Human Reliability Assessments: Using the Past (Shuttle) to Predict the Future (Orion)

Diana L. DeMott, Sr. PRA/HRA Analyst, SAIC

Mark A. Bigler, CRE, Sr. PRA Analyst, NASA

Key Words: Human Reliability, PRA, HRA, Risk Assessment

SUMMARY & CONCLUSIONS

NASA (National Aeronautics and Space Administration) Johnson Space Center (JSC) Safety and Mission Assurance (S&MA) uses two human reliability analysis (HRA) methodologies. The first is a simplified method which is based on how much time is available to complete the action, with consideration included for environmental and personal factors that could influence the human's reliability. This method is expected to provide a conservative value or placeholder as a preliminary estimate. This preliminary estimate or screening value is used to determine which placeholder needs a more detailed assessment. The second methodology is used to develop a more detailed human reliability assessment on the performance of critical human actions. This assessment needs to consider more than the time available, this would include factors such as: the importance of the action, the context, environmental factors, potential human stresses, previous experience, training, physical design interfaces, available procedures/checklists and internal human stresses. The more detailed assessment is expected to be more realistic than that based primarily on time available.

When performing an HRA on a system or process that has an operational history, we have information specific to the task based on this history and experience. In the case of a Probabilistic Risk Assessment (PRA) that is based on a new design and has no operational history, providing a "reasonable" assessment of potential crew actions becomes more challenging.

To determine what is expected of future operational parameters, the experience from individuals who had relevant experience and were familiar with the system and process previously implemented by NASA was used to provide the "best" available data. Personnel from Flight Operations, Flight Directors, Launch Test Directors, Control Room Console Operators, and Astronauts were all interviewed to provide a comprehensive picture of previous NASA operations. Verification of the assumptions and expectations expressed in the assessments will be needed when the procedures, flight rules, and operational requirements are developed and then finalized.

1 INTRODUCTION

NASA has been a pioneer in space since its inception and is committed to managing the risks inherent in developing and employing new technology in space. Early implementation of risk reviews and assessments (including: Hazards Analyses, FMEA, PRA, HRA, design reviews, et.al.) in the design phase is intended to improve safety and reduce costly re-works by finding major risk contributors that can be eliminated or mitigated early in the process. However, there are challenges in implementing methodologies originally intended to assess the risk profile for a completed functional operation.

During the process of performing a PRA, the actions of humans associated with the systems and equipment failures are often identified late in the process. Having sufficient information available to determine the potential risks of human errors associated with these failures is generally based on a combination of information available, experience, judgment and assumptions. The less information available to perform an assessment, the greater reliance on using assumptions to supplement the information needed to arrive at a reasonable evaluation of risk.

2 THE PAST – SHUTTLE PROGRAM (1981-2011)

NASA has experience with manned spaceflight since its' first manned mission in 1961. The wealth of knowledge and experience culminating with the Shuttle program and current International Space Station (ISS) operations provides NASA with a unique position of having over 50 years of experience with getting humans to space and exploring there. This also provides NASA with a proven track record for:

- Developing training programs (crew, console, operations and ground support)
- Implementing consistent process and program reviews and technical assessments
- Developing assessment criteria and methods to analyze and assess capabilities and safety
- Providing information and support before, during and after a mission

2.1 History

By the end of the Shuttle program, common practice for NASA programs and missions was to perform extensive pre-planning and training of crew and control console operators prior to flight. Extensive mission planning for training requirements, qualification requirements, simulator experience, process development, procedures and flight rules was completed and implemented after being thoroughly vetted by NASA Launch and Flight Operations. These tasks were performed years before the first flight and routinely updated as flights occurred. This resulted in Crew and console operators having predetermined, well defined roles and actions governed by procedures, checklists and flight rules.

Probabilistic Risk Assessment (PRA) and Human Reliability Analysis (HRA) were introduced into the NASA culture in the late 1980s [1]. The Shuttle PRA/HRA was a living analysis with multiple iterations to assess and document the design changes, system modifications, new assessments and other changes that occurred during the life of the program. The PRA was developed and subsequent changes made following the guidelines set out in the Probabilistic Risk Assessment Guide for NASA Managers [2] and provided the basis for the methodology used and application of the concepts for use in assessing human reliability for NASA missions [3]. The concepts used to develop the methodology were based on the Nuclear Regulatory Commission's (NRC) Technique for Human Error Reliability Prediction (THERP) methodology [4] for the basic screening process and Cognitive Reliability and Error Analysis Method (CREAM) [5] for the more detailed assessments. These generic concepts were adapted to better reflect the differences inherent in NASA missions and capabilities. These practices were also augmented to reflect the uniqueness of the Shuttle program [6].

