a failure probability estimate should account for the outcomes of all previous flights of vehicles developed and launched in similar circumstances. For example, the following five factors may be considered as part of the determination of what constitutes all previous flights of vehicles developed and launched under similar circumstances: (1) the vehicle's design characteristics, (2) the vehicle's development and integration processes, including especially the extent of integrated system testing, (3) the related work experience of the launch and development team members, (4) the outcomes of all previous flights of similar vehicles developed and launched by the launch operator, and (5) the country where the vehicle was developed and launched. Due to the small data set available on launches of new ELVs, it may be impractical to parse the flight history database using all of these factors. A CSWG investigation of historical failure probabilities revealed that the probability of failure on the first and second launches of a new launch vehicle is highly dependent upon the launch experience of the developer. Specifically, the worldwide flight history of expendable launch vehicles from 1980 to 2002 reveals that launch operators that have never launched vehicles successfully before had eight failures in 11 launch attempts. Worldwide flight history for "experienced launch vehicle developers" over the same period indicates five failures in 18 launch attempts. Many factors may influence the level of experience of a launch vehicle developer. However, in the results of the recent CSWG investigation, the term

---

<sup>11</sup> See NASA's "Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners" available at <http://www.hq.nasa.gov/office/codeq/doctree/praguide.pdf>.

“experienced launch vehicle developer” corresponded to developers that had produced at least one launch vehicle with a demonstrated probability of failure less than or equal to 33%<sup>12</sup>.

For a launch vehicle with two or more flights, the FAA’s performance standard specifies that a statistically valid failure probability estimate should account for the outcomes of all previous flights of the subject vehicle and account for changes in the vehicle configuration. Evolved Expendable Launch Vehicles (EELVs) are examples of launch vehicles designed to fly in various configurations. For the medium class of EELVs, “changes in the vehicle configuration” include flights with various combinations of payload fairings and solid rocket motors. A valid probability of failure analysis might consider some configurations sufficiently similar to treat as Bernoulli trials of a subject vehicle, such as the EELVs that use a single common core booster. A valid probability of failure analysis might consider other configurations, such as a heavy class EELV, as distinct due to important differences that may influence the probability of failure, such as flight loads, flight environment, vehicle design characteristics, vehicle processing, and the like. In order to permit the development of different approaches in this area, this guideline does not currently specify how to account for changes in the vehicle configuration, merely that they should be accounted for.

Certain applications of Bayesian statistics, with input data from the generic flight history of vehicles developed and launched under similar circumstances, and qualitative measures associated with the launch developer or operator, constitute at least one potentially valid statistical method to make failure probability estimates for a launch vehicle with fewer than two flights<sup>13</sup>. A failure probability analysis for a launch vehicle with fewer than two flights can satisfy the FAA’s performance standard using expert opinion under certain circumstances. Because the validity of a statistical

---

<sup>12</sup> The probability of failure was based on the reference values in Table A.

<sup>13</sup> For example, see S.D. Guikema and M.E. Pate-Cornell, *Journal of Spacecraft and Rockets*, Vol 41, No.1 pp. 93-102 (Jan-Feb 2004). Also, see the “degree of belief interpretation” of probability in NASA’s “Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners” available at <http://www.hq.nasa.gov/office/codeq/doctree/praguide.pdf>

analysis depends greatly on the specific data under consideration, the FAA evaluates the statistical validity of a failure probability estimate on the basis of the circumstances and data available.

### **4.3 Discussion of the Failure Probability Adjustments**

Adjustments away from the reference value of the failure probability may be necessary for various reasons. Failure probability adjustments away from the reference value may account for the nature of launch outcomes in the flight history of the subject vehicle. For example, a failure might be weighted heavily if the failure mode demonstrated a lack of quality control on the part of the launch vehicle developer, while a generic failure would not justify a significant departure from the reference value. Also, a subject launch vehicle or launch vehicle sub-system may have demonstrated a high degree of reliability when operated within a limited and well-defined parameter range, but then demonstrated less reliability when operated outside that parameter range. An example of this is the observed correlation between ambient temperature and incidence of O-ring blow-by observed for the Space Transportation System (STS) solid rocket boosters prior to STS 51-L. In such cases, it may be reasonable to make adjustments away from the reference value to account for the nature of launch outcomes under distinct environmental conditions.

