Evolving Reliability & Maintainability Allocations for NASA Ground Systems

Gisela Munoz
Red Canyon Software
Kennedy Space Center, FL 32899
321-867-8212
Gisela.A.Munoz-Luethi@nasa.gov

Jamie Toon
Millennium Engineering & Integration
Kennedy Space Center, FL 32899
321-867-6741
Jamie.A.Toon@nasa.gov

Troy Toon
Millennium Engineering & Integration
Kennedy Space Center, FL 32899
321-867-1915
Troy.T.Toon@nasa.gov

Timothy C. Adams
NASA Kennedy Space Center
Kennedy Space Center, FL 32899
321-867-2267
Tim.Adams@nasa.gov

David J. Miranda
NASA Kennedy Space Center
Kennedy Space Center, FL 32899
321-867-5219
David.J.Miranda@nasa.gov

***Abstract*— This paper describes the methodology that was developed to allocate reliability and maintainability requirements for the NASA Ground Systems Development and Operations (GSDO) program's subsystems. As systems progressed through their design life cycle and hardware data became available, it became necessary to reexamine the previously derived allocations. Allocating is an iterative process; as systems moved beyond their conceptual and preliminary design phases this provided an opportunity for the reliability engineering team to reevaluate allocations based on updated designs and maintainability characteristics of the components. Trade-offs in reliability and maintainability were essential to ensuring the integrity of the reliability and maintainability analysis. This paper will discuss the value of modifying reliability and maintainability allocations made for the GSDO subsystems as the program nears the end of its design phase.**

TABLE OF CONTENTS

1. INTRODUCTION

Subsystems under NASA's Ground Systems and Development and Operations (GSDO) program located at the Kennedy Space Center (KSC) have evolved to support future space programs, serving both NASA's design reference missions for the Space Launch System (SLS) and commercial opportunities. GSDO requires a safe, reliable, maintainable, and available complex system of subsystems to successfully support launch activities. In order to achieve this, a launch availability requirement must be established and decomposed to reliability and maintainability requirements that are then allocated to each subsystem based on their complexity and contribution to each launch attempt. The reliability, maintainability, and availability (RMA) analysis for each subsystem verifies these requirements. Reliability allocations are determined by GSDO program goals, predicted performance from previous programs, and historical performance of legacy subsystems and components. The reliability engineer must also consider the maintainability characteristics of each subsystems and its components to determine what, if any, trade-offs are needed between reliability and maintainability to reach the availability requirement. The mean corrective maintenance time or mean time to repair (MTTR) is of particular interest to the reliability team, because unlike other forms of downtime, these values can be quantitatively predicted and analyzed in the design phase. This paper will discuss how allocations were initially created and then adjusted as GSDO evolved through its design life cycle.

2. GSDO LAUNCH AVAILABILITY

GSDO subsystems along with the SLS and Orion programs have been allocated a Launch Probability Technical Performance Measure (TPM) to ensure the success of future missions. This TPM required an integrated effort between the programs and was calculated using Discrete Event Simulation (DES) modeling. The cross-program team developed a DES model to determine the probability of launch after the start of the countdown window. These results were then in turn allocated down to each of the programs [1]. Currently, the objective launch probability of the overall architecture is to be no less than 90% for each launch attempt. In order to assess the capability of the architecture, a DES model utilizing historical data and current operational definitions provided input parameters to the launch probability allocations for each program. The GSDO DES team tracks and quantifies launch probability risk due to ground system delays, human error, scheduling conflicts with other customers, and weather.

For the GSDO reliability team, the launch probability

allocation was decomposed to two requirements, Inherent Launch Availability and Operational Availability. As shown in Figures 1 and 2, these allocations were further decomposed to reliability and maintainability requirements for the GSDO subsystems.

