A Method and Model to Predict Initial Failure Rates

Harry W. Jones, Ph.D., MBA, NASA Ames Research Center

Key Words: reliability estimates, over-optimism in reliability, reliability gap

SUMMARY & CONCLUSIONS

It has long been well known that actual system reliability typically falls well short of early estimates. Failure rates are often ten or more times higher than anticipated. Many reasons have been given for this, but over-optimism is the fundamental cause of too-favorable reliability predictions. Most forecasts of reliability are essentially best-case scenarios, as are predictions of budget and schedule. Confident engineers assemble estimates bottom-up, including the known factors and ignoring problems that they hope won't happen. Traditional reliability estimation is based on simply summing up the component failure rates. This ignores most actual failure causes. The way to reduce over-optimism is to use the historical system level failure rate from similar projects. Adjustments should not be made based purely on engineering judgment, but only if there is so logical quantitative justification. The traditional component-based reliability estimate is useful as a lower bound on the system failure rate. The difference between this lower bound component-based reliability and the historical system level reliability indicates how much of the total failure rate is due to system level problems rather than component failures.

1 INTRODUCTION

The traditional system failure rate estimate is simply the sum of the component failure rates. Actual failure rates are usually higher and often much higher, showing that this failure rate estimator is inaccurate. The failure causes that make actual reliability fall short of the estimated reliability are well-known and include problems in design, manufacturing, operations, and management. Failures are caused by design errors, interface problems, system level effects, unanticipated environmental effects, and operator error. Specific problems include misunderstood operational environment, use of low reliability components, manufacturing quality problems, inadequate and unrealistic testing, inaccurate reliability prediction techniques, inconsistencies in failure classification and data collection, and short term management focus on cost and schedule leading to insufficient effort to improve reliability.

These failure causes are difficult to anticipate and estimate, but they inevitably appear in the system level failure rate data. The actual level of failures not caused by components depends on the system design maturity and the organizations reliability knowledge and effort. There is an over-optimistic tendency to assume that historical failure rates can easily be improved.

1.1 *Over-optimism*

The component-based reliability estimate is readily accepted as reasonable because of a natural optimism bias, the observed fact that estimates are usually too close to the best case, which Kahneman calls the planning fallacy. A way to avoid over-optimism is to base reliability estimates on the actual reliability of similar projects [1].

Although the general failure causes are well known, it seems very difficult to make accurate reliability predictions. A first step in reducing over-optimism can be made by simply multiplying the best-case failure rate by a factor of 10 or 20, as suggested by historical experience.

The initial failure rate estimate can be corrected using actual failure rate data obtained during test and operations. The inverse of the system failure rate is the system Mean Time Before Failure (MTBF). Initial testing often produces infant mortality, occurring well before the estimated system MTBF. The highest failure rate causes have the shortest MTBFs and cause the earliest failures. Early failures are often due to design or component selection errors which are usually diagnosed and fixed, in a process called reliability growth. As some of the failure causes are corrected, the initial failure rate declines and may ultimately approach the best case failure rate based on the component failure rates.

2 ESTIMATED FAILURE RATES ARE OFTEN MUCH HIGHER THAN ACTUAL FAILURE RATES

There is usually a significant gap between predicted reliability and actual operational reliability. One study of military avionics found that failure rates can be 7 to 20 times higher than predicted [2] [3]. The estimate produced by traditional reliability analysis is too low.

3 TRADITIONAL RELIABILITY ANALYSIS

Traditional reliability analysis assumes that the system failure rate is determined by the component failure rates. Failure rate data is collected in handbooks and reliability analysis using reliability block diagrams is used bottom-up to estimate the overall system failure rate. If all components are needed and there is only one of each, and if the component failure rates are small, the system failure rate is the sum of the component failure rates. When this approach was first established in the mid-1900's, systems were much simpler and components such as electronic tubes accounted for nearly all the system failure rates. Since then, much higher quality

components have reduced component-caused failures and greater system complexity has led to failures caused by problems in management, requirements, design, interfaces, manufacturing, and software. These factors are not addressed in traditional reliability prediction methods. [4]

4 EXPLANATIONS FOR THE RELIABILITY GAP

The explanations as to why estimated failure rates are much lower than actual failure rates include two kinds of problems with traditional analysis. The estimator assumptions can be questioned. Only component failures are included.

