NASA/TM-2006-214535
NESC-RP-06-108/05-173-E

NASA Engineering and Safety Center's
Super Problem Resolution
Human Factors Team Report

Design, Development, Testing, and Evaluation: Human Factors Engineering

Bernard Adelstein and Alan Hobbs
NASA Ames Research Center, Moffett Field, California

John O'Hara
Brookhaven National Laboratory, Upton, New York

Cynthia Null
NASA Langley Research Center, Hampton, Virginia

December 2006

The NASA STI Program Office . . . in Profile

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA Scientific and Technical Information (STI) Program Office plays a key part in helping NASA maintain this important role.

The NASA STI Program Office is operated by Langley Research Center, the lead center for NASA's scientific and technical information. The NASA STI Program Office provides access to the NASA STI Database, the largest collection of aeronautical and space science STI in the world. The Program Office is also NASA's institutional mechanism for disseminating the results of its research and development activities. These results are published by NASA in the NASA STI Report Series, which includes the following report types:

- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counterpart of peer-reviewed formal professional papers, but having less stringent limitations on manuscript length and extent of graphic presentations.

- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.

- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.

- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or co-sponsored by NASA.

- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.

- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services that complement the STI Program Office's diverse offerings include creating custom thesauri, building customized databases, organizing and publishing research results ... even providing videos.

For more information about the NASA STI Program Office, see the following:

- Access the NASA STI Program Home Page at ***http://www.sti.nasa.gov***

- E-mail your question via the Internet to help@sti.nasa.gov

- Fax your question to the NASA STI Help Desk at (301) 621-0134

- Phone the NASA STI Help Desk at (301) 621-0390

- Write to:
  NASA STI Help Desk
  NASA Center for AeroSpace Information
  7115 Standard Drive
  Hanover, MD 21076-1320

NASA/TM-2006-214535
NESC-RP-06-108/05-173-E

NASA Engineering and Safety Center's
Super Problem Resolution
Human Factors Team Report

Design, Development, Testing, and Evaluation: Human Factors Engineering

Bernard Adelstein and Alan Hobbs
NASA Ames Research Center, Moffett Field, California

John O'Hara
Brookhaven National Laboratory, Upton, New York

Cynthia Null
NASA Langley Research Center, Hampton, Virginia

National Aeronautics and
Space Administration

Langley Research Center
Hampton, Virginia 23681-2199

December 2006

Available from:

NASA Center for AeroSpace Information (CASI)
7115 Standard Drive
Hanover, MD 21076-1320
(301) 621-0390

National Technical Information Service (NTIS)
5285 Port Royal Road
Springfield, VA 22161-2171
(703) 605-6000

NASA Engineering and Safety Center's
Super Problem Resolution Human Factors Team Report

Design, Development, Testing, and Evaluation: Human Factors Engineering

December 2006

Table of Contents

Acknowledgements

Report Authors:

John O'Hara, BNL/DOE
Alan Hobbs, ARC/SJSUF
Bernard Adelstein, ARC

Thank you to the following NESC Human Factors SPRT members for their thoughtful comments.

Al Ahumada, ARC
Rudy Aquilina, ARC
Immanuel Barshi, ARC
Barbara Burian, ARC/SJSUF
John Caldwell, ARC/AFRL
Key Dismukes, ARC
Jessica Mock, JSC
Cynthia Null, NESC LaRC
David Woods, OSU
David Gertman, INEL/DOE

Also, thank you to the following individuals for their valuable input.

Jerry R. Goodman, JSC
Charles D. Wheelwright, JSC
Tim Barth, KSC
Charles Olsen, JSC/Lockheed Martin

Design, Development, Testing, and Evaluation:
Human Factors Engineering

1.0 Introduction

1.1 Role of Human Factors in Design, Development, Testing, and Evaluation (DDT&E)

NASA Procedural Requirements (NPR) 7120.5C, Appendix M, 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."

Thus, humans, not only as the flight crew, but also as designers, manufacturers, and ground support are considered part of the spacecraft system. All elements of the system are influenced by human performance. In turn, human performance is influenced by many aspects of system design, including the equipment that personnel interface with, training they receive, procedures they use, and teamwork needed for personnel to work with each other to perform their various roles. These aspects of system design are addressed by human factors engineering (HFE).

HFE is a basic element of the design of many complex human-machine systems in addition to spacecraft systems, such as aircraft, military systems, computer systems, process control facilities, and medical devices. The Institute of Electrical and Electronics Engineers' (IEEE) Systems Engineering Standard 1220 (1998, pp.3-4) states that "the design of the products and life cycle processes should consider the human as an element of the system in terms of operators, maintainers, manufacturing personnel, training personnel, etc., for the purpose of understanding the human-system integration issues and ensuring that the system products are producible, maintainable, and usable." Numerous other systems engineering and U.S. Department of Defense (DoD) standards include HFE as a key component of the overall design and evaluation process. The application of HFE is most important in the design of "high-risk, high-reliability systems" where failures can have significant consequences.

The effectiveness and reliability of these systems is a function of (1) the technical performance of system hardware/software; (2) the effectiveness of the human elements of the system, including personnel performance, operational procedures, and training; (3) the operational environment—human-machine systems may be very effective in one operational environment, but not in another; and (4) the interaction of all three. Thus, HFE is a crucial element in system development, acquisition, and evaluation conducted by NASA.

The NASA Systems Engineering Handbook (NASA 1995, p.18) specifies HFE as one of the specialty disciplines upon which Systems Engineering (SE) must rely and that will have important contributions *throughout the system life cycle* (NASA 1995, p. 34). The NASA

Systems Engineering Handbook states that the Systems Engineering Management Plan "should contain, as needed, the approach to HFE" (NASA 1995, p. 44), and, that demonstrating "human factors considerations of the proposed design support the intended end users' ability to operate the system and perform the mission effectively" is part of successful preparation for preliminary design review (NASA 1995, p.67).

NASA Procedural Requirements NPR 8705.2A "Human-Rating Requirements for Space Systems" explicitly mandates the application of HFE in the throughout the development life cycle of spacecraft systems and addresses of the roles typically filled by HFE. NPR 8705.2A's requirements, as they relate to the material in this chapter, are cited in the corresponding sections and subsections below.

The general approach to HFE described in this chapter is consistent with that used for complex human-machine systems in other domains, such as those involving the military (DoD), transportation (Department of Transportation), and nuclear energy (Nuclear Regulatory Commission).