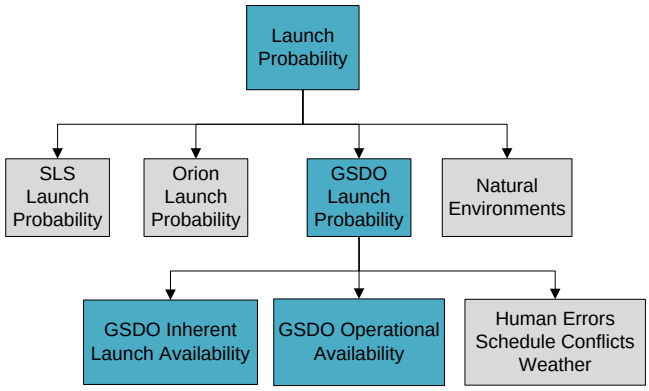

Figure 1 – GSDO Launch Probability & Availability

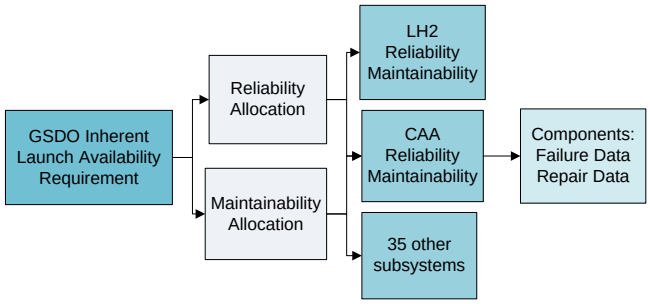

Figure 2 - GSDO RMA Subsystem Allocations

Inherent Launch Availability is defined as all the subsystems that are required to support and actualize a successful launch. The availability requirement states that GSDO will have an inherent launch availability of at least 98% within the timeframe of 24 hours prior to the launch attempt. Operational Availability is defined as all the subsystems that are required to repair and support systems after a launch scrub is called which could require a launch vehicle roll back scenario to the Vehicle Assembly Building (VAB). The operational availability requirement states that GSDO will have an operational availability of at least 80% with a timeframe of 360 hours, beginning with the start of the first launch attempt plus 14 days prior to the next launch attempt. This definition of operational availability contrasts with the definition found in the literature, which includes forms of downtime associated with all maintenance tasks. The inherent launch availability requirement has not changed while the operational availability requirement has been updated since the RMA effort began [2]-[3]. The methodology used to achieve these requirements has been updated to reflect the current status of subsystem designs.

3. ALLOCATIONS

The allocation methodology employed included previously used historical data from prior programs and subsystem subject-matter expertise in combination with common reliability allocation techniques to ensure conformance with launch probability and availability requirements. As systems progressed through their design life cycle and more data became available with the supplier hardware, it became necessary to reexamine the previously derived allocations. Allocating is an iterative process; as systems moved beyond the conceptual and preliminary design phases there was an opportunity for the reliability engineering team to reevaluate allocations based on updated designs and maintainability characteristics of components.

One factor for reallocating requirements was the number of systems under analysis. Previous research [2] included 42 subsystems under analysis for Inherent Launch Availability and 12 subsystems for Operational Availability; these numbers have been updated to 37 subsystems for Inherent Launch Availability and 14 for Operational Availability. As subsystem designs progressed, it was determined that some subsystem's components were absorbed by other subsystems and others were found to be essential to Operational Availability rather than Inherent Launch Availability.

Another factor was the increase in hardware as subsystem's reached their final design reviews. The original allocations were based on preliminary designs and did not account for additional components and changes to the launch architecture (e.g. flight vehicle, ground systems). As the program approached its critical design milestone, eighteen subsystems were not meeting their requirements. This high number led the team to consider whether the initial requirement was incorrect or whether reallocations were necessary. It is recommended in practice that any design changes, including modifications to the system architecture, warrant reallocation of requirements. However, there is a lack of case studies in the literature verifying this suggestion. During reallocation, trade-offs between reliability and maintainability were essential to ensuring the integrity of RMA analyses. For example, four recommended techniques for allocating maintainability did not apply to GSDO subsystems [4]; these methods are recommended early in the design phase and do not reflect the current status of GSDO system designs which vary in complexity and operation.

