Applying Design for Reliability to Increase Reliability Confidence

Eduardo V. Cota, Raytheon Missile Systems
Louis Gullo, Raytheon Missile Systems
Ram Mujal, Raytheon Missile Systems

Key Words: Design for Reliability, FRACAS, Cost Savings, Long-term Corrective Action, Predictions, Confidence

SUMMARY & CONCLUSIONS

Design for Reliability (DfR) is focused on demand versus capability modeling, where demand is the functionality, environmental conditions and timing conditions that the customer needs from the system. Capability is the "as-designed" robustness of the system along with the design requirements specified for the system performance. The goal of the method described in this paper is to apply DfR guidance to use test data to measure system reliability. Test data is used to demonstrate improved system capability to satisfy customer demands. Applying DfR activities as a guide, allows engineers to identify and characterize reliability drivers and develop mitigation plans to increase system reliability and provide a quantified measure of reliability growth. Reliability drivers are prioritized to reduce the scope and cost of a reliability program and ensure appropriate attention is placed on high risk capability concerns.

1 INTRODUCTION

This paper applies activities developed using DfR as a guide to provide a quantitative measure of reliability using test data. The measure of reliability is used to demonstrate reliability improvement for prioritized system functions. The following activities improve reliability for prioritized failure modes:

1. Understand system and requirements
2. Model system functions and set goals
3. Plan data collection, analysis and modeling
4. Collect test data
5. Assess and prioritize failure modes
6. Design mitigation plan
7. Plan test events
8. Manage reliability confidence

Applying the identified activities provides a method to develop a quantitative measure for reliability. Reliability measures that can be compared to reliability goals for system functions to verify that system reliability requirements are being met. The quantitative measure of reliability is developed by using available test data and planned test events for a key performance parameters for critical system functions. This paper provides a detailed description of each activity, including an example, which demonstrates how the identified activities can provide a quantitative measure to demonstrate reliability improvement. A system level functional Failure Mode Effect and Criticality Analysis (FMECA) is the reliability tool used for each activity, to house and maintain resulting system functions with their associated quantitative data and assessed severity.

1.1 Problem Description

Reliability is the probability that an item can perform its intended function, for a specified interval, under stated conditions, without failure. Reliability may be assessed using standards, such as IEEE-STD-1413 or MIL-HBDK-217F. The resulting reliability assessment using industry standards will drive reliability engineers to set capability priorities on system components with the lowest assessed reliability, which may not be applicable to the system under analysis. The resulting reliability assessment does not provide an indication of how well the system being developed is performing or what system performance parameter is driving system reliability. Not knowing which performance parameter is driving system performance, does not allow the reliability engineer the ability to support program decisions.

Using the identified activities in this paper requires the use of system test data for verifying and validating system performance against the customer's requirements, environmental conditions or timing conditions. This system test data is usually mapped to system functional block diagrams. The issue with using the results from a test program to provide a quantitative measure of reliability is that current reliability models, such as reliability block diagrams, model system components. In order to use the results of a test program, reliability goals and system reliability models must be mapped to the system functions that can be associated with a system functional block diagram.

Using test data also requires the use of hypothesis testing to show that test data is the same as flight data. Test data performance results may have not been equal to the timing and environmental conditions seen in flight. When hypothesis testing statistically proves that performance results from test data is not the same as flight data then there is a need to quantify the difference to use test data to measure reliability.

Because of schedule and cost constraints, not all system performance parameters are analyzed or tested enough to verify required reliability levels. Because of schedule and cost

constraints, a method is needed to prioritize system capability gaps to provide a quantitative measure of system reliability.

1.2 Example

Consider a system, which converts battery power (V) to provide a set of voltage forms (V1 and V2), which are used to power a light source. Recent test activities have resulted in low light source performance, the measured light is dimmer than expected. The reliability engineer on staff is tasked to identify all potential causes of the low light source performance and provide a prioritized mitigation plan. The reliability engineer must also provide a quantitative measure of the dim light source on system reliability, identify potential sibling issues, set Reliability goals and generate reliability models to increase reliability confidence. Reliability goals are set to meet the contracted Reliability of 0.90. Figure 1, provides a physical block diagram of the system.

