DEFINING RELIABILITY AND ROBUSTNESS FROM A HUMAN FACTORS PERSPECTIVE

Alan Hobbs[(1)], John O'Hara[(2)], Bernard Adelstein[(3)] & Cynthia Null[(4)]

[(1)] San Jose State University/NASA Ames Research Center, Moffett Field, CA, USA. alan.hobbs@nasa.gov
[(2)] Brookhaven National Laboratory, Upton, NY, USA. ohara@bnl.gov
[(3)] NASA Ames Research Center, Moffett Field, CA, USA. bernard.d.adelstein@nasa.gov
[(4)] NASA Langley Research Center, Hampton, VA, USA. cynthia.h.null@nasa.gov

ABSTRACT

A human factors team was tasked with assessing best practices for developing a crewed space vehicle that is both reliable and robust. The team identified two broad dimensions of human factors relevant to reliability and robustness, namely, the attributes of the product, and the processes used to develop the product. The "product" includes hardware, software, documentation, training systems, and procedures throughout all phases of the system life, including construction, testing, operation and maintenance. Three key attributes of the product are the extent to which task demands are within human capabilities, the capacity of the system to cope with human error, and the ability of the system to make use of unique human capabilities during non-routine situations. The "process" dimension of human factors relates to the human systems engineering program that starts in the early stages of design, and continues throughout the life of the system. There are, of course, no guarantees that a formal consideration of human factors throughout the design process will identify all the relevant human issues. However, in the absence of such a consideration, problems are virtually assured.

1. INTRODUCTION

NASA Procedural Requirements document 7120.5E defines a system as: "The combination of elements that function together to produce the capability required to meet a need. The elements include all hardware, software, equipment, facilities, personnel, processes, and procedures needed for this purpose" [1]. Thus, humans, not only as the flight crew, but also as designers, manufacturers, and ground support are considered part of the spacecraft system. The system qualities of reliability and robustness have been a focus of attention in recent years, yet it is not clear how to evaluate these qualities in a system.

In 2006, the Astronaut Office at NASA Johnson Space Center (JSC) requested that the NASA Engineering and Safety Center (NESC) assess best practices for developing a crewed space vehicle that is both reliable and robust. For the purposes of this assessment, the NESC defined reliability as being "free of failures throughout its mission" and robustness as "tolerant of unexpected conditions should they arise". The NESC assigned various teams to the range of spacecraft subsystems including propulsion, structures, avionics, software, and the human element. In each case, teams were asked to consider how reliability and robustness can be achieved. The conclusions of the human factors team are briefly summarized in this paper. It is no simple matter to evaluate the impact of the engineered elements of the system, such as avionics, structures and software, on reliability and robustness. More complex still is how to define the meaning of reliability and robustness in terms of human factors. This paper provides a summary of an NESC-sponsored project to define the meaning of reliability and robustness in terms of human systems integration. For a complete coverage of this topic, refer to the full report [2].

1.1 Scope of our analysis

While human-system interactions occur in all phases of system development and operation, the human factors team restricted its work to the elements that involve "direct contact" with spacecraft systems. Such interactions encompass all phases of human activity during the design, manufacture, test, operation, and maintenance phases of the spacecraft lifespan. We therefore consider practices that accommodate and promote effective, safe, reliable, and robust human interaction with spacecraft systems. By restricting our scope to "direct contact" with the spacecraft, we by no means dismiss the importance of management and organizational factors in system performance [3].

1.2 Interaction across disciplines

Human Factors Engineering (HFE) must interact with all engineering discipline areas. Some of the linkages to the other disciplines are readily apparent, because spacecraft propulsion, guidance, navigation, and control (GN&C), avionics, mechanism, life support, and software systems must be operated and monitored by the flight crew and ground support personnel for mission success. Likewise, all of the disciplines impact

flight crew performance, health, and safety. For example, structures, materials, and safety and mission assurance (S&MA) affect habitability, health, and safety. Propulsion systems impose significant acceleration and vibration loads on the vehicle and crew during launch, again with obvious design implications for crew performance, health, and safety.