4. METHODOLOGY

Software

The GSDO RMA team uses the PTC's Windchill Quality Solutions (WQS) (formerly Relex) software tool for analysis. WQS is a reliability analysis tool that uses common standards for reliability prediction, contains databases of failure data for mechanical, electrical, and electromechanical assemblies, and uses numerical methods to provide results for RMA analyses. The RMA team uses two of WQS's modules for analysis: Reliability Prediction and Reliability Block Diagrams (RBD).

The user can create parts lists in the Reliability Prediction module for all components in the subsystem under analysis either by entering user-defined data or using the software's

prediction libraries. This module assigns failure rates to each part using various methods. WQS uses MIL-HDBK-217F parts count methodology to assign failure rates. The software does have the capability to use newer methods such 217Plus, which requires several pieces of additional information, such as operating temperature and other environmental factors. This data is difficult to collect for all subsystems during the design phase but can be collected during the testing and validation phases. To maintain consistency between the analyses MIL-HDBK-217F is used for calculations.

The RMA team enters user-defined data when manufacturer failure rate or MTBF are published; also when available, historical failure rates can be entered in to the component list. The Non-electronic Parts Reliability Database (NPRD), Electronic Parts Reliability Database (EPRD), and other ancillary handbooks are used for RMA analysis. The NPRD and EPRD libraries use field failure rate data; these libraries are also incorporated into the software used for analysis, when manufacturer or historical data is not available. These capabilities allow the RMA team to develop a complete parts library for the subsystem under study from a variety of reputable sources.

The primary modeling tool for analysis is the RBD. The configuration of the components within the RBD reflects the functionality of the subsystem and accounts for redundancy and backup systems. For subsystems that have built in redundancy in to their design, an RBD can also demonstrate the logical connection between components. Generally, the larger and more complex a subsystem design is the larger the RBD model will be. An RBD does not represent the physical location or configuration of components; only components that are required to function for the successful performance of a subsystem are included. All results of RMA analyses are derived from the WQS's RBD module.

RBDs can be modeled in multiple layers of single and parallel configurations. RBDs can also be modeled in multiple configurations: series, parallel, or series-parallel. At the subsystem level, the RBD models are a combination of these options. At the top level, all systems are mutually independent of one another and are modeled serially. For the Inherent Launch Availability requirement, failure of any of the 37 subsystems will result in a launch scrub scenario.

A sensitivity analysis is performed using Monte-Carlo probabilistic simulation for reliability and availability calculations. The Monte-Carlo technique uses a selection of random numbers during the simulation process of 1,000,000 iterations. This approach confirms the consistency and accuracy of the results. A confidence interval of 95% is selected for analysis.

There are limitations to any software analysis tool. Within the capability of WQS, and in order to maintain consistency across all analyses, all calculations were made assuming exponential distribution for failure and repair data.

Reliability Allocations

The concise definition for reliability is the probability that an item (e.g. subsystem, component) will perform its intended function with no failures during a given period of time under specified operation conditions. Reliability is expressed, in equation (1), as the probability that a system (or component) will fail *at or after* a predetermined time t,

$$R(t) = \Pr\{T \geq t\} \tag{1}$$

In general, failures that occur randomly or by chance events are modelled by the exponential distribution. This distribution is also known as the Constant Failure Rate model, meaning components fail at a constant rate independent of component design, operating time, and age. For reusable launch systems, like those being analyzed independent analyses of historical data have determined that failure data can follow the exponential distribution [5]. The reliability equation, as expressed in (2), for the exponential distribution is

$$R(t) = e^{-\lambda t} \tag{2}$$

where λ is the subsystem or component failure rate and t is the mission time. Failure rate is also expressed, in equation (3), as the reciprocal of the Mean Time Between Failures (MTBF). MTBF represents the average time an item is operational between failures.

$$\lambda = \frac{1}{MTBF} \tag{3}$$

In order to accurately model subsystems, components are chosen that most closely resemble parts found in the subsystem under study. For RMA analysis, failure rate data (λ or MTBF) is supplied by the manufacturer, through prediction part libraries, ancillary handbooks, or historical data from previous programs. Prediction part libraries are depositories of parts and assemblies failure rates collected from multiple sources.

