Comparison Modeling of System Reliability for Future NASA Projects

Amanda M. Gillespie, ASQ CRE, SAIC
Mark W. Monaghan, Ph.D, SAIC
Yuan Chen, Ph.D, NASA LaRC

Key Words: RBD, Importance Measure, Cut Set, Fussell-Vesely, Comparison Modeling

SUMMARY & CONCLUSIONS

A National Aeronautics and Space Administration (NASA) supported Reliability, Maintainability, and Availability (RMA) analysis team developed a unique RMA analysis methodology using cut set and importance measure analysis in order to comparison model proposed avionics computing architectures. In this paper we will present this efficient application of the RMA analysis methodology for importance measures that includes Reliability Block Diagram (RBD) Analysis, Comparison modeling, Cut Set Analysis, and Importance Measure Analysis. We will also demonstrate that integrating RMA early in the system design process as a key to success by providing a fundamental decision metric supporting design selection.

The RMA analysis methodology presented in this paper and applied to the avionics architectures enhances the usual way of predicting the need for redundancy based on failure rates or subject matter expert opinion. Using the RBDs and the minimal cut sets, along with the Fussell-Vesely (FV) factors, importance measures are calculated for each functional element in the architectures [1]. This paper presents an application of the FV importance measures and presents an improved methodology for using importance measures in success space (instead of failure space) to compare architectures. These importance measures are used to determine which functional element would be most likely to cause a system failure, thus, quickly identifying the path to increase the overall system reliability by either procuring more reliable functional elements or adding redundancy [2].

This application of the RMA analysis methodology, using RBD analysis, cut set analysis, and the importance measure analysis, allows the avionics design team to better understand and compare the vulnerabilities in each of the architectures, enabling them to address the deficiencies in the design architectures more efficiently, while balancing the need to design for optimum weight and space allocations.

1 INTRODUCTION

A trade study was performed to evaluate various avionics computing architectures from the perspectives of reliability, mass, power, data integrity, software implementation, and hardware and software integration for future NASA programs. A set of RBD models were developed to analyze the reliability of and rank the various computing system architectures. These reliability analysis modules allowed for ease and consistency in calculating reliability, cut sets, and importance measures.

First the RBD modules were created, and then cut set analysis was performed to determine those functional elements most likely to cause a failure within the architecture, i.e., which functional elements had the largest unreliability. Finally, FV importance measures were calculated for each functional element in each of the architectures. Then identical functional elements were grouped to allow for comparison between the architectures and provide the understanding of which functional elements had the most significant impact on system reliability.

2 SCOPE

This paper documents the reliability engineering methodology developed for the RBD comparison, cut set analysis, importance analysis, and improvement recommendations for the architectures for future NASA launch vehicles.

3 ASSUMPTIONS

To ensure that the RBD modules for each of the architectures were comparable, repeatable, and auditable, various assumptions were documented, including functional element failure rates, fault tolerance, mission duration, and cable and connector assumptions.

3.1 Functional element Failure Rates

The failure rates for the functional elements in the architectures were estimated based on the existing avionics system reliability databases. To facilitate comparison, the same failure rates were assumed for the same functional elements, interconnects, and topologies for the various architectures. All functional elements were assumed to have an exponential failure rate distribution. Due to the proprietary nature of these failure rates, they will not be listed in this paper.

The functional element failure rates were based on existing avionics architectures used aircraft, and a failure rate environmental conversion was made to the prediction (to SF environment). The conversions were made in accordance with

the System Reliability Center (SRC) environmental matrix [3].

3.2 Fault Tolerance

Avionics systems have evolved over time to incorporate fault tolerance within the system architecture. The capability to survive a functional element fault has driven multiple avionics system configurations [4]. In the Delta family of launch vehicles, the avionics systems have evolved over time based on reliability and fault tolerance [5]. Several examples of various avionic system architectures are plausible. The NASA avionic architecture team selected the systems to be evaluated based on fault tolerance capability.

