Launch Vehicle Reliability and Risk Metrics Definition and Estimation in Relation to Requirements

Sergio Guarro[a]
[a] The Aerospace Corporation, El Segundo, California, USA

Abstract: The reliability of a launch vehicle (LV) is a factor that has great weight and influence on overall satellite and spacecraft mission risk. For this reason, launch reliability and risk metrics have traditionally been identified by U.S. Government agencies as parameters on which numerical threshold values are to be set. The type of reliability metrics which are defined and sought to be controlled by means of such requirements can make a significant difference in the choice of methods of estimation that an assessor may apply with sufficient realism and predictive value of the ensuing results. Past practices, prevailingly based on the formulation and estimation of "Design Reliability" parameters, have rarely been valuable as estimators of actual LV operational risk and reliability. A recent shift towards the use of "Mission Reliability" requirements and metrics is a positive development. This development calls for the application of new reliability estimation methods, which are discussed in general terms in this paper. These methods require the collection of system specific process and mission data, and thus constitute a significant departure from the handbook-based approaches widely applied in the Design Reliability estimations of the past.

Keywords: Launch vehicles, reliability requirements, Design Reliability, Mission Reliability, mission risk.

1. INTRODUCTION

The risk of losing a satellite mission over the time span of a system design life, which is typically in the order of seven to twelve years, is generally dominated by the risk of a launch failure, i.e., by what happens in first handful of minutes, or hours at most for the more complex types of orbit insertion. This consideration has provided a strong motivation for setting rather stringent reliability requirements in the design and/or procurement of launch vehicle (LV) systems by U.S. Government organizations that utilize these systems for their space missions. The EELV (Evolved Expendable Launch Vehicle) program provides an example of how the approach to setting this type of requirements is presently evolving. That is, while earlier versions of the requirements identified the "Design Reliability" parameter as the key performance parameter (KPP) for LV systems and services being procured by the program, the most recent version of the program requirements has shifted, for the same role and purpose, to the use of the "Mission Reliability" parameter. As discussed in the following, this represents a shift with significant practical implications from the reliability assessment and quantification perspective.

This paper provides a discussion and clarification of the reliability terms, and associated metrics, that are relevant in the context just introduced above. It also provides an in-depth discussion of the technical implications, also quite significant, that the evolution of the reliability requirements has on the modelling and estimation approaches that may effectively be used to demonstrate compliance with the quantitative reliability requirements associated with a specific type of metric. In general, it can be observed from the start that the present evolution in the nature of LV reliability requirements reflects a recognition that, historically, compliance with the formerly used Design Reliability threshold values has not been a good indicator or predictor of actual LV system reliability performance in operational terms (i.e., throughout a series of actual launches carried out by a certain type of LV model or family). That is, a quantitative estimation of LV Design Reliability, as defined and interpreted in past practice, is not a good predictor of actual LV success rate, and of its logic complement, LV launch risk.

2. LAUNCH VEHICLE RELIABILITY TERMINOLOGY AND CONTRIBUTING FACTORS

The most recent EELV requirements documentation provides the following definition of "Mission Reliability" [1]:

"EELV Mission Reliability: *The probability that the EELV System will perform intended functions, from Final Command for Liftoff through delivery of each EELV Payload to its specified injection orbit and completion of Collision and Contamination Avoidance. Mission reliability is calculated for each mission-specific instantiation (mission specific combination of design and process)."*

The parenthetical phrase at the end of above definition indicates that Mission Reliability is determined by the two principal contributions of "design" and "process." What is intended by the latter two terms is further clarified by additional language provided in the requirements documentation. More specifically, with regard to **Design Reliability**, the same documentation states:

*"Vehicle **Design Reliability** is analytically derived from experience-based estimates of component and subsystem reliability. Vehicle Design Reliability is the product of the reliability parameters relative to each "as-designed" major component of the overall LV design (e.g., structure and mechanical reliability, propulsion, and thrust vector control reliability; avionics and guidance reliability, electrical power subsystem reliability, staging events/systems).*

Design reliability accounts for potential mission failure modes resulting from random parts failures offset by the redundancy of the design. It does not account for failures resulting from system design errors."

Process Reliability is also defined as follows:

*"The second element, **process**, must take into account mission failures caused by design, assembly, infrastructure, and ground processing or workmanship errors. These failures can be categorized as one-of-a-kind process escapes and can normally be corrected if detected."*

The above definitions differ from corresponding definitions provided in the earlier version of the requirements documentation [2], which, for comparison purposes, are also provided below.

Earlier EELV Mission, Design, and Process Reliability definitions:

*"**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 (Contamination and Collision Avoidance Maneuver). Mission reliability takes into account both vehicle design and process reliabilities. 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). **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)."*

A practical problem arising when using these earlier definitions was that they indicated Design Reliability as a system parameter that fully measures the reliability of a given design, i.e., including the effect of "*mission failure modes that have their genesis in the design of system hardware, component integration architecture, and software*." According to such definitions, Design Reliability models should account for, and quantify, the probability of LV mission failures due to design errors, i.e. errors possibly incurred in the execution of the LV design processes, such as the incorrect sizing of components, or the misjudgement of the effect of mission environments on components, or errors in the specification of software logic. In their actual models and estimations, however, LV Design Reliability assessments have always assumed the system design to be free from such errors, and have only accounted for the redundancy aspects of a design.

