Initial Criticality Assessments to Guide FMEAs on Rocket Engine Hot Fire Testing

René Fernandez, NASA GRC
Jeff Riddlebaugh, Leidos, Inc.
Hugo Martinez, NASA JSC
Kevin Berry, SAIC (Science Applications International Corporation)

Key Words: FMEA, R&M Applications in Aerospace, Fault Tolerance and Safety Critical Systems

SUMMARY & CONCLUSIONS

Presented is an explanation of the use of the Initial Criticality Assessment (ICA) technique, a triage process for prioritizing required Failure Modes and Effects Analysis (FMEAs), for the European Service Module's main propulsion system's hot-fire test bed at White Sands New Mexico. Rather than instinctively performing many FMEAs of subsystems, or one large system level FMEA where every subcomponent is analyzed, the ICA guided an informed analysis of only the hardware that had a large impact to hazards. The low criticality hardware was documented via the ICA and no FMEA was performed; the work could then focus on the high criticality hardware. Thus a savings of Program resources was achieved. The experiences gained in creating these ICAs for this international collaborative project confirmed that the need for continuous communication across the technical teams is one of the greatest areas of emphasis.

1 INTRODUCTION

The European Space Agency (ESA) is developing the European Service Module (ESM), with its primary contractor, Airbus Defence and Space in Germany, for delivery to the National Aeronautics and Space Administration (NASA). The module will be equipped with a total of 21 engines to support NASA's Orion spacecraft: one U.S. Space Shuttle Orbital Maneuvering System-Engine (OMS-E), eight auxiliary thrusters and 12 smaller RCS (Reaction Control System) thrusters. The main ESM propulsion system, used for large translational maneuvers, consists of one OMS-E. Figure 1 shows an exploded view of the major Orion components. From right to left: the Launch Abort System (LAS), the Crew Module (CM), and the ESM. At the extreme left, or the bottom, of the ESM, is visible the single exhaust nozzle of the OMS-E.

To qualify the design of the ESM propulsion subsystem (PSS) an all-steel Propulsion Qualification Module (PQM) structure is used to test the propulsion systems on Orion, including "hot firing" of the OMS engine, thrusters, and RCS. The PQM has been developed as a hot-fire test bed to be tested at the NASA White Sands Test Facility (WSTF). One of the objectives of the testing is to assure that the OMS-E can be safely operated with the PQM. Testing will also demonstrate that the PQM can set the proper upstream pressures and temperatures for the OMS-E to operate nominally given the PQM has never been tested in hot-fire operation with OMS-E before. In order to safely conduct the test campaign, hardware such as the engine subassembly, fluid feed lines, valves, electrical power lines, instrumentation, stiff links, installation Ground Support Equipment (GSE) [1], and diffuser [whose objectives are to collect the exhaust of the OMS-E to actively cool down the exhaust gases, reduce thermal exchanges, and create a vacuum at OMS-E level before igniting], had to be analyzed for any hazards and failure modes.

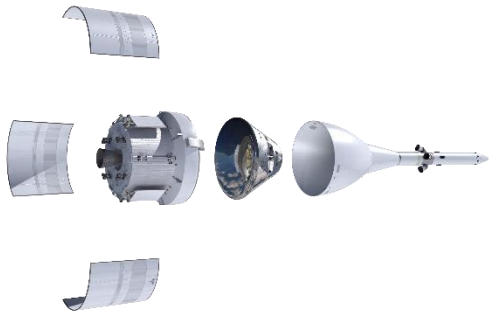

Figure 1: Orion Spacecraft Components Exploded View

As with most Manned Spaceflight vehicle development programs, the planned test schedule was impacted by multiple delays that limited the time available for analysis. This paper describes NASA's process, governed by the Multi-Purpose Crew Vehicle (MPCV) Program Requirements, for efficiently considering all failure modes of all flight hardware and Flight Critical GSE. Although the PQM Hot-Fire test campaign was a ground test campaign, the OMS-E Project performed the Safety and Reliability analysis to flight rigor, as well used an actual spaceflight asset, OMS-E SN-108, which has flown on

31 flights, and has accumulated a total of 162 burns and 4.01 hours of total burn time. A process called Initial Criticality Assessment (ICA) was used, similar to a triage process, in order to arrive at required FMEAs. The ICA allows for more efficient use of limited time by focusing the analyst's efforts on high criticality potential failures.