1.2 Scope of Human Factors Section

While human-system interaction occurs in all phases of system development and operation, this chapter on Human Factors in the DDT&E for Reliable Spacecraft Systems is restricted to the elements that involve "direct contact" with spacecraft systems. Such interactions will encompass all phases of human activity during the design, fabrication, testing, operation, and maintenance phases of the spacecraft lifespan. This section will therefore consider practices that would accommodate and promote effective, safe, reliable, and robust human interaction with spacecraft systems. By restricting this chapter to what the team terms "direct contact" with the spacecraft, "remote" factors not directly involved in the development and operation of the vehicle, such as management and organizational issues, have been purposely excluded. However, the design of vehicle elements that enable and promote ground control activities such as monitoring, feedback, correction and reversal (override) of on-board human and automation process are considered as per NPR8705.2A, Section 3.3. Finally, while Section 9.0 (Environment Control and Life Support Systems) of the DDT&E Report will explicitly treat environmental and life support matters (e.g., radiation, atmosphere), these environmental factors directly modulate human performance and therefore are an important consideration in crew-related human factors discussed here.

1.3 Interaction between Human Factors Interaction and Other Disciplines

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 systems will not only have to consider flight crew factors. Spacecraft systems will have to be designed, built, operated, and maintained in an effective, efficient, and safe manner by ground personnel.

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 entire 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 provided in Figure HF-1 schematizes interrelations with the NESC discipline areas from a human factors viewpoint for the different phases of the spacecraft system life cycle, in terms of ground and flight crew operations.

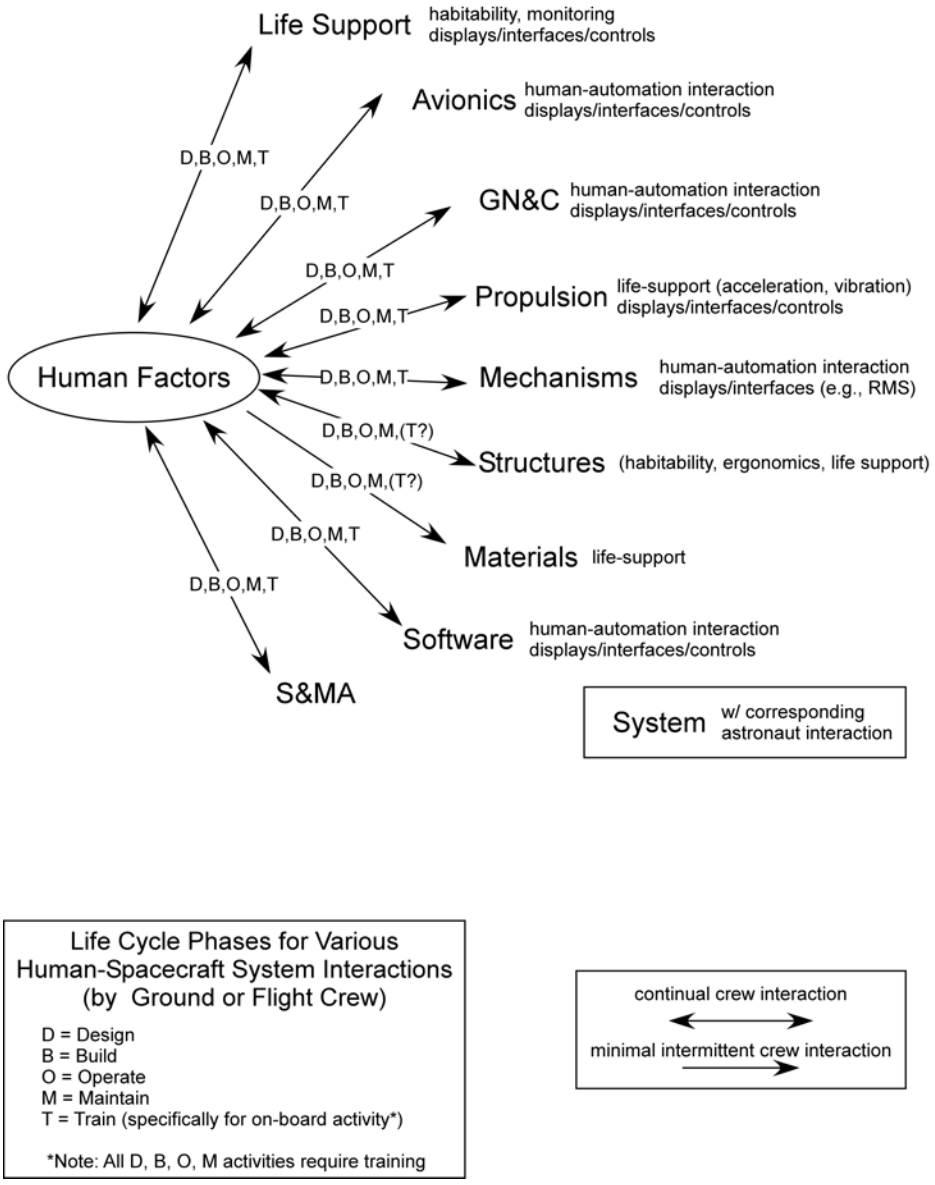

Figure HF-1. Human Factors Discipline Influence Diagram

2.0 Key DDT&E HFE Attributes that Ensure Robust and Reliable Spacecraft Systems

Key attributes that ensure robust and reliable systems can be divided into the attributes of the product and the attributes of the processes used to develop and operate the product.

2.1 Human Factors Product Attributes

The spacecraft system design products include hardware, software, systems documentation, training systems, and procedures. HFE issues relate to all aspects of the system life, including design, build, test, operate and maintain, across the spectrum of operating conditions (nominal, 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, and astronauts and ground support personnel.

A 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 nominal, 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. 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 to tolerate and recover from human error. NPR 8705.2A Section 3.1 specifies that "space systems shall be designed so that no two failures result in crew or passenger fatality or permanent disability." The NASA Safety Manual (NASA NPR 8715.3, Requirement 25215) also requires sufficient system redundancy to tolerate two failures or two human operator errors (fail-safe or fail operational[1]) when loss of life or mission critical events could occur, but permits one-failure (fail-safe) tolerance in cases where the lesser consequences of system loss or damage or personal injury could occur. The two-failure tolerance concept is not limited to NASA, and is also referred to in MIL-STD-882D (DoD, 2000, p.14).

Error tolerance can be achieved in three ways, as specified in NPR 8705.2A, Section 3.1.5:

[1] From the glossary of NPR 8715.3, "fail-safe" is the ability to sustain a failure and retain the capability to safely terminate or control the operation, while "fail-operational" is the ability to sustain a failure and retain full operational capability.