The Design Reliability definition provided by the most recent version of the EELV requirements documentation, and quoted above, is less subject to potentially incorrect interpretations. A residual gap between the definition and the "as applied" Design Reliability estimation practice, however, remains where it is stated that Design Reliability is derived from *"experience-based estimates of component*

and subsystem reliability." This gap exists because Design Reliability quantification, as to-date executed by the major U.S. launch vehicle providers, is for the most part not based on estimates derived from launch vehicle experience, but on handbook and software tool databases that condense data from automotive and other ground applications. This practice can have a significant impact on the validity and accuracy of the results, because the underlying data does not reflect the effect that the severe environments experienced in a launch vehicle mission may have on reliability. These effects are absent, or present in much reduced intensity and severity, in the applications and operations from which the handbook and software tool data and failure rate or probability formulations were originally extracted or derived.

2.1 Rationale and Evidence for Focus on Mission Reliability

From the perspective of the spacecraft owner organizations that procure launch vehicle services, there is little doubt that Mission Reliability should be key reliability performance parameter (KPP) on which to set requirements. In fact, such organizations have a direct interest in knowing as accurately as possible, and keeping as low as possible if this does not translate into prohibitively high launch service cost, the probability that an expensive payload be lost due to a launch vehicle failure.

If obtaining realistic early estimations of the probability of launch success or failure is viewed as a primary objective for a LV reliability engineering and analysis program, the change of focus from Design Reliability to Mission Reliability requirements and consequent estimation priority is easily understood and justified. In fact, as mentioned earlier, Design Reliability analysis results have been poor predictors of LV risk, i.e., of the per-mission rate at which LV-induced spacecraft mission losses may be incurred over a series of missions and launches. More specifically, launch vehicle Design Reliability estimations have consistently produced "optimistic" results, i.e., predictions of system reliability that have seldom been matched by the actual LV launch success rates. When examined from the point of view of the quantified probability of failure (POF = 1 – Reliability), the figures predicted by Design Reliability analyses often have been lower than the per-mission failure rates actually experienced, by one order of magnitude or more [3]. An example of this is shown in Table I, which is based on publicly available data [4, 5] (and intentionally refers to a vehicle and associated optional upper stage which are no longer in use). Although vehicles of more recent design have in general proven to be more reliable than the vehicle referred to in the table, the gap between Design Reliability predictions and actual performance persists to the present time as a general trend, for reasons that we further discuss in the following.

Table I – Example of Launch Vehicle Design vs. Demonstrated Reliability

	Design Reliability	Per-mission Success Rate	Design POF	Per-mission Failure Rate
LV – Version w/o Upper Stage	0.9975	0.9487	2.5×10^{-3}	5.13×10^{-2}
LV – Version with Upper Stage	0.9853	0.875	1.47×10^{-2}	1.25×10^{-1}

A comprehensive collection and root-cause categorization of launch vehicle failure and anomaly records, covering the vehicle families illustrated in Fig. 1 in the period from 1981 to the present time, has been maintained at The Aerospace Corporation. The database categorization of root-causes follows the definitions provided in Table II, and is illustrated by Figs. 2a and 2b. This information, which is further discussed below, helps explain why Design Reliability, as commonly defined and estimated in practice, is not a good predictor of actual launch vehicle reliability performance. The Pareto bars shown in Fig.2 assign failures and anomalies to four principal root cause categories defined in Table II. The table actually shows the definitions of a total of seven sub-categories which are assigned in the Aerospace Corporation database. Of these, as also indicated by the table, two are sub-categories of the "Design Process Error" category, and three of the "Production Process Error" category. Thus, for the purpose of the current discussion, the categorization can be reduced to the four categories shown in the figure, which include a "Random" category" for failure or anomaly events where there was no identifiable error in the design or post-design processing of the affected

component, and an "Unknown" category referring to failures or anomalies for which lack of data, or more in general of sufficient diagnostic information and documentation, prevented the determination of an underlying cause. Also note that in the LV database the term "failure" is used when a part or component completely lost its ability to function, whereas the term "anomaly" is used for events where a component or part was functioning, but was, in form or function, significantly outside of its design specifications.

