Pitfalls and Precautions when using Predicted Failure Data for Quantitative Analysis of Safety Risk for Human Rated Launch Vehicles

Glen S. Hatfield(1), Frank Hark(2) James Stott, Ph.D.(3)

(1) Bastion Technologies Incorporated, 17625 El Camino Real #330, TX 77058, USA,
Emails: glen.s.hatfield@nasa.gov, frank.hark@nasa.gov

(2) *NASA Marshall Space Flight Center, Huntsville, AL 35812, USA ,Email: james.e.stott@nasa.gov,*

ABSTRACT

Launch vehicle reliability analysis is largely dependent upon using predicted failure rates from data sources such as MIL-HDBK-217F. Reliability prediction methodologies based on component data do not take into account risks attributable to manufacturing, assembly, and process controls. These sources often dominate component level reliability or risk of failure probability.

While consequences of failure is often understood in assessing risk, using predicted values in a risk model to estimate the probability of occurrence will likely underestimate the risk. Managers and decision makers often use the probability of occurrence in determining whether to accept the risk or require a design modification. Due to the absence of system level test and operational data inherent in aerospace applications, the actual risk threshold for acceptance may not be appropriately characterized for decision making purposes. This paper will establish a method and approach to identify the pitfalls and precautions of accepting risk based solely upon predicted failure data. This approach will provide a set of guidelines that may be useful to arrive at a more realistic quantification of risk prior to acceptance by a program.

INTRODUCTION

In today's environment, cost, schedule, and safety risk are paramount in the aerospace industry. Many companies and government agencies are allowing predicted reliability data to be used to determine if a component, assembly, system, and ultimately the vehicle, meet safety requirements. Typically, Safety engineers use subjective methods or they may use quantitative methods to assess the likelihood of a specific failure scenarios occurrence. Quantifying the risks would be the first choice in assessing risk; however, some programs allow the use of predicted failure data to quantify the risk accomplished by the modeling of failure scenarios. Failure data typically come from MIL-HDBK-217F, which is outdated and has been discontinued by the Department of Defense (DoD). The values are generally overly optimistic, as can be seen by comparison with demonstrated data. These values are adjusted for the specific failure mode distributions that causes a specific failure event. These values often misrepresent the actual risk when managers are considering accepting or rejecting the risk. In either case, the cost of redesign or loss of the asset may represent a significant failure for the program. This paper will examine the differences in using predicted vs. demonstrated data methods. One method uses epistemic error factors, and the other uses calculated error factors per the formulation found in SAPHIRE version 8 [2]. Examining these differences will identify the pitfalls and demonstrate the need for precautions.

In addition, testing which is used to validate the product is also being reduced to realize even further cost and schedule savings, often at the expense of reliability and safety. Decreased electrical, electronic, and electro-mechanical (EEE) parts grades have also been allowed in certain instances. In other areas, it has been proposed to reduce thermal cycling, burn in, and thermal vacuum testing to provide even further cost and schedule reduction. These measures may actually increase the risk of failure by not knowing if the reliability has been met as well as allowing infant mortality failures to occur while on the launch pad. Unidentified latent failures that are undetected due to reduced testing may manifest during flight. All of these issues may very well increase the overall risk to a point that the true risk is unknown, especially when predicted values are used in modeling the risk, and uncertainty surrounding the model is now in question.

Precautions should be made aware when using predicted data to assess safety risks due to pitfalls of unidentified or incorrectly identified failure data and associated uncertainty. Predicted data does not take into account manufacturing, assembly, and operational processes. When quantifying risk, the actual risk reported and used in the decision making process may misrepresent both the outcome and associated uncertainty.

The predicted and demonstrated data models utilize epistemic and aleatory error factors (EF), which represent the uncertainty in each model.. A lognormal distribution is assumed for both models and the resulting mean risk and system uncertainties are then compared.

1 ESTIMATING FAILURE RATES

1.1 MIL-HDBK-217F

This approach quantifies failure rates at the component level, which is modified, based on a component's, environment, temperature range, and quality. When used in similar environments, the differences between system applications may be significant. Correct application by the user is a limitation of the prediction method.

The example model below demonstrates the effect of predicted reliability data.

The Model basis: MIL-HDBK-217F [5] stress method, environment is Airborne Uninhabited Fighter (AUF). Quality factors are those of the highest level for the specific part analyzed. Temperatures, where applicable, are baselined at 130 deg. C, stress loads, where applicable, are between 90 and 100%. Devices are procured with normal manufacturer's screening consisting of temperature cycling, constant acceleration, electrical testing, seal test, and external visual inspection. It is assumed that the component manufacturer also performs all screens and tests to the applicable MIL-PRF [6] or equivalent MIL-STD-883 screening method. Component types modeled are CMOS digital gate arrays, low frequency diodes, bipolar transistors, resistors and capacitors.