Spacecraft human factors relate not only to flight crew, but also the personnel who design, build, operate, and maintain the system. During the design process, therefore, all other disciplines need to be fully aware of the impact their products will have on personnel (both flight crew and ground personnel) as part of the system as a whole, throughout the system life cycle. Therefore, HFE interacts with the other disciplines so that designs of future spacecraft systems not only respect human limitations, but also benefit fully from human capabilities. The influence diagram shown in Fig. 1 illustrates the interrelations between human factors and other discipline areas for each phase of the spacecraft system life cycle, in terms of ground and flight crew operations.

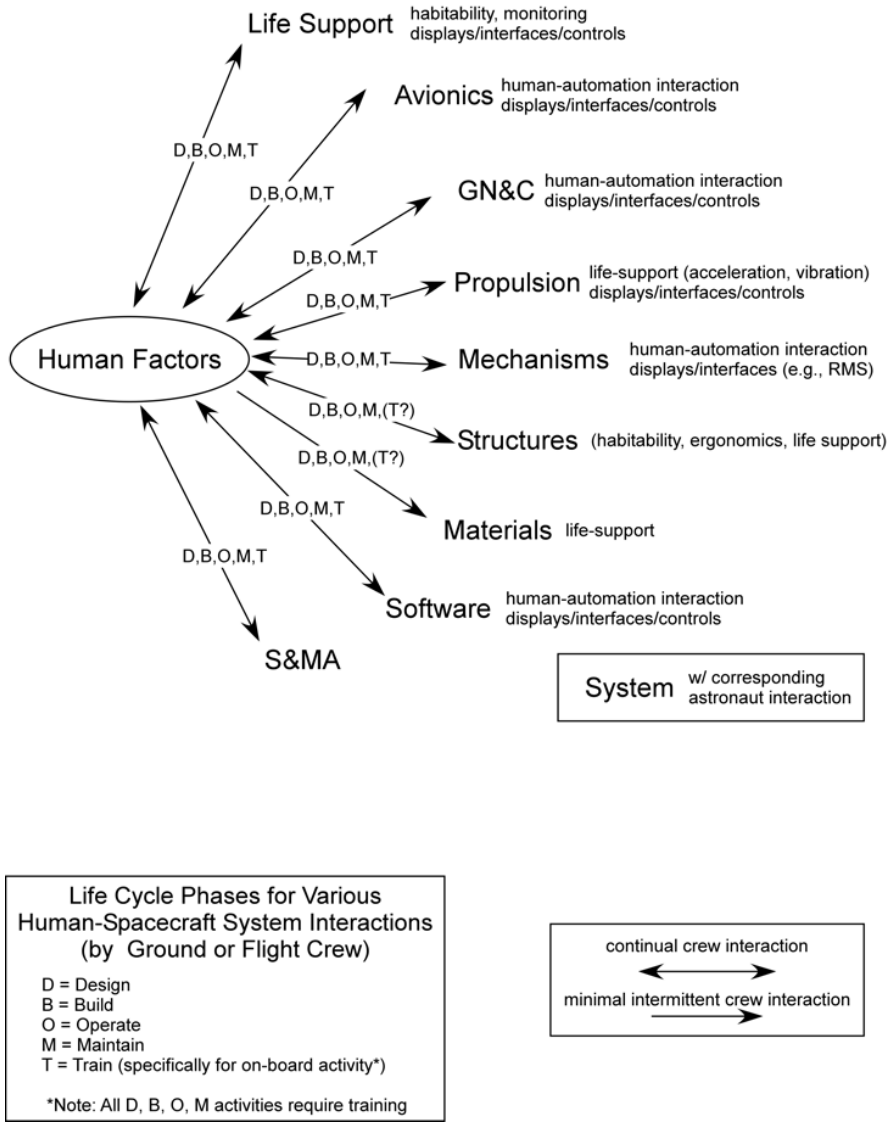

Figure 1. Interactions between human factors and other disciplines

2. PRODUCT AND PROCESS IN RELATION TO RELIABILITY AND ROBUSTNESS

The key attributes that contribute to system reliability and robustness can be divided into attributes of the product and attributes of the processes used to develop and operate the product.

2.1 Attributes of the product

The spacecraft system includes products that take the form of hardware, software, systems documentation, training systems, and procedures. Human Factors Engineering (HFE) deals with each of these products during all phases of the system life, and across the spectrum of operating conditions (normal, contingency, and emergency). HFE aspects relate to all people who come into contact with the spacecraft, including design and construction personnel, pre-launch test and verification personnel, astronauts and ground support personnel.