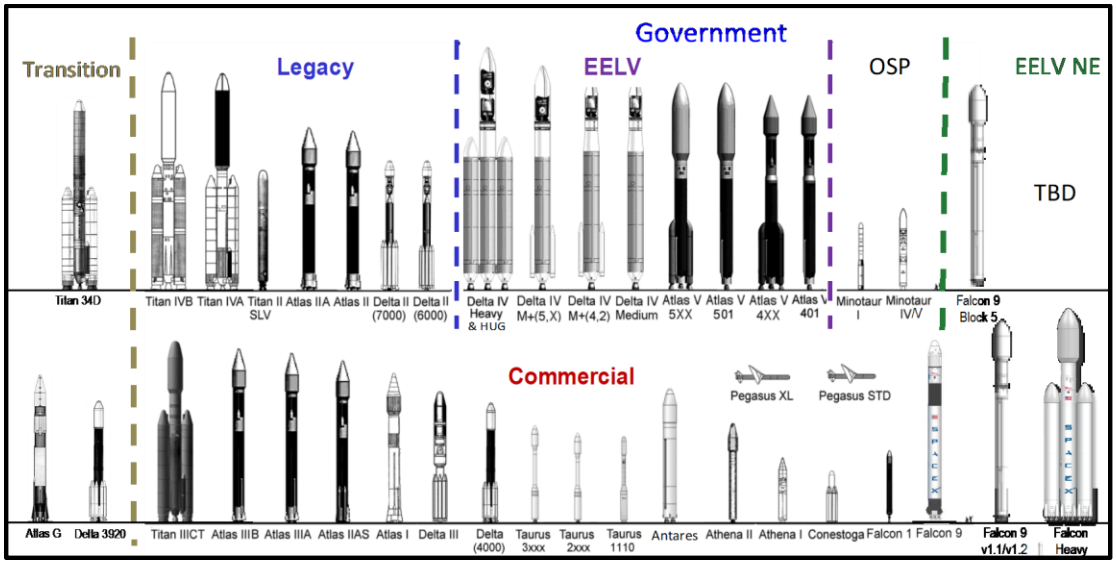

Figure 1 - Launch Vehicle Families Included in Failure and Anomaly Database

Table II – Definition of Failure and Anomaly Cause Categories

Cause Category Classification for Component-level LV Mission Failures and Anomalies		Definition
Random		Failure / Anomaly caused solely by the random behavior of a component or part, when determined that: the componenet/part was operating within its design parameters, both the hardware and software design were free of errors, and the consequent manufacture, assembly, and launch preparations did not introduce errors or defects.
Design Process Error Induced	Design Analysis Induced	Failure / Anomaly caused by errors in the Systems Analysis portion of Launch System design and operation. These include errors in defining the environments, loads, dynamics, events, mission design, or operating conditions of the Launch System.
	Design Engineering Induced	Failure / Anomaly caused by Engineering errors in the Launch System design process. These include errors in the specification, selection, qualification, or application of any LV or GSE component or part. These also include errors in the ground/flight software logic or design.
Prodctn. Process Error Induced	Process Engineering Induced	Failure / Anomaly caused by post-design Engineering errors introduced during the Manufacturing or Launch Operations process. These include errors in Engineering instructions to the Production process or Engineering judgement in anomaly disposition.
	Manufacturing / Launch Operation Induced	Failure / Anomaly caused by Production errors introduced into the Launch System fabrication and mission-preparation processes which result in a significant deviation of hardware or software components or operating characteristics that differ from their design requirements. These include errors in the manufacture, assembly, handling, testing, software build, or inspection requirements of the Launch System elements for a particular mission.
	Workmanship Induced	Failure / Anomaly caused by human errors introduced by Technicians or other Operators during the Manufacturing or Launch Operations process. These include errors introduced in the manufacture, assembly, handling, testing, software data entry or coding, or inspection of the Launch System elements for a particular mission where the instructions or other process directions are error free.
Unknown Cause		Failure / Anomaly for which available data and/or documentation is insufficient to permit assignment to one of the other categories defined in this table.

The key observations from the data presented in Figs. 2a and 2b that are relevant to the present discussion can be summarized as follows:

a. Both LV failures and LV anomalies are overwhelmingly due to errors in design or process. There is no evidence in the LV mission record of failures inherently due to "random" failure causes, which are the types of failures exclusively accounted for in the component failure rate databases and formulations used as the foundation of Design Reliability models. When

expanding the view to also consider anomalies, random causes of failure still account for a practically negligible fraction of all anomalies.

b. Critical LV components exhibit per mission failure rates that are significantly higher than the rates provided by reliability handbook and software-tool formulations. This can be deduced by noting that all of the 37 component failures reported on Fig. 2a resulted in a failure of the LV system, and also noting that the data plotted on the figure is relative to a total of 597 LV missions from 1981 to the present time. This translates to a failure rate estimate, for the "average" LV included in the record, of about 6.2 x 10^{-2} per mission, i.e. about 1 failure every 16 missions in the average, whereas LV system-level estimates based on component failure rates and probabilities provided by handbook and software-tool formulations have been typically in the range between 5 x 10^{-4} and 5 x 10^{-3}, i.e., between 1 failure every 2000 and 1 failure every 200 missions.

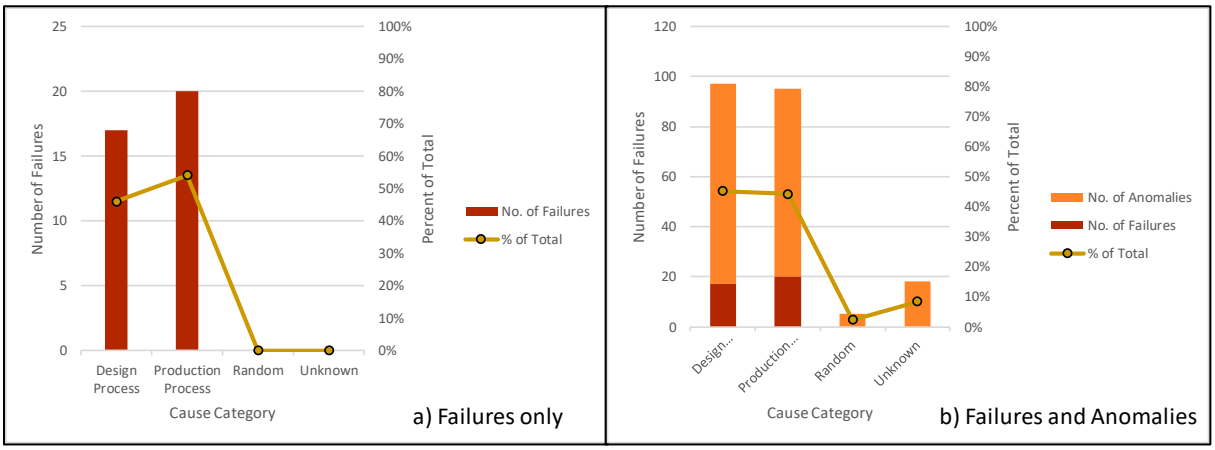

Figure 2 - LV Component Failures and Anomalies by Cause Category

The LV operational experience also strongly points at the high intensity stressor environments present in LV missions (i.e., vibration, shock, and thermal effects) as being driving factors that make the presence of any error-induced defects in hardware or software become mission-critical. I.e., the LV stressor environments are unforgiving of any error, however "small," that may be introduced in the design, manufacturing and processing of a vehicle.