The applicable adjustment factors for the prediction model components may be found in MIL-HDBK-217F [5]

The predicted failure rates and MTTF for each component is shown in Table 1

MIL-HDBK-217F Failure Rates

Component	Failure Rate	MTTF
Digital Gate Array	2.47e-8	40.485,830
Diode (LF)	4.25e-7	2,350,012
Transistor	3.53e-7	2,829,562
Resistors (RCR)	1.42e-7	7,058,767
Capacitors (CCR)	1.37e-8	72,878,861

Table 1.

A representative system fault tree was built using SAPHIRE 8 for predicted values as is seen in Figure 2.

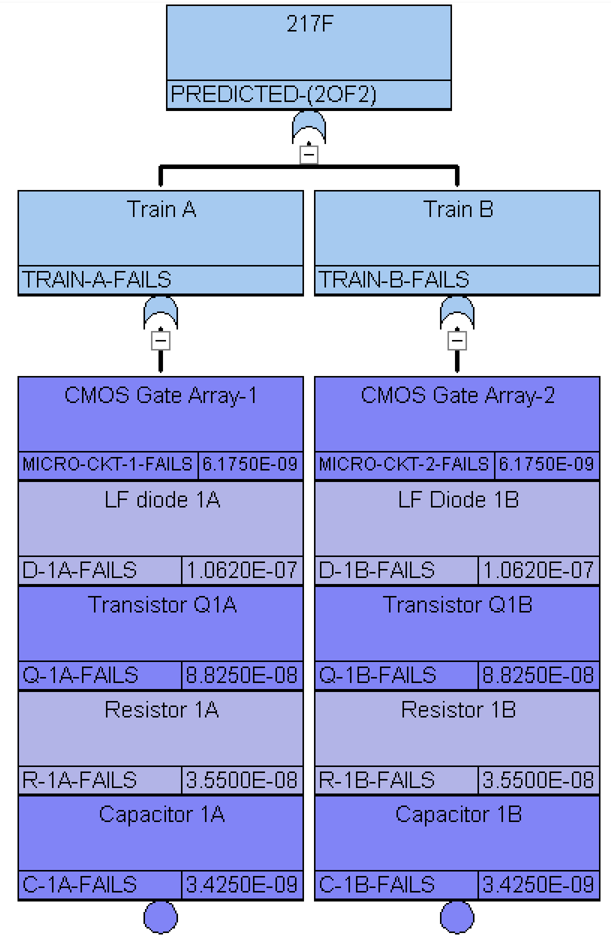

Figure 2
Predicted Value Fault Tree

An epistemic error factor value of 8 was selected for all components, which were taken from the Data Source Classification Application [1], as seen in Table 2.

Error Factor Data Source Classification Approach[1]

Data Source Classification Approach			
Source	Source Description	Source Application	Error Factor
New Hardware	MIL-HDBK-217F	Same Component	8
		Like Component	9

Table 2.

1.2 Demonstrated Failure Rates

This approach quantifies failure rates by using same components taken from the Quanterion Automated Databook using EPRD-2014, NPRD-2016, and where applicable FMD-2016 [3]. The same components used in the predicted model are selected where several years of failure data was found. Adjustments for varying environments were adjusted to the AUF environment by using MIL-HDBK-338 [4]. The mean values and standard deviations were calculated. The Error Factors were calculated using Eq.1. [2].

$$EF = e^{1.645}\sqrt{\ln(1 + (\sigma_{ln}/\mu_{ln})^2)} \qquad (1)$$

SAPHIRE 8 Error Factor Calculation

The demonstrated failure rates and MTTF for each component are shown in Table 3.

Demonstrated Failure Rates

Component	Failure Rate	MTTF
Digital Gate Array	2.93e-6	341,491
Diode (LF)	2.49e-6	400,267
Transistor	9.38e-7	1,065,719
Resistors (RCR)	2.77e-6	360,577
Capacitors (CRH)	1.06e-6	934,798

Table 3.

A representative system fault tree was built using SAPHIRE 8 for demonstrated values is seen in Figure 4

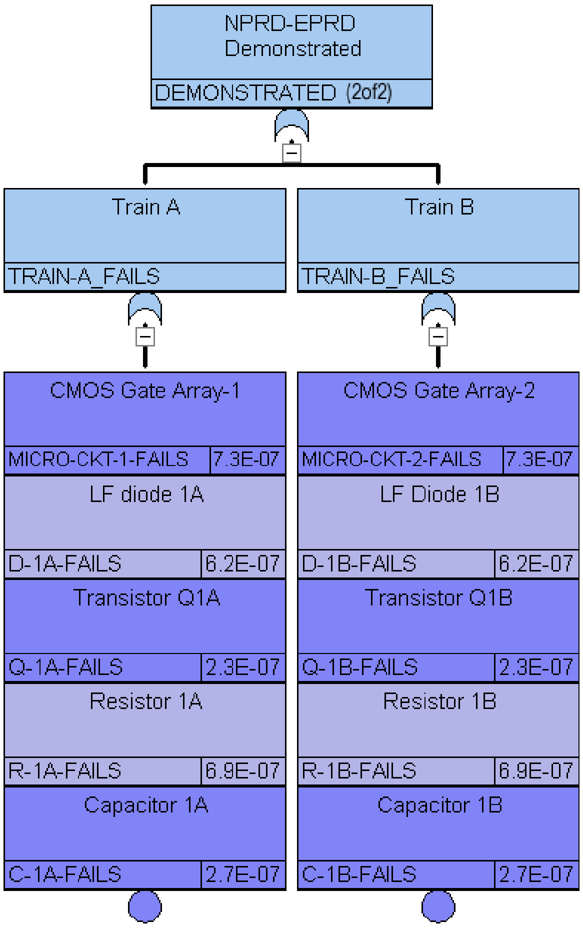

Figure 4
Demonstrated Value Fault Tree

Demonstrated lognormal uncertainty (EF) was calculated using Eq. 1. The values in Table 4, were applied to their respective components.