A reliable and robust design is one that addresses three key aspects of HFE:

1. System demands are designed to be compatible with human capabilities. The tasks demanded of people can be performed reliably under normal, contingency, and emergency conditions. This attribute is supported by the use of HFE design analyses, HFE guidelines and standards, and thorough test and evaluation.

2. The system is designed so that human capabilities can be brought to bear on non-routine, unanticipated problems. This is a key attribute that provides system resilience. The intelligent adaptation of humans to novel situations can significantly contribute to mission success in the face of situations that were not anticipated when the system was designed and evaluated. In contrast to automated systems, humans possess unparalleled abilities to solve problems and deal with unanticipated situations [4]. A robust system keeps the flight crew and other personnel in the loop and enables them to take action when novel situations arise.

3. The system is designed with the anticipation that human error is certain to occur. NASA's human rating requirements for space systems previously specified that "space systems shall be designed so that no two failures result in crew or passenger fatality or permanent disability" [5]. This principle, sometimes referred to as two-fault tolerance (2FT) was also referred to in earlier versions of the U.S. Department of Defense Standard Practices for System Safety [6]. The NASA Safety Manual still requires, in certain situations, sufficient system redundancy to tolerate two failures or two human operator errors (fail-safe or fail operational) when loss of life or mission critical events could occur. One-failure (fail-safe) tolerance is permitted in cases where the lesser consequences of system loss or damage or personal injury could occur [7].

Table 1. Three principles of reliability and robustness, with examples of their application at different phases of the system life cycle

Design Principle	**System Life Cycle Phase**			
	Manufacture	Test	Operate	Maintain
1. System demands are compatible with human capabilities and limitations.	Knowledge, skills and abilities involved in manufacturing can be objectively defined and evaluated.	Test and verification tasks are within human perceptual-motor envelope.	Human-system interface is consistent with human performance standards.	Maintenance tasks are within human capabilities.
2. System can tolerate and recover from human errors.	Components are designed to make incorrect assembly difficult.	Test and verification tasks are not performed by the same staff who manufactured the system being tested.	Appropriate interlocks make it difficult to do dangerous things.	Simultaneous maintenance of redundant systems is avoided.
3. System enables utilization of human capabilities in non-routine and unpredicted situations.	Construction personnel are able to identify and log problems.	Output of test results are sufficiently detailed to enable identification of abnormal states.	System keeps human operators in the loop and permits humans to take control in the event of unexpected events.	If necessary, non-routine trouble-shooting and system repair is possible.

Robustness to error can be achieved in three ways [5]:

(a) Undesired but predictable errors are blocked, such as through the use of interlocks or design features that prevent dangerous actions from being carried to completion.

(b) Errors that are not blocked can be detected and recovered, e.g., through the ability to "undo" erroneous actions. There must be a means to detect errors and gracefully recover from errors when they are made.

(c) Undesired deviations that are not blocked, detected, nor are recoverable, will have consequences that are minimized wherever possible.

Tab. 1 lists these three broad principles of robustness, and provides examples of how they can be applied at different phases of the system life cycle.

2.2 Attributes of the process

To evaluate reliability and robustness from a human factors perspective, we must consider not only the attributes of the *product* as eventually delivered, but also the human factors engineering processes that occur during the system life cycle. To be effective, human factors engineering processes must be integrated with other engineering activities and applied throughout the life cycle of the system, from concept planning, through operations and ultimately decommissioning.

Fig. 2 shows an idealized product development process, proceeding from initial concept development on the left of the figure to operational introduction of the product on the right. Planning for the HFE program begins at the start of the design process, and sets in motion a series of critical activities, including analysis of the tasks that must be performed by humans, the design of the user interface, and eventual in-service monitoring. These processes of course, do not guarantee adequate human system integration. Yet in their absence, problems with the user interface are virtually assured. Detailed coverage of these topics can be found in the cited report of the U.S. Nuclear Regulatory Commission [8]. For additional information, refer to the U.S. Navy Human Systems Integration Guide [9] and Department of Defense Acquisition Guidebook [10]. In the following, we illustrate the process by focusing on five key human factors activities. Refer to [2] for a treatment of all the HFE activities shown in Fig. 2.