Figure 1 System Physical Block Diagram

Serial Number	Provide V	Generate V1	Generate V2
001	5.5	3.3	1.64
002	5.45	3.32	1.35
003	5.56	3.29	1.55
004	5.53	3.28	1.36
005	5.44	3.29	1.59
006	5.52	3.31	1.6
007	5.55	3.31	1.61
008	5.65	3.33	1.39
009	5.44	3.25	1.36
010	5.43	3.34	1.38
011	5	3.27	1.37
012	5.45	3.3	1.61
013	5.56	3.29	1.6
014	5.53	3.31	1.37
015	5.44	3.3	1.39
016	5.52	3.32	1.58
017	5.55	3.29	1.6
018	5.65	3.28	1.59
019	5.44	3.29	1.39
020	5.43	3.31	1.35

Table 1 Functional Test Data

Inherent in the Power converter design is a derating exception, the derating exception is on the circuitry that generates V1. During the buildup of the light source, the battery, power converter and light source are tested individually. Battery tests verify the Batteries ability to "Provide V", which is expected to be 5.5V. Power converter tests verify the Power Converters ability to "Generate V1" and "Generate V2". The expected value for "Generate V1" is 3.3V. The expected value for "Generate V2" is 1.5V. Test results, for twenty units are available to the Reliability engineer, as shown in Table 1.

Along with the test results provided in Table 1, are the test limits for each test parameter. The test limits for 'Provide V' is between 5.75V and 5.25 V. The test limits for 'Generate V1' are between 3.35V and 3.2V. The specified limits for 'Generate V2' are between 1.65V and 1.35 V.

2 DESIGN FOR RELIABILITY DEFINITION AND PROCEDURES

2.1 Design For Reliability

Design for Reliability is a process, which per the RAMS 2013 tutorial "Design for Reliability – Tools and Processes" [1], which includes the following activities shown in figure 2:

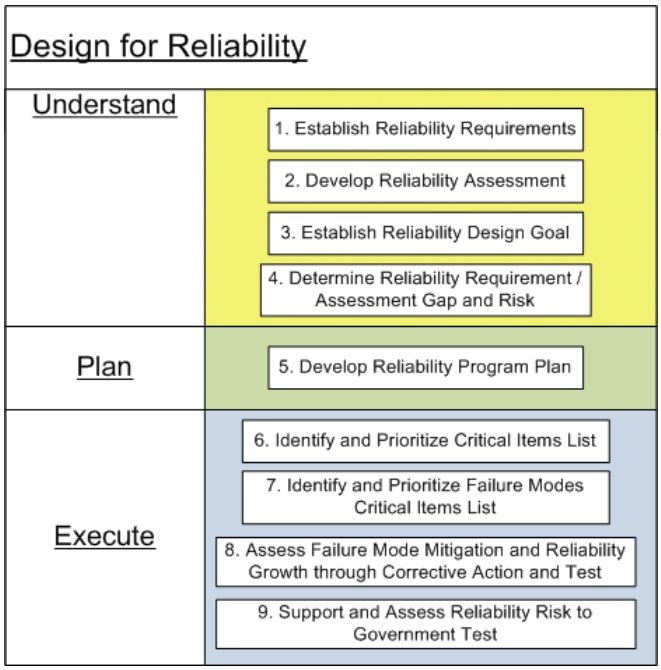

Figure 2 DfR Process

The activities shown in Figure 2, are used for the example provided in this paper to demonstrate increased reliability confidence after a recent failure. Figure 2 is largely aligned to the identified activities mentioned previously for developing quantitative measures for reliability. Portions of the DfR activities are used to link system components to planned test events that measures an expected system response and demonstrate reliability improvement. The measured system response is described herein as a system function.

2.2 Understand

The activities used in the 'Understand' portion of the DFR process include

- Understand system and requirements (Replacing Establish Reliability Requirements)
- Model system functions and set goals (Replacing Develop Reliability assessment and Establish Reliability Design Goals)

The activities identified decompose a system into its functions and each function is provided a reliability requirement and goal. Reliability goals are assigned to each function such that the resulting Request for Proposal (RFP) requirement is achievable. Each reliability goal is set according to available reliability data.

The resulting system functions are assigned to system test events, such that the resulting test data can be fitted into Probabilistic Density Function (PDF), which is used to calculate the functions reliability to verify compliance to functional reliability goals.