2.2 Overview of the HRA Process:

HRA is used to identify and quantify Human Error Probability (HEP) events based on the design and operation of the space craft and launch support capabilities. The information is provided to design and operations personnel for use in identification of ways to eliminate, mitigate or reduce the calculated HEP. The assessment is intended to describe, both qualitatively and quantitatively, the probability of human errors which could cause system or operational failure. By performing these assessments which model human actions with their corresponding failure in a PRA, a more complete picture of the risk and risk contributions can be shown.

The first step in the process is to review the human actions and interactions needed to perform the task. For screening purposes, a matrix of "Time Available" versus "Performance Conditions" is used to identify a generic (or screening) risk value. The screening values should be conservative. The HRA performed will continue to evolve as additional information regarding time available, design specifics, training requirements, environmental conditions, stress, complexity of actions, familiarity with tasks and other associated factors becomes available. This is an iterative and collaborative process which continues throughout the program life. The overall probability of failure is based on a combination of human errors needed to produce a failed task and the probability that the individual will commit these errors.

Figure 1 provides a simplified flowchart of the process NASA JSC S&MA uses to perform a quick and conservative screening assessment of identified human errors which will later be followed by a more detailed assessment of those human actions that are higher risk contributors to the overall risk for crew or mission. Using an initial screening technique provides a quicker turn-around time for an initial assessment and a more efficient use of resources.

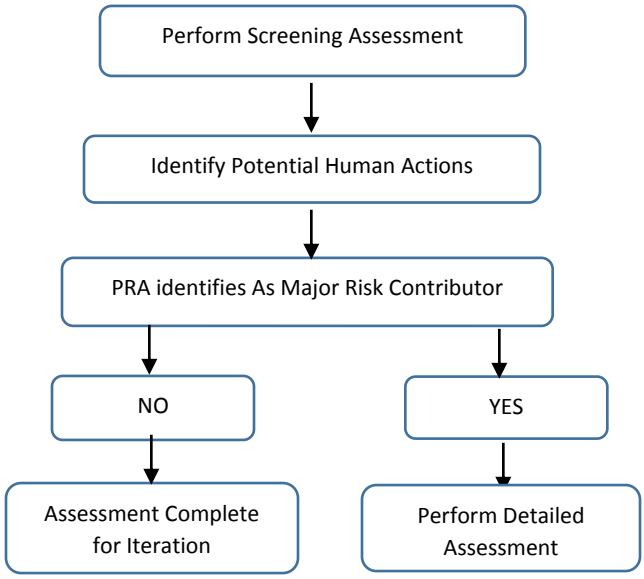

Figure 1 Simplified Flowchart of NASA HRA Process

An overview of the methods used to perform a "screening" assessment and a more "detailed" assessment are described below.

2.3 Screening/Simplified Methodology

The majority of human actions identified as having the potential to contribute to defined failure criteria for Loss of Crew (LOC) or Loss of Mission (LOM) metrics, are initially quantified with an analysis methodology that is based on THERP, as described in the Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278 (4). For screening purposes, a matrix of "Time Available" versus "Performance Conditions" is used to identify a generic (or screening) risk value. The screening values are expected to

provide a relatively quick and conservative method to identify risk-dominant human errors. The goal of a screening evaluation is to identify high risk actions or activities and determine human error risk contributions. The task analysis involves identifying the steps of the procedure and assessing the probability that a step may be incorrectly carried out, or identifying erroneous actions that can directly lead to LOC or LOM. Using an initial screening analysis should provide a relatively quick and inherently conservative value so that lack of detailed modeling does not lead to underestimation of the risk.

Types of human actions modeled include those required for normal operation of a system. In general, recoveries and work-arounds are only modeled if the scenario becomes dominant in the risk profile. Recovery actions modeled would only include those actions that if not performed correctly could directly contribute to LOC/LOM.

Screening methodology based on modified THERP are used for the initial assessments based on the following considerations:

- Limited human interaction and tasks, less complex situations or more benign failure results
- Uses less detailed information
- Time to complete
- Task complexity
- Environmental factors, stress, familiarity, etc.
- Uncertainty

2.4 Detailed Methodology

A more detailed assessment provides a better understanding of which elements cause or contribute to the identified risk of human error; providing a basis for validating the risk and potentially influence future actions to eliminate or mitigate the risk. Human errors that are large risk contributors to overall failure are evaluated using a version of the methodology described in CREAM [5]. These assessments are generally performed when sufficient information is available.