HFE program planning. HFE program planning includes identifying (1) the general HFE program goals and scope, (2) the high-level concept of operations for the new system, (3) HFE design team skills necessary to conduct subsequent HFE activities, (4) engineering procedures to be followed (such as quality assurance and the use of an issues tracking system), (5) the description of HFE products and documentation of analysis and results, and (6) key milestones and schedules to ensure the timely completion of HFE products. The results of the planning activity should be documented in a human factors program plan that can be used to manage the overall HFE effort. The NASA Procedural Requirement (NPR) for systems engineering requires a human systems integration plan as part of the overall systems engineering approach [11]. Additional information on HFE Program Planning can be found in the following sources [1,5,8,12,13].

Operational experience review (OER) and lessons learned. New design projects should be based on a thorough understanding of the strengths and weaknesses of existing or similar designs. The Operational Experience Review (OER) and lessons learned activity should identify positive as well as negative experiences. In essence, the best place to start a design project is by understanding the lessons learned from similar systems in the past. A variety of data sources can be used, including: databases of event reports and summaries; interviews and walkthroughs with personnel; and communication with other facilities and organizations. The OER and lessons learned information should be documented to provide a clear indication of the issue identified, the design activities to which it is relevant, and its criticality. The OER should be maintained and made readily accessible to the design team.

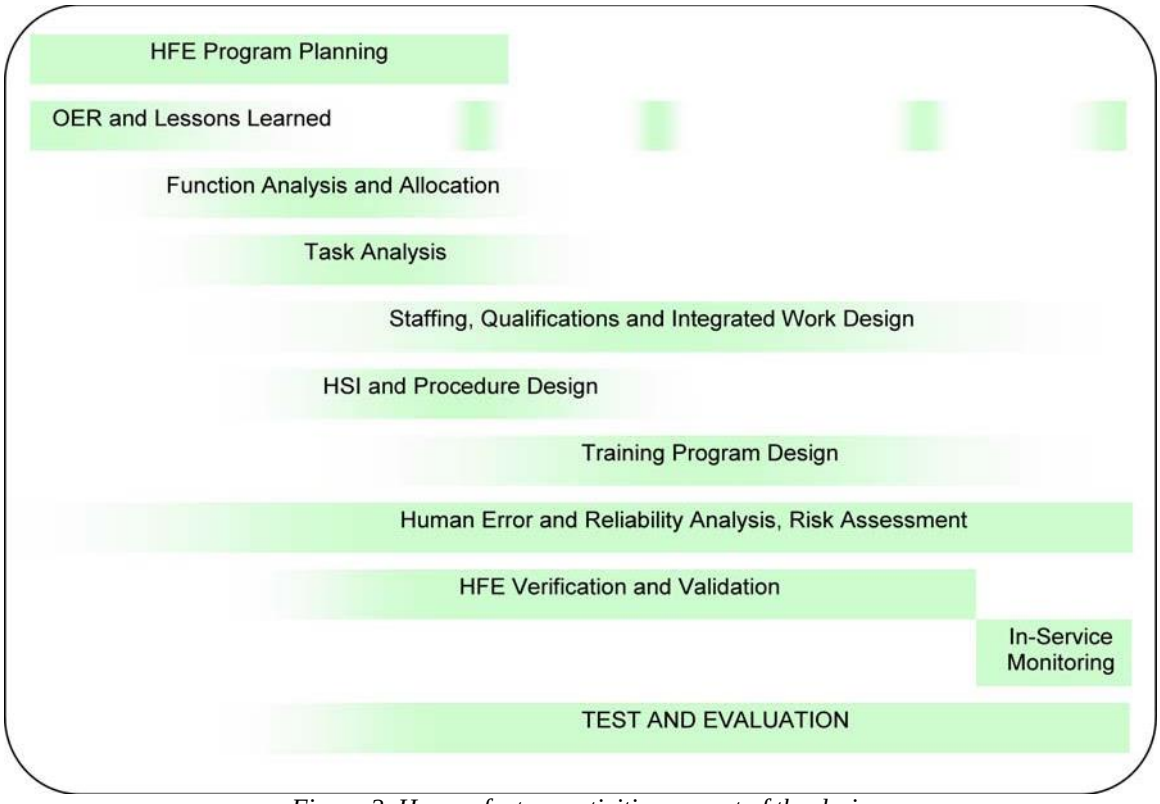

Figure 2. Human factors activities as part of the design program.