Demonstrated Error Factors

Component	Error factor
Digital Gate Array	4.61
Diode (LF)	4.1
Transistor	4.09
Resistors (RCR)	4.67
Capacitors (CCR)	3.91

Table 4

1.3 Model Parameters

Both models were constructed in the same fashion. Model logic was based on two parallel strings requiring a two of two output logic to achieve functional output. Each strings components are in serial with a single failure causing a loss of function for that string. The mission time is one quarter of an hour. All components were correlated to each individual type. Fifty thousand Monte Carlo trials were ran with identical seed values.

1.4 System Uncertainty Calculations

The system level uncertainty for each model type was then computed based upon the method in Figure 5 [1]. . Quantitatively, the error factor represents the spread of the lognormal distribution about the median. The Error Factor is represented as the 95th divided by the median [1]. System uncertainty for each model type is based on this method.

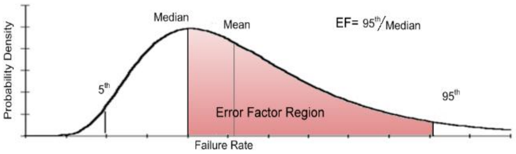

Figure 5.
Lognormal Probability Density Function

2 Results

The two models were then solved in SAPHIRE 8 by performing Monte Carlo trials, the results of which were used to calculate the system level uncertainty. The end results were then compared with the results as shown in Table 5.

Predicted vs. Demonstrated results

Model Type	Risk (1/N)	Uncertainty
Predicted	1/2,111,041	4.08
Demonstrated	1/196,657	2.3

Table 5.

3 CONCLUSION

As one can see, the results in Table 5 are vastly different. The risk value is 11 times less for the predicted model. If used for a quantitative assessment when considering the risk in a decision scenario, the risk may be misrepresented. In the case of uncertainty, the dispersion of the risk is two times greater in the predicted model.

This indicates that demonstrated data lowers uncertainty and predicted uncertainty range may necessitate further effort to collect additional data.

This difference gives rise to identify the pitfalls and precautions when developing quantitative models, which are used to assess and accept risk.

3.1 Pitfalls

The pitfalls one may experience are:

- Predicted failure data are overly optimistic.
- Predicted failure data does not take into account manufacturing, assembly and quality process controls, which are primary failure drivers.
- Predicted failure data may mislead managers into accepting a level of risk that is not commensurate with the actual risk.
- Predicted data should not be used to assess system reliability against reliability requirements.

3.2 Precautions

Precautions when using predicted failure data.

- If a concerted effort to obtain realistic data is not done, the resulting risk model may not be valid.
- Failure databases are difficult to locate and may be more difficult to obtain permission to access.
- Equal quality components must be used in developing risk models.
- Evaluate and adjust environments, if necessary.
- The source of data must be documented for traceability.

Obtaining valid data to perform risk modeling requires an understanding of the nature of the problems in obtaining and analyzing data to be used in modeling a system or in performing a system analysis to determine if the risk of a particular failure scenario is worth accepting, or if a redesign or system modification is warranted.

4 Summary

System design is constrained by Safety, Reliability, and Quality requirements as well as design standards. The purpose being to assure safety, which is generally related to quality of product, design, and testing.

These bounds are where the risks lie, and must be fully recognized, understood, minimized, and eventually accepted or redesigned to a level, which then meets acceptable risk.

As programs and projects proceed, risks are accepted at these bounds. The bounds over time become eroded by the acceptance of risk, and at some time, the aggregate risks may well exceed these bounds. This may result in a falsely perceived level of confidence, and allow a project to proceed to a state of potential disaster, which may result in a loss of life and physical property.

1. Mohammad AL Hassan, Steven Novack, Rob Ring, *Data Applicability of Heritage and New Hardware for Launch Vehicle Reliability models*, Huntsville Society of Reliability Engineers RAM VIII Training Summit, November 3-4, 2015
2. SAPHIRE 8.0.9, Idaho National Laboratory Battelle Energy Alliance Idaho Falls, ID 83415
3. Quanterion Automated Databook, Version 4.2.1.67, Quanterion Solutions Incorporated, Copyright 2013-2015
4. Electronic Reliability Design handbook (MIL-HDBK-338B), October 1, 1998
5. Military Handbook, Reliability Prediction of Electronic Equipment, (MIL-HDBK-217 Rev. F Notice 2)
6. Military Performance Specifications, (MIL-PRF-xxxxx),