4.1 *Objections to the usual reliability estimation assumptions*

Traditional reliability analysis makes several unrealistic assumptions. They are that all system failures are due to component failures, that the failures are independent, that the component failure rates are accurately known, and that repair or replacement of a failed part returns the system to its original good-as-new condition.

In reality, component failures are a small part of all reported failures. Common cause failures are not independent. All spares of a particular component may fail for the same reason, an internal manufacturing fault or some excessive system stress. Component failure rates are often optimistic underestimates. Repairs may not restore the system to its original condition. Repairs are often imperfect and they may introduce other defects leading to failures of other parts.

4.2 *Objections to component-based reliability estimation*

A system is much more than the sum of its parts. An integrated system is designed to produce system level performance of a different kind than that of its components. Just as systems have system level performance, they have system level failures. Yet "System integration and interfacing is seldom considered." [2] "Many reported failures are not caused by part failures at all, but by events such as intermittent connections, improper use, maintainers using opportunities to replace 'suspect' parts, etc." [2]

A survey of "Experts' Opinions on the Reliability Gap," found some significant contributors were as follows:

- Definitions – inconsistencies in failure classification and data collection
- Design – use of low reliability components, lack of derating, interface problems, system level effects
- Environment - misunderstood operational environment
- Management – short term focus on cost and schedule leading to reduced reliability effort with little time and funds for testing, repair, and design correction
- Manufacturing – quality problems, process errors, inadequate testing
- Operations – misuse, accidents, operator error
- Prediction - inaccurate techniques, assumptions, data [2]

The causes for underestimated failure rates include the assumptions of the prediction techniques, lack of understanding the operational environment, manufacturing problems, design problems, and short-term management focus limiting design and test effort. [3] The direct cause of actual high failure rates is the combination of high system complexity and limited time and budgets. [2] [3] To this can be added a lack of understanding of how to design for reliability, of what is the best obtainable reliability, and how to achieve it within given budget and schedule constraints.

5 OVER-OPTIMISM

A fundamental cause of all overly favorable predictions is over-optimism. The Nobel laureate, Daniel Kahneman, explored how humans think in his best-selling 2011 book, Thinking, Fast and Slow [1]. He found that planning estimates are usually over-optimistic, unrealistically close to the best case, and not based on similar cases. Over-optimism usually persists beyond the planning phase of a project and into the execution phase. Psychological optimism produces two effects, over-optimistic estimates and overconfidence that the low estimates will be met. Over-optimism is not only not cured by increased subject matter expertise; it is encouraged! Good models and accurate data can help produce the illusion of certainty, predictability, and controllability.

Kahneman mentions that the planning expert Flyvbjerg endorsed the idea of taking a broader or outsider view to cure the over-optimism as "the single most important piece of advice regarding how to increase accuracy in forecasting." The outside view can be implemented by using the statistics of similar cases in a method called reference class forecasting. Reference class forecasting simply focuses on the historical results of similar projects. Overall historical top-down estimation is both much easier and much more accurate than detailed bottom-up estimation. [1]

5.1 *Over-optimism in cost and schedule estimates*

System cost and schedule, like failure rate, are often underestimated due to over-optimism. Just as the system failure rate is often estimated bottom-up as the sum of the component failure rates, the system cost can be estimated as the sum of the component, design, integration, and test costs without failures, redesign, and retest, and the system schedule can be estimated as the sum of sequential development task times without allowance for failures causing rework and retest or externally imposed delays. Several different top-down cost estimators exist for aerospace systems, but user adjustments for difficulty and use of engineering judgment often introduce over-optimism. Actual costs and schedules can be several times the original estimates, and failure rates are typically many times higher than the original estimates.

