Quantitative Launch and Space Transport Vehicle Reliability and Safety Requirements: Useful or Problematic?

Sergio Guarro[a]
[a] ASCA Inc., Redondo Beach, USA

Abstract: The setting of quantitative reliability or safety requirements for launch and space-transport vehicles (LVs , STVs) is an established practice in the space business, applied via related provisions in the contracts by which LV and STV development and acquisition activities are assigned to supplier organizations. At face value this is a reasonable approach to establishing a desired level of safety and reliability for space missions, a compelling need given that extremely valuable payload, or even human life in the case of crewed vehicles, may be at stake. However serious issues presently make the approach difficult to successfully implement, ranging from ambiguities in the requirement definitions themselves, such as the often encountered separation of the definitions of LV reliability into "design" and "mission," to lack of realism in the setting of the requirement values in relation to the state of advancement of the current LV / STV technology and to the magnitude of the uncertainty in reliability and risk assessments relying on the currently available quantification data. These issues and the resulting hindrance to the very reliability and safety assessment techniques the setting of quantitative requirements is in theory designed to foster and stimulate are identified and discussed.

Keywords: Launch vehicle (LV), space transport vehicle (STV), reliability requirement, safety requirement, risk threshold.

1. INTRODUCTION

Safety and reliability are compelling needs for launch and space-transport vehicle (LV, STV) systems, given that very valuable scientific or operational payloads, and even human life, may be at stake. The practice of setting quantitative reliability and safety risk thresholds for these systems is well established in both the Department of Defense (DoD) and NASA areas of the space business, and is also applied in terms of defining formal contractual requirements when launch or space vehicle services are procured. For example, the Air Force has established both a "design reliability" and a "mission reliability" requirement at the onset of the Evolved Expendable Launch Vehicle (EELV) program and is applying the same requirements for any new entrant entity who seeks to qualify a LV vehicle to carry DoD payloads to orbit. In the NASA world, the Commercial Crew Development (CCDev) program has established risk-threshold and safety requirements in terms of Loss-of-Mission (LoM) and Loss-of-Crew (LoC) probability, for the integrated LV-STV systems that are being developed by competing contractor teams.

The practical application of quantitative LV / STV requirements that can be directly useful to the improvement of actual system reliability and safety, presents, however, challenges that are far from being solved at the present time. This paper discusses the issues producing these challenges and their effect on how reliability and risk requirements are ultimately interpreted and addressed in program and acquisition contexts, also in view of the present state-of-the-art of LV / STV risk and reliability estimation. To this end, it reviews the common definitions of risk and reliability that are relevant to LV / STV estimations and discusses their theoretical and practical interpretations, then proceeds to a discussion of the data and methods available for reliability estimation at various LV system maturity stages, using examples from past and recent studies. This discussion leads to practical considerations concerning the meaning of typical reliability estimations that are generated in common space industry practice, and their degree of correspondence and consistency with the theoretical definitions of the parameters they seek to quantify. Final observations and comments are drawn from these considerations on the usefulness of the use of quantitative LV risk and reliability requirements in the current typical form that they take within contractual acquisition contexts; and on the possibility, for the organizations that seek to procure or self-regulate the development of LV and/or STV systems, of adopting alternative, more flexible approaches.

2. QUANTITATIVE LV / STV RELIABILITY AND SAFETY REQUIREMENTS

Quantitative LV and STV reliability and safety requirements are defined in terms of probabilistic parameters of one type or another. While the setting of a quantitative threshold value for a performance parameter may in general appear to provide a clear-cut way of establishing a system requirement, in the particular domain of reliability and safety the specific choice of parameter upon which a requirement is established, and the interpretation, by the parties involved, of its meaning and of the methods considered acceptable to demonstrate compliance may vary significantly. To gain an understanding of how significant an impact this may have it is useful to review and discuss some of the more common definitions and interpretations of the parameters of interest.

2.1. Reliability and Safety Parameter Definitions

The U.S. Air Force Space and Missile Systems Center (AF/SMC) and NASA are major Government organizations that have made and are continuing to make use of quantitative reliability and safety requirements in the procurement and development of LV and STV systems. Quantitative safety parameters are also used by the launch ranges of both the Air Force and NASA organizations to certify and authorize LV launches at the U.S. launch sites.

References [1] and [2] give definitions for various parameters that AF/SMC uses to set LV reliability requirements in programs such as the Evolved Expendable Launch Vehicle (EELV) Program, as reported below:

> ***Inherent Reliability:*** A measure of reliability that excludes effects other than those proceeding from the item's design and the application of the design within an ideal operating and support environment [1].
>
> ***Demonstrated Reliability:*** The reliability of the current configuration based upon objective evidence, *i.e.*, data, gathered during past performance or test under specified conditions [1].
>
> ***Design Reliability***: Vehicle design reliability accounts for potential mission failure modes that have their genesis in the design of system hardware, component integration architecture, and software (including those pertaining to staging events and CCAMs[*]) [2].
>
> ***Mission Reliability:*** Mission reliability, measured from launch commit, is the probability of successfully placing the payload into its delivery orbit with the required delivery accuracy and then executing a CCAM. Mission reliability takes into account both vehicle design and process reliabilities [2].
>
> ***Process reliability:-*** Process reliability includes consideration of failure modes introduced by manufacturing, infrastructure, assembly, ground processing, and system integrating activities (including payload mating activities performed by EELV) [2].

More specifically, the Air Force EELV Program has established numerical threshold requirements for "Design Reliability" and "Mission Reliability," as defined above.