The measures for reliability and availability are commonly expressed in terms of 9s. For example, the values of reliability allocations that subsystems are required to meet range from two-9s (0.99) to over three-9s (0.999), meaning they are expected to be 99% or 99.9% reliable. When modeled serially, the product of all subsystem reliabilities, expressed in equation (4), will determine the reliability of GSDO subsystems.

$$R_{GSDO} = \prod_{i=1}^{n} R_i(t) = R_1 * R_2 * \ldots * R_n \tag{4}$$

Maintainability Allocations

Maintainability is a design parameter which describes the ability of a subsystem to be restored or repaired to an operational state within a given time period. Maintenance is the action to restore or repair a system to an operational state. Maintainability is expressed, in equation (5), as the

probability that a system (or component) can be repaired *at or before* a predetermined time t,

$$M(t) = \Pr\{T \leq t\} \quad (5)$$

The inclusion of maintainability in subsystem design can reduce system downtime by decreasing the Mean Time to Repair (MTTR). There are four subsets to system downtime: corrective maintenance, preventative maintenance, administrative delay time, and logistics delay time. The RMA analysis at this time only includes corrective maintenance time. It is a challenge and not a recommended practice to predict estimates for preventative maintenance and delay times; the greatest variability in time exists during these actions. A general corrective maintenance cycle can included many phases from when the failure occurs to when the repair is completed. The phases of corrective maintenance under analysis included: fault detection, localization and isolation, disassembly, repair or replacement, reassembly, and functional checkout [6]. Corrective maintenance or MTTR, is the unscheduled maintenance tasks to restore a system to an operational state as a result of system failure. For GSDO, the RMA team is concerned with the time frame between disassembly and functional checkout, as shown in Figure 3.

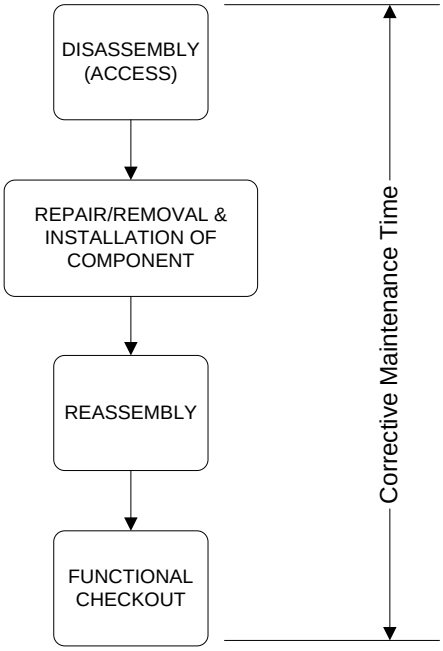

Figure 3 – Corrective Maintenance Cycle

Many of the GSDO subsystems contain legacy hardware and the numerous upgrades to subsystems are similar in accessibility and maintainability compared to their predecessors. Therefore, there is a strong case for quantitatively predicting correct maintenance for subsystem components. These factors combined with subject matter expertise from operations engineers involved with subsystem upgrades and available historical data from repair reports provided the RMA team with conservative, yet realistic estimates for MTTR. The RMA team initially uses their best engineering judgment for MTTR estimates based on a 3-shift, 24 hour operation for launch activities. For example, the initial estimate for a faulty solenoid valve which is to be removed and replaced, would be 8 hours (1 shift). This estimate would then be submitted to the subsystem operations and design engineers for verification. Adjustments were made based on subject matter expertise input.