In conclusion to this section, the above evidence underscores that, to be realistic as an estimator of true LV operational reliability, a reliability model cannot altogether exclude consideration of the possibility and likelihood of errors in design and process. The Mission Reliability parameter definition, and the new focus on this latter parameter, represent EELV program steps that may help LV reliability assessment practice to develop in this direction.

2.2. Contributions to Overall System Reliability

Both the current and past versions of the EELV requirements refer to LV Mission Reliability as being determined by the two distinct composing elements of Design Reliability and Process Reliability. However, as mentioned earlier, the term Design Reliability may be subject in practice to different interpretations. To avoid potential misinterpretations ensuing from the inherent ambiguity of the term, it is useful to look at the distinctions that can be made, on the basis of operational flight evidence like the one discussed in the preceding section and summarized in Fig. 2, with regard to the principal types of contributions, including design, to LV unreliability (i.e., POF). Once defined, such distinctions can be related in unequivocal fashion to the terminology adopted by the current version of the EELV requirements documentation.

With the above in mind, the following three principal components of LV system reliability / unreliability contribution can be considered and identified from the point of view of their underlying root-cause attributes:

A. **Theoretical Reliability**, i.e.: *The reliability determined solely by the redundancy characteristics of the LV design and by the random failure rate characteristics of the design components and parts, when it is assumed that both the design and the constituting hardware and software, at all levels of indenture and assembly, are free of errors or defects.*
B. **Design-Process Reliability**, i.e.: *The probability that no errors or defects capable of producing a mission failure are introduced, at any level of hardware and software indenture or assembly, by the system design definition and specification processes and activities.*
C. **Production-Process Reliability**, i.e.: *The probability that no errors or defects capable of producing a mission failure are introduced, at any level of hardware and software indenture or assembly, by the part and component production, assemblage, integration, and test processes and activities.*

The above breakdown of reliability contributing elements, which is based on the distinctions among failure root-causes that can be made on the basis of the actual collective LV flight record up to the present, can be related to the categories and terminology of both the previous and current versions of the EELV requirements documentation, as shown in the illustration provided by Table III below.

Table III – Correspondence of LV Mission Reliability Contributing Factors

Earlier EELV Definitions	Root-Cause Based Definitions	Current EELV Definitions
Design Reliability	Theoretical Reliability	Design Reliability
	Design-Process Reliability	Process Reliability
Process Reliability	Production-Process Reliability	

The table reflects the mapping of the definitions of Design Reliability and Process Reliability, when interpreted literally as given in the two versions of the EELV requirements (see also Section 3), to the three categories of reliability defined above on the basis of the contributing component failure root-cause. Thus, when comparing it to the more recent EELV definitions, the term "Theoretical Reliability" (essentially a shorthand for "Error-free Design Reliability" or "Random Contribution Reliability") directly corresponds to the current EELV definition of "Design Reliability;" whereas "Design-Process Reliability" and "Production-Process Reliability," in combination, map into the definition of "Process Reliability." When comparing with the earlier EELV definitions, however, it is the combination of the "Theoretical Reliability" and "Design-Process Reliability" elements that maps into the "Design Reliability" definition, if the latter is taken literally.

3. METHODS FOR LV MISSION RELIABILITY ASSESSMENT AND ESTIMATION

Regardless of the interpretation of reliability terms that, per the discussion in the preceding section, may be extracted from one type of definition or another, the practical reality is that until the present time reliability models and quantifications produced by LV providers have primarily covered the Theoretical Reliability portion of the overall Mission Reliability contributions. This portion has generally been referred to as "the launch vehicle Design Reliability," even though, as pointed out earlier, it does not account for failures resulting from possible errors introduced in the execution of the system design definition and specification processes. Although this approach essentially leaves out any contributions to unreliability that may be resulting from either design or production processes, it has generally been in the past considered acceptable in the EELV program context and beyond, i.e., even in the generation of considerable portions of LV risk models produced for or by NASA. In the EELV context this was consistent with the past focus on Design Reliability as a KPP. However, with the elevation of Mission Reliability to KPP role, and as per the evidence and considerations presented in Sections 2.1 and 2.2, the reliability quantification practices routinely applied for Design Reliability estimation purposes can no longer be relied upon for the estimation of the "non-random" contributions (i.e., potential design and process errors) to LV mission risk and overall Mission Reliability. The following sections discuss possible approaches for modelling and quantifying Mission Reliability, with primary reference to the most recent EELV program definitions and requirements.

3.1 LV Reliability Models

In the majority of cases, the reliability or probability of failure (POF) of a complex engineering system cannot be reliably quantified via a direct collection of success and failure statistics at the whole system level. In the assessment of newly designed systems this is because those success and failure records that are deemed directly applicable, because they are extracted from sufficiently similar systems, are rarely available in statistically usable form and quantity. Even systems that have been operational for a while present a similar challenge, as the design and the mode of operation typically has changed over time, and the records relative to older instantiations of the system of concern have become of uncertain applicability if extrapolated to newer versions of the system. For all the above reasons, the "repeatability under same conditions" prerequisite to the estimation of probability from empirical tests is in most cases not satisfied when the test or operational record concerns a large and complex system.