Frequently cited reasons for poor estimates are poor estimating methods and lack of good data. This certainly applies, but if it was the only cause of error, estimates would sometimes too pessimistic, and this rarely happens. Over-optimism causes too low cost, schedule, and failure rate estimates. Kahneman notes that "The optimism of planners and decision makers is not the only cause of overruns." "Errors in the initial budget are not always innocent." [1] Project advocates may assume that the cost, schedule, and performance requirements are soft and that additional time and money can be provided or requirements reduced if needed.

6 ENGINEERING JUDGMENT CANNOT BE TRUSTED

Engineers develop a trained judgment and can produce highly effective intuitive decisions simply by following their gut. An engineering judgment comes to mind with a feeling of rightness but without obvious reasons. There are several problems with using engineering judgment. It has no conscious basis, so the reasons behind it cannot easily be explained. Intuitive judgments seem obviously right and are strongly emotionally held, so it is difficult to challenge them. Over-confidence and over-optimism often distort engineering judgment. The problems of engineering judgment can be reduced by using logical, fact-based analysis. [5]

6.1 *NASA shuttle failure analysis was over-optimistic*

A contractor study of space shuttle risk found the solid-fuel rocket boosters had a failure rate of about 1 in 40. However, rather than use this historical data, NASA made an "engineering judgment" and "decided to assume a failure probability of 1 in 1,000" or even 1 in 10,000. [6] An Air Force review noted that the "arbitrary assignment of risk levels apparently per sponsor direction" had "no quantitative justification at all." The Air Force found that the boosters' track record "suggest[s] a failure rate of around one-in-a-hundred." [6]

NASA's internal analysis also minimized risk. A failure in the solid rocket booster (the failure that destroyed Challenger) was assigned a probability of 1 in 100,000. [6] Even after the Challenger accident, the NASA chief engineer thought the actual risk "would be 10 to the minus 5 … based on engineering judgment." [6] After Challenger, risk analysis found that the actual probability of a fatal accident was about 1 in 100. [7] The simple direct use of historical data would have been far superior to using engineering judgment in this extreme case of over-optimism.

7 REDUCING OVER-OPTIMISM

The suggested cure for over-optimism is to base estimates on actual historical data from similar projects. Traditional reliability estimation neglects many failure causes. Even for components, there is an optimistic tendency to assume that historical failure rates can be easily improved.

Reliability estimates can be made more realistic by basing them very closely on actual historical data from similar projects. The major problem is finding similar projects with relevant data. Adjustments from similar project's data should be based only on observable quantitative differences, such as design generation, parts count, and test hours. It would be helpful to provide two estimates, the traditional best-case estimate based on bottom-up summation of parts failure rates and a top-down estimate based on historical data from similar systems. It would be reasonable to expect a strong reliability growth program, test it - break it - fix it, to gradually reduce the high initial failure rate and approach the historical level of reliability for similar systems, but not the best case reliability.

8 USE OF SIMILAR HISTORICAL DATA

A similar system uses similar technology to perform a similar function in a similar environment. [4] "Since field data on a similar-system is the best starting-point for quantification of the new-system reliability, it should be used to the maximum extent possible." [4]

There is a need for a "methodology that translates the observed value from the predecessor system to the conditions of interest for the new system. This translation consists of beginning with the observed failure rate on the predecessor system and adjusting it to account for differences in complexity, temperature, environment, and processes." [4]

9 ACTUAL FAILURE CAUSES AND RATES

Relatively few failures are due to components. This has been observed in electronic, military, and space systems.