Function analysis and allocation. Every spacecraft system has one or more missions that it is designed to achieve. To achieve a mission, various functions have to be performed, such as GN&C and life support. The term function allocation, as used here, simply refers to the allocation of responsibility for conducting functions, or parts of functions, to personnel (flight and ground crew), to automated systems, or to some combination of the two. In some cases, the best alternative may be to flexibly allocate functions so they can be performed either by the crew or automation depending on the crew's goals and priorities in the current situation. As functions are analyzed, their requirements become better defined. At some point, functions or parts of functions are assigned to the available resources, which include hardware, software, and human elements. The overall purpose of function analysis and allocation is to ensure that functional requirements are sufficiently defined and analyzed so that the allocation of functions to the available resources can take advantage of the strengths of each resource. In other words, the goal is to make use of automation and human capabilities in ways that maximize overall function accomplishment. Detailed coverage of functional allocation can be found in the work of Billings [14], and the following sources [8, 12]

Task analysis. Task analysis refers to a family of techniques that provide detailed information about what is needed to perform tasks. Generally, the term "task" is used to refer to a group of activities that have a common purpose. Some tasks are sequential and well defined, like starting a system. Other tasks are ill defined and not sequential, like fault-detection and troubleshooting. Kirwan and Ainsworth [15] list over 40 tasks analysis techniques, each of which is suited to a particular situation or objective. For example, Link Analysis is a method of analyzing the layout of equipment and consoles based on task demands. Operational Sequence Analysis is a method of examining the detailed behavioral aspects of tasks that are fairly well defined and sequential. Hierarchical Task Analysis is a method of decomposing higher-level functions to the information and controls that personnel need to perform their tasks. Cognitive Task Analysis is a method for analyzing the diagnosis and decision-making process and is best suited to examining tasks that are ill-defined and very dependent on the expertise of the user. In combination, these methods provide powerful tools for identifying task requirements. Task analysis information has many uses in subsequent analyses, including: staffing, procedure design, training, and human error and reliability analysis.

Human error and reliability analysis. Even when the system is at an early stage of definition, it is possible to broadly identify error risks and ensure that these are explicitly considered during the design process. As the project progresses through analysis to definition and design, iterative analyses will identify potential human

errors and human factor risks in progressively finer levels of detail. The aims of a human error analysis are to identify critical areas where system demands may be incompatible with human capabilities, and identify critical areas where the system is vulnerable to human error. These could be areas where the two-fault tolerance principle is breached. Given the early stage of system development, the initial human error hazard analysis will be characterized by a qualitative approach applied at a broad level of granularity.

The initial human error analysis would consider nominal as well as off-nominal operations in all stages of the system life cycle, from design to construction, operation and maintenance. The initial human error hazard analysis would draw on information from operational experience reviews, incident and accident databases, and relevant experience from other industries and settings.

Two analysis techniques guide the human error hazard analysis.

1. Fault Tree Analysis (FTA) is a top-down approach, starting with a list of potential catastrophic scenarios and then working down to identify how these could occur. During the human error analysis, the emphasis is naturally placed on the human actions that could jeopardize a mission or lead to loss of life. Although probability estimates are commonly inserted into fault trees, even without this level of detail, fault trees can help the analyst identify situations where the system is vulnerable to human error.

2. Human Factors Process Failure Modes and Effects Analysis (HFPFMEA) is a bottom-up approach that identifies how personnel interact with human/machine interfaces, what errors are possible, and what consequences would result from errors. Information from fault trees, as well as preliminary function analysis and task analysis, assists in the HFPFMEA process [16]. The two approaches of FTA and HFPFMEA are complementary and information from one approach is used to refine and guide the other.

Test and evaluation. This activity is an integral part of the entire HFE process and spans the full design life cycle. Tests and evaluations can be conducted for a variety of purposes, including the resolution of design tradeoffs, the evaluation of new designs, and to provide information and feedback from users. Common test and evaluation methods include: User interviews; surveys and rating scales; focus groups; computer modeling; and walk-throughs using drawings, mockups, and prototypes [17,18,19].