As an alternative to direct estimation, the techniques applied for reliability or risk assessment of such complex systems rely on models that decompose the system into a logic structure of lower level components, for which statistical data deemed usable for the model quantification can be collected from various sources [3]. These may include what practitioners refer to as "generic" or "non-system-specific" data sources, i.e., collections of component performance data from systems and contexts other than the system and mission of concern. When such generic sources are used, however, it becomes critically important to the quality of the reliability quantification process that the component operating conditions and stressor environments under which the "generic" reliability data is collected be substantially similar to those of the mission of concern. If this precondition is not satisfied, the probability and reliability estimates derived from such data cannot be assumed to be directly applicable and valid. This caveat cannot be over-emphasized, especially when the system of concern is a launch vehicle system, where the stressor environments that affect reliability are severe, and the choice of readily applicable and verifiable data sources is limited. Indeed, large discrepancies between early predictions of launch vehicle reliability and actual records of system success rate (i.e., "demonstrated reliability"), have been observed when the former were based on the use of generic data collected in quite different systems and environments for the quantification of LV system reliability models. The reliability values displayed in Table I of Section 4 are an example of how large such discrepancies have been in some cases.

In essence, a system model decomposition and quantification process is based on the assumption that when individual system components and parts of similar characteristics are used across different systems, their failure and reliability record from earlier uses can be considered as being representative of future performance for similar functions and under similar conditions. Consequently, the associated component-level probability estimations are assumed to be usable as inputs to the models developed to obtain reliability estimates for newer system in which these components are used. The main purpose of the system decomposition into appropriate logic models is thus to express the reliability or POF of the system as a function of the corresponding probabilities estimated for, and assigned to, its basic components. Once the latter are determined in quantitative terms, the model yields the quantification of the reliability or POF of any other higher-level portion of the system, including the whole system itself. Per the above, how far down the model decomposition may go in the functional hierarchy of the system hardware and software would generally depend on the level of indenture at which applicable component failure rate and probability data is determined to be available.

In summary, the typical reliability or risk assessment process for a complex system can be described as consisting of two principal steps:

A. a ***reliability model development*** step that decomposes the system in top-down fashion, and logically represents the success or failure of the system in terms of the success or failure of its constituting hardware, software, and human components;
B. a ***reliability model quantification*** step that quantifies reliability and/or POF values, starting from input estimates for components at the lowest levels of indenture of the reliability model,

and obtaining higher level subsystem and system values from mathematical expressions or algorithms that reflect in probability terms the logic structure of the system design and associated models.

The above does not imply that the two listed steps, as described, are all that is involved in a system reliability estimation. Besides what is referred above and in the following as the "***reliability model***," which essentially describes in binary logic form the redundancy characteristics of a system design, other statistical and probabilistic models, in the form of logic and mathematical formulations or algorithms, are also applied to obtain, from raw data, the probability parameters that are used as actual inputs to the reliability model itself. In this paper, these are referred to as "***estimation models***."

An relevant observation concerning the types of system reliability contributions that have been defined and discussed in the preceding sections of this paper, i.e., Mission Reliability, Design Reliability, and Process Reliability, is that such contributions can usually be calculated using as a basic reference framework the same system reliability model, which is developed to represent the logic design structure of the system of interest. The specific type of system reliability parameter estimation which can be produced utilizing that same system model is then actually determined by what type of data is selected and applied to derive the component-level reliability parameter estimates that are used as inputs to the system model. This remains basically true regardless of the choice of logic formats – e.g., reliability block diagrams (RBDs), fault trees (FTs), success-trees (STs), event trees (ETs), and combinations thereof – according to which the system model is constructed, since all such formats are essentially equivalent in information content and produce the same results for a given system when consistently applied and quantified with the same probability and reliability input data. Given this, the remainder of this paper will not further discuss reliability logic-model choices, and places instead its focus primarily on the subject of data analysis and component-parameter estimation models, as applicable to the quantification of the categories of reliability identified in the preceding discussion.

3.2 LV Reliability Quantification

In addressing the topic of launch vehicle reliability quantification, this paper makes reference to the three types of contribution identified by the middle column of Table II, and uses the mapping illustrated by the table to refer to the corresponding categories of contribution identified per the definitions formerly and presently used in the EELV program context. As stated earlier, the use of the three categories "Theoretical," "Design-Process," and "Production-Process" is adopted here because it bestt reflects the nature of the existing reliability data.

3.2.1 Quantification of Theoretical Reliability

Per the definition given in Section 2.2, the term Theoretical Reliability is used in this paper to refer to the reliability attributable to a LV system, if such a system could be designed and produced completely free of errors or defects, so that its reliability metric would be solely determined by the intrinsic characteristics of its parts and components and by the degree of fault-tolerance and redundancy built into its logic design. From this definition, and from the earlier general discussion on the reliability assessment process, it follows that a valid quantification of such a system metric may be obtained by executing the two following steps:

A. Development of a system reliability model that decomposes the system into its components and correctly represents the system redundancy and fault-tolerance design features, down to the level of indenture at which quantification data is available and applicable.