NASA has also used quantitative reliability requirements in LV programs. In addition, it has used probability threshold values for "Loss of Mission" (LOM) and "Loss of Crew" (LOC) for its crewed space programs. LOM and LOC probability requirements are presently being used in the Commercial Crew Development (CCDev) Program. Reference [3] defines these parameters as reported below:

> ***Probability of Loss of Mission (P(LOM)):*** Probability of a critical failure occurring, resulting in loss of one or more mission objectives [3].

[*] CCAM : Contamination and Collision Avoidance Maneuver

Probability of Loss of Crew (P(LOC)): Probability of loss of crew across all mission phases [3].

The same reference also relates the P(LOM) and P(LOC) parameters to other "proxy parameters", among which "subsystem inherent reliability" and "system inherent reliability." Explicit definitions for these latter attributes are not provided in [3].

2.2. Interpretation of the Reliability and Safety Parameter Definitions

With respect to the definitions provided in the preceding section, the following basic observations can be made:

a. The definitions of "Design Reliability" in [1] and "Inherent Reliability" in [2] are essentially equivalent, and include consideration of only causes of LV / STV failure that are associated with the characteristics of a design that is implemented without human errors in system fabrication, assembly and launch processing. In practice, as will be further discussed in the following, the interpretation of these definitions is even more restrictive, in the sense that, somewhat paradoxically, design reliability assessments also exclude the contribution of system design errors.

b. "Mission Reliability" is generally intended to include consideration of all possible causes of failure of a LV or STV mission.

c. Safety parameters like LOM and LOC are directly related to LV / STV reliability parameters. In quantitative terms in fact P(LOM) is the complement to unity of Mission Reliability; and the relation of P(LOC) to P(LOM), although more complex, is conceptually self- evident.

The basic definitions of reliability parameters that are applied to LVs and STVs correspond to a conceptual model according to which the reliability / unreliability contributions relevant to such systems can be classified in two broad categories:

A. Contributions resulting from the inherent design characteristics of the LV system;

B. Contributions from the processes that transform the formulated design into an actual vehicle, readied for launch.

A general metric termed "design reliability" conforming to the above classification would therefore express the probability that a launch vehicle, whose parts and components are fabricated and assembled according to a given design specification, with no errors introduced by the fabrication, assembly and launch preparation processes, will successfully execute a mission for which it has been designed. A metric of this kind corresponds to both the "Inherent Reliability" and "Design Reliability" definitions reported above from [1] and [2] respectively.

The second category of reliability / unreliability contributions determines what [2] defines as the "Process Reliability." Reference [2] also states that the combination of design and process reliability determines "Mission Reliability," which represents the probability of successful execution of a specified type of mission by a given type of launch vehicle. From this it follows that an estimation of mission reliability, if well executed with the support of credible data, should produce a good estimator of the actual success ratio over a sufficiently representative number of standard missions carried out by a given type of launch vehicle.

The mission success ratio, *i.e.*, the number of successful missions divided by the number of missions launched on a given LV system, is commonly used as a representation of LV "Demonstrated Reliability," as defined in [1] and above. When interpreted in this fashion, mission reliability predictions and demonstrated reliability values should track each other closely. However it may be more appropriate to treat the term "demonstrated" as a potential attribute of any type of reliability parameter, referring to the type and quality of the estimation carried out for such a parameter. That is, given a "demonstrated mission reliability" estimated using the actual mission success and failure record for a given vehicle type, estimators representing the "demonstrated design reliability" or "demonstrated process reliability" portions of mission reliability may also be obtained by sorting the same mission data records according to the corresponding root cause category, *i.e.*, distinguishing the fraction of failures caused by design errors from the fraction caused by process errors.

2.3. Challenges in Practical Application of Quantitative Requirements

A serious challenge to the use of quantitative LV / STV reliability or safety requirements lies in the fact that, as discussed at some length in this paper, LV and STV reliability and risk estimation processes, which are the necessary accessory to any demonstration or verification of such requirements, are subject to great variability in both their mode of execution and in the results that they may produce, in large part depending on the choice of sources and on the interpretation of applicability for the basic data available to quantify the reliability and safety models. The effect of this is that translating an estimation or verification goal into credible procedures and results, at the level of accuracy that may be desirable for certain specific intended uses, is in the end possible under some, but by no means all, conditions. Accordingly, the results produced are in general not as straightforward and easy to interpret as potential users would like them to be.

A closely related issue, in the sense that it is also driven by the validity and/or availability of basic reliability data sources, involves the actual meaning of formal quantitative requirement thresholds set on the LV or STV design reliability, or on other reliability or safety parameters. As discussed in Section XX, design reliability estimates do not usually provide a good prediction of actual system success rate, and that other, in principle more realistic, types of reliability estimations that are based on the flight and test record of LV or STV components, cannot be generated without large bands of uncertainty, especially in the earlier phases of a system development. Under these conditions it is difficult to select and establish meaningful quantitative reliability or risk requirements for acquisition purposes. For example, it takes many years of operational life for a given system to accumulate a number of successful missions large enough to demonstrate that it can satisfy a specified level of reliability at a sufficient level of statistical confidence, that is, to meet what is usually called a "demonstrated reliability" level.

3. DATA AND METHODS FOR LV / STV RELIABILITY ESTIMATION

The degree of correspondence of estimations obtained from various possible LV data sources to the theoretical definitions of specific types of reliability parameters is in practice determined by the nature of the data at hand and by the assumptions made in the use of such data in the models applied in the estimation process.