Maintainability is the counterpart of reliability, both are contributors to a subsystem's availability. The goal of maintainability is to reduce lifecycle costs by mitigating a "design it now and fix it later" conflict. Historically, repair times have been modelled using the lognormal distribution. For reusable launch ground systems, like those being analyzed, independent analyses of historical data have determined that repair times can follow either a lognormal or exponential distribution [5]. For subsystem analyses, software limitations only allow for an exponential distribution for repair data.

Assuming constant repair rates (or exponential distribution) for subsystem components, the probability of completing a repair in time t or less can be determined. The maintainability function, in equation (6), for an exponential distribution of repair times is

$$\mathrm{M(t)} = 1 - e^{-\mu t} \quad (6)$$

where μ is the constant repair rate and t is the allocated time to repair for the subsystem. The constant repair rate is also expressed as the reciprocal of MTTR as expressed in equation (7),

$$\mu = \frac{1}{MTTR} \quad (7)$$

The maintainability function determines the probability of completing a repair within a specified time In general, a maintainability allocation has an MTTR for each subsystem using one of these recommended methods: failure rate complexity allocation, equal allocation, and statistically-based calculated allocation [4]. The equal allocation method could not be used for GSDO; this method assumes that an MTTR allocation is independent of a subsystems failure rate and can be distributed equally among the subsystems. This is not feasible because GSDO subsystems vary in complexity such as ease of access, type of repairable components, and type of subsystem. For example, some GSDO subsystems are strictly electrical subsystems, while others are a combination of electrical, mechanical and electromechanical subsystems. The statistically based allocation method is not applicable either; this method assumes a lognormal distributions for repair times. The failure rate complexity method, while practical, assumes that subsystems with the lowest reliability will be assigned the lowest MTTR values. In reality, a complex system of systems will include a variation of low and high reliability systems with a variety of component and aggregate subsystem MTTRs.

For GSDO, it would have been impractical to assign MTTR values using one of these methods. Therefore, MTTR values were assigned based on type of system, ease of access, and the weighted failure rate of components. An internal analysis

of historical ground system delay times determined that the MTTR for ground systems is about 50 hours. Using this estimate as a guide and with subject matter expertise input, subsystems which contained a majority of mechanical or electro-mechanical hardware were assigned higher MTTR values than electrical subsystems. Mechanical subsystems were allocated a maximum MTTR of 30 hours. Electrical subsystems which contained quick remove and replace hardware were allocated the lowest MTTR values, between 15 and 20 hours. To calculate the total mean corrective maintenance time for a subsystem ($MTTR_{SS}$), the MTTR for each component is weighted against the individual component's failure rate. The mean corrective maintenance time is expressed in equation (8) as

$$MTTR_{SS} = \frac{\Sigma(\lambda_i \cdot MTTR_i)}{\Sigma\lambda_i} \quad (8)$$

where the $MTTR_{SS}$ is calculated using each ith component failure and repair data. This approach is also used to determine the MTTR for all GSDO subsystems, as expressed in equation (9),

$$MTTR_{GSDO} = \frac{\Sigma(\lambda_{SS} \cdot MTTR_{SS})}{\Sigma\lambda_{SS}} \quad (9)$$

The MTTR for a subsystem or component represents the average number of hours for a component or subsystem to be restored to an operational state after an unexpected failure.