2.3 Plan

The activities used in the 'Plan' portion of the DFR process include

- Plan data collection, analysis and modeling

Once the system reliability RFP requirement has been decomposed down to system functions, the Reliability engineer formally documents a reliability plan. The reliability plan provides a detailed description of reliability tools and activities used to verify and maintain compliance to system reliability requirements. The plan describes data fitting guidelines and techniques to fit test event data into a PDF that verify compliance to reliability goals. In order to ensure that the plan is achievable within planned system test program, the plan should detail how and when test data is collected and analyzed. Efforts are needed when developing the plan to determine if sufficient test data under specified environmental conditions are available to meet reliability goals.

The reliability plan also includes a detailed description of reliability tools and criteria for Critical Items List (CIL) and reliability scoring. The CIL and reliability scoring help prioritize failure mode analysis and mitigation efforts during the Execution portion of the DfR process. Reliability tools such as the Failure Modes Effects and Criticality Analysis (FMECA) is used as part of the tailored DfR activities to manage and analyze the cause, severity and probability of failure for each potential function failure mode. Each function failure mode Probability of Failure (PoF) is one minus the reliability of the function under analysis.

$$\text{PoF} = 1 - \text{Reliability} \quad (1)$$

Reliability tools include fault trees, which are used to identify, prioritize and analyze system functions that contribute to a systems mission event under analysis. For example, consider a system which uses the light source during night mission, the event under fault tree analysis is provide light. The functions that contribute to provide light include provide V1, provide V2 and provide light source. During the planning effort, the fault trees basic events are limited to these identified functions.

The plan also includes reliability testing which is used to provide test data to demonstrate compliance to Mean Time Before Failure (MTBF) requirements, identify system failure modes above system environmental specifications and accelerate system wear out and aging failure modes to verify compliance to system service life requirements.

The resulting reliability plan is used to set the level of effort for the tailored DFR activities and is used to provide consistent results.

2.4 Execute

The tailored activities, which map to the Execute portion of the DFR process include

- Collect test data
- Assess and prioritize failure modes (Replacing "Identify and Prioritize Failure Modes Criticality Items List")
- Design mitigation plan (Replacing "Assess Failure Mode Mitigation and Reliability Growth through Corrective Action and Test")
- Plan test events
- Manage reliability confidence (Replacing "Assess Reliability Growth through Corrective Action and Test" and "Support and Assess Reliability Risk to Government Test")

The tailored activities are performed to the levels and guidance defined in the reliability plan. The plan provides a detailed description of the reliability tools such as the FMECA and fault tree. During the execute tailored activities the FMECA is extended from functional failure modes down to the piece part level, functional physics of failure and inherited Failure Reporting Analysis and Corrective Action lessons learned from previous similar system functions. The basic events of the system fault tree are extended to the prioritized failure modes of each system function. Given the extension of the FMECA and Fault Tree Analysis (FTA), a reliability assessment is developed for each function and function failure mode according to the guidelines identified in the reliability plan.

After a failure, collected data is analyzed to provide a reliability assessment to determine the failure effects on the functions reliability. FRACAS efforts support the reliability assessment by isolating the failure to a single root cause and assign appropriate corrective action. Once the root cause is identified and corrective action is implemented, the reliability engineer uses test data, according to the reliability plan, to show reliability improvement such that reliability goals are met.

In summary, during the Execute DFR process the reliability engineer is responsible for ensuring that reliability goals are met according to prioritized failure modes analyzed. Failure modes can be obtained from multiple sources, including but not limited to; FRACAS efforts, lessons learned, , electrical stress analysis, and PoF.

3 APPLICATION OF DFR TO THE PROBLEM

3.1 *Understand the Problem*

Considering the example provided, the reliability engineer is assigned the task of determine the effect on system reliability of a recent light source failure. In order to understand the failure and task, the reliability engineer begins efforts by determining the system reliability requirement. The system reliability requirement is 0.9. Once the reliability

requirement is known the reliability engineer collects available reliability information to determine a method for allocating the system reliability requirement to system functions. While collecting available reliability information the reliability decomposes the system into its functions. In order to provide a light, the system must perform the functions as shown in the Figure 3:

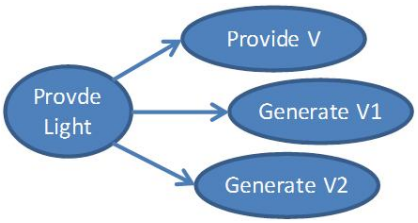

Figure 3 System Functional Block Diagram

As shown in Figure 3, in order to provide light, the system must provide V to generate V1 and V2.