The reliability analysis for the selected avionic systems to be studied assumed one-fault tolerance for each function element, i.e., more than one failure in any single functional element was deemed to be a failure. The configuration of the functional elements provided the fault tolerance capability. For example, more than one of the three Inertial Navigation Units (INU) would result in a system failure. In addition, only hard or non-recoverable failures of the functional elements were considered in the analysis. The impact of a functional element operating in a degraded stated was not taken into consideration.

For a self-checking pair (SCP) functional element configuration, it was assumed that, for the flight computers, switches, or buses, the self-checking pair consists of two flight computers or two switches or two buses, which needed to have data agreement to be successful. Therefore, the SCP functional elements were in a series configuration for reliability calculations (2-of-2 in agreement for success).

For a triplex voter (TV), the functional unit configuration was assumed to consist of three functional units plus majority voting logic, with the functional elements in a parallel configuration for reliability calculations (2-of-3 in agreement for success).

3.3 Channelized and Fully-Cross Strapped Configurations

A channelized configuration was assumed to be such that only functional elements of the same channel could share data, i.e., Flight Computer-1 (FC-1) only shared data with switch-1 (SW-1), and SW-1 could only share data with Data Acquisition Unit-1 (DAU-1), Main Propulsion System-1 (MPS-1), etc. Figure 1 shows the RBD configuration of the channelized architecture.

A fully-cross strapped (FCS) configuration was assumed to be such that all functional elements could share data, i.e., FC-1 could share data with all switches, and all switches could share data with all instrumentation/sensors and effectors/actuators. Figure 2 shows the RBD configuration of the SCP architecture.

3.4 Mission Duration

The reliability analysis was performed for a time period of up to nine months (6,480 hours) for mission scenarios that could potentially require an Earth departure stage and long mission duration.

3.5 Cables and Cable Connectors

The different architectures were modeled with and without cabling as part of the RBD analysis. The request to model cabling was made in order to identify a potential difference when cabling is installed into the models. The cable input to the functional element was modeled as having their individual failure properties. The cabling assembly RBD "block" was assumed to be comprised of the cable, supports, and connectors. The cable assembly was assumed to be routed from the source to the destination individually.

4 RELIABILITY BLOCK DIAGRAMS (RBD)

A RBD provides a pictorial representation of the architecture's reliability performance. The RBD demonstrates a logical connection of functional elements needed for system success. The RBD does not identify the avionics system topology but rather the functional element logical connection [6]. The particular assemblies identified by the RBD blocks identify system operational functions. Figure 1 shows the Relex© RBD representation of a SCP, channelized architecture, and Figure 2 shows the Relex© RBD representation of a FCS, TV architecture.