Data usable for estimation of LV reliability parameters of interest may come from a range of sources, but in general can be classified according to a combination of the following key attributes:

A. "Generic" vs. "specific" data;
B. Data obtained in "mission equivalent" vs. "non-mission equivalent" environment conditions.

The first type of classification refers to whether the reliability data to be used for the estimation of reliability parameters of a given item has been obtained from handbook compilations relative to items considered generically similar to that item, or whether it comes from test or operational records pertaining to that item or other essentially identical items. The second refers to whether the data comes from test or operation at the same level of reliability stressor-environments (e.g., vibration, thermal-cycling, or other failure-inducing environmental conditions) as those to be withstood during the mission(s) for which the reliability estimation is intended.

In terms of estimation methods, the reliability or failure probability of any complex system, including LVs or STVs, is generally calculated in one of two ways:

- A "direct estimation" can be carried out when direct observations of mission success and failure records for the system of interest, or test records deemed to have mission-equivalent information value, are available.

- An "indirect bottom-up estimation" is carried out when:
  a) the redundancy characteristics of the system, in terms of its constituting subsystems and components, are known and a logic model that represents them can be constructed; and
  b) data enabling the quantification of reliability for the individual components appearing in the system reliability logic model is available.

  When both above conditions are met, an estimate of system reliability can be "indirectly" derived by first using the available data to estimate reliability parameters for all the individual system components appearing in the system model, and then using the latter as input upon which standard logic-probabilistic rules are applied to calculate the system reliability parameters, according to the component reliability relations described by the system reliability model.

From the above it can be inferred that, depending on what combination of estimation model, (*i.e.*, "direct" or "indirect") and data (*i.e.*, "generic" or "specific"; "mission equivalent" or "non-mission equivalent") are used in an estimation process, a resulting system reliability estimate may in the end have different degree of representation and predictive value with respect to a specific reliability parameter identified according to one of the definitions discussed in Section 2.1. To gain a better insight into the question of LV / STV reliability parameter estimation fidelity and value, a review and discussion of the related practices and techniques is given in the following subsections.

3.1. Standard Industry Practice for Design Reliability Estimation

The space industry practice for estimation of the "design reliability" of a launch vehicle is generally based on a bottom-up indirect estimation utilizing a system reliability model, commonly in the form of a reliability block diagram (RBD), fault-tree (FT) or equivalent binary logic format. The model is then quantified at the part or component level primarily by means of handbook data, *e.g.*, using failure rate data from MIL-HDBK-217 for electronic parts and from NPRD-95 for mechanical parts and components. Subsystem and system level estimates of reliability are then obtained by combining the part and component estimates according to the logic structure of the system reliability model. The system reliability model reflects the part and subsystem functionality required to achieve mission success at the system level, as well as any redundancy features included in the system design to increase reliability. In these design reliability estimations only components for which generic handbook data compilations do not exist are assessed via component-specific test and/or flight information, or other types of ad-hoc assessments. Primary example of this are the liquid rocket engines and solid rocket motors that may be used in a given vehicle.

As a result of the nature of the models and data used, and of the assumptions made in the utilization of such models and data, a typical design reliability estimation only reflects the redundancy characteristics of a given LV design and the inherent random failure characteristics of its parts and components. For some of the redundant elements, common cause failure (ccf) effects may also be taken into account using empirical ccf factors. Important to note is that a standard design reliability estimation excludes not only the potential contribution to system failure of fabrication, assembly or pre-launch processing errors, but also any design errors in parts and system specifications and logic, including errors resulting from misjudgement of stressor environments to be withstood, or from mistakes in the choice of materials used in parts or components, or from use of faulty logic in a software module, *etc*.

From the last observation it follows that, in system procurement contexts where the definition of design reliability given in [2] and repeated in Section 2.1 applies, the industry practice of applying this exclusion in LV / STV "design reliability" assessments appears to be in contradiction with the definition, and may put in question the validity of such assessments as a means of demonstrating compliance with requirements set in accordance with that definition. Such a question may have even greater relevance in light of the large incidence that design errors have been found to have in actual LV mission failures, especially in the first few flights of a new system design (see Section 4.2).

3.2. Process and Mission Reliability Estimation

The estimation of reliability metrics other than "design reliability" is not codified in any standard space industry practice. In general, in order to include all realistically possible contributions to the probability of failure of a system, a reliability estimation must account not only for the inherent random failure characteristics of each component, but also for the possibility of errors in its design or processing – where the term "processing" refers to all the post-design fabrication, assembly and integration steps needed to produce the component and include it in a mission-ready LV system.