Availability Allocations

Availability, which is a function of reliability and maintainability, is the probability that a repairable subsystem will operate satisfactorily at a given point in time during the period of analysis (estimated to be 24 or 360 hours). There are many ways of expressing availability, whether inherent or operational. It is the goal of the RMA team to produce relevant and best estimates for how subsystems will operate at the critical point during launch countdown (i.e., at the time of launch or T-0). Inherent Availability is the probability that a system will perform satisfactorily at any given time under specific operating conditions in an ideal support environment. Typically, Steady-State Inherent Availability is expressed in equation (10) as

$$A = \frac{MTBF}{MTBF+MTTR} = \frac{uptime}{uptime+downtime} \quad (10)$$

where uptime and downtime are considered the basic statistics for assessing a system's performance. For GSDO, the performance specification is measured at 24 or 360 hours. Therefore, in order to assess a subsystem's design, the point (or instantaneous) availability is used. When both the failure distribution and the repair distribution are based on the exponential distribution, point availability is expressed in equation (11) as

$$A(t) = \frac{\mu}{\lambda+\mu} + \frac{\lambda}{\lambda+\mu} e^{-(\lambda+\mu)t} \quad (11)$$

where μ is the subsystem's repair rate, λ is the subsystem's failure rate and t is the specified mission time or point in time for the subsystem to be available. As with reliability, when modelled serially, the product of all subsystem availabilities, as expressed in equation (12), will determine the availability of GSDO subsystems.

$$A_{GSDO} = \prod_{i=1}^{n} A_i(t) = A_1 * A_2 * \ldots * A_n \quad (12)$$

Using equation (12), will also verify the Inherent Launch Availability and Operational Availability requirements.

5. CONCLUSIONS

As NASA design reference missions are further developed, a robust ground systems architecture is needed. The RMA team analyzes GSDO subsystems to quantitatively determine if subsystems will meet the Inherent Launch Availability and Operational Availability requirements. These requirements exist to ensure that ground systems are safe, reliable, maintainable, and available to successfully support launch activities. The team provides recommendations to design teams with the intent to ensure that the design meets program level requirements. The RMA analysis is intended to verify that upgrades in design, in combination with legacy systems, meet the RMA allocations. If a subsystem is unable to meet its allocations, the RMA team will consult with the design team's engineers to determine if a design change is feasible or a suitable operational workaround exists. When multiple subsystems were not meeting their requirements, an opportunity existed to determine whether the requirement was incorrect or reallocation was necessary. The RMA team determined that significant increases in the number of components and changes to the launch architecture since the effort began required the team to reassess the allocations.

As stated in the beginning of this paper, it is recommended in practice that any design changes including modifications to the system architecture warrant reallocation of requirements. After reassessing GSDO subsystems, the following recommendations are offered:

- Any increase in the number of components without a change in the design strategy (e.g. quality of hardware, redundancy) will result in a change in the calculated measures for reliability and maintainability. This will affect the calculated availability; therefore, reallocation should be considered.

- Using hardware that historically has higher failure rates and are considered single points of failure (e.g. valves, transducers) will have an impact on the estimated reliability of the subsystem.

- Significant changes to the system architecture, such as the addition or removal of subsystems will affect the overall calculated availability requirement; therefore, reallocation should be considered

6. FORWARD WORK

In order to verify and validate the GSDO requirements it is essential that the RMA team continues to be involved in the testing and integration activities leading up to system certification. Developing an analysis set that includes all forms of downtime – logistics, administrative, preventative, and conditional-based maintenance should be completed during system testing to ensure verification. These results can be compared to the requirements; recommending further improvements if necessary. As more data becomes available, these estimates can be used to further refine the number of maintenance personnel required to complete a repair. Proper training of personnel and optimizing spares inventory using top-rated contributors to unavailability of subsystems will keep repair times to a minimum. The RMA team will be an integral part of certifying ground systems to support launch. As GSDO moves forward to operations and sustainment, RMA can use collected data from testing and verification to provide trending data, reliability growth opportunities, and implement a reliability-centered maintenance approach to sustaining long term performance of ground systems.

REFERENCES

[1] E. Staton, G. Cates, R. Finn, K. Altino, K. L. Burns, and M. D. Watson, "Use of DES Modeling for Determining Launch Availability for SLS," presented at the *AIAA SpaceOps Conference*, Pasadena, CA, 2014.