Failure probability adjustments away from the reference value may account for corrective actions taken in response to a failure of the subject launch vehicle, or other subject launch vehicle modifications that may affect reliability. For example, a subject launch vehicle or launch vehicle sub-system may have demonstrated, based on actual flight history, a relatively high degree of reliability after a corrective action was taken. In such cases, it may be reasonable to make adjustments away from the reference value to account for the demonstrated reliability after a corrective action was taken. In such cases, the demonstrated failure probability based on the flight history after the corrective actions could serve as a useful guideline for the adjusted failure probability estimate.

Failure probability adjustments away from the reference value may account for the demonstrated quality of the engineering approach to launch vehicle processing. If a launch operator

demonstrates a substandard level of quality control in its engineering approach to launch vehicle processing, then it may be reasonable to make adjustments away from the reference value. Also, if a launch operator demonstrates a change in quality control, then adjustments away from the reference value are justified. In all cases, the final failure estimate should be within the confidence limits shown in Table A, based on the entire flight history of the subject launch vehicle.

The CSWG developed a rating system that combined all the factors identified that may influence the probability of failure of a launch vehicle into a numerical value referred to as a “quality index.” The CSWG investigated various weighting schemes to account for all the factors identified that may influence the probability of failure of a launch vehicle. The CSWG performed statistical analyses to identify the weighting scheme that produced an optimal correlation between the CSWG ratings and the demonstrated failure probability for orbital launch vehicles with first launches between 1980 and 2002.

The CSWG investigated a hierarchical Bayesian model based on the “quality index” values and flight history of orbital launch vehicles with first launches between 1980 and 2002. The results of a prototype hierarchical Bayesian model indicated good agreement with the demonstrated probability of failure for orbital launch vehicles with first launches between 1980 and 2002. Therefore, the FAA expects that such a hierarchical Bayesian model may provide a formal framework to adjust the probability of failure by accounting for factors that influence the probability of failure. Also, the FAA expects that such a hierarchical Bayesian model may provide a more accurate estimate of the probability of failure for the first two launches of an expendable orbital launch vehicle.

#### **4.4 Discussion of the Independent Assessment**

Recognizing the central importance of probability of failure estimates to any risk analysis, the FAA and Air Force obtained independent assessments of the proposed probability of failure guidelines. Two outside technical reviews were obtained by the CSWG. An Independent Assessment Team (IAT), composed of Futron Corporation and Professor Ali Mosleh of the University of Maryland, was

tasked to provide a thorough, well-documented, and objective assessment of the proposed requirements and supporting documentation. Similarly, Professor Valen Johnson of the University of Michigan reviewed the draft guidelines and developed the hierarchical Bayesian statistical approach mentioned in section 4.3. More specifically, both review teams were asked to (1) evaluate the validity of the FAA's performance standard, and if necessary make recommendations for improvement or suggest an alternative; (2) evaluate the validity of the methodology guidelines for producing launch vehicle failure probability estimates; and (3) evaluate the clarity, usefulness, and validity of the proposed supporting documentation. The IAT also performed a validation of the launch event outcome database developed for the CSWG by ACTA Incorporated. Professor Johnson and the IAT examined the validity of the observations made on historical data, statistical interpretation, approach and criteria used to develop reference and baseline launch failure probabilities, and the proposed use of the resulting numbers in the performance standard. Key conclusions of the evaluations were that the proposed performance standard, the methodological framework, and the supporting documentation are, as a whole, technically valid given the practical constraints underlying an assessment of expendable launch vehicle failure probabilities.

The reviewers assessed the validity and usefulness of the proposed methodology and performance standards. The reviewers reported positive features of the proposed methodology that include simplicity, justifiable conservative tendencies, and allowance for alternative methods of estimating launch failure probability, subject to reasonable quality requirements. The IAT found that some of the methodological proposals by FAA do not adhere to the mathematical rigor of the classical statistical theory. However, the IAT also found that mathematical rigor based on classical statistical theory cannot be fully adhered to since the scarcity of the directly relevant statistical data limits practical use of such methods.