9.1 *Electronic systems failure data*

Table 1 lists the predominant failure causes for electronic systems with the percentage of failures attributed to each of the them. [4] Intermittent components lead to maintenance actions and are often replaced, adding to the logistics burden, so should be included in the failure rate. [4]

Table 1 – Failure Causes for Electronic Systems

Components (22%)	Failure resulting from a part not performing its intended function.
No defect (20%)	Intermittent failures that cannot be reproduced.
Manufacturing (15%)	Failures resulting from errors in manufacturing.
Induced (12%)	Failures resulting from an externally applied stress such as environment or maintenance.
Design (9%)	Failures resulting from bad design.
Wear out (9%)	Failures resulting from wear out.
Software (9%)	Failure due to a software fault.
System Management (4%)	Failures to interpret system requirements or provide the resources required.

9.2 *Military and space systems failure causes*

A study of over 500 military systems found a consistent result, that "only 20% of the field problems encountered were hardware reliability problems." [2] It was also found that "human error is the cause for a large proportion (i.e., from 20 to 50%) of all equipment failures." [2] Interfaces, the environment, system level problems, and human error "have historically caused the large majority of launch vehicle and spacecraft failures." [8]

10 DUANE-CROW RELIABILITY GROWTH

Duane observed that if N(t) is the number of failures occurring until time t, the cumulative failure rate, N(t)/t, often declines as a fractional power of the cumulative test time, t. The cumulative failure rate is

$$N(t)/t = k\, t^{-\alpha} \quad (1)$$

The reliability growth rate is α, the downward slope of N(t)/t versus t. It usually varies from 0.2 to 0.6. [9] [10]

Crow provided a theoretical basis for the Duane model by assuming that failures occur according to a non-homogeneous (time-varying) Poisson process with a power law mean value function, m(t). The mean number of failures over time is

$$m(t) = k\, t^{\beta} \quad (2)$$

where β is between zero and one. The expected cumulative failure rate is

$$N(t)/t = m(t)/t = k\, t^{\beta-1} \quad (3)$$

The Crow and Duane reliability growth models are equivalent, with the Duane α equal to Crow's 1 - β. The parameter k is the same in both. The reliability growth parameters are usually estimated from the failure time data. [9] [10] Here we will use a modified reliability growth model to estimate the initial failure rate as testing begins.

10.1 *Applying the Duane-Crow reliability growth model*

Crow used a 56 failure data set to illustrate reliability growth. [11] A graphical Duane model fit to the data gives

$$\text{Duane } N(t)/t = 0.640\, t^{-0.283} \quad (4)$$

Crow's computational analysis of this data, based on an assumed non-homogeneous Poisson process, found

$$\text{Crow } N(t)/t = 0.217\, t^{-0.073} \quad (5)$$

The data and models are shown in Figure 2.

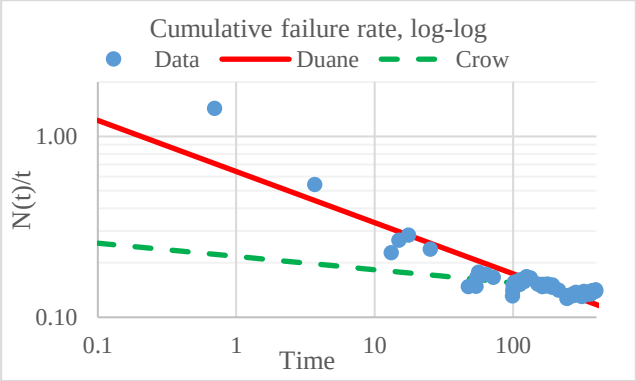

Figure 2. Failure rate N(t)/t with Duane and Crow models

The downward slopes showing reliability growth differ. The Crow model does not reflect the early infant mortality data and gives a barely noticeable projection of future reliability growth.

10.2 *Crow's data does not show long term reliability growth*

Figure 3 shows the cumulative failure rate, N(t)/t plotted versus time, t, but in a linear rather than log-log graph. A two part failure model is also shown, rather than the single model equation used by Duane and Crow.