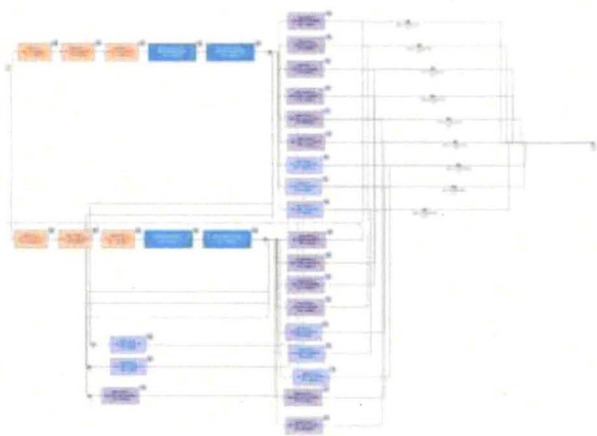

Figure 1: Example of SCP, Channelized Configuration RBD

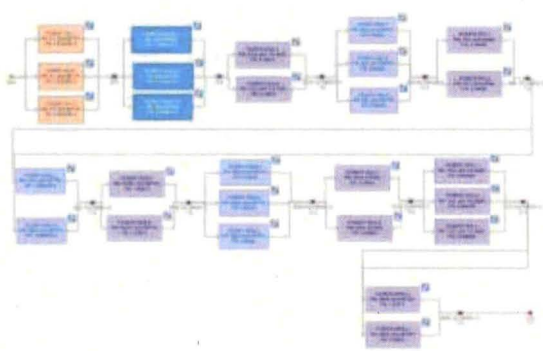

Figure 2: FCS, TV Configuration RBD

The RBD model does not demonstrate physical

configuration, cannot predict mass, does not estimate power consumption, and cannot guarantee the reliability values demonstrated are capable of being achieved. However, when RBDs from different architectures or systems have the same assumptions (failure rates, fault tolerance, etc), the RBDs can provide the ability to rank architectures by order of magnitude comparison, in which case the design engineer can determine the most reliable system architecture [7].

The architecture RBD calculations take into account the objectives and related engineering defined aspects of each system configuration from an assessment of operational success. The RBD is assembled in a success path for the system. The series representation indicates a system in which each block is dependent upon the success of the system. Parallel block configurations indicate a group of blocks that provide active redundancy or standby redundancy.

RELEX© was used as the primary reliability modeling tool. The various architectures were modeled into different RBD configurations using the failure rates as identified in Table 1. By using the same failure rates, the only variance in results would be due to the RBD configurations identifying the variant in configuration of the architectures. This allows for a normalized comparison of the architectures.

In the RELEX© model the operation simulation (OpSim) model was used to depict the RBDs. Results were calculated using both analytical and Monte-Carlo Simulation calculations with 1,000,000 iterations. For the Monte-Carlo Simulations, the confidence level was set at 95%.

5 RBD ANALYSIS AND RELIABILITY RESULTS

The various avionic architectures were evaluated; the quantity of functional elements included in each, and the redundancy configuration for each, and the architecture fault tolerance are listed below:

1. Fully Cross-Strapped Switched Triplex Voter (FCSSTV)
2. Partially Cross-Strapped Switched Triplex Voter (PCSSTV)
3. Channelized Bussed Triplex Voter (CBTV)
4. Fully Cross-Strapped Self-Checking (FCSSC)
5. Fully Cross-Strapped Bussed Self-Checking (FCSBSC)
6. Channelized Bussed Self-Checking (CBSC)

5.1 Architecture RBD Reliability Results Summary

Figure 3 and Table 1 show the reliability results for the six architectures. The reliability results are calculated at 9 months (6,480 hours) and include the failure contribution from cabling.

Although these results were significant in eliminating two of the architectures (CBTV and CBSC), additional RBD comparison data was needed to ensure the vulnerabilities of each architecture was understood.

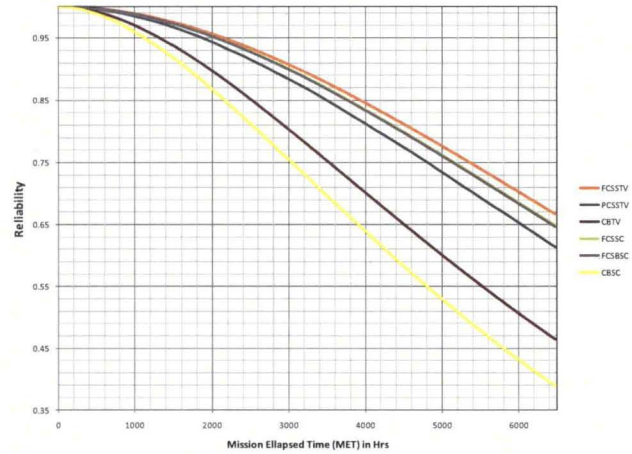

Figure 3: Architecture Reliability Comparison Results: Reliability versus Mission Elapsed Time (MET)

Architecture	R (6480 hrs)
FCSSTV	0.666999
PCSSTV	0.613596
CBTV	0.464581
FCSSC	0.648547
FCSBSC	0.646730
CBSC	0.389427

Table 1: Architecture Reliability Results

6 CUT SET ANALYSIS

Cut set analysis provides clear indication of where the most likely failure paths would be depending on the accuracy of the RBD and the accuracy of the failure data of the functional elements. A cut set is a set of basic events [failures] where the joint occurrence of these basic events results in the failure of the system [2]. Each cut set can contain anywhere from one to all functional elements, depending on the system architecture. A minimal cut set is defined as a set that "cannot be reduced without losing its status as a cut set" [8].