The goal of an Initial Criticality Assessment (ICA) for flight hardware, and flight critical GSE, is to assess each function, and to determine if loss or degraded performance of the function could result in: loss of life and/or loss of flight vehicle (Criticality 1); damage to a flight vehicle system; or Loss of Mission (Criticality 2) if not detected and corrected. The analyst then ranked the impact of that hardware on Safety and Reliability. Crit 1 and Crit 2 flight hardware and flight critical GSE on OMS-E then had detailed FMEAs created whereas Crit 3 (defined as all other failures not covered by Criticalities 1 and 2) hardware was not further analyzed for Safety and Reliability. Although the PQM test campaign was a ground test and not a space flight test, the high energy propellants had the potential for loss of a spaceflight asset (the SN-108 engine) in case of a catastrophic failure, as well as Loss of Mission because a major failure could potentially delay the planned launch date as well as the specific mission of the PQM Project. Figure 2 shows the relative size of the PQM as it is being installed in Test Stand 301 located at the WSTF

Figure 2: PQM Being Installed at WSTF TS-301

This paper summarizes the analysis process, presents actual ICA forms for the OMS-E hardware, for Crit 1, Crit 2, and Crit 3; and some selected (but not all) resulting FMEAs for the Crit 1 and Crit 2 categories. Also discussed are the lessons learned from the analysis and suggestions for improvements to the Reliability and Maintainability community.

2 ORION FMEA/CIL REQUIREMENTS

The Orion Program has a document [2] governing the development of Hardware Failure Modes and Effects Analysis/Critical Items List (FMEA/CIL). The objective of this document is to establish a consistent framework for uniform implementation of Failure Modes and Effects Analysis (FMEA) and Critical Items List (CIL) tasks for the Multi-Purpose Crewed Vehicle (MPCV) Program. To fulfill this objective, the document defines basic process, ground rules and assumptions, data fields, and terminology for performance of the FMEA/CIL tasks. The Prime Contractor and Government Furnished Equipment (GFE) Flight Projects shall develop the FMEA/CILs for their respective hardware. The OMS-E Project is one such GFE project within the Orion Program. The Program is responsible for FMEA/CIL methodology guidance, assurance that the FMEA specific design guidelines are adequately addressed, and the integration of the FMEAs with other Programs (such as Space Launch System [SLS] and Ground System Development & Operations [GSDO]) where effects or causes cross Program interfaces.

2.1 FMEA/CIL During the design and development phase

During the preliminary and detailed design phases, the purpose of the FMEA is to provide input to MPCV risk assessment and risk management activities and assist in assessing the MPCV design's compliance to design requirements. The CIL process was established to assure the advancement of necessary engineering hardware controls that are implemented and maintained (e.g., design features, tests, inspections, operations and process controls), which will ensure that the critical hardware will receive the proper focus to support the flight mission successfully.

During the design and development phase, when design criteria, mission requirements, and conceptual designs are being established, the FMEA is used to evaluate the design approach and to compare the benefits of competing design configurations. The FMEA provides a systematic identification of failure modes for evaluation and identifies potentially critical single failure points for possible elimination. The FMEA keeps pace with design cycles and requirements in order to maintain constant identification and tracking of potential critical failure modes.

The CIL serves as a tool to develop and document the engineering hardware controls that are implemented and maintained to assure that critical component failure modes are well understood and evaluated for proper control of risk.

2.2 FMEA/CIL During the *Operations Phase*

Once the design is baselined, the purpose of the FMEA/CIL is fundamentally changed. The FMEA/CILs, formerly tools for influencing design, now become tools for documenting the requirements needed to control causes of critical failure modes. Projects assess all design changes for impact to the FMEA/CIL as part of the design change evaluation. This is to assure that potential critical failure modes are not introduced without Program approval. If a design change eliminates a critical item, the FMEA for the item is updated. If the design change does not

eliminate the critical item, the CIL retention rationale are revised as necessary, and program acceptance documentation developed.

During the operations phase, the status of each CIL item and changes are reviewed and approved through the same process as the initial CIL. Projects provide a status of all CIL items as part of the Flight Readiness Review (FRR) process and as part of the Certification of Flight Readiness (CoFR).