B. Quantification of the system reliability model using component-level reliability data that has the following requisites:

    a. The data is obtained from sources (i.e., operations and/or tests) where the components of concern were used for the same functions and under the same stressor-conditions as in the system of concern.

b. The data does not include any failure or anomaly counts that reflect either an error in component design (e.g., incorrect specification of "form and fit," incorrect definition of functional performance margins, etc.), or an error in component "processing" (e.g., error in manufacturing, assembly, test, calibration, etc.).

3.2.2 Quantification of Design Process and Production Process Reliability

Definitions of Design Process and Production Process Reliability were also provided in Section 2.2. The Design Process Reliability definition refers to the probability of carrying out the formulation and specification of a system design without introducing "design errors," i.e., errors resulting in system specification defects of "form and fit" with respect to the functionality and level of performance that the system is required to have in order to successfully execute its mission(s). The Production Process Reliability definition refers to the probability of carrying out all the steps that are downstream of the design steps, including manufacturing, assembly, and mission preparation, and any sub-steps thereof, without introducing any "production errors," i.e., errors resulting in significant hardware or software defects with respect to the characteristics that the design specifications prescribe for all system components, in order for these to be able to successfully carry out their functions in any given system mission.

To sum the above up it can be said that:

- Design errors are errors in the design execution process which result in erroneous component and/or system specifications.
- Both design and production errors often have a "human error" as their root cause, although exceptions to this can also occur (for example when a robotic production line produces component defects because a piece of machinery drifts out of its tolerance limit without immediate detection).
- Production errors are errors in the system fabrication and mission-preparation process which result in a significant deviation of hardware or software component characteristics from their design specifications (where "significant" is intended as a deviation greater than the tolerance limits specified by design).

When considering either type of error, the interest of the reliability assessor will be more specifically focused on the subsets of errors which are significant enough to result in critical system defects and faults, i.e., defects or faults that are sufficiently severe to cause a system failure during the execution of a mission. It must be noted that a cause-effect relation between errors and mission effects, including the extreme effect of a mission failure, can exist regardless of the amount of time that may pass in between. In fact, both design and production errors typically occur, time wise, long before the execution of a mission where their effect may become manifest. Generally, unless they are detected by inspection and test processes, the component defects or faults introduced by an error will lay dormant in the system until mission execution time, when the affected components are activated to perform their functions. At such time any such component defect or fault may produce a system performance deficit or an outright loss of system critical functionality and consequent mission failure.

The above observations have the purpose of providing perspective and background for the discussion that follows of the approaches to quantification of design process and production process reliability. These approaches may be characterized in different ways, but it is useful to classify them primarily by one of the following attributes:

A. Predictive Quantification: quantification based on human error models utilizing "generic" data and information, i.e., data and information which is not specifically and directly related to the system being assessed.

B. Process-data Based Quantification: quantification based on statistical data pertaining to the rate of occurrence and detection of errors in design or production processes, respectively.

C. Mission-data Based Quantification: quantification based on the classification of mission anomaly and failure data into the relevant root cause categories, i.e.:
   a. Design errors
   b. Production errors
   c. Random part / component failures

Further discussion of each of the above approaches is provided in the subsections that follow below (Sections 3.2.2.1, 3.2.2.2, 3.2.2.3). In actual practical applications, the approaches may be used in combination. A discussion of how this may be accomplished is also given in a dedicated subsection (Section 3.2.2.4).

3.2.2.1 Predictive Quantification

A "predictive" approach considers a particular design or production process as a series of steps or tasks involving human activity or machine automated executions. A conceptual depiction of the logic sequence of events that may cause a mission failure as the result of an initial design or production error if provided in Figure 3. The figure shows that this kind of mission failure may occur if a significant design or production error occurs first, and that error escapes any detection in all the subsequent checkpoints built into the design and/or production process.

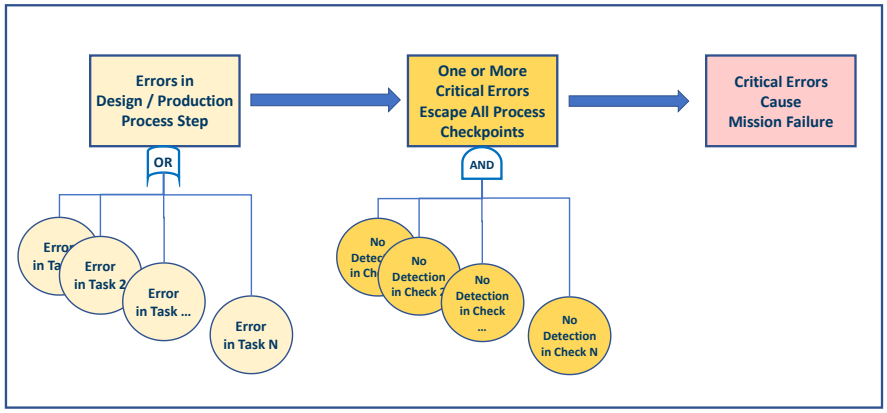

Figure 3 – Conceptual Process Error to Mission Failure Event Sequence

Following the conceptual logic model of Fig.4, the probability of mission failure due to a process error, POF_{PE} , can be calculated according to the following general conditional probability formulation:

$$POF_{PE} = p(CE) \times p(EE \mid CE) \quad (1)$$

where:

p(X) = Probability of Event X
CE = Critical Error
EE = Error Escape
EE / CE = Error Escape, given that Critical Error has occurred

In a Predictive Quantification type of analysis, the probability of a critical error occurring in any one of the process steps of concern, p(CE), can be estimated using either:

a. a human reliability predictive model, for steps executed as human tasks
b. a hardware / software reliability model concerning the equipment executing process steps, for steps executed by automated machinery or robotic tasks.