CREAM, developed by Erik Hollnagel, expands on THERP by considering the effects of performance assessment shaping factors such as:

- Effectiveness of procedures for limiting or encouraging errors
- Familiarity and experience with process, procedures and equipment
- How the environment affects the potential for human errors to occur
- How personnel physical and mental stresses affect performance
- How personnel react as complexity increases

The technique described in the book was modified to include aspects from THERP regarding dependency and uncertainty models since CREAM did not address those areas. Using a modified CREAM methodology provided more precise human error probability estimates using more specific task data and detailed task analysis. This modified CREAM based method was used for the Shuttle PRA.

2.5 Why this worked for Shuttle

When the initial HRA assessments were performed for the Shuttle program, there was a wealth of knowledge and experience documented in the lessons learned, operating experience, incident reports, flight rules, crew task analysis documents, process documentation, training records and operating procedures. Having information from years of experience introduced a large amount of material on crew tasks to review, with the understanding that only a few would eventually be identified as major risk contributors. The two step methodology was selected to fit the need. This process used the quicker and less resource intensive initial screening evaluation followed by a more detailed analysis, which was only performed as needed, providing an effective use of resources without compromising the final product value.

3 The Present: Orion Vehicle (2016)

In general, HRA is performed on existing processes and equipment. This means that the information used to develop the assessment is based on equipment that exists, and has detailed designs and schematics available, as well as real world experience regarding human actions and interactions. Procedures and processes are available and often have been in effect for some time. Training, lessons learned, previous errors, and problems affecting human reliability are available and can be accessed.

Performing an assessment of human error for a project or program in the design phase provides a host of challenges since the program is expected to continue to evolve as additional information regarding time available, design specifics, training requirements, environmental conditions, stress, complexity of actions, familiarity with tasks and other associated factors evolve throughout program development and implementation. This is an iterative and collaborative process where some aspects can become very fluid. Even with these types of challenges, performing a PRA/HRA during the design phase can provide valuable information on potential areas for improving the risk profiles before design changes become more costly. Early use of these risk methodologies can provide Program management with additional information regarding risk and risk drivers during different design and production stages which can influence changes that clarify or reduce risks and add to the information available for management decisions regarding design and operational changes. The PRA can also be used to determine if the program is meeting risk based requirements.

3.1 Current Situation – Critical Design Phase

Initial PRAs for the various elements of the Orion program are performed years prior to actual mission launch. There is limited information available to use in performing a human event assessment during the design phase. Early program documentation can include: preliminary design information, mission requirement documents, and design requirement documents. Information available from previous human space programs includes: previously documented operational experience, previous knowledge and understanding of ground personnel support and crew experience.

Identifying the human actions that can lead to failure under identified failure scenario conditions is challenging, given the lack of physical systems, procedure, flight rules, displays and control equipment which do not exist in early design phases. The PRA in these early stages is based on identified failure scenarios. Assumptions made for these failure scenarios identify if human actions are needed to support success. Identifying how humans can cause failures under the myriad of variables at this point is more difficult.

The results from these human error assessments can provide input to determine overall project risk, and assess resulting risk severity. The results of these preliminary assessments are intended to be conservative values which incorporate uncertainty involved with attempting to predict potential events and scenario development with notional information.

3.2 Using NASA Program and Organizational Experience

Although designs and technology can change radically, basic human tasks and actions, and the conditions surrounding their performance are unlikely to change if the organizational processes and policies are the same. Assuming this concept as the starting point, the analyst can predict the most likely human actions and human reliability for a similar scenario.

Since NASA has been performing launches and operating space vehicles for years, it is reasonable to use previous NASA programs and performance to predict NASA personnel training and reactions during similar situations or scenarios. NASA's approach for mission preparation includes a thorough review of all design information, studies, and assessments by operations and support staff to identify crew activities and necessary actions well before mission specific training begins. Identification and completion of plans and procedures for normal operations and contingency plans and procedures for potential problems and failure scenarios are developed for crew use in training and during the mission. For unidentified scenarios that arise during the mission, the ground support staff assesses the situation and provides plans and guidance to address the problem. Organizational support for the crew includes teams of experienced, effective and knowledgeable individuals who can cover any questions related to design, operations and anticipated crew environment and conditions. Support and monitoring is available continuously, with experts on call.

Many of the conditions that may affect crew performance have been experienced before by previous crews. These would include: ascent and descent G-forces, weightlessness (movement, tools, materials), limited space, life support requirements (heat, cold, air, water, etc.), maintenance and monitoring tasks, spacesuit/flight suits, communications equipment, emergency exit conditions, limited access to equipment or components, visors restricting vision, deluge during emergency egress, waiting for recovery after landing, etc. Although each mission phase has different working conditions to address, general situations and conditions will be similar to past experience even though the specific initiating events may differ.