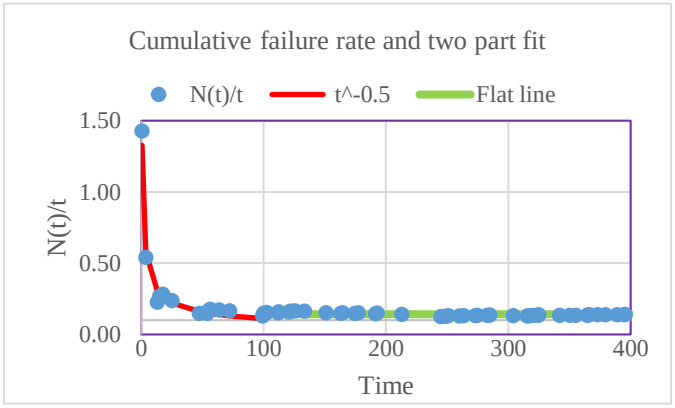

Figure 3. Cumulative failure rate

A Duane-Crow model equation with $N(t)/t = 1.11\, t^{-0.5}$ fits the data from time 0 to 100. The high initial failure rate declines and becomes constant. A flat line fits the data points from time 100 to 400. It is well known, and illustrated by the "bathtub curve," that failure rates often decline strongly during an initial period of "infant mortality," and then tend to be constant during the operational phase. Using a Duane-Crow log-log line fit to the early data exaggerates the long term reliability growth potential, since the limiting failure rate is zero for large time. The best predictor of the long term failure rate would be the failure rate at the end of the reliability growth effort, assuming no "end-of-life" increase in failure rate occurs. Reliability growth and long term operation have different failure rate behavior and require different models.

11 *THE abcd RELIABILITY GROWTH MODEL*

The explanation of failure mode correction suggests a two phase model of failure rate, an initial period of reliability growth and a later period of constant failure rate.

11.1 *Reliability growth components*

The expected components of a failure rate model are shown in Figure 4.

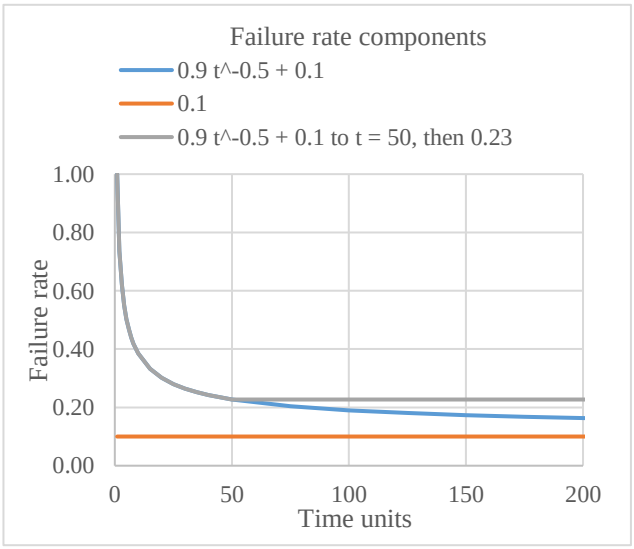

Figure 4. The three failure rate components

There are three failure rate components in Figure4, a correctable and declining failure rate equal to $0.9\ t^{-0.5}$, a constant random failure rate of 0.1, and a constant correctable but uncorrected failure rate. At time equal to 50 time units, the failure correction process is completed. A correctable failure rate of 0.13 remains, producing a constant total failure rate of 0.23 after time 50. Continuing to remove the remaining failure modes would have produced the continually declining failure rate shown.