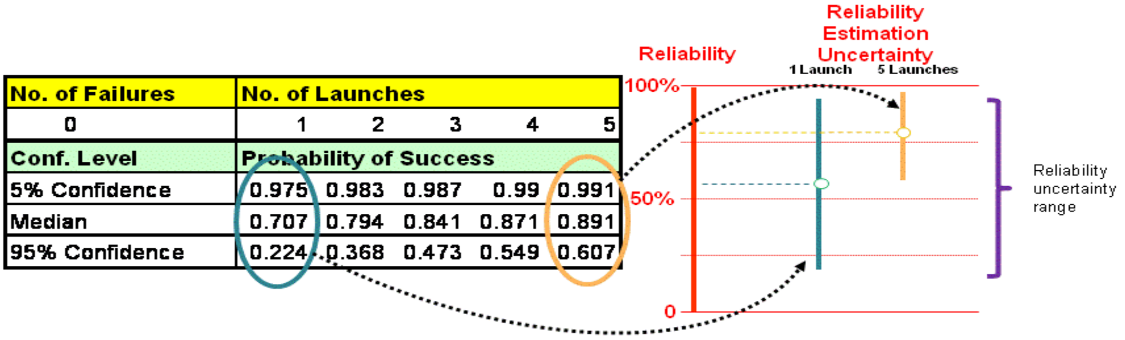
Regardless of the level of indenture and detail that may be used in a model to estimate the contribution of design or process errors to system reliability, the probabilistic quantification of a mission reliability model cannot primarily be based on generic handbook information such as that provided by MIL-HDBK-217, NPRD-95 and similar compilations. By their very nature these in fact do not include the records of occurrence of such kinds of errors for the categories of components that they address, nor that of any issues of design or process at the higher subsystem or system level. To provide meaningful estimates of such contributions to the reliability and/or unreliability of a LV system, the quantification of a mission reliability model must include data and information, such as rate or frequency of design and process defects and "escapes," that reflect the nature and quality of the design and post-design processes applied in the development and launch of the specific LV system being addressed.

3.3. Demonstrated Reliability Estimation

Given a number of launches that have been executed and recorded for a launch vehicle of concern, its “demonstrated reliability” can be estimated using common statistical methods, such as those discussed in [4] and [5]. “Demonstrated reliability” is estimated under the assumption that both the vehicle design and the mission profile have remained the same across all the observed launches. It must be noted that in the assessment of actual LV systems these assumptions are generally not satisfied, because mission profiles and physical environments always differ from one launch to the next, and the design and components of a typical LV system can be modified or even changed substantially over the years of its operational life. In the most common forms of estimation, however, this "moving target effect" is not addressed because of the difficulty of formulating defensible models that may serve the purpose.

In a simple estimation, the "evidence" of S successes and F failures in N mission trials (with N = S + F) is typically and relatively simply modelled as the result of "Bernoulli trials," where the "demonstrated reliability" is represented by the parameter p = “probability of success” in any given trial. To estimate p from the existing evidence (the S and F numbers observed after N trials are completed), one can use either a "classical Maximum Likelihood Estimation" (MLE) or a “Bayesian Estimation” (BE) [4, 5]. The classical approach may not be very helpful when, as often is the case, there are only a few trials and no failures; under such conditions the estimator MLE(p) = S / N = 1 (*i.e.*, 100% reliability) squarely falls on the "optimistic" side of the reliability range.

Bayesian estimation models may vary in complexity, but in general they assume a prior distribution for the reliability parameter of interest, meant to give an initial representation of the range of uncertainty for that parameter, and then update this distribution making use of test and/or operational mission evidence. From the updated reliability distribution one can obtain various types of estimates, such as the mean-value estimate, and percentile values that represent estimations at any desired level of confidence (or "credibility," which is the term preferred by Bayesian statisticians). In one of the simplest forms of Bayesian estimation, if a uniform prior distribution of p between 0 and 1 is initially assumed and the evidence is still the same as stated above for the MLE example, the mean value estimate of p is BE(p) = (S+1) / (N+2). The various percentiles of p can also be readily obtained. The effect of uncertainty can be seen in the figure below, as expressed by the 5th to 95th confidence range around the 50th percentile value for the 1st through 5th launch.



No. of Failures	No. of Launches				
0	1	2	3	4	5
Conf. Level	Probability of Success				
5% Confidence	0.975	0.983	0.987	0.99	0.991
Median	0.707	0.794	0.841	0.871	0.891
95% Confidence	0.224	0.368	0.473	0.549	0.607

Reliability
Reliability Estimation Uncertainty
1 Launch
5 Launches
100%
50%
0
Reliability uncertainty range

Figure 1: Demonstrated Reliability Uncertainty for Launch Vehicles

It can also be shown how the estimated mean, median (50th percentile), 5th and 95th percentile values of p progress as N increases, if one makes the best case assumption that the outcomes are all successes, or if one or more failures are assumed to occur at some point. Thus one can for example show that 48 launches without any failures are needed to demonstrate 98% as the mean value estimate of p. To achieve a 50% confidence in a reliability value of 98% we have to set the 50th percentile of p equal to .98 (98%), which yields N = 34. If a higher level of confidence is desired that the reliability is at least 98%, the minimum value of N increases dramatically. For example N = 114 with no failures is required to demonstrate 98% reliability at 90% confidence.

Figure 2 below plots the required number of flights to demonstrate reliability at 50% confidence for 0, 1, and 2 failures and Figure 3 plots the demonstrated reliability for 0 failures at 5%, 50%, and 95% confidence. These results represent naïve statistics in the sense that they do not account for the characteristics of the failure mechanisms nor for the effects of the corrections made. In fact, per what was stated earlier, these plots represent demonstrated reliabilities for assumed unchanging common vehicle design, mission profiles and conditions. In reality all such factors do change substantially in the course of the operational life of a LV, as well exemplified by the case of the LV system known generically under the name "Titan IV"[†]: if the LV name is taken at face value to represent a well defined LV system with fixed characteristics, the "Titan IV" flight record can be summarized to be 35 successes and 4 failures in 39 missions. However, if one looks at the variations of design and mission configurations, the picture changes substantially, because:

1. Two major versions of the LV "main body" – *i.e.*, the liquid rocket engine stages 1 and 2 plus the two solid rocket motor stage 0 boosters – were used over the years, and called respectively Titan IVA and Titan IVB. The latter used very different solid rocket motors and substantially different avionics and electrical power distribution systems.
2. Titan IV missions flew in three different configuration arrangements. In the first configuration the mission was carried out by the Titan IVA or IVB without an upper stage (*i.e.*, with only the "main body" as described above). In the second, the Inertial Upper Stage (IUS), powered by a solid rocket motor, was stacked on top of the main body and used to place a payload into its desired orbit. In the third, the cryogenic "Centaur" upper stage was used for the same purpose.