NASA astronauts have a shared background of training, studies and mission preparation. Specific crew members are selected for their ability to work together, and have trained together for a year or more prior to any mission. Support personnel include teams of experienced, effective and knowledgeable individuals who provide a cohesive support team for each mission.

Since this is an exceedingly specialized group of individuals in a highly regimented environment, future operations are not expected to fundamentally change how people perform under the stated conditions. Our solution has been to consider using the years of previous experience that NASA has for crewed vehicle operations, and assume that future training, processes, procedures and operations will conform to the same rigorous standards and be equally effective during future operations. For normal operations, planning prior to a mission should have identified processes and procedures for situations.

3.3 Performing the Assessment

For a predictive HRA, certain basic assumptions are needed as a starting point. These include the assumption that adequate planning for operations, procedures, and human factors designs (displays and controls, spacesuits and other equipment) have been performed and cover known situations adequately. Also, that crew and operations personnel actions and activities have been identified and rigorously reviewed to ensure that adequate planning has occurred for crew safety and mission success. Based on past performance, the assumption that NASA personnel are extensively trained and adequately prepared for the tasks expected of them can also be made. The same methodology developed during the Shuttle program (as well as Apollo) and adapted as needed in the program design phase, is used in the human reliability assessments during the different phases of the current Orion program, including the use of an

initial screening assessment followed by a more detailed assessment for higher risk contributors.

3.3.1 Screening Assessment

In the case of the Shuttle program, the intent was to review human actions performed to determine which actions contributed to safety and mission risk, and to what extent. Although the number of tasks to review was large, these tasks were specific and documented. Trying to identify all possibilities for human error during a mission during the design phase is neither productive nor realistic. Given the generic nature of the failure scenarios, a variety of potential actions can be postulated that could affect failure risk. Many of these could be eliminated based on specific equipment design, adequate training or during procedure development. Therefore, the focus is narrowed to those actions that are integral to the failure scenario which can be identified in early risk assessments. These encompass only the specific task or action that a human must perform to achieve success in the postulated failure scenario. The result identifies fewer human error events for inclusion at this early stage of the program.

The methodology used for this screening assessment is based on THERP which accounts for variable factors such as time available, dependency and working conditions. This type of screening assessment allows an analyst to provide a HEP based on less detailed information in a shorter period of time. However, the HEPs tend to be more conservative and may not accurately identify the risk due to the lack of information available for the assessment.

3.3.2 Detailed Assessment

For this phase, human error events identified as major risk drivers are considered in more depth, and a detailed assessment is performed using details provided by "domain" experts. Additional information is gained through interviews with subject matter experts (Astronauts, Flight Operations, systems analysts, etc.) for specific failure scenarios to identify cognitive functions for tasks and Common Performance Conditions (CPCs), also called Performance Shaping Factors (PSFs), which affect human performance. Based on scenario development, the CPCs may be different for each task or action performed. These CPCs show the influence (positively or negatively) to the risk of human error for the defined task under these defined conditions. A value for "nominal" generic conditions is used as a starting point, and is transformed into a value associated with a particular task or action using nine CPCs.

These CPCs are based on those described in Reference 5 and include: Adequacy of Organization, Working Conditions, Adequacy of Man-Machine Interface (MMI) & Operational Support, Availability of Procedures/Plans, Number of Simultaneous Goals, Available Time, Time of Day (Circadian rhythm), Adequacy of training & Preparation and Crew Collaboration Quality. For identified human error events, this is an iterative process as additional information is developed and available.

4 The Future – Challenges and Solutions

In order to provide a "reasonable" assessment, assumptions are made based on previous NASA programs and performance, as well as current program documents and requirements. Using the same PRA assumption that these are "mature" flight estimates, implies all planning, process and procedures would have been thoroughly vetted and revised to perform as desired. Changes to design, policy, procedures and training should be generated based on the assessments to lower the risk of occurrence of human errors. These types of changes can assist in lowering the potential error or failures resulting from human actions in the final design.

HRA development during preliminary design and reviews need to address the following challenges:

Problem	Why this a problem	Solution	Acceptability
Available Information	Concept and requirement documents allow multiple paths for success and limits available specifics.	Using past experience	For the areas identified, it is unlikely that NASA operations will change what years of development and experience have shown as effective.
Identify potential failure significant human error	Multiple ways to cause failure based on many different permutations of events (too many "what ifs").	Using past experience identify single action that would cause failure.	At this point in program, the risk values are high level estimates, so using the human action that must occur for success or failure provides a reasonable estimate.
Manpower/ Resources	Always limited.	Screening vs. detailed	Concentrating on high risk contributors is more effective use.
Assumptions	• Consistency between programs • Reasonableness • Most probable development of events	Using past experience	Provides basis for rationale and results.
How conservative	Major risk contributors need to be defensible to ensure resources versus reward	Screening vs. detailed	Each method provides conservative risk estimates.
Using the Results	Interpretation.	Integrate into program reviews.	Inform management and reviewers of potential risk concerns.