3. CONCLUSIONS

The work described in this paper was directed at design issues pertaining to space vehicles; however the principles are applicable to a wide range of products and systems, ranging from simple household objects to advanced technological systems. Careful attention to the design of human system interfaces can make a significant contribution to the overall performance of complex systems. It must be noted however, that good design of components does not guarantee the performance of the overall system. Furthermore, managing the performance of a highly complex system involves more than just ensuring adequate interface design. Organizational factors are at the heart of system performance, and while acknowledging this key area, we have not attempted here to deal with the organizational issues associated with the management of complex systems.

This paper introduced three key product attributes, or principles, that contribute to reliability and robustness. These were the extent to which task demands are within human capabilities, the capacity of the system to cope with human error, and the ability of the system to make use of unique human capabilities during non-routine situations. Over the last half century, human factors practitioners have directed much of their attention towards the first and second of these principles. The third principle has received less attention, yet it is important to acknowledge the positive as well as the negative contribution that human performance makes to system operation.

Ensuring effective human system integration requires the application of human factors principles early in the design process. A structured approach to human factors can save a great deal of trouble later in the life of the system in terms of re-design, training and safety incidents. There are of course, no guarantees that a formal consideration of human factors throughout the design process will identify all the relevant human issues. However neglecting these areas is almost certain to result in a system lacking in reliability and robustness.

REFERENCES

1. National Aeronautics and Space Administration (2012). *Space Flight Program and Project Management Requirements*). NASA Procedural Requirement NPR 7120.5E. Washington DC: Author.

2. Adelstein, B., Hobbs, A., O'Hara, J., & Null, C. (2006). *Design, development, testing, and evaluation: Human factors engineering* (NASA/TM-2006-214535). Hampton, VA: NASA Langley Research Center.

3. Reason, J. (1997). *Managing the risk of organisational accidents*. Aldershot: Ashgate.

4. Reason, J. (2009). *The human contribution. Unsafe acts, accidents and heroic recoveries.* Aldershot: Ashgate.

5. National Aeronautics and Space Administration (2004). *Human Rating Requirements for Space Systems*. NASA Procedural Requirement NPR 8705.2A. Washington DC: Author.

6. Department of Defense (2000*). Standard practice for System Safety*. MIL-STD-882D. Washington DC: Author.

7. National Aeronautics and Space Administration (2008). *General Safety Program Requirements*. NASA Procedural Requirement NPR 8715.3C. Washington DC: Author.

8. O'Hara, J., Higgins, J., Fleger, S. & Pieringer, P. (2012). *Human factors engineering program review model.* (NUREG-0711, Rev. 3). Washington, D.C.: U.S. Nuclear Regulatory Commission.

9. U.S. Navy. (2005). *Human systems integration guide*. Washington DC: Author.

10. Department of Defense. (2006). *Defense acquisition guidebook*. Washington DC: Author.

11. National Aeronautics and Space Administration (2013). *NASA Systems Engineering Processes and Requirements.* NASA Procedural Requirement 7123.1B. Washington DC: Author.

12. Department of Defense. (2011). *Human Engineering Requirements for Military Systems, Equipment and Facilities*. (MIL-STD-46855A). Washington, D.C.: Office of Management and Budget.

13. National Aeronautics and Space Administration (2007). *Systems engineering handbook.* NASA/SP-2007-6105. Washington DC: Author.

14. Billings, C. (1997). *Aviation automation: The search for a human-centered approach.* Mahwah, NJ: Lawrence Erlbaum Associates.

15. Kirwan, B. & Ainsworth, L.K. (1992). *A guide to task analysis*. London: Taylor and Francis

16. NASA. (2002). *Human reliability analysis (HRA) Final Report. Volume VII: Human Error Analysis Methodology*. (JSC report 29867). Johnson Space Center, TX: Author.

17. O'Hara, J., Stubler, W., Brown, W. & Higgins, J., (1997). *Integrated-system validation: Methodology and review criteria* (NUREG/CR-6393). U.S. Nuclear Regulatory Commission, Washington, D.C.

18. Charlton, S. & O'Brien, T. (Eds.) (2002). *Handbook of Human Factors Testing and Evaluation* (2nd Edition). Hillsdale, New Jersey: Lawrence Erlbaum, Associates, Inc.

19. Meister, D. (1986). *Human factors in testing and evaluation*. Amsterdam: Elsevier.