Once the minimal cut sets were identified, a comparison was made to determine if the system with the least reliability contained the most failure paths, thus, making a recommendation for the most reliable architecture based on the number of minimal failure paths. It was quickly determined that, in general, the more cut sets an architecture had, the less reliable it tended to be. However, as the difference in reliability between the architectures became smaller, a conclusion as to the most reliable architecture could not be drawn from the number of cut sets alone due to the difference in number of functional elements and their configuration in each of the architectures. Table 2 shows the architectures ranked from most reliable to least reliable and the number of minimal cut sets calculated for each.

Architecture	Reliability	# of Minimal Cut Sets
FCSSTV	0.666999	75
FCSSC	0.648547	67
FCSBSC	0.646730	73

Architecture	Reliability	# of Minimal Cut Sets
PCSSTV	0.613596	195
CBTV	0.464581	267
CBSC	0.389427	304

Table 2: Architecture Ranking and Number of Minimal Cut Sets

7 IMPORTANCE MEASURES IN SUCCESS SPACE

Part of the decision analysis in selecting a specific architecture includes determining which of the functional elements can lead to high risk scenarios. In order to assess the importance of functional elements in the architecture or the sensitivity of the architecture reliability to changes in the functional element's input failure rates, several importance (or sensitivity) measures are available [2]. "Importance measures quantify the criticality of a particular functional element within a system design. They have been widely used as tools for identifying system weakness, and to prioritize reliability improvement activities." [9]

The various measures are based on slightly different interpretations of the concept of functional element importance. Intuitively, the functional element importance should depend on the location of the functional element in the system, the reliability of the functional element in question, and the uncertainty in the estimate of functional element reliability [10].

Typically, importance measures are used in failure space, or for Fault Tree Analysis (FTA). However, these importance factors can be defined in success space (RBD Analysis) by calculating the measures based on the total success of the system instead of the total risk. Some importance factors do not preserve their meaning in success space; therefore, they fail to rank the functional elements appropriately. However, all importance measures provide one with a single number for each functional element that can be used as part of a comparative analysis.

There are five importance measures generally accepted for use: Birnbaum, Criticality, Fussell-Vesely (FV), Risk Reduction Worth (RRW), and Risk Achievement Worth (RAW) [11]. The Birnbaum measure depends on the system configuration and is typically used to determine the degree of redundancy and appropriateness of the system's logic. The Criticality measure is a weighted version of the Birnbaum, which takes into account the ratio of functional element failure probability and system reliability. The FV is the fractional contribution of risk to the system of all scenarios containing that specified functional element versus the contribution of all failure scenarios in a system. The RAW is the ratio of the conditional system unreliability if the functional element is not present (always failed) with the actual system unreliability. The RRW is the ratio of the actual system unreliability with the (conditional system unreliability if the functional element is replaced by a perfect functional element (never fails) [10].

Due to the limitation of the Relex© software program in calculating importance measures in success space, all importance measures had to be calculated by hand. The Birnbaum, Criticality, RAW, and RRW measures proved significantly time consuming, as the conditional reliability calculations had to be made by performing multiple runs in Relex© to obtain values (20 or more runs per architecture). However, Relex© calculations quickly provided minimal cut set unreliability values that could then be used to calculate the FV for all functional elements.

Figure 4, Table 3, and Table 4 show the comparison of the Birnbaum, Criticality, FV, RRW, and RAW results for the functional elements in a single architecture. The Birnbaum and Criticality measures yielded nearly identical results and rankings when compared to each other. The FV measures differed slightly from the Birnbaum and Criticality measures, but the primary contributor to the unreliability of the architecture (over 21% of the unreliability in all three measures) remained the same. The RRW and RAW measures seemed to provide little value added when applied to the cut sets in success space, with all functional elements having similar contributions to the overall unreliability of the architecture, appearing to be based on failure rate data alone. Thus, making the RRW and RAW importance measures seemingly unsuitable for use in success space.