11.2 *The abcd model*

The mathematical model in Figure 4 is

$$\text{Failure rate} = 0.9\ t^{-0.5} + 0.1 \text{ from } t = 0 \text{ to } 50 \quad (6a)$$

$$= 0.9\ 50^{-0.5} + 0.1 = 0.23 \text{ after } t = 50 \quad (6b)$$

A simple abcd mathematical model for reliability growth and failure rate decline is

$$\text{Failure rate} = a\ t^{-b} + c \text{ from } t = 0 \text{ to } t_d \quad (7a)$$

$$= d + c \text{ after } t_d, \text{ where } d = a\ t_d^{-b} \quad (7b)$$

The reliability growth effort continues and the failure rate declines until the time t_d when reliability improvement stops and the failure rate becomes constant. Depending on t_d, most or only a few of the correctable failures will be removed.

11.3 *The abcd model for the Crow data set*

The abcd model is applied to the Crow reliability growth data set. Figure 3 showed a rough fit to the Duane-Crow data set, with failure rate equal to $1.11\ t^{-0.5}$ to time 100. The abcd model gives a better fit.

$$\text{Failure rate} = 1.37\ t^{-0.99} + 0.14 \text{ from } t = 0 \text{ to } t_d = 100 \quad (8a)$$

$$= 0.01 + 0.14 = 0.15 \text{ after } t_d = 100 \quad (8b)$$

The remaining correctable failures are few since the reliability growth time, $t_d = 100$ is long compared to the random failure MTBF = 1/c =7.1.

12 PREDICTING THE INITIAL FAILURE RATE USING THE abcd MODEL

Reliability growth models were developed to predict the reliability improvement and test time that can be expected based on initial testing. The model parameters of the reliability growth parameter and the required test time were obtained by curve fitting or computations based on the initial failure rate data. Here we use the abcd reliability model to predict the initial failure rate, based on reasonable assumptions about reliability growth, test time, and the final failure rate.

$$N(t)/t = a\ t^{-b} + c \text{ from } t = 0 \text{ to } t_d \quad (9)$$

We assume that d, the remaining correctable failure rate, is y times the final long term failure rate, c.

$$N(t_d)/t_d = a\ t_d^{-b} = d = y\ c \quad (10)$$

$$a = c\ y\ t_d^{\ b} \quad (11)$$

The value of b depends on the design and can be estimated based on past experience. The values of t_d and y reflect the reliability improvement period and the acceptable level of uncorrected failures that could be corrected, d = y c. However t_d and y are strongly inversely related. If t_d is doubled, the minimum MTBF of the remaining failure modes is also doubled, and this reduces d, the number of undetected correctable failures, and also reduces y. This reduces the expected variation of the factor $y\ t_d^{\ b}$. The model is

$$N(t)/t = c\ y\ t_d^{\ b}\ t^{-b} + c \text{ from } t = 0 \text{ to } t_d \quad (13)$$

The initial failure rate at t = 1 is

$$N(t)/t = c\ y\ t_d^{\ b} + c \quad (14)$$

Comparing this to the Duane-Crow data set model, b = 0.99, c = 0.14 and $t_d = 100$. The initial failure rate at t = 1 is 1.37 + 0.14 =1.51, approximately equal to the first data point, 1.43. At $t_d = 100$, failure rate = c + d = 0.01 + 0.14 = 0.15.

The reliability growth parameter b is typically 0.2 to 0.8. The long term constant failure rate c can be estimated as equal to the total component based failure rate. The scale factor that multiplies c is $y\ t_d^{\ b}$, and here is equal to 137/0.14 = 9.8. Comparisons to data indicate that this is a typical value.

13 ESTIMATING THE RELIABILITY GAP

The quantitative reliability gap data is very limited but consistent:

- Failure rates can be 7 to 20 times higher than predicted using parts-based estimates. [2] [3]
- Electronic components account for only 22% of failures. [4]
- Only 20% of the field problems were hardware. [2]

Experience indicates that the actual failure rate can be a factor of 5 to 10 even 20 times the traditional parts-based failure estimate. This suggests that an estimate of the initial failure rate could be roughly 10 times the components-based failure rate. This might make sense if the parts count is a good indicator of general system complexity and that this correlates with the overall failure rate. However this seems implausible when we remember that the other failure causes include extrinsic factors such as environment and human error. This requires only a minor adjustment to the usual easily obtained component-based failure rate estimate. It seems that the only way to estimate the initial failure rate and reliability gap is to use the initial failure rate of similar systems, perhaps adjusted for degree of similarity.