2.3 Initial Criticality Assessment (ICA)

Projects perform an Initial Criticality Assessment (ICA) of the Flight Critical GSE that are transferred to NASA to assess each function and determine if loss or degraded performance of the function could result in loss of life, or damage to a flight vehicle system which could result in, worst-case, criticality category 1 or 2 failures in-flight if not detected and corrected prior to launch. This assessment is performed without regard to available redundancy. Standardized ICA forms are provided by the MPCV Program. For those functions determined to be non-critical, no further FMEA effort is required, but the Project retains the ICA performed on functions determined to be non-critical as part of the Program documentation. For those functions identified as critical or not covered by an ICA, the Project then performs a full FMEA/CIL analysis.

3 THE DEVELOPMENT OF OMS-E SPECIFIC ICA

It must be noted that the majority of the PQM testing at WSTF is Airbus directed on Airbus owned hardware. The OMS-E specific portion of the testing, also known as a "Passenger Test," is the one exception to this Airbus ownership. The OMS-E hardware is NASA property and the test conditions are NASA directed. Therefore the work split was as follows. For System Safety and Reliability analysis on the PSS, Airbus performed the Hazard Analysis (HA) and FMEAs. NASA WSTF performed the HA and FMEAs on the ground support and institutional facilities. But because the OMS-E is NASA owned hardware and Export Control restrictions prevent Airbus from knowing all the internal technical details of the engine, it was up to the NASA Project to perform the engine specific HA and FMEAs.

3.1 Ground Support Equipment and Test as You Fly

In developing ICAs specific to the OMS-E, an interface line was drawn between the engine and the Airbus propellant supply lines, mechanical interfaces, electrical power & signals, and instrumentation, as well as WSTF test instrumentation. From the OMS-Engine perspective, both, WSTF ground test instrumentation and Airbus instrumentation and supply lines were treated as Ground Support Equipment (GSE). Again, from the engine perspective, the instrumentation lines from WSTF as well as all the lines from Airbus are required supporting equipment for the OMS-E to function successfully.

NASA has a Test Like You Fly (TLYF) philosophy that requires a Project to conduct high fidelity ground tests that simulate not just the actual spaceflight hardware, but also the environments, test conditions, processes, and plans. Although MPCV 70043 only requires the performance of an ICA for "flight hardware and NASA developed Flight Critical GSE" it was decided to perform these ICAs for the PQM ground test campaign in order to conduct the analysis with "Flight Rigor" and to protect an actual flight test article, SN 108.

3.2 Ground Rules and Assumptions

Because an FMEA had been performed for the actual spaceflight mission [3], only the unique interfaces/environments of this PQM ground test article were analyzed via HA and FMEA. Philosophically, the work split can be viewed as: Airbus analyzed failures in their propulsion system, WSTF analyzed failures in their ground systems, and the OMS-E Project analyzed failure propagation at the interfaces with the engine.

With the above clarifications, the following ICA assumptions were in effect:

1. To be used to help analyze the effects of GSE failure during PQM Testing only on the OMS-E.
2. GSE failure cannot cause harm to anything but the OMS-E.

Each component may have had more component specific assumptions applicable to their ICA.

3.3 Analysis Documents and Process

Figure 3 shows a close up of many of the components that make up the PQM test article: supporting structure, harnesses, propellant tanks, Helium (He) pressurization tanks, feed lines, Auxiliary thrusters, RCS, etc. It's important to state that due to US Export Control Laws a full technical diagram for prints of the PSS and the OMS-E could not be included in this paper. In addition to PQM and test facility blueprints, the main document that was referenced was the OMS-E Delta Qualification Hot-Fire Test Plan [4]. This document contains engine subassembly details, electrical and mechanical interfaces, tables of instrumentation, engine firing sequence and facility purges, as

well as facility requirements.