(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, such as 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 from, will have consequences that are minimized wherever possible. One way to achieve this is to build redundancy (e.g., tolerance to any combination of two failures or inadvertent actions) into the system (NPR 8705.2A Section 3.1.3, Requirement 34422).

Table HF-1 lists these three principles of robustness, and provides examples of how they would be applied at the design stage to different phases of the system life cycle. The phases chosen to illustrate these principles include the Manufacture, Test, Operate, and Maintain stages of system life.

Table HF-1. Role of HFE in Design for Reliability/Robustness. Good practices with examples of how these principles can be brought to bear during the design of different phases of the system life cycle.

Design Principle	**System Life Cycle Phase**			
	Manufacture	**Test**	**Operate**	**Maintain**
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 envelope.	Human-system interface are consistent with human performance standards	Maintenance tasks are within human capabilities.
System enables utilization of human capabilities in non-routine and unpredicted situations			System keeps human operators in the loop and permits humans to take control in the event of unexpected events.2	If necessary, non-routine trouble-shooting and system repair is possible.
System can tolerate and recover from human errors 1. Undesired errors are blocked 2. Detect and recover from errors 3. Minimize consequences of uncorrected errors	Components designed to make incorrect assembly difficult	Provide requirement for independent test verification	Appropriate interlocks, make it difficult to do dangerous things System state is made apparent	**Avoiding simultaneous maintenance of redundant systems**

[2] It may be difficult to return control to the human in some situations. For those situations, a second automated system may be essential, built with a different foundational basis so that one type of failure cannot take out both systems.

2.2 Human Factors Process Attributes

The following are the key practices of an HFE program to help ensure that NASA's systems are reliable and robust.

2.2.1 Integrate HFE into the Design Process

To achieve the key product attributes identified above, HFE should be fully integrated into the overall engineering process from the outset as required by NPR 8705.2A (Section 1.6.4.1, Requirement 34346). This will help ensure timely and complete interaction with other engineering activities. Experience has shown that when HFE activities are performed independently from other engineering activities, their impact and effectiveness is greatly decreased. Moreover, including HFE at the beginning of a project helps ensure that user needs can be addressed early in the design process before changes become too costly. Often when problems are identified late in a design project, corrections reflect "band-aid" fixes rather than optimal solutions. [ref. DDT&E Report, Section 2.1, Figures 2.1-1 and 2.1-2,] The HFE activities described in this document provide the means to accomplish this objective.

2.2.2 Use a "Top-Down" Hierarchical Approach

The HFE aspects of a system should be developed, designed, and evaluated on the basis of a systems analysis that uses a "top-down" approach. Top-down refers to an approach starting at the "top" of the hierarchy with the system's high-level mission and goals. These are divided into the functions necessary to achieve the goals. Functions are allocated to human and system resources. Each function can be broken down into tasks. The tasks are analyzed to determine the cognitive, perceptual, motor, and ergonomic demands placed on human operators and then to identify the alarms, displays, procedures, controls, etc. that will be required for task performance. Task requirements reflect performance demands imposed by the detailed design of the system. Tasks are arranged into meaningful jobs to be performed by personnel who will operate and maintain the system. The interfaces, support systems, procedures, and training are designed to best support personnel in performing their tasks. The detailed design (of the interfaces, support systems, procedures, and training) is the "bottom" of the top-down process. Of course, there are also requirements that stem from the detailed design of individual systems and components. These are captured when personnel tasks are analyzed.

2.2.3 Apply HFE throughout the System Life Cycle

Application of HFE is mandatory for the full life cycle of any human-rated space systems program (NPR 8705.2A, Section 1.6.4.1, Requirement 34346). The life cycle spans concept planning through operations, and ultimately decommissioning and disposal. HFE is sometimes thought of as a "usability" check of the final design. Relegating consideration of user needs to final design checking, however, will make design changes difficult and costly to incorporate. HFE activities must be performed early on, beginning at the system's initial planning stages, e.g., what should be automated and how much automation to incorporate into the design. Otherwise, it may be too late to compensate.

2.2.4 Rank the HFE Effort to Focus on the Areas of Greatest Significance

HFE activities should be ranked. This means that the design organization should ensure that a process is in place to adjust the level of HFE design and evaluation effort to its need in the design process. Such an approach enables the application of HFE to be directed to where it will

have the most impact. Moreover, these points all need to be considered in context which requires analysis of the (space) environment, specific operational demands, and the effects on human performance.

- For each subsystem, identify how and when humans will interact with the spacecraft system during all stages of its life cycle (design, development, assembly, testing, operation, and maintenance).
- Identify scenarios in which human error and human performance variability could degrade subsequent system reliability.
- Critical human activities should be prototyped either in vivo or via computer simulation.
- Interactions between activities should be identified, attention given to scheduling of human activities to avoid temporal, spatial bottlenecks, and conflicts as well as to avoid complex multi-task demands at specific during which human performance is known to be less than optimal.
- Rate human reliability *threats* in terms of probability and criticality.
- Develop countermeasures.
- Demonstrate that significant human reliability threats have been addressed at the design stage. Consider these from the standpoint of coupled human-system design, addressing hardware/software systems as appropriate.

2.3 Managing the Risk of Human Error (Initial Human Error Hazard Analysis)

Early in the development process, it is critical to identify potential hazards that could originate from human error. Even though the system may be at an early stage of definition, it is possible to broadly identify error risks and ensure that these are explicitly considered in design activities. 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. Section 3.6 presents a more comprehensive summary of human error and human reliability analysis methods applicable to various aspects of HFE program development and design.

The NASA Safety Manual (NPR 8715.3, Requirement 32126) specifies a Preliminary Hazard Analysis (PHA) will be started early in the project development process. The initial identification of human error risks would most likely be carried out as part of the PHA as a human error hazard analysis.

The aims of the initial human error analysis are to:

1. Identify the critical items list (CIL) of system demands that may be incompatible with human capabilities.

2. Identify the CIL where the system is vulnerable to human error, particularly 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 rather than an excessively probabilistic approach
- A broad level of granularity

The initial human error analysis would consider:

- Normal as well as non-normal operations
- All stages of the system life cycle, from design, build, and operate, to maintain

The initial human error hazard analysis would draw on information from:

- Lessons learned
- Operational Experience Reviews
- Incident and accident databases
- 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 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, and particularly where the two-error tolerance principle has been breached.

2. Human Factors Process Failure Modes and Effects Analysis (HFPFMEA) is a bottom-up approach that identifies: how people interact with human/machine interfaces; what errors are possible; and what consequences would result. Information from fault tree analyses, as well as preliminary function analysis and task analysis assists in the HFPFMEA process (JSC, 2002).