Using MIL-STD-217F predictions, the predicted system reliability for each of the system functions was determined to be 0.975 for generate V1, 0.99 for generate V2 and 0.995 for generate light. In order to set reliability goals for each function, the reliability engineer allocates the 0.9 system reliability requirement using the apportionment method as shown in the equations 2 through 7.

$$R_{GenerateV1Goal} = 0.9^{0.63} = 0.936 \quad (2)$$

$$R_{GenerateV2Goal} = 0.9^{0.25} = 0.974 \quad (3)$$

$$R_{ProvideVGoal} = 0.9^{0.12} = 0.987 \quad (4)$$

$$0.63 = \ln(0.975)/\ln(0.975*0.99*0.995) \quad (5)$$

$$0.25 = \ln(0.99)/\ln(0.975*0.99*0.995) \quad (6)$$

$$0.12 = \ln(0.995)/\ln(0.975*0.99*0.995) \quad (7)$$

The resulting reliability goals are used to determine how system reliability is effected by test failure or from issues identified through design analysis.

3.2 *Plan*

After decomposing the system into it functions and setting goals, the reliability engineer identifies when in the build process the functions are tested. In order to identify when functions are tested the reliability engineer collaborates with the integration and test team. The collaboration ensures the function parameters are being monitored, collected and managed to support reliability data collection and analysis. The plan details how the data collected is analyzed. When analyzing the data, data is fitted into a best fit Probability Density Function (PDF) and Cumulative Density Function (CDF). The resulting PDF and CDF is measured against system demands to determine the unreliability of the system [4]. Methods and further reading on calculating reliability using PDFs and CDFs can be found in "Dynamic Stress-Strength Approach for Reliabilit Prediction"[5]. Reliability is calculated from the resulting CDF, where the probability of failing under the lower specified test limit is equal to CDF at the lower specified limit.

$$P(X < LSL) = CDF(LSL) \quad (8)$$

The probability of being above the specified test limit is 1 – CDF at the upper specified limit of the test.

$$P(X > USL) = 1 - CDF(USL) \quad (9)$$

For example, V, V1, V2 and the light source is collected and provided for 20 tests as shown in Table 1.

Included in the plan is a preliminary fault tree for the dim light failure. The resulting fault tree is shown in Figure 4.

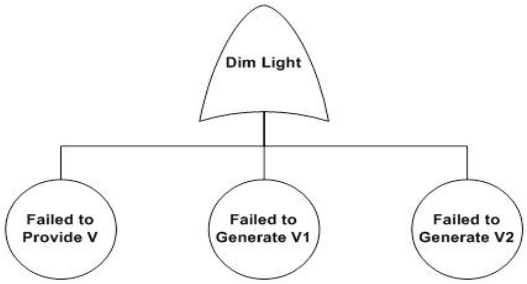

Figure 4 System Fault Tree Diagram

Efforts are planned to fill in the fault tree to analyze derating, FRACAS and tolerance failure modes as they become available. The resulting reliability plan describes how the fault tree is used to manage failure modes and the analysis needed to identify potential failures.

The final reliability plan for the light failure investigation is presented to program management for review and acceptance before executing the plan.

3.3 Execute

Beginning with the FTA developed as part of the reliability plan, the initial basic events are decomposed further to determine all potential causes of the dim light performance. During the planned derating stress analysis, the inherent derating exception in the circuitry used to generate V1 was identified and added to the fault tree. Using a FMECA, it was determined that the derating exception could cause a part on the V1 circuitry to overstress open, whose end effect would cause V1 to go to zero. In order to determine the probability of an overstress, test data for V1 is fitted into a PDF to determine the probability of being outside V1 specified limits. The resulting PoF is 0.0076, which demonstrates that the derating exception is not a priority for a reliability mitigation plan. The low PoF of 0.0076 yields a reliability of 0.9924, which is greater than the allocated reliability of 0.936 (see Figure 4).