13.1 *The reliability gap seems very unpredictable.*

The reliability growth model is based on the expectation

that high probability failures will appear in early testing and be removed. In the ideal case for failure rate prediction, all the failure modes would have constant failure rates. Consider a group of high rate failure modes. Which one happens first and when it occurs compared to its MTBF are random events. Testing identical systems can very easily produce different initial failure rates. Then add the fact that environmental effects and human error are not constant, but may occur any time or never, and the initial size of the reliability gap seems very unpredictable.

14 DISCUSSION

Prediction errors can be expected. "Reliability prediction is not a simple task and it is almost an impossible task for new, highly sophisticated, state-of-the-art equipment." [2] However, failure rate estimates based on historical experience are less likely to be over-optimistic and more likely to be accurate. Unbiased failure rate estimates can help lead to better reliability specifications, planning, design, and testing and ultimately to better reliability.

REFERENCES

1. D. Kahneman, *Thinking, Fast and Slow*, Farrar, Straus, and Giroux, New York, 2011.
2. K. C. L. Ma, "Experts' Opinions on the Reliability Gap and Some Practical Guidelines on Reliability Growth," Thesis, Air Force Institute of Technology, January 18, 1989. https://apps.dtic.mil/dtic/tr/fulltext/u2/a202625.pdf Accessed 6/25/2019.
3. P. E. Miller and R. I. Moore, "Field reliability versus predicted reliability: An analysis of root causes for the difference," Proceedings of the Annual Reliability and Maintainability Symposium, 1991.
4. W. Denson, "The History of Reliability Prediction," IEEE Transactions on Reliability, vol. 47, no. 3-SP, September, 1998, pp. 321-8.
5. G. P. Hodgkinson, E. Sadler-Smith, L. A. Burke, G. Claxton, and P. R. Sparrow, P. R., Intuition in Organizations: Implications for Strategic Management, Long Range Planning 42, 2009, pp. 277-297.
6. T. E. Bell and K. Esch, "The Challenger Disaster: A Case of Subjective Engineering," Jan. 28, 2016 (June 1989), https://spectrum.ieee.org/tech-history/heroic-failures/the-space-Shuttle-a-case-of-subjective-engineering, accessed July 24, 2018.
7. E. Paté-Cornell and R. Dillon, "Probabilistic risk analysis for the NASA space Shuttle: a brief history and current work," Reliability Engineering & System Safety, V. 74, 3, December 2001.
8. E. L. Morse, B. F. Putney, J. R. Fragola, Reliability Growth and the Caveats of Averaging: a Centaur Case Study, Proceedings IEEE Annual Reliability and Maintainability Symposium, 2011.
9. Duane, J. T., "Learning Curve Approach to Reliability Monitoring," IEEE Transactions on Aerospace, Vol. 2, No. 2, 1964, pp. 563-566.
10. Yamada, S., and S. Osaki, "Reliability growth models for hardware and software systems based on nonhomogeneous Poisson processes: a survey," Microelectronics Reliability, Vol. 23, No. 1, 1983, pp. 91-112.
11. Crow, L. H., Reliability Analysis for Complex, Repairable Systems, US AMSAA Technical Report No. 138, December 1975.

BIOGRAPHY

Harry W. Jones, Ph.D., MBA
N239-8
NASA Ames Research Center
Moffett Field, CA 94035, USA

e-mail: harry.jones@nasa.gov

Harry Jones is a NASA systems engineer working in life support. He previously worked on missiles, satellites, Apollo, digital video communications, the Search for Extra Terrestrial Intelligence (SETI), and the International Space Station (ISS).