The two approaches of FTA and HFPFMEA are complimentary and information from one approach is used to refine and guide the other. The relation between the two approaches is depicted schematically in Figure HF-2.

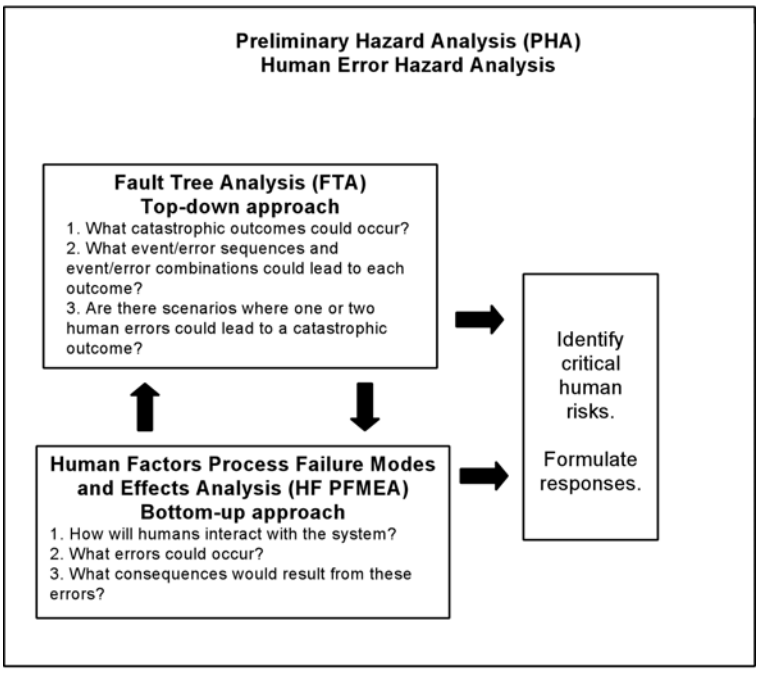

Figure HF-2. Preliminary Hazard Analysis: Human Error Hazard Analysis

3.0 Human Factors Engineering Activities

This section describes the HFE activities that should be performed to support human reliability. These activities, listed in Figure HF-3, provide the means of implementing the key attributes identified in Section 5.2. Figure HF-3 represents the relative timing of HFE activities with respect to the system design stages. Figure HF-3 indicates that a number of activities can occur in parallel and shows that the intensity of effort associated with each activity grows and diminishes through the course of the DDT&E program.

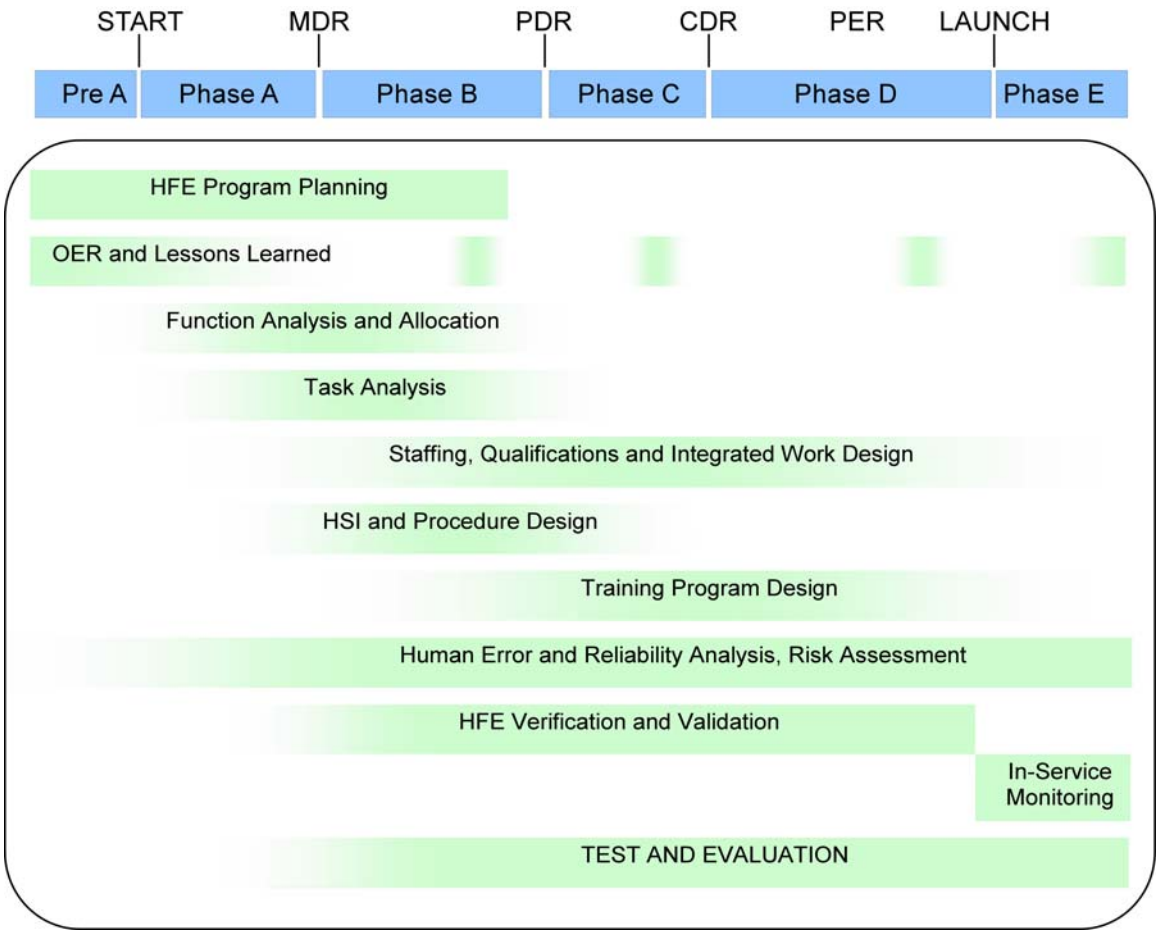

Figure HF-3. HFE Activities as Part of the Design Program

The intent of Figure HF-3 is solely to represent the relative phasing and intensities of HFE activities in a general program. This figure, however, does not illustrate any of the interactions between the eleven different activities. In practice, such interactions could link any one activity with many different combinations of the other listed HFE activities. Moreover, these combinations could be expected to change with successive iterations during the entire program life cycle. Most significantly, the precise details of phasing and intensities of activities will of course vary between one development program and another.