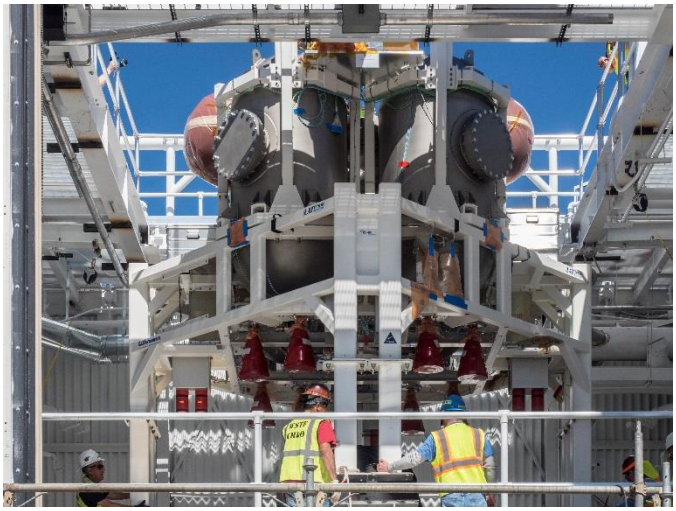

Figure 3: PQM Propulsion System Components

Similar to what is typical in the generation of FMEAs, the Analyst met with the engine Subject Matter Expert (SME) as well as the PQM SME multiple times to determine the Failure Modes and Failure Effects of the components being analyzed. After these and the associated criticality was determined, a larger team review of the draft ICA was conducted before it was finalized for release.

For those components that were ranked with a criticality of 3, see Figure 4 as a sample, no further analysis work was performed. The ICA was signed and kept by the Project as a formal record that due diligence was indeed performed in analyzing the Failure Modes of the specific component. Note that as in an FMEA, the Failure Modes and Failure Effects are identified, but no analysis relative to detection, corrective action(s), mitigations, etc. are performed. There is a field reserved for Rationale which can be used similarly to the Remarks or Comments field in many FMEAs. This Rational field clarifies that no harm to ground test personnel, engine, flight crew, or spaceflight mission would occur as a result of a failure, but only a loss of test data.

Hardware Name *OMS-E PQM GSE*
Date *07/27/2017*

Initial Criticality Assessment (ICA)

1	ITEM NAME:	Oxidizer Inlet Pressure Transducer	
2	ITEM PART NUMBER:	POI	
3	DOCUMENT/REPORT DATE:	07/10/2017	
4	FUNCTION: The GSE &/or ADS PQM hardware provides excitation voltage to and obtains data from the Oxidizer Inlet Pressure Transducer, which measures pressure in the oxidizer inlet line.		
5	GROUNDRULES/ASSUMPTIONS: • The excitation of and output acquisition and processing for the Oxidizer Inlet Pressure Transducer is performed by GSE &/or ADS PQM hardware equipment. • GSE failure cannot cause harm to anything but the OMS-E. • This ICA is to be used to help analyze the effects of GSE &/or ADS PQM hardware failure during PQM Testing only on the OMS-E. • Connectors and wire/cabling within the Secondary Flight Instrumentation Harness is considered part of this instrumentation function.		
6	FAILURE MODES: a) Failure to provide excitation voltage to transducer b) Failure to respond correctly to transducer output		
7	FAILURE EFFECTS: a) Failure to provide excitation voltage to transducer: incorrect voltage from GSE or open circuit. No pressure data from the oxidizer inlet line would be recorded. No harm is caused to personnel, engine, or mission. b) Failure to respond correctly to transducer output: the transducer provides a signal to the GSE but the GSE does not properly track it. Incorrect pressure data from the oxidizer inlet line would be recorded. No harm is caused to personnel, engine, or mission.		
8	CRITICALITY CATEGORY:	3	
9	DETAILED FMEA REQUIRED:	No	
10	RATIONALE: • No failures will harm test personnel, engine, crew, or mission. • Failures only result in loss of data. • This transducer is redundant as GSE transducer upstream of the engine will detect over-pressurization of oxidizer inlet line.		
11	Jeffrey Riddlebaugh	*Signature On File*	216-433-5839
	PREPARED BY (printed)	PREPARED BY (signature)	PHONE NO
12	CONCURRENCES:		
	Brian Reed		
	SUBSYSTEM MANAGER (printed)	SSM SIGNATURE	DATE
	Rene Fernandez	Rene Fernandez	07/10/17
	SAFETY AND MISSION ASSURANCE (S&MA) (printed)	S&MA SIGNATURE	DATE
14	APPROVALS:		
	CHAIR (printed)	CHAIR SIGNATURE	DATE

JSC Form 1300 (Rev April 26, 2000) (MS Word September 1999)

Figure 4: Sample ICA for a Pressure Transducer

4 ICA REQUIRING FMEA

Those components that were ranked with a criticality of 1 required a full FMEA be performed. As an example, because of the potential of propellant leakage causing a fire or explosion in a high value test facility and test equipment, Figure 5 shows one of the Crit 1 ICAs. Note that the Rationale field makes clear that although this is a ground test, and thus no spaceflight crew or mission would be lost, the potential damage to the facility, equipment, and ground crew is what makes this a Criticality 1 failure.