Data fitting for the battery provided V identified a test failure. Researching FRACAS efforts for the test failure revealed that the battery outputted 5V, when the specified limits are 5.75V to 5.25V. The resulting PoF for the 'Provide V' function is 0.06113, which is a priority for further mitigation efforts. The resulting reliability of 'Provide V' is 0.939, which is below the allocated value of 0.987.

Data fitting for the generate V2 functions identified a distribution with high variability. The resulting PoF is higher for high variability test results. The resulting PoF for the 'Generate V2' is 0.2061, which is a high PoF making it

another priority for further mitigation efforts. The resulting reliability for the low PoF is 0.794, which is well below the functions allocation of 0.974 (see Figure 5).

Once all supporting functions to generate the light source have been identified and analyzed, the fault trees from the reliability plan is updated. The updated fault tree uses the resulting PoF for test data collected and analyzed, as shown in the Figure 5.

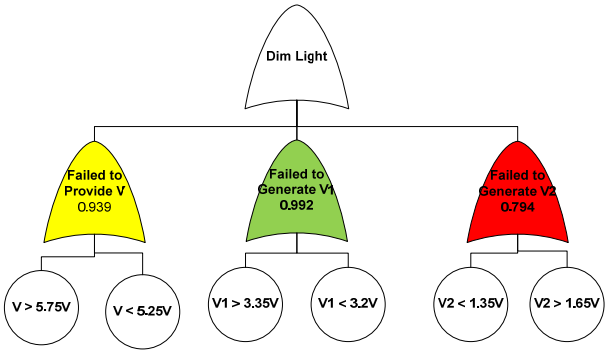

Figure 5 Updated System Fault Tree Diagram

Using the resulting fault trees, FRACAS priorities are set to investigate 'Generate V2' and 'provide V' basic events.

Root cause investigations revealed that high variability in V2 is the root cause of 'Generate V2' low reliability results. Root cause was validated when the failure was repeated on an engineering unit. As part of FRACAS efforts, corrective action is put in place to reduce the level of variability in V2 outputs. In order to verify corrective action effectiveness, control limits are set in place to ensure that 'Generate V2' variability is one sigma (s) from expected 1.5V value. The upper control limit was set to 1.55V and the lower control limit was set to 1.45V. Control limits are set using the resulting sigma value calculated in equation 10, which sets the mean value of 1.5V three sigma (n = 3) away from the USL and LSL.

$$s=(USL - \mu)/n =(1.65-1.5)/3 =0.05 \quad (10)$$

If test data is within control limits, the resulting sample test data set is six standard deviation from specified limits. A test population with six standard deviations between specified limits yields a reliability of 0.9973. Using equations 11through 13, 0.9973 is derived assuming a normal distribution of the data with a mean of 1.5V and 0.05V standard deviation.

$$P(X<LSL) = CDF(LSL) \quad (11)$$

$$P(X>USL) = 1 - CDF(USL) \quad (12)$$

$$R_{GenerateV2Goal}=1-P(X<LSL)-P(X>USL) \quad (13)$$

Post-corrective action sample data increases reliability confidence as the sample population increases and test data stays within control limits. Once the test population meets control limits and reliability allocations, the program can state that the corrective action effectively removed the high variability failure mode, capability drivers were mitigated and can provide a quantitative measure of reliability growth. Before the reliability effort the 'Generate V2' reliability allocation was set to 0.974, after corrective action the resulting allocation was increased to 0.9973, which is a reliability growth of 0.0233. The resulting reliability increase is provided with a level of confidence as test data continues to be within control limits.

During this investigation of the 'Provide V' data set, test value of 5V was identified. The 5V was root caused to a test setup error. After the test set up was corrected, the battery was retested to a valve of 5.45V. The resulting reliability of 0.999685, assuming the dataset in a normal distribution with a mean of 5.5045V and stand deviation 0.0692V applied to equations 11 through 13. Given the 'Provide V' findings, the function is no longer a reliability concern and therefore no additional corrective action is needed.