The human factors and human reliability disciplines not only levy requirements [e.g., Human Systems Integration Requirements (HSIR)] on space system design, HFE experience and human performance capabilities inform and help define mission and vehicle design goals as part of overall SE process. Consequently, early HFE activities should be integrated with, and conducted in concert with, early SE activities. Figure 2.3-3, Iterative Risk Based System Design Loop, in the SE Section of the DDT&E Report (Dec 2006) is augmented to indicate the key part that HFE needs to play from the program outset. As shown in Figure HF-4, HFE not only has a role in reliability analyses, HFE establishes a portion of the requirements for the spacecraft program (HSIR and Constellation Architecture Requirements Document, CARD). HFE also helps SE define operations concepts and needs (Mission Operations Directorate). Moreover, HFE helps

delimit permissible physics for the spacecraft system—the crew will need not only to survive the physics of the space environment but perform well enough to ensure mission success. Finally, HFE affords a more comprehensive reliability analysis because human operators (crew and ground) are part of the space system.

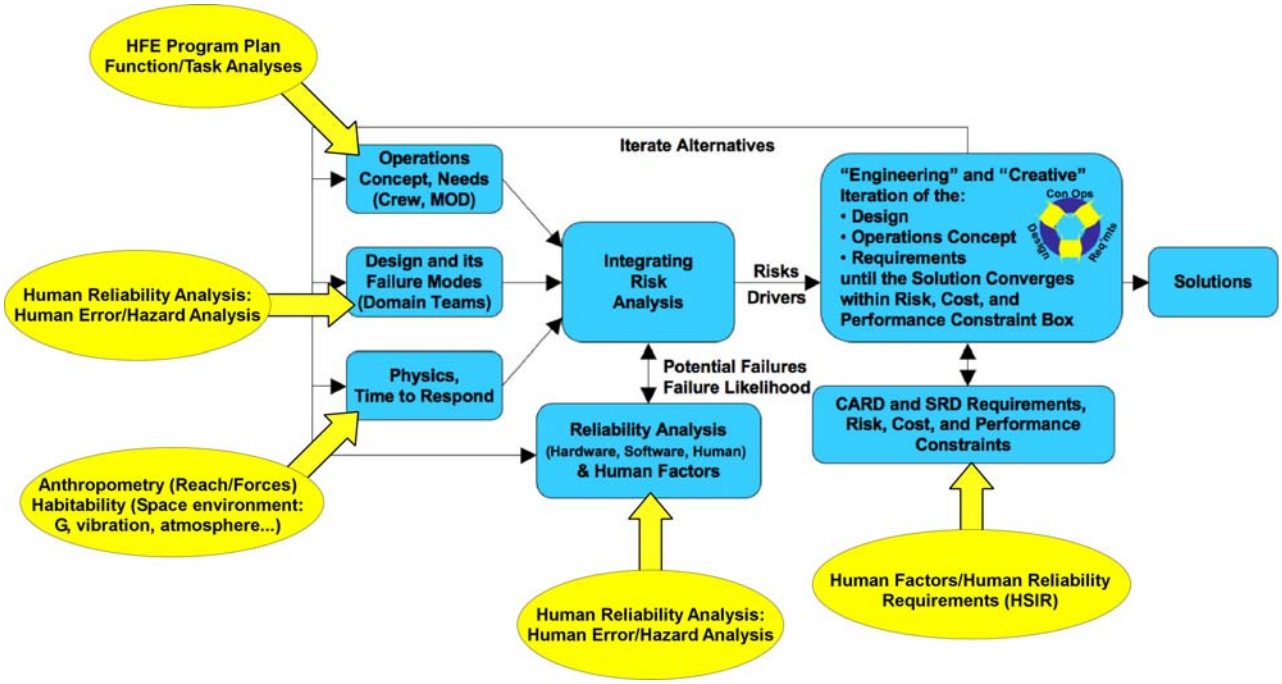

Figure HF-4. Integration of HFE in the Iterative Risk-Based System Design Loop. HFE contributions (yellow ovals) point to specific Systems Engineering activities to which they must be linked.

It is important to note that human performance can be quite sensitive to seemingly minor aspects of a system's design. For example, like many complex systems, a spacecraft has a large information system that the flight crew access through a small number of cockpit video display units. The crew accesses this information using features provided by the human-system interface (HSI), such as menus or links. When these features are poorly designed, the workload associated with accessing information increases and pilots will be reluctant to access needed information, especially during an emergency, when workload management is already an issue. However, this sets up a situation where the failure to access all the information needed impairs the crew's situation awareness leading them to misdiagnose the situation or take an incorrect action. Thus, supporting human reliability requires careful attention to all of the HFE activities discussed in this chapter.

Each of the activities listed in Figure HF-3 is described in its own subsection below. The description in each subsection addresses three aspects of the particular activity:

- its purpose and objectives
- the key methodological elements of the activity
- sources of additional information

Key methodological elements described here can be used to evaluate a proposed design program across all Constellation (e.g. CEV, LSAM) systems. The design program should describe how these activities and their key methodological elements are addressed. This information can also be used to assess the design itself. Two additional considerations should be noted. First, the terminology used in this chapter generally conforms to typical use in SE. However, a specific design and development program may use different language when describing the same activities. This is completely acceptable. It is important that the design program accomplishes the objectives regardless of the terminology used.

Second, design is an iterative process. While the activities are presented below in serial fashion, the reader should recognize that many of the activities described below will be performed throughout the course of the design and development program and will occur in parallel with each other. Thus for example, there may be a preliminary allocation of function before any analysis work begins, e.g., as part of a procurement specification. However, the allocation will be analyzed further as part of that HFE activity to better specify the basis for allocating functions. The function allocation may be revised across the design process as the design becomes more detailed and evaluations of system performance are made.

3.1 HFE Program Planning

This activity involves planning for the HFE aspects of a design and development program. This includes identifying (1) the general HFE program goals and scope, (2) high-level concept of operations for the new system, (3) HFE design team skills necessary to conduct subsequent HFE activities (responsibilities of the main design team and contractors should be clearly stated), (4) engineering procedures (such as quality assurance and the use of an issues tracking system) to be followed, (5) description of HFE products and documentation of analysis and results, and (6) key milestones and scheduled 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.