[2] A. M. Gillespie and M. W. Monaghan, "Allocating Reliability & Maintainability Goals to NASA Ground Systems," presented at the *Annual Reliability and Maintainability Symposium*, Orlando, FL, 2013.

[3] J. L. Gernand, A. M. Gillespie, and M. W. Monaghan, "Constellation Ground Systems Launch Availability Analysis: Enhancing Highly Reliable Launch Systems Design," presented at the *AIAA SpaceOps Conference*, Huntsville, AL, 2010.

[4] MIL-HDBK-470A, Designing and Developing Maintainable Products and Systems, Revision A, Department of Defense, 1997.

[5] W. D. Morris, N. H. White, C. E. Ebeling, "Analysis of Shuttle Orbiter Reliability and Maintainability data for Conceptual Studies," presented at the *AIAA Space Programs and Technologies Conference*, Huntsville, AL, 1996.

[6] B. S. Blanchard, D. C. Verma, "The Measures of Maintainability," in *Maintainability: A Key to Effective Serviceability and Maintenance Management*, New York, NY, USA: Wiley, 1995, pp. 88-113.

BIOGRAPHIES

Gisela Munoz *received a B.S. in Aerospace Engineering and a M.S in Human Factors & Systems from Embry-Riddle Aeronautical University in 2010 and 2013. Ms. Muñoz is currently a Reliability Engineer for the Ground Systems Development and Operations program with Red Canyon Software and Engineering. She also has experience in systems engineering and research for emerging technology prototypes in aviation, and ground operations and processing for crew systems with United Space Alliance.*

Jamie Toon *received a B.S. in Mechanical Engineering from Florida Institute of Technology in 2007 and a M.S. in Engineering Management from the University of Central Florida in 2011. Ms. Toon has worked at Kennedy Space Center for over 10 years and is currently the Lead Reliability Engineer for the Ground Systems Development and Operations program with Millennium Engineering & Integration. She also has substantial experience in systems engineering, including engineering and integration for ground support equipment with Lockheed Martin, operations integration and reliability engineering with Science Applications International Corporation, and ground operations and maintenance processing with United Space Alliance.*

Troy Toon *received a B.S. in Industrial Engineering from the University of Central Florida in 2013. Mr. Toon is currently pursuing an M.S. in Industrial Engineering, also from the University of Central Florida, with an expected completion in 2016. He is currently a Reliability and Simulation and Modeling Engineer for the Ground Systems Development and Operations Program with Millennium Engineering & Integration. He also has systems engineering and reliability analysis experience with Productivity Apex Incorporated.*

Timothy C. Adams *is a Senior Reliability Engineer for the Engineering Directorate at NASA's John F. Kennedy Space Center. He has been with NASA for over 28 years with 22 of these years in quantitative Reliability and related engineering assurance disciplines. He advocates and presents the reliability discipline to be understood and embraced by management and applied by systems, design and safety engineers. He is the technical editor for the KSC Reliability web site and supports the American Society for Quality (ASQ). He is an ASQ Certified Reliability Engineer (CRE) and participated in the ASQ committee to review the CRE exam. His education is in Mathematics, Competency-based Education, and General.*

David J. Miranda *has been with NASA and Kennedy Space Center (KSC) for nine years and is currently the Ground Systems Development & Operations (GSDO) Program's Operations Analysis Lead. In 2006 he received a B.S. in Aerospace Engineering from the University of Central Florida (UCF) and followed that in 2009 with a M.S. in Industrial Engineering, and a Masters in Business Administration also from UCF. He has worked on multiple discrete event simulation projects for the Constellation Program, led the Center's Spaceport Innovators group, been the lab manager for KSC Design Visualization, and project lead for KSC software development projects. More recently he has served as project manager for the Integrated Display and Environmental Awareness System (IDEAS) project under the Space Technology Mission Directorate's Game Changing Development Program.*