When weighing the time needed to perform the importance measure analysis versus the benefits that were to be achieved, the FV was chosen in order to efficiently obtain the quantitative importance measures for each functional element for a comparative analysis.

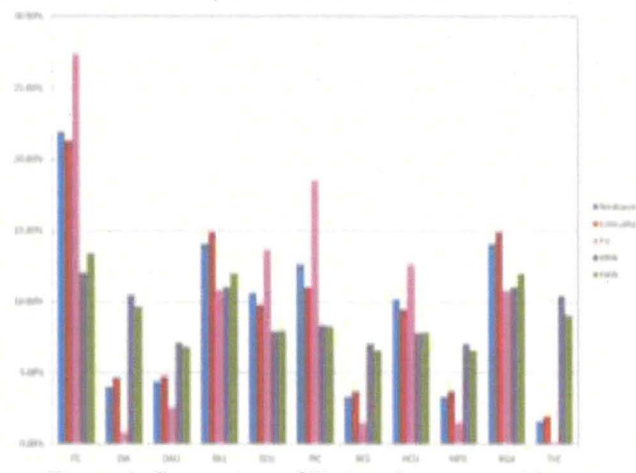

Figure 4: Comparison of Various Importance Measure Results

Birnbaum		Criticality		FV	
FC	21.93%	FC	21.32%	FC	27.38%
INU	14.07%	INU	14.92%	PIC	18.54%
RGA	14.07%	RGA	14.92%	ECU	13.63%
PIC	12.62%	PIC	11.01%	HCU	12.62%
ECU	10.59%	ECU	9.74%	INU	10.74%
HCU	10.15%	HCU	9.45%	RGA	10.74%
DAU	4.36%	DAU	4.72%	DAU	2.54%
SW	3.97%	SW	4.63%	RCS	1.47%
RCS	3.30%	RCS	3.67%	MPS	1.47%
MPS	3.30%	MPS	3.67%	SW	0.76%

Birnbaum		Criticality		FV	
TVC	1.63%	TVC	1.94%	TVC	0.12%

Table 3: Comparison of Birnbaum, Criticality, and FV Importance Measure Results

RRW		RAW		FV	
FC	12.03%	FC	13.42%	FC	27.38%
INU	11.00%	INU	11.97%	PIC	18.54%
RGA	11.00%	RGA	11.97%	ECU	13.63%
SW	10.45%	SW	9.65%	HCU	12.62%
TVC	10.41%	TVC	9.04%	INU	10.74%
PIC	8.32%	PIC	8.22%	RGA	10.74%
ECU	7.88%	ECU	7.94%	DAU	2.54%
HCU	7.79%	HCU	7.87%	RCS	1.47%
DAU	7.09%	DAU	6.80%	MPS	1.47%
RCS	7.02%	RCS	6.56%	SW	0.76%
MPS	7.02%	MPS	6.56%	TVC	0.12%

Table 4: Comparison of RRW, RAW, and FV Importance Measure Results

7.1 Fussell-Vesely (FV)Importance for Functional Elements

The FV is the probability that at least one minimal cut set that contains the functional element (i) has failed at time (t), given that the system is failed at time (t) [10]. In other words, the functional element FV is the sum of the unreliability of the minimal cut sets containing the functional element, divided by the sum of the unreliability of all of the system's minimal cut sets.

The functional element FV can be expressed as percentage contribution to unreliability of the overall system (so that all functional element importance measures add to 100% of the system unreliability). The functional element FV was divided by the sum of all functional element FVs to obtain the percentage contribution. The FV reflects how much relative improvement may be available from improving performance of a specific functional element. Change in the failure rates of the functional elements (or adding redundancy to account for the high failure rate) with the highest FV percent contribution will have the most significant effect on increasing system reliability.