Once this Fuel Feed Line Interface Flange was identified as being a Crit 1 ICA, the analysis team immediately set out to determine if a new dedicated FMEA was required, or if this Failure Mode was covered in one of the existing Program FMEAs (there are: Spaceflight Mission, Test Facility System, & PQM PSS FMEAs). The team determined that this particular Failure Mode and Failure Effect was not covered by the NASA created Spaceflight Mission and Test Facility FMEAs.

Since the PQM PSS FMEA was owned by Airbus Defence and Space, and was being developed concurrently to the ICA analysis, the NASA Reliability and Maintainability (R&M) team held a telecom with the Airbus R&M team to determine if this Failure Mode and Failure Effect in this ICA was covered. The detailed review of the Airbus PQM PSS FMEA revealed that indeed it was addressed and thus a new NASA FMEA would not be required.

Hardware Name: *OMS-E PQM GSE*
Date: *07/27/2017*

Initial Criticality Assessment (ICA)

1	ITEM NAME:	Fuel Feed Line Interface (Flange)	
2	ITEM PART NUMBER:		
3	DOCUMENT/REPORT DATE:	07/10/2017	
4	FUNCTION: Delivers propellant fuel from the PQM Test Article to the OMS-E Fuel Inlet port.		
5	GROUNDRULES/ASSUMPTIONS: • Fuel Feed Line is ADS PQM hardware. • Fuel Feed Line failure cannot cause harm to anything but the OMS-E. • This ICA is to be used to help analyze the effects of GSE &/or ADS PQM hardware failure during the PQM Testing Campaign only on the OMS-E. • Connection hardware is considered part of the line. • Filling the line with fuel is upstream of the interface and will not be discussed in this ICA.		
6	FAILURE MODES: a) Failure to maintain pressure b) Failure to contain fuel c) Routing failure		
7	FAILURE EFFECTS: a) Failure to maintain pressure: a constriction or incorrect geometry in the line causes a pressure drop. Fuel will not flow as intended through the line. Sufficient pressure drop would lead to chamber pressure or fuel injector temperature redlines to shut engine down. Otherwise test results may be skewed. Poses no immediate threat to personnel, mission, or test article. b) Failure to contain fuel: line leaks, cracks, or bursts. Pressure drop would lead to chamber pressure or fuel injector temperature redlines to shut engine down. Structural failure of line will release fuel into test chamber where it could cause fire or explosion damaging test article or equipment and potentially harming test personnel. c) Routing failure: excess load exists at the connection site of the engine and fuel feed line. The fuel feed line may impart a torque on the engine side of the interface, potentially damaging the engine.		
8	CRITICALITY CATEGORY:	1	
9	DETAILED FMEA REQUIRED:	Yes	
10	RATIONALE: • Worst case failure is fuel leak into chamber creating hazards to safety and equipment. This is also a criticality 1 failure for test facility. • No harm to crew or mission should occur.		
11	Jeffrey Riddlebaugh	*Signature On File*	216-433-5839
	PREPARED BY (printed)	PREPARED BY (signature)	PHONE NO
12	CONCURRENCES:		
	Brian Reed		
	SUBSYSTEM MANAGER (printed)	SSM SIGNATURE	DATE
	Rene Fernandez	Rene Fernandez	07/10/17
	SAFETY AND MISSION ASSURANCE (S&MA) (printed)	S&MA SIGNATURE	DATE
14	APPROVALS:		
	CHAIR (printed)	CHAIR SIGNATURE	DATE

JSC Form 1380 (Rev April 26, 2000) (MS Word September 1999)

Figure 5: Sample ICA for the Fuel Feed Flange

5 LESSONS LEARNED

Multiple lessons were learned as a result of this analysis work. One is that because of the inevitable compression of available analysis time available prior to the start of major ground test campaigns, the use of a screening method (such as ICA) to triage the high hazard impact FMEAs from those with lower impacts is necessary. Another Lesson Learned was the need to clearly state the ground rules and assumptions driving the ICA and FMEA studies. There were multiple times where the ICA failure effects and criticality were changed due to updates to the driving ground rules and assumptions.