When the above is considered, the mission record statistics also change substantially. The Titan IVA has a record of 2 failures in 22 missions, both due to problems in the "main body" itself, whereas the Titan IVB "main body" record consists of 0 failures in 17 missions. Two Titan IVB missions did fail, but these failures were caused by the IUS (Inertial Upper Stage) and Centaur upper stage, respectively, after the other stages had performed successfully. This type of situation is not

[†] The Titan IV LV system was developed in its entirety under U.S. Air Force sponsorship and flew for the last time in the year 2005. It is used to provide exemplification of the subjects covered in this paper because the U.S. Government held from inception full ownership of technical data pertaining to his design and operation without any proprietary restrictions by the contracting developer. Furthermore, to preempt any possibility of disseminating sensitive material, the Titan IV information used for exemplification in this paper has been drawn exclusively from public sources like [5] and [6].

uncommon with LV families, and therefore the selection of records upon which a "demonstrated reliability" estimation is based may ultimately depend on a judgment call made by the assessor. In general, because of such "moving target" situations, the statistical record upon which a "demonstrated reliability estimate" is to be based may be smaller, and the estimate uncertainty correspondingly larger, than what it may be obtained by aggregating, in simple but perhaps not entirely defensible fashion, all the records pertaining to different versions of LVs and associated missions summarily classified under the same name.

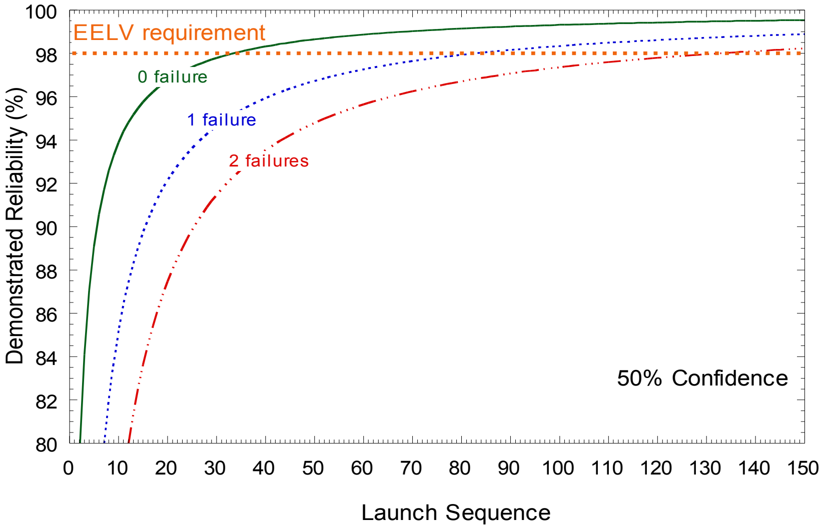


Figure 2: Demonstrated Reliability at 50% Confidence

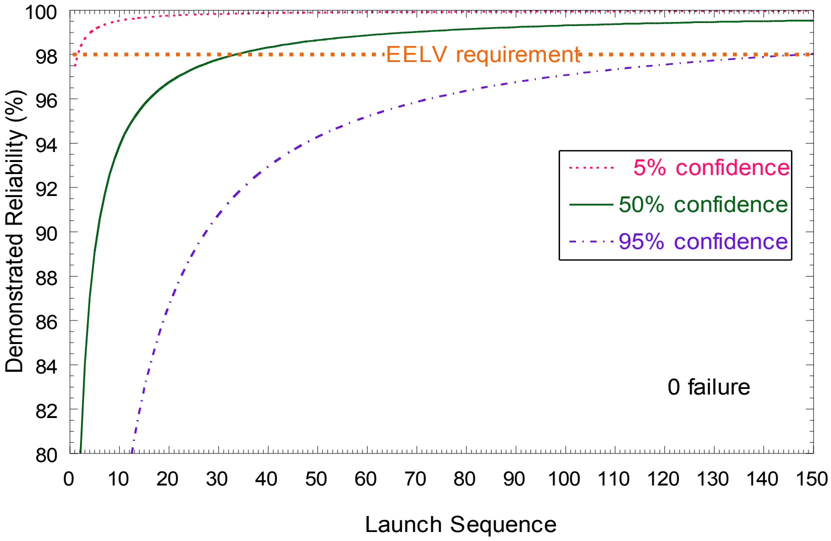


Figure 3: Demonstrated Reliability at 5%, 50%, and 95% Confidence

3.4. Experience-Based Reliability Decomposition Models

A type of estimation that can provide early insight into the mission reliability of a given LV system has been developed using logic decomposition models similar to those used in typical "bottom up" reliability models [5]. This approach differs from the latter in that the lowest-level composing elements of the model correspond to major components, rather than piece-parts, and thus can be quantified with actual mission data collected at the major component level, rather than with handbook data at the part level. The approach takes advantage of the fact that in many cases even a new design uses major components (such as the engines, or the guidance electronics) that are modified versions of components that have flown in earlier LV systems. It is in most cases reasonable to assume that such components will perform with similar levels of reliability in the new system and their record in earlier systems is accordingly used alongside any available flight or test data for the current system, to obtain POF and reliability estimates.