Once the functional element FV percent contributions were calculated for all functional elements and all architectures, a comparison of functional element importance between the various architectures can be made. The implementation of the FV to compare functional elements within the different architectures proved somewhat more involved than first anticipated. Most architectures contained redundancy with two or more of the same functional element functions within each; however, there was not a one-to-one correspondence. For example, the TV architectures (FCSSTV, PCSSTV, and CBTV) contained three FCs, while the SCP architectures (FCSSC, FCSBSC, and CBSC) contained four FCs. Therefore, the functional element functions were grouped for comparison by summing the contributions of all like-functional elements in the architecture. Table 5 shows the example of how this was done for FCs.

Architecture	FC-#	FV %	FC	FV %
FCSSTV	FC-1	9.12%	FC	27.36%
	FC-2	9.12%		
	FC-3	9.12%		
PCSSTV	FC-1	6.66%	FC	19.98%
	FC-2	6.66%		
	FC-3	6.66%		
CBTV	FC-1	15.83%	FC	39.29%
	FC-2	7.63%		
	FC-3	15.83%		
FCSSC	FC-1A	8.35%	FC	33.39%
	FC-1B	8.35%		
	FC-2A	8.35%		
	FC-2B	8.35%		
FCSBSC	FC-1A	8.51%	FC	34.04%
	FC-1B	8.51%		
	FC-2A	8.51%		
	FC-2B	8.51%		
CBSC	FC-1A	11.08%	FC	44.33%
	FC-1B	11.08%		
	FC-2A	11.08%		
	FC-2B	11.08%		

Table 5: Example of Functional element grouping for Importance Measure Comparison

Once all functional element functions were grouped, a few functions were unable to be compared. For example, CBTV and CBSC had Bus functional element contributions, while the other Architectures did not. Overall, though, this worked to determine which functional elements were most likely to cause a failure. The results are shown in Figure 5.

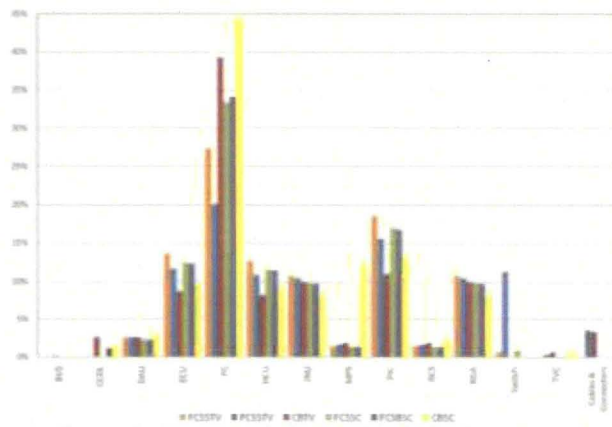

Figure 5: Functional element FV Calculations per Architecture

The functional element importance measures provide the designer with more information than a single reliability calculation comparison may provide. Architecture selection is made based not only on reliability calculations, but on weight, space, cost, risk to the mission, etc, and the additional importance measure calculations provide comparison data to

allow the designer to make more informed trade decisions in a more efficient and effective manner. The difference in vulnerabilities of the architectures can easily be compared using the importance measure analysis.

Different distributions of the functional failure contributions indicate different reliability improvement paths for the architectures. Intermediate states can be modeled to include the impact of failure data integrity on the reliability and integrity of the architectures. These results can be used not only to determine the most efficient and cost-effective way to increase reliability of the architecture.