Table 1 Summary of Challenges and Potential Solutions

This is a starting point and is expected to evolve through a number of iterations as the project matures and changes. The use of assumptions and surrogate data provides a place to start, but can only be proven correct or appropriate as assumptions become reality. Any changes or modifications in design, process or procedure can affect the results of an assessment. These rationales are based on NASA's unique history and experience and some aspects may not apply to other industries.

5 References

1. Safie, F.M., Stutts, R.G. and Z. Huang, 'Reliability and Probabilistic Risk Assessment- How They Play Together"

2. Stamatelatos, Michael et.al, *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners*, NASA Office of Safety and Mission Assurance, NASA Headquarters, (2011), Washington. D.C.

3. Boyer, R., Stewart, M., Cross, R. and Turner, J., *Space Shuttle Probabilistic Risk Assessment Overview,* 2006 PSAM

4. Swain, A. D. & H. E. Guttman, "*Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*", *NUREG/CR-1278 (1983),* Washington D.C.

5. Hollnagel, E., *Cognitive Reliability and Error Analysis Method: CREAM*, (1998), Elsevier.

6. Hamlin, T., Canga, M., Boyer, R. and Thigpen, E., *2009 Space Shuttle Probabilistic Risk Assessment Overview*, 2010, ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20100005659.pdf

BIOGRAPHIES

Diana L. DeMott – Sr. HRA/PRA Analyst
SAIC
2450 NASA Parkway
Houston, Texas 77058 USA

e-mail: diana.l.demott@saic.com, diana.l.demott@nasa.gov

BS Nuclear Engineering and MBA, began working career in the nuclear power industry with positions that included: systems engineer, licensing engineer, system safety and PRA specialist. Tasks included: trend analysis, root cause analysis, FMEA, project management, risk assessment and prioritization, auditing, development of specifications and requirements, equipment reliability and probabilistic risk assessment (PRA). Moving out of the nuclear arena, worked as a consultant for clients such as GE and CSX providing services in the area of quality improvement (QI) techniques and facilitation. Moving to Houston, entered the Aerospace industry as a Senior PRA Analyst working on NASA's Johnson Space Center (JSC) Safety & Mission Assurance (S&MA) contract with tasks that included review and development of fault and event tree models based on mission and system design, development of human reliability assessments for Shuttle and development of PRA models in 2012 for a conceptual Mars Mission. Currently works for SAIC supporting an integrated Orion mission PRA and developing HRA assessments for flight crews and flight operations personnel expected to operate the next manned NASA missions. Member of SRE and an AIAA standards committee member.

Mark A. Bigler, CRE
Sr. PRA Analyst, Integrated Aborts PRA Lead
National Aeronautics and Space Administration
Safety & Mission Assurance Directorate
Johnson Space Center
2101 NASA Parkway
Houston, Texas 77058 USA

E-mail: mark.bigler-1@nasa.gov

B.S. in Electrical Engineering from New Mexico State University and an M.S. in Nuclear Engineering from Texas A&M University. Began career serving four years as an officer in the Nuclear Navy. Served aboard the USS California (CGN-36) as a Mechanical Division Officer and later as an Electrical Division Officer. Also served as an Engineering Watch Officer responsible for overseeing operations of nuclear propulsion plants. After completing naval tour, joined the reliability engineering group at the Houston Light & Power South Texas Project Nuclear Plant for three years. Later entered the aerospace industry as a reliability analyst for Lockheed Martin in the system safety group, responsible for performing failure mode effects analysis and hazard analysis on several projects. After leaving Lockheed Martin, worked for SAIC almost 10 years. During that time, responsible for several Shuttle system PRAs. In last two years at SAIC, served as PRA Analyst Technical Lead. In that role, oversaw a PRA team that updated the Shuttle PRA and started development of Constellation and Orion PRA models. Joined the NASA JSC S&MA Analysis Branch in November 2007. Led efforts to develop an EVA PRA for the Hubble servicing mission and range safety PRAs for Ares 1-X and PA-1 flight tests. Currently responsible for risk analyses related to integrated aborts. Also support efforts related to PSA for the Commercial Crew Program. In 2005, became a Certified Reliability Engineer.