The major-component-level decomposition approach provides a partial remedy to the limitations of a "demonstrated reliability" estimation for new LV systems produced by the lack of sufficient statistical data at the "whole-system" level. However, even with this approach it remains difficult to demonstrate very high reliability at a high confidence level, as often demanded by formal acquisition requirements.

4. EXAMPLES AND COMPARISONS OF RELIABILITY ESTIMATION RESULTS

To give practical perspective to the points discussed in the preceding sections, it is useful to consider some representative results of LV reliability data analyses performed in the past.

4.1. Design Reliability Predictions vs. Actual Reliability Performance

Design reliability predictions based on bottom-up models have often produced values of reliability considerably higher than the success-ratio values eventually resulting from actual performance. Comparisons for LV families currently in use can be difficult because of generally low numbers of actual flights for a given LV configuration and also because of the ambiguity sometimes applied by ongoing programs in the classification of a flight as successful or not (e.g., declaring as successful a mission in which actually the prescribed payload orbit was not achieved by the launch vehicle). A more straightforward example that can be used without incurring these problems is again relative to the now discontinued Titan IV family, which flew 39 missions between 1989 and 2005. Table I shows the design reliability values published for this vehicle alongside its success and failure ratio at retirement, which also coincide with the "classical" MLE reliability and POF (probability of failure) estimation values, respectively. In POF terms, the difference between the design reliability model prediction and the success-ratio value amounts to a factor of about 20 for the basic vehicle configuration inclusive of core and boosters, and of about 10 for the configuration inclusive of the Centaur upper stage. For simplicity, in this comparison no distinction is made between Titan IVA and IVB performance. This is just one example but it well illustrates the issues that may arise in the estimation of reliability parameters and metrics.

Table I: Design vs. Demonstrated Reliability of Titan IV Launch Vehicle

	Design Reliability	Success Rate	Design POF	Failure Rate
Titan IV Excluding Upper Stage	0.9975	0.9487 (37 successes in 39 missions)	2.5×10^{-3}	5.13×10^{-2} (2 failures in 39 missions)
Titan IV with Centaur Upper Stage	0.9853	0.875 (14 successes in 16 missions)	1.47×10^{-2}	1.25×10^{-1} (2 failures in 16 missions)

4.2. Categorization of LV Failure Causes

The gap between design reliability predictions and reliability performance in actual missions can be better explained and understood by examining the identified causes of LV mission failures and major anomalies. This is shown in Figures 4, 5 and 6, which plot the number of failures and anomalies by root-cause for US launches of SLVs (small launch vehicles), MLVs (medium launch vehicles) and HLVs (heavy launch vehicles) in the time period between 1957 and early 2011.

From the figures it can be seen that non-design and non-process related "random" component failures, which de-facto as discussed in Section 3.1 are the only type of failures that the handbook sources of design reliability assessments contemplate, account for a small fraction of the overall LV anomaly rate in actual missions, and account for no known failures. On the contrary the record shows that the failure rates are largely driven by design, workmanship and process errors for all three classes of vehicles. This confirms that any prediction solely based on the random failure rate quantification used in design reliability models is likely to largely under-predict the LV system probability of failure and over-predict its reliability.