REFERENCES

1. W.S. Gough, J. Riley, J.M. Koren, "A New Approach to the Analysis of Reliability Block Diagrams," *Proc. Ann. Reliability & Maintainability Symp.* (Jan.) 1990, pp. 456-464.
2. B.M. Ayyub, *Risk Analysis in Engineering and Economics*, New York, Chapman & Hall/CRC, 2003.
3. D. Nicholls *ed.*, *System Reliability Toolkit*, Reliability information Analysis Center (RAIC), 2005.
4. R. Hammett, "Design by Extrapolation: An Evaluation of Fault Tolerant Avionics," *IEEE AESS Systems Magazine,* (April) 2002.
5. J.M. Palsulich, B.J. Schinnerer, *Launch Vehicles for Low-Cost Planetary Missions,* Elsevier Science Ltd., 2002.
6. P.D.T. O'Connor, *Practical Reliability Engineering, 4th Edition*, Wiley, 2006.
7. M.L.O. e`Souza, T.R. de Carvalho, *The Fault Avoidance and The Fault Tolerance Approaches for Increasing the Reliability of Aerospace and Automotive Systems*, Society of Automotive Engineers Inc., 2005.
8. W.R. Blischke, D.N. Prabhakar Murthy, *Reliability: Modeling, Prediction, and Optimization*, Wiley, 2000.
9. J.E. Ramierez-Marquez, D.W. Coit, "Composite Importance Measures for Multi-State Systems with Multi-State Functional elements," *IEEE Transactions on Reliability*, vol. 54, (Sept) 2005, p.517.
10. M. Rausand, A. Hoyland, *System Reliability Theory: Models, Statistical Methods, and Applications, 2nd Edition*, Wiley, 2003.
11. J. Apt, "Human Spaceflight Risk Management," *Encyclopedia of Aerospace Engineering,* Wiley, 2010.

ACKNOWLEDGMENTS

The authors would like to thank Glen (Spence) Hatfield, Duane H. Pettit, Joseph M. Schuh and Dr. Robert Hodson, who contributed to the development and review of the RMA analysis methodology described in this paper.

BIOGRAPHIES

Amanda M. Gillespie, ASQ CRE
SAIC-LX-2
Operations & Checkout Bldg, M7-0355
Kennedy Space Center, FL 32899 USA

e-mail: amanda.gillespie-1@nasa.gov

Amanda M. Gillespie is a Reliability Engineer with SAIC at NASA KSC, FL. At KSC, Amanda has performed RMA analysis for various NASA projects and programs. As a part of the KSC RMA team, along with Dr. Monaghan, Amanda works with multiple engineering teams to evaluate and increase the operational and inherent availability of the systems. Amanda received her BS in Applied Mathematics from the Georgia Institute of Technology in 2000. Amanda is a member of the American Society for Quality (ASQ) Reliability and Statistics Societies. Amanda received her ASQ Certified Reliability Engineer (CRE) certification in January 2011.

Mark W. Monaghan, Ph.D
SAIC-LX-2
Operations & Checkout Bldg, M7-0355
Kennedy Space Center, FL 32899 USA

e-mail: mark.w.monaghan@nasa.gov

Mark W. Monaghan received his Ph.D in Applied Decision Science from Walden University in 2008. Mark is a Reliability Engineer with SAIC at NASA KSC, FL. At KSC, Dr. Monaghan has performed RMA analysis for various NASA projects and programs. As a part of the KSC RMA team, along with Amanda Gillespie, Dr. Monaghan works with multiple engineering teams to evaluate and increase the operational and inherent availability of the systems. He is a senior member of Institute of Electrical and Electronic Engineers (IEEE) Industrial Application Society (IAS). He is also a member of American Institute of Aeronautics and Astronautics (AIAA) and the ASQ Reliability Societies.

Yuan Chen, PhD
NASA LaRC
Electronic Systems Branch
5 N. Dryden Street, MS 488
Hampton, VA 23681 USA

e-mail: yuan.chen@nasa.gov

Yuan Chen received her Ph.D. Reliability Engineering from the University of Maryland at College Park, Maryland, in 1998, with a Graduate Fellowship from the National Institute of Standards and Technologies. She is currently a senior member of technical staff with the Electronic Systems Branch, NASA Langley Research Center, Hampton, Virginia. Dr. Chen's research area has been focused on the development of and reliability methodologies on microelectronic devices/systems for space applications. She has authored and co-authored over 40 technical papers, and is a senior member of IEEE and AIAA.