Additional information on HFE Program Planning can be found in the following sources:

NPR 8705.2A Sec 1.6.4.1 (Requirement 34346)
NPR 7120.5C Sec 3.2.1.2d
MIL-HDBK-46855
O'Hara et al. (2004) NUREG-0711
O'Hara et al. (2005) EPRI

3.2 Operating Experience Review and Lessons Learned

New design projects should be based on a thorough understanding of the strengths and weaknesses of existing designs that are similar and of the new technology that will be used. Operating experience reviews (OERs) help provide this information. OERs should be held periodically during the project/program cycle, as designs change, operations change, or other developments occur. OERs should be implemented as a series, first as a stand-alone, and then

subsequent ones as an element of the existing design review cycle. Each OER is performed to understand (1) current or planned work practices so the potential impact of planned changes, such as the introduction of new systems and new responsibilities and tasks or the introduction of new performance schedules, can be assessed, (2) operational problems and issues may be addressed in a new design or modification of an existing design, and (3) relevant domain experience with candidate system technology approaches.

Key methodological elements are:

1. The 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 for similar systems in the past. With respect to HFE, similarity in terms of overall mission of the system and of anticipated HSI designs should be considered.

2. A variety of data sources can be used, including: available documentation, including databases and event reports and summaries[3], interviews, and walkthroughs with personnel, and communications with other facilities and organizations.

3. OER information items that are identified should be prioritized by the design organization. Since OER information is useful only if it is available to the members of the design team who can make use of the information, it is desirable to classify the information according to design topics for which it is relevant, e.g., automation, procedures, and training. Finally, items should be prioritized based on their importance to mission success and human performance.

4. 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 importance. The OER should be maintained and readily accessible to the design team.

5. The identification of operating experience and the lessons learned from it should be an ongoing activity throughout the design project.

Additional information on OER can be found in the following sources:

NASA Lessons Learned Information System searchable database
(http://nen.nasa.gov/portal/site/llis)
EPRI (2005)
O'Hara et al. (2004) NUREG-0711

[3] A frequent problem encountered when utilizing existing experience databases and event reports is the lack of human performance-related information. For example, the Aerospace Corporation Space Systems Engineering database employed by the Systems Engineering Discipline (DDT&E Report, Systems Engineering, Section 1.2) provided negligible detail on the few human performance related system failures reported. Another factor is that even when human related failures are reported, the descriptions are not specific, often using a "catch-all" phrase such as "workmanship" to describe process and implementation failures, e.g., DDT&E Report Section 2.0 (SE), Figure 1.2-3. HFE practitioners should strive to improve experience-capturing databases by including fields that will support the development of HFE lessons learned. See also Section 4.2.1.

3.3 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 automatic systems, or to some combination of the two. In some cases, the best way may be to flexibly allocate functions so they can be performed either by the crew or automatically depending dynamically on the crew's goals and priorities in the current situation. The allocation is made on the basis of a function analysis to determine what is required to perform the function. Using the results of the function analysis, responsibility is allocated in a way that best ensures overall accomplishment of the function.

As functions are analyzed, their requirements become better defined. At some point, those functions or parts of a function are assigned to the available resources, which include hardware, software, and human elements (and, of course, combinations of them). 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. In other words, make use of automation and human capabilities in ways that maximize overall function accomplishment.

Decisions about automation are very much intertwined with the role of personnel in operations and the specific responsibilities personnel will have in accomplishing system functions. Flight and ground crew performance is essential to overall system performance, reliability, and safety. Therefore design decisions that have a negative impact on human performance can ultimately compromise spacecraft system performance. The most significant negative impacts on flight crew and other personnel of poorly designed automation are:

- Loss of situational awareness – greater degrees of automation can often result in a loss of situational awareness, or at least greater difficulty in gaining situation awareness.
- Loss of vigilance due to trust and complacency – when personnel come to trust the automation, they can become complacent and less vigilant in monitoring the system's performance. Personnel will thus become less likely to intervene when they should.
- Workload extremes – greater automation is often associated with lower workload (sometimes to the point of boredom). This can happen when the automation is functioning properly or when periods of extreme workload occur during an automation failure and personnel must intervene.
- Degradation of skills – since automatic systems are usually reliable, human performance of the function is rare and personnel skills for performing the actions are degraded over time. Also, it should be noted that human performance capabilities fluctuate across time as a function of physiologically based circadian influences.

Thus, the objective of this analysis is to specify the roles and responsibilities of personnel and automation in the performance of system functions, including how they may be changed as a result of various types of failure conditions.

Key methodological elements are:

1. Conduct Function Analysis - The first step is to define the functions needed for the mission and the available trade space that include: (1) determine the objectives, performance requirements, and constraints of the design, such as required speed, accuracy, reliability, etc.; (2) define the activities that must be accomplished to meet the objectives and required performance; (3) define the relationships between functions and subsystems (e.g., configurations or success paths) responsible for performing the functions; and (4) define trade-off priorities and constraints. Function characterization includes:

    - Purpose of the function
    - Cues indicating that the function is required
    - Cues indicating that the function is available (the subsystems/means of performing the function that are available)
    - Actions needed to perform the function
    - Time and performance requirements and constraints for performing the function
    - Information that indicates the function is operating (the subsystem/means of performing the function are operating)
    - Information that indicates the function is achieving its purpose
    - Information that indicates that operation of the function can or should be terminated
    - Potential failures of the function and alternative means for function attainment
    - Cues to identify each of the postulated failures

The level of description of the characterization begins at a general level and becomes better defined as the design details emerge.

2. Define Scenarios for Evaluation – As the demands on personnel are not constant across different operations, events, and situations, several scenarios should be identified for use in the evaluation. Each scenario is likely to involve multiple functions. A sufficient number of scenarios should be developed to provide a basis to evaluate all the functions for which allocation is to be examined.

3. Conduct Function Allocation Evaluation – This analysis is performed for each scenario. As the whole function analysis and allocation process is iterative, this analysis can begin at the earliest design stages. Allocations can be refined or adjusted as more information about performance is known and evaluations are conducted. Information supporting this evaluation includes:

    - Estimated function performance requirements as determined from function analysis, such as speed, accuracy, reliability, and workload
    - Capabilities and limitations of personnel and hardware/software

- Prior operational experience; i.e., knowledge of which allocations have been problematic and which have been successful are considered as a basis for allocation
- Results of tests and evaluations

To make these allocations, the following should be assessed.

Identify Mandatory Function Allocations – Consider first whether an allocation is mandatory as required by regulations (e.g., NPR8705.2A Sections 3.2 and 3.3), NASA policy, or accepted practice.

Identify Functions that are Central to the Human Role – Certain functions are central to the human role based on the desired concept of operations. The strong preference is for these functions to be performed by personnel. If a function is not central to the human role, it may be advisable to automate it so that its performance does not interfere with functions that are central to that role.