4 SUMMARY OF TAILORED DFR ACTIVITIES TO INCREASE RELIABILITY CONFIDENCE

In order to show increase reliability confidence, the system under analysis must be decomposed to its functional elements. The resulting functional elements must be linked to test events that provide an indication of function performance under specified environmental and timing conditions. Once all functions have been identified and linked to a test event, reliability goals are assigned using reliability data available for a given function. Reliability allocations are set such that the combination of all allocation results in a system reliability that meets RFP reliability requirements. Throughout the design and manufacturing of the system reliability tasks, such as derating analysis, FMECA, FTA and FRACAS are used to identify, prioritize and mitigate failure modes according to functions and their associated test data. Once failure modes are mitigated, collected test data is used to increase reliability confidence by corrective action effectiveness. To demonstrate corrective action effectiveness, control limits and tighter reliability allocations are set in place to show that test results are behaving as expected.

The example provided throughout this paper assumes test data fits into a normal distribution and reliability is calculated around specified limits. Therefore, when applying the methods identified in this paper special consideration is needed for PDF fitting and measures of goodness of fit to a particular set of PDFs. Special attention is also needed to determine actual failure limits. This paper assumes that specified limits represent the failure limit of system function.

REFERENCES

1. Tananko, Dmitry and Cooper, Howard, "Design for Reliability – Tools and Processes ", RAMS 2013
2. "Reliability Program Standard for Systems Design, Development, and Manufacturing", GEIA-STD-0009,
3. "Electronic Reliability Design Handbook", MIL-HDBK-338, 13 November 2008
4. "IEEE Standard Framework for Reliability Prediction of Hardware", IEEE-STD-1413
5. M.G. Masi, L Peretto, and R Tinarelli, "Dynamic Stress-Strength Approach for Reliability Prediction", in International Instrumentation and Measurement

BIOGRAPHIES

Eduardo V Cota
1151 Herman Rd
Tucson, AZ, 85734, USA

e-mail: eduardo_v_cota@raytheon.com

In 2006, Eduardo graduated from the University of Arizona with a minor in mathematics and a BS in Systems Engineering. Eduardo works for Raytheon Missile Systems, Engineering Product Support Directorate (EPSD), Reliability Engineering Department located in Tucson, AZ for six years. In 2012, Eduardo received his Masters degree in Systems Engineering from Johns Hopkins University. As a Reliability Engineer, Eduardo has performed countless part de-rating analysis, reliability predictions, Failure Modes Effects and Criticality Analysis for one-shot and continuous systems. Eduardo has performed FRACAS efforts on development programs and recently on a high rate production line.

Louis Gullo
3360 E Hemisphere
Tucson, AZ, 85706, USA

e-mail: Lou.Gullo@raytheon.com

Lou Gullo works for Raytheon Missile Systems, EPSD, Reliability Engineering Department located in Tucson, AZ. He is a leader of several special projects including a new storage reliability handbook for missiles, software reliability methods and automated electrical stress analysis methods. He has 30 years experience in military, space and commercial programs. He recently co-edited, co-authored and published a book, titled: “Design for Reliability”. He previously worked for Raytheon Integrated Defense Systems, Honeywell, Texas Instruments, Flextronics, Tyco/Sensormatic, and the US Army. He is a retired US Army Lieutenant Colonel. Lou has a BS degree in Electrical Engineering from the University of Connecticut in 1980. He is an IEEE Senior Member, an elected member of the Administrative Committee (ADCOM), and appointed as the IEEE Reliability Society Standards Committee Chair. He is a member of the Reliability and Maintainability Symposium (RAMS) Management Committee and Secretary/Treasurer for RAMS 2013. He is a member of the Reliability Maintainability Supportability Partnership (RMSP) Board of Directors. He is a member of the IEC TC-56 and VITA 51 standards committees.

Ram Munjal, PhD
1151 Herman Rd
Tucson, AZ, 85734, USA

e-mail: Ram_l_Munjal@raytheon.com

Ram Munjal is a Principal Systems Engineer in the Space Systems Design Department at Raytheon Missile Systems, Tucson, AZ. He has 28 years of progressive experience in modeling, analysis and simulation of Radar and Missile systems and for the past 4 years as Lead Analyst for the System Operation Performance Team. He earned his master degree in Physics in 1976 and PhD degree in Physics in 1978 from the College of William and Mary in Williamsburg, VA. He has taught graduate courses in Digital Systems and Digital Signal Processing at the GWC Whiting School of Engineering, Johns Hopkins University. He is a qualified Raytheon Six Sigma™ specialist. He is currently contributing as Data Analyst to implement Probabilistic Risk Assessment (PRA) approach into the Reliability Assessment program.