The need for continuous communication in an international collaborative project such as this is perhaps the most important lesson. As mentioned above, the R&M analyst updated the ICA Failure Modes and Effects, as well as Criticalities based on multiple meetings with the Subject Matter Experts (SMEs) as the PQM PSS was being developed and better understood. Although mostly out of NASA's control, a more timely review of the Airbus provided PQM PSS FMEA may have negated the need for a last minute international telecom to determine if the Failure Mode and Effect identified in the ICA was covered.

REFERENCES

1. "Standard For The Design And Fabrication Of Ground Support Equipment," NASA-STD-5005C.
2. Orion Multi-Purpose Crew Vehicle (MPCV) Program Hardware Failure Modes and Effects Analysis/Critical Items List (FMEA/CIL) Requirements Document, MPCV 70043 Revision B, June 10, 2015.
3. Failure Modes and Effects Analysis For Orbital Maneuvering System – Engine (OMS-E), E&TS-2014-001.
4. Multi-Purpose Crew Vehicle (MPCV), OMS-E Delta Qualification Hot-Fire Test Plan, EIO-PLN-0014 Revision A, February 8, 2017.

BIOGRAPHIES

René Fernandez
Program and Project Assurance Division
MS 86-1 NASA Glenn Research Center
21000 Brookpark Road
Cleveland, Ohio 44135, USA

e-mail: rene.fernandez-1@nasa.gov

Rene Fernandez earned his BS, MS, and did Doctoral work in Mechanical and Aerospace Engineering from Case Western Reserve University. Currently, he is the SMA Lead for the OMS-E/TVC Project at the Glenn Research Center in Cleveland. Previously, he served as the CoNNeCT SMA Team Lead, the GRC Reliability Engineer on the ASRG (Advanced Stirling Radioisotope Generator) project, and performed wind tunnel and flight research on air-breathing propulsion systems. Mr. Fernandez has published over 25 technical papers on the research he has been involved with.

Jeff Riddlebaugh
Leidos Inc.
MS 162-1 NASA Glenn Research Center
21000 Brookpark Road
Cleveland, Ohio 44135, USA

e-mail: jeffrey.m.riddlebaugh@nasa.gov

Mr. Riddlebaugh earned his BS degree in Electrical Engineering from the University of Michigan and MS degree in Electrical Engineering from the Ohio State University. From 1974 to 1987 he did electronic development and design work for RCA Corp., Gould Inc., and Goodyear Aerospace Corp. Since 1987 he has provided Safety and Mission Assurance Engineering support to the NASA Glenn Research Center while employed by Analex Corp., Raytheon Corp., Science Applications International Corp., ARES Corp., and Leidos Inc. His work during this period has been primarily in the disciplines of electrical, electronic and electromechanical parts engineering and reliability engineering.

Hugo Martinez
Division NC311
NASA Johnson Space Center
2101 NASA Parkway

Houston, TX 77058, USA

e-mail: hugo.e.martinez@nasa.gov

Hugo Martinez is the Crew and Service Module Propulsion SMA Lead at the Johnson Space Center in Houston. He performed System Engineering and Integration for several unmanned future projects, such as the lunar water extraction mission, RESOLVE, future habitat MMSEV, and demonstration of a retrorocket descent technology for manned Mars entry and descent (PDC). Prior to that, he served as Shuttle Propulsion team lead in the areas of System Engineering and Safety and Mission Assurance at the Johnson Space Center in Houston from 1990 to 2011. Previously, he supported the Shuttle Program as a Cryogenics Engineer at the Kennedy Space Center in Florida. He has a BS in Mechanical Engineering from the University of Texas at Austin, and an MBA from the University of Houston-Clear Lake.

Kevin Berry

SAIC Inc.
NASA Johnson Space Center
2450 NASA Parkway
Houston, TX 77058, USA

e-mail: kevin.s.berry@nasa.gov

Kevin Berry is a Safety and Reliability Engineer for SAIC under Contract to the NASA JSC.
Kevin Berry is a Safety and Reliability Engineer for SAIC under Contract to the NASA JSC. He has a BS in Mechanical Engineering from Colorado State University, and an MBA from Regis University. From 1988 to present, he has performed safety, reliability, and quality assurance tasks for Space Shuttle, Commercial Orbital Transportation System, and Commercial Crew Programs. These include Failure Modes and Effects Analysis, Hazard Analysis, and Quality Engineering. Currently, he is the SAIC lead for the OMS-E/TVC Project at JSC.