Identify Function Characteristics that Indicate Automation is Essential – Evaluate function characteristics to determine whether automation is essential, e.g., where it can be expected that the demands exceed human capabilities. Specifically, automation should be considered for any function having these requirements and characteristics:

- Manual performance of the function raises health and safety concerns
- The function has to be performed very rapidly
- The function requires precision that exceeds human capabilities
- The required performance reliability exceeds typical human reliability

Next, it must be determined whether it is technically feasible to automate the task, and if so, whether it is cost effective. Even when automated, there may be reasons to design in some level of human involvement, e.g.:

- The function is a core human responsibility
- There are situations where circumstances could make the automatic response inappropriate
- It is desirable to keep personnel "in the loop" in the event that they have to take over control
- It is important to keep personnel involved to support their other functional responsibilities
- Human involvement is a deliberate choice to require attention and effort from personnel in order to preclude boredom

If none of these reasons exists and it is cost-effective to do so, then full automation is recommended. Note that this does not mean personnel will not have to be aware of the automatic actions. If some human involvement is warranted, then some of the basic activities needed to perform the function should be designed for partial automation.

In the paragraphs immediately above, functions that are central to the human role were considered, but also have characteristics indicating that automation is essential. However, if automation is not essential, the next consideration should be whether the function has characteristics indicating some automation is warranted (e.g., where automation is not essential, but the characteristics challenge human performance). Specifically, some automation support should be considered for any functions having the following characteristics:

- Very complex to perform
- Requires many repetitive actions (such actions can produce fatigue and boredom that can negatively impact human performance)
- Creates high cognitive workload
- Creates long periods of boredom
- Must be performed during physiological circadian low points
- Creates high physical workload or fatigue
- Performance of the function interferes with performance of another function

When these characteristics exist, full manual performance may be error prone, thus some support should be developed. If it is both feasible and cost effective to automate, then automating parts of the function should be considered. Where it is not feasible or cost effective to automate, then the function should be performed manually and task supports should be developed to assist personnel performance.

When automation is desirable or essential, but is not feasible, the need for the function to be performed must be reconsidered. Similarly, if necessary task support is very complex, the task should be reconsidered.

4. Evaluate Allocations across Scenarios – As noted above, the demands on personnel may not be constant across different scenarios. When the same allocation result is obtained across scenarios, then a static allocation can be designed. That is, the function will always be manual, fully automatic, partially automatic, or manual with task support. When the allocations change across scenarios, the functions are candidates for dynamic allocation; e.g., performed manually in some situations and automatically in others.

5. Evaluate Overall Personnel Role – It is important to evaluate the net effect of all human allocations to ensure that a logical and coherent role for personnel has been defined and that it is within acceptable workload levels.

6. Verify Allocations – Verification of the acceptability of the allocations is a continuous and ongoing process. While initially qualitative evaluations as discussed here are necessary, allocation acceptability is continuously evaluated as part of later design activities. When mockups, simulators, and other tools become available, function allocations can be evaluated by measuring actual performance.

Additional information on Functional Requirements Analysis and Allocation can be found in the following source(s):

Billings (1997)
DoD (1998)
EPRI (2005)
O'Hara et al. (2004)

3.4 Task Analysis

To accomplish their assigned functions, personnel must perform tasks. Generally, the term "task" is used to refer to a group of activities that have a common purpose. The objective of task analysis is to specify the requirements for successful task performance, e.g., what alarms, information, controls, communications, and procedures are needed.

Task analysis is actually a family of techniques. For example, Kirwan and Ainsworth (1992) list over 40 tasks analysis techniques. A single technique is not adequate for all situations because tasks can be very different from one another. Some tasks are sequential and well defined, like starting a system. Other tasks are ill defined and not sequential, like fault-detection and troubleshooting. Different task analysis methods are better suited to different tasks. 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 very ill defined and very dependent on the expertise of the user. In combination, these methods provide powerful tools for identifying task requirements.

While the specific methodology depends on the type of task analysis performed, some of the key methodological elements are outlined below:

1. Select Tasks to Analyze – It may not be necessary to perform task analysis on all tasks. For example, if a system function is well known and essentially unchanged from predecessor systems, it may not be necessary to reanalyze it. Other tasks should be analyzed.

2. Develop High-Level Task Descriptions – Once the tasks to analyze are selected, the actual task analysis is a matter of developing a high-level task description and decomposing a high-level description to a level of detail precise enough to identify the requirements for performance. Thus, task analysis is a continuation of the process of hierarchical decomposition that began in function analysis. The basic elements of a task description are:

    - Purpose – The reason a task is performed (usually to accomplish a function or higher-level element in a functional decomposition).
    - Task Initiation – The conditions, events, or situations that indicate that it is time to perform the task.

- Preconditions – The initial conditions that must be met before a task can be undertaken (including role of interlocks).
- Time – The time constraints, if any, on task performance: time available for the action and time required to do it.
- Task Termination – The conditions, events, or situations that indicate that it is time to stop the task.
- Failures – Things that can go wrong, identifying cues and alternative actions.

The actual starting point for the analysis depends on what information is already available. Existing system documentation and analyses, subject matter experts, operational procedures, discussions with personnel, walkthroughs, and evaluations are all potential sources of information for task analysis.

3. Develop Detailed Task Descriptions – Developing detailed task descriptions involves the following steps:

   - Further decomposition of tasks from high-level to low-level descriptions
   - Evaluating the completeness of the task decomposition
   - Identifying the relationship between task elements (such as which tasks are sequential and which have to be performed in parallel)
   - Developing a timeline if time-criticality or workload problems are suspected
   - Identifying additional considerations as needed

4. Identify Task Requirements – Once the task is decomposed to a sufficient level of detail, the specific requirements for personnel to properly perform the task should be identified. The categories of task requirements are identified in Table HF-2. These requirements are a major input to HSI, procedure, and training design. All of the items listed in Table HF-2 are not necessarily needed in every task analysis.

Table HF-2. General Task Requirements Considerations

Categories of Requirements	Examples
Information Requirements	• Parameter values (units, precision, and accuracy) • Display format (analog format device, numerical readout, binary status indicator) • Parameter trends (e.g., rate of change, direction of change) • Parameter limits (e.g., normal ranges, hi/lo alarm limits) • System or equipment state (e.g., operating state, availability) • Cautions/warnings • Feedback required to indicate adequacy of task performance • Task-related alarms
Decision-making Requirements	• Evaluations to be performed by user • Criteria for making decision • Risks associated with making a wrong decision
Response Requirements	• Type of action to be taken • Time available and temporal constraints • Accuracy needed • Frequency • Reach and movements needed to take an action • Alternate means of accomplishing the action (e.g., backup controls)
Communication Requirements	• Personnel communication (such as for trouble shooting or when multiple users work on the system) • Human-machine communication demands
Workload	• Physical, cognitive, overlap of tasks (serial versus parallel versus concurrent tasks)
Task Support Requirements	• Special and protective clothing • Special tools • Job aids or reference materials required
Workplace Factors	• Workspace envelope required by action taken • Typical and extreme environmental conditions, such as lighting, temp, noise

It is crucial that the task analysis for any one function/subsystem be conducted in the context of the overall set of tasks that must be performed in the same timeframe. Designs that may be completely adequate if the operator has no other tasks may be dangerously inadequate in the presence of competing task demands.