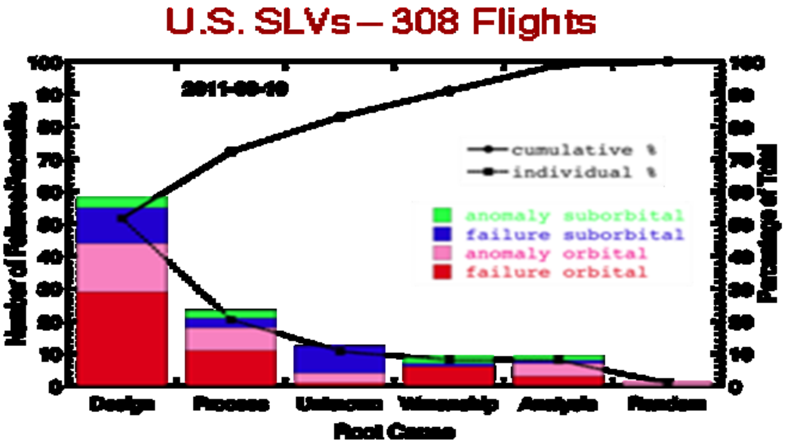


Figure 4: Failure and Anomaly Root-causes for Small Launch Vehicles

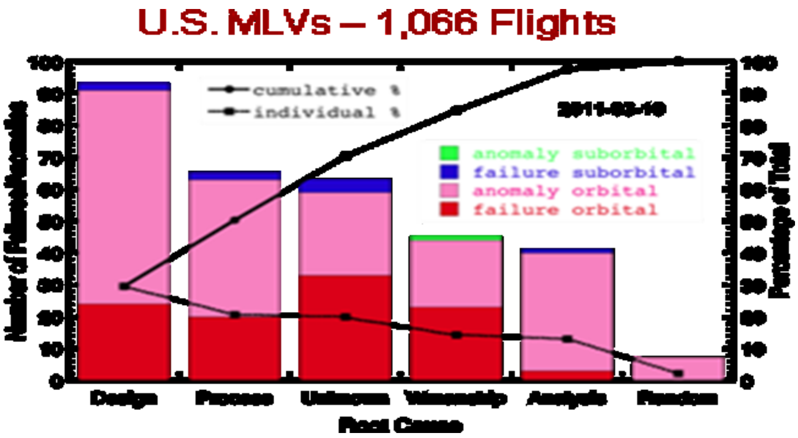


Figure 5: Failure and Anomaly Root-causes for Medium Launch Vehicles

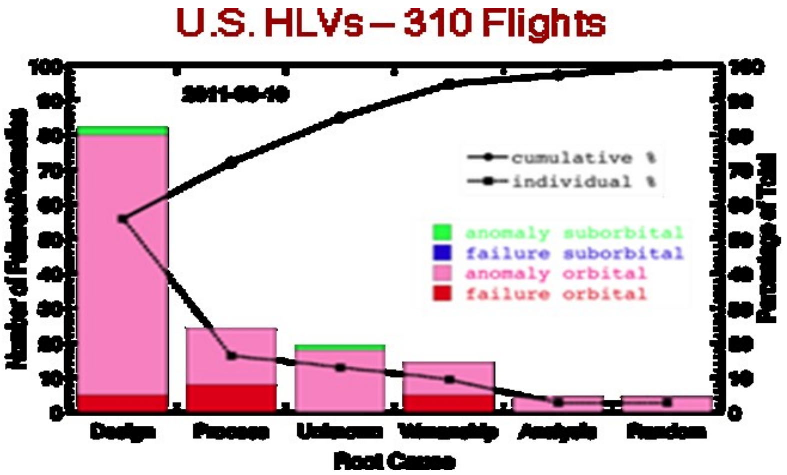
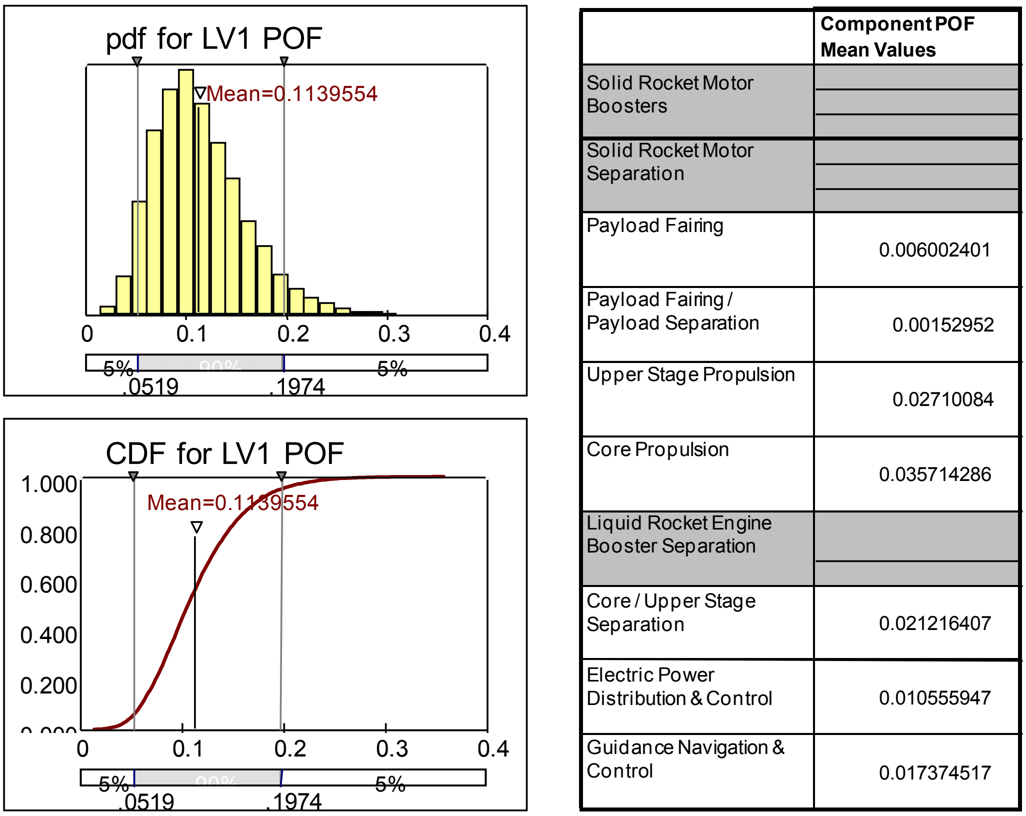


Figure 6: Failure and Anomaly Root-causes for Heavy Launch Vehicles

4.3. Experience-Based Decomposition Model Results

An example of results provided by experience-based reliability decomposition modeling (as discussed earlier and documented in [4]) is shown in Figure 7. Part a) of the figure shows the calculated probability density function (pdf) and the cumulative distribution function (cdf) for the probability of failure (pof) for a given LV model . Part b) shows the mean value contributions of the LV subsystems to the overall system mean value pof. As part a) of the figure shows, the application of this type of approach does not necessarily solve the issues resulting from the typical objective of reliability requirement setting, *i.e.*, early demonstration of high reliability at high level of confidence. However, as part b) shows, the method does generally provide good insight of where, among the system major components, the reliability performance risk of a given LV design resides in relative terms, based on the past flight record of such components. This information can be very valuable in providing an objective basis for prioritizing and directing reliability and mission assurance activities relative to the new LV system of concern.