With regard to the above formulations it is noted that a critical error is here defined as follows:

***Critical Error**: an error producing a hardware or software component defect or fault which, if not detected and corrected before the mission operation of that component, will make it fail to perform its function during the mission.*

To quantify eqn.(1), the probability of a critical error, p(CE), may be obtained directly from an estimation model, e.g., one of the available human reliability model formulations. Human reliability

estimation models that can be used in a Predictive Quantification have been developed and documented in relation to nuclear power plan probabilistic risk assessment (PRA) applications, as well as in early U.S. Air Force and Navy studies [6-8]. In cases where the estimation models might provide an aggregate rate of critical and non-critical errors in various kinds of tasks, the critical error probability may be calculated as the product of the probability of a generic error occurring, times an estimated fractional value representing the ratio of critical errors to all errors. I.e.:

$$p(CE) = p(GE) \times f_C \qquad (2)\ ,$$

where:

GE = Generic Error (i.e., error of any severity)

f_C = number of critical error / total number of errors

Per eqn.(1), once the probability that a critical error occurs is estimated, the quantification process would also requires the estimation of the probability, p(EE │ CE), that such error not be detected in any of the standard downstream process checkpoints, such as inspections and/or tests. If any of the process checkpoints consist of human inspection or test processes, human reliability estimation models may also be applied to determine the POF / reliability of the corresponding steps and tasks.

In concluding the discussion of this section, it is noted that the illustration in Fig.4 and the formulations in eqns.(1) and (2) are conceptual, in that they do not attempt to depict the level of indenture – i.e., component or assembly level, etc. – at which the estimation may be actually applied in practice. The latter is a modelling choice for the analyst to decide upon, depending on factors that may include the similarity or difference among process steps executed in the design and production of various types of components, and the corresponding differentiation among the reliability model formulations for such steps and tasks.

3.2.2.2 Process-data Based Quantification

The preceding section on Predictive Quantification has discussed the conceptual form of a possible ***estimation model*** for process failure probabilities. Such a model, or an equivalent one, would be applied as a pre-processing element in the reliability model quantification, and used to enable the insertion of estimated process-induced failure probability values into an overall system reliability model developed in one of the common logic formats (e.g., RBD, FT, ET, etc.) that have been mentioned earlier in Section 3.1.

A Process-data Based Quantification procedure would typically use an ***estimation model*** of similar conceptual form, including formulations like eqns.(1) and (2). However Process-data Based Quantification differs from Predictive Quantification in a key element, i.e. in that, instead of estimating probability values on the basis of generic guidelines and formulations based on generic data, it uses statistical data directly collected for the design and production steps of the LV system of concern to estimate the probability parameters that appear in equations like (1) and (2). That is, the estimation is directly based on process control data recorded from the design and production lines of the LV system of interest, or, if such data is not available in sufficient measure to support meaningful estimations, from the corresponding processes of similar systems to which the analyst has direct access. The main data of interest to enable the estimation process will primarily consist of error rate and escape rate statistics concerning all the major system design and production steps, from design specification all the way to launch preparation and readying processes.

3.2.2.3 Mission-data Based Quantification

Mission-data Based Quantification is the last basic type of quantification approach to be discussed in this paper. It differs from the two methods discussed earlier in Sections 3.2.2.1 and 3.2.2.2 because it directly uses anomaly and failure data pertaining to already executed missions. These missions usually would include not only all those already executed by the LV system of interest, but also missions of other LV systems that are sufficiently similar to it, overall or in some of their components. The existence of close similarity provides the rationale for use of the related data for estimations concerning the system of concern.

Unlike Predictive Quantification and Process-data Based Quantification, the Mission-data Based Quantification approach does not rely on either generic or system-specific data pertaining to the execution of design or production process steps. Instead, it sorts actual mission data into the three basic categories of root causes that can be used, respectively, to estimate the three types of reliability contributions defined in Section 2.2, i.e., Theoretical Reliability, Design-process Reliability, and Production-process Reliability. As illustrated by Figure 4, the three data categories are:

a. Random component failures and anomalies
b. Design error induced failures and anomalies
c. Production error induced failures and anomalies

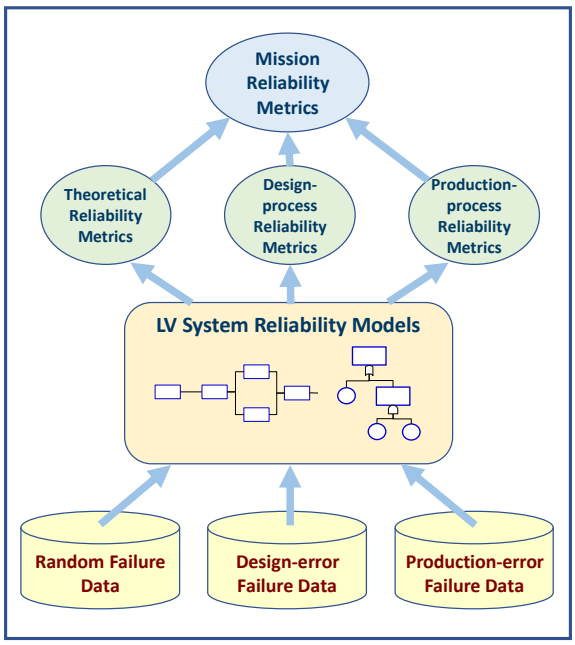

Figure 4 – Use of Mission Data in Reliability Quantification

Once collected and sorted into the three above categories, the data can be used according to standard statistical estimation techniques, e.g., classical or Bayesian estimation, to quantify the system reliability logic models (RBDs, FTs, etc.). When a model is quantified solely with the "random failure" type of data, it will provide Theoretical Reliability figures of merit; when solely with "design error" data, Design-process Reliability figures of merit; and when solely with "production error" data, Production-process Reliability figures of merit.