	Component POF Mean Values
Solid Rocket Motor Boosters	
Solid Rocket Motor Separation	
Payload Fairing	0.006002401
Payload Fairing / Payload Separation	0.00152952
Upper Stage Propulsion	0.02710084
Core Propulsion	0.035714286
Liquid Rocket Engine Booster Separation	
Core / Upper Stage Separation	0.021216407
Electric Power Distribution & Control	0.010555947
Guidance Navigation & Control	0.017374517

a) POF distribution functions

b) LV component POF contributions

Figure 7: LV Reliability Risk Assessment Model Results

5. CLOSING OBSERVATIONS AND COMMENTS

The above review of definitions and approaches relative to the estimation and practical use of LV reliability estimates suggests some important observations and conclusions that are summarized in the following.

The first key observation concerns the practical meaning and interpretation of a typical LV "design reliability" model and associated results. As discussed at some length in the main body of this paper, in general this type of model not only does not account for the contribution to LV system failure from errors in fabrication and processing, but also excludes the contribution of possible errors in the system design, such as errors in correctly characterizing the stressor environment factors and designing the system components with sufficient margins against such environments. Thus, it is important to keep in mind that, contrary to what the term may seem to suggest, a "design reliability" estimate does not necessarily represent the effective reliability of a LV design, even if that design is executed without errors in the fabrication and processing phases preceding an actual mission. In essence, these models do provide value during the design execution process in that they characterize and evaluate some important reliability design attributes (*i.e.*, reliability logic, redundancy and fault tolerance, *etc*.), but they should not be attributed the role of reliability predictors.

A second important observation that proceeds from the above discussion is that the actual "mission reliability" of a launch vehicle, *i.e.*, the probability of successfully completing a typical LV mission, is mostly driven not by the random part or component failures accounted for in design reliability estimates, but by design and process errors. Because of this, a design reliability estimate produces system reliability values that are typically quite higher than those produced by mission reliability estimates that account for the latter types of potential errors, and as just pointed out above, for this reasons, a design reliability estimate cannot be interpreted to be a good predictor of the success rate that a LV system will achieve over a number of actual missions. Consequently, establishing and verifying requirements for design reliability does not necessarily provide a strong assurance that the LV system will achieve a high level of true mission reliability.

A third observation is that “demonstrated reliability” estimations, although useful for understanding overall system performance including both design and process errors, provide results at a limited level of confidence in the early life of a LV family, i.e. before a sufficiently high number of flights of a specific vehicle configuration have occurred. In addition, because in many cases the design of a LV vehicle undergoes very significant changes over the operational life of the system and because actual missions are flown by different configurations among a LV family "options," the number of statistically relevant flights may remain in practice quite limited for a long period of time, and high confidence estimations may never become achievable based solely on such data.

A fourth observation is that the estimates provided by "mission reliability" models and processes, and in particular the "decomposition models" discussed in Sections 3.4 and 4.3, can be very valuable for identifying areas of the LV system design and processes that carry more reliability risk, and for accordingly prioritizing reliability improvements and assurance activities. However, because of the nature and limited pool of the data they need to employ, one must remain aware of the inherent uncertainty in the output provided.

In conclusion, severe limitations continue to exist in the state of the art of LV and STV reliability assessment processes. Design reliability assessments are constructed under assumptions and with data that exclude the proven, most-frequent causes of LV / STV mission failures, whereas mission reliability assessment methods based on more reliable but less than abundant data produce results that are generally less optimistic (and therefore often not politically palatable) and associated with relatively wide ranges of statistical uncertainty. Reliability analyses, when used for other than technically realistic objectives of incremental system evaluation and improvement, i.e., especially in the sensitive arena of requirement setting and verification may quickly become quite problematic, primarily because the limitations that have been discussed at length in this paper are often in direct contrast with the necessity to demonstrate compliance with quantitative requirements that may have been set without sufficient awareness and understanding of such limitations. More specifically, greater awareness may be needed in the launch vehicle technical community of some objective but important realities, such as: the apparent weak correlation between design reliability figures of merit and actual LV family success rates; and the practical obstacles to demonstrating at a reasonable level of confidence, in the early phases of a LV system development, formal compliance with reliability requirements or goals set at high threshold values, e.g., 97% or higher.

6. REFERENCES

[1]. U.S. Air Force, Space Systems and Missile Center (SMC), *"Reliability Program for Space Systems,"* Standard SMC-S-013, (13 June 2008).

[2]. U.S. Air Force Space Command, *"EELV System Performance Requirements Document*," (18 June 1998).

[3]. National Aeronautics and Space Administration, *"Exploration Systems Architecture Study – STI 11-182 (ESAS), Appendix 2D (FOM Definitions),"* (as of May 30, 2012).

[4]. M.E. Pate`-Cornell and S.D. Guikema, "*A Probabilistic Analysis of the Infancy Problem of Space Launch Vehicles*," Proceedings of 7th Probabilistic Safety and Management Conference (PSAM 7), Springer, pp. 2193-2198, (Berlin, June 14-18, 2004)

[5]. S. Guarro and E. Tomei, "*Launch Vehicle Development Risk Projection Methodology*," Proceedings of 7th Probabilistic Safety and Management Conference (PSAM 7), Springer, pp. 2187-2192, (Berlin, June 14-18, 2004)

[6]. S. Isakowitz, *"International Reference Guide to Space Launch Systems, Second Edition,"* AIAA Press, (1995).

[7]. "*Titan IV,"* Wikipedia, the free encyclopedia, en.wikipedia.org/wiki/Titan_IV