As discussed in the following section, Mission-data Based Quantification is most frequently used in combination with other types of quantification procedures. This is because, although the data that it hinges upon is the most applicable and realistic, it is also rarely available in sufficient measure to support a high degree of confidence statistical and probabilistic estimation to be based solely on it.

3.2.2.4 Combination of Quantification Methods

In a practical execution context, the methods of reliability quantification discussed in the preceding three sections may be applied in combination, usually according to steps executed in a time staggered sequence that would reflect the availability of different types of information and data in the design and development life cycle of a given LV system.

At the early stages of design and development, a Mission Reliability estimation including the estimation of Design-process and Production-process Reliability would usually rely on a Predictive Quantification approach, as actual system-specific data would normally be yet available at such stages. When process control statistics would begin to be collected and become usable, the predictive results may then be updated. This may be formally done via a Bayesian estimation that uses the predictive results to set up "prior distributions" for the reliability metrics of interest, which are then mathematically combined with the newly obtained and system-specific process data via Bayes

theorem, yielding updated "posterior distribution" results. The results derived in this fashion would thus represent a combination of Predictive and Process-data Based Quantification.
The updating process can be iterative, in the sense that, any time new data is collected and becomes available, this data can be used in a further Bayesian estimation update that uses the previous posterior distribution results as prior distributions and obtains new and updated posterior results. Thus, the process can also be used to bring Mission-data Based Quantification into the overall estimation process. To execute this, the posterior distributions derived from the use of Predictive and/or Process-data Based Quantification can be used as Bayesian prior distributions to be updated with mission data. The results of a Bayesian updating carried out in this fashion would then be the product of the combined use of all three approaches that have been discussed in the preceding sections, i.e.: Predictive, Process-data Based, and Mission-data Based Quantification.

4. CONCLUSIONS

Past LV reliability assessment practice has primarily concerned itself with the estimation of LV Design Reliability. In addition, the term Design Reliability itself has been in practice not inclusive of the consideration that errors may be present in a given design, so that LV Design Reliability estimates have in general only indicated the Theoretical Reliability that the system may have if considered free of any error in design and production (i.e., post-design fabrication, assembly etc.), and subject only to random part and component failures. This has resulted in a wide dichotomy between Design Reliability estimates and the actual reliability achieved by typical LVs, as the operational record of the recent past has overwhelmingly indicated. Furthermore, such record also shows that the causes of LV mission failures (and anomalies) have resided in factors related not to random part and component performance, but to errors in design and/or production of a ready-to-launch system. The LV reliability analysis community is presently being incentivized to address these issues by new forms of LV requirements that emphasize Mission Reliability as the principal reliability performance parameter upon which quantitative threshold values are set as goals or requirements. The shift from Design Reliability to Mission Reliability modelling and estimation requires a new approach to LV data collection and utilization. This paper has identified and discussed practical pathways that can be followed for such an approach. These pathways de-emphasize the utilization of handbook and software-tool failure rate formulations, whose applicability to LV components subject to extreme stressor environments cannot be validated, and call for the use of actual LV design, process, test and mission data, complemented by the application of appropriate reliability parameter estimation models that, consistently with both recent and past LV operational record and evidence, take into account the possibility of design and production errors as drivers of LV Mission Reliability performance.

Acknowledgements

The material presented in this paper has been collected and produced thanks to the multi years sponsorship of the U.S. Air Force Space Systems and Missile Center (SMC) EELV Program and of The Aerospace Corporation Space Launch Division. The author is also indebted to Edmardo ("Joe") Tomei, former Chief Engineer of the latter organization, for the patient collection, compilation and organization of the data upon which much of the discussion in this paper has been based.

References

[1] *"Evolved Expendable Launch Vehicle Program System Performance Requirements Document,"* Rev. A, Space and Missile Systems Center, LE-S-001, 19 June 2017.
[2] *"Evolved Expendable Launch Vehicle Program System Performance Requirements Document,"* Rev. B, Space and Missile Systems Center, 11 October 2011.
[3] S. Guarro, *"On the Estimation of Space Launch Vehicle Reliability,"* International Journal of Performability Engineering, Vol. 9, No.6, November 2013, pp.619-631.
[4] S. Isakowitz, *"International Reference Guide to Space Launch Systems,"* Second Edition, AIAA Press, 1995.

[5] *"Titan IV,"* Wikipedia, the free encyclopedia, en.wikipedia.org/wiki/Titan_IV.
[6] J.A. Forrester, et al., *"An Overview of the Evolution of Human Reliability Analysis in the Context of Probabilistic Risk Assessment,"* Sandia National Laboratory Report SAND2008-5085, January 2009.
[7] D. Meister, *"Comparative Analysis of Human Reliability Models,"* Bunker Ramo Corporation Report L0074-1U7, November 1971.
[8] I.A.Irwin, et al., *"Human Reliability in the Performance of Maintenance,"* Aerojet-General Corporation Report LRP 317/TDR-63-218, May 1964.