Task analysis provides detailed information about what is needed to perform tasks. This information has many uses in subsequent analyses, including: staffing, error analysis, HSI and procedure design, training, and verification and validation (V&V).

Additional information on Task Analysis can be found in the following sources:

Crandall et al. (2006)
Diaper (2004)
DoD (1998)
EPRI (2005)
Kirwan & Ainsworth (1992)
O'Hara et al (2004)
Shraagen et al. (2000)
Vicente (1999)

3.5 Staffing, Qualifications, and Integrated Work Design

In the task analysis discussed above, the requirements for performance of human task responsibilities were determined. The objective of this activity is to determine how those tasks should be assigned to crewmembers and what overall staffing levels are required. In particular, the analysis is intended to accomplish the following: (1) allocate human tasks to individual crewmembers; (2) evaluate the qualifications needed for crewmember positions to accomplish their assigned tasks; and (3) evaluate the overall impact of all tasks when they are considered in an integrated fashion. Note that the term "crewmember" here encompasses both flight crew and ground personnel.

Key methodological elements are:

1. Assign Tasks to Crewmembers – Tasks need to be assigned to individual crewmembers. The main considerations in assigning tasks are the general areas of responsibility defined by current practices (workload is also important and will be addressed in the next method element). It is important from a human performance standpoint, to keep the task responsibilities of crewmembers related to each other. Assigning tasks on the basis of their relationship to general areas of responsibility supports situation assessment and awareness. When a crewmember works on related tasks, it is easier to maintain focus on the area of responsibility. Conversely, when a crewmember is assigned an ad hoc group of unrelated tasks, the demands associated with shifting attention between tasks detracts from maintaining situational awareness and the ability to properly monitor status and detect deviations.

2. Evaluate Integrated Task Demands and Staffing Levels – Crewmember responsibilities are defined as the complete set of tasks that the crewmember is expected to perform. The focus of this analysis is to examine the impact of task assignments on these responsibilities. A key consideration involves workload. Workload should be assessed and task assignments revised if workload is too high or low. NPR 8705.2A Section 3.4 addresses requirements for flight and ground crew workload. Also, fatigue from extended work periods and human circadian factors must be considered since reaction time and cognition are known to change as a function of the 24-hour body clock. The evaluation of integrated task demands can use

several methodologies. First, a tabletop assessment can be made by talking through the tasks. Task descriptions and detailed task analyses should be available to support the evaluation. Another way of performing this evaluation is to have crewmembers go though scenarios using simulators, mockups, and prototypes.

3. Evaluate Teamwork – In most complex systems, crewmembers work as teams. Behaviors that are typically identified as important elements of teamwork include having common and coordinated goals, maintaining shared situational awareness, engaging in open communication, and cooperative planning. Members of successful teams monitor the status of others, back each other up, actively identify errors, and question improper procedures. The allocation of individual tasks or a change in the overall responsibilities of individual crewmembers can impact teamwork. Thus this potential effect should be evaluated using operations and training experts, following the evaluation of integrated task demands.

Another important consideration is new HSI technology. An often unintended and unanticipated impact of technology, such as the introduction of intelligent agents, is its effect on crewmember's responsibilities and team processes.

4. Evaluate Staff Qualifications – Personnel will require specific knowledge, skills, and abilities (KSAs) in order to perform their assigned task. The staffing and task analyses should be evaluated by operations and training experts to identify the needed KSAs for each crewmember.

Additional information on Staffing, Qualifications, and Integrated Work Design can be found in the following sources:

DoD (1998)
EPRI (2005)
O'Hara et al. (2004)

3.6 Human Error, Reliability Analysis, and Risk Assessment

This activity is performed to evaluate the potential for, and mechanisms of, human error in system operation and maintenance. Human error analysis can be performed for any number of reasons related to the optimization of training, performance, equipment design and safety. Human reliability analysis (HRA) implies a systems model where in conjunction with equipment reliability considerations, the probability of human failure is determined for risk-significant actions and decisions. When performing either human error analysis or human reliability analysis, significant personnel tasks including aspects of human-system interaction described earlier in this chapter will be analyzed in detail such that the circumstances and conditions surrounding them are sufficiently understood to allow for the identification and implementation of error-tolerant design strategies (minimize personnel errors, allow their detection, and provide recovery capability). These insights can be applied to manage the potential for errors through the design of the HSIs, procedures, training, and automation. Significant tasks are those that impact mission success, the safety of system operations, and where personnel safety is an issue. For example, when considering significant tasks for in-flight operations, any errors that have the potential to contribute to loss of mission or loss of crew would be analyzed and the means to

make current designs error-tolerant identified. NPR 8702.5A (Section 1.6.2.3, Requirement 34399) requires the Program Manager "develop systems engineering models, compatible with the risk model developed ... to estimate and allocate component, subsystem, and *human reliability* values throughout the development and operation of the system." For a review of current HRA methods with potential applicability for CEV, see Chandler et al. (2006).

Key methodological elements are:

1. Identify Personnel Tasks to Analyze – When analyzing complex systems, detailed error analysis of all personnel actions is not feasible. Therefore, it is typically necessary to develop screening criteria to select the actions to evaluate. There are several approaches that can be used. First, the task analysis conducted should have had an assessment of task failures. This can provide input to identify significant human actions. Second, qualitative information can be obtained from subject matter experts and system personnel to identify important tasks. Third, failure analysis techniques, such as HFPFMEA can be used to systematically assess the potential for human task failures. Finally, formal risk models, such as PRA, also called Probabilistic Safety Analysis (PSA), can be used to quantitatively identify the effect of human task failure on measure of system risk. HRA is the term used to describe the human factors analysis to determine the probability of human error of tasks modeled in the PRA.

An overview of the HRA process can be found in Systematic Human Action Reliability Procedure (SHARP) (EPRI 1999) and in IEEE STD 1082 (IEEE 1997). These procedures help the HRA analyst to determine specific significant risk events. As part of this process models are developed that include human and machine components represented in fault trees. Failure probabilities are determined for equipment- and human-related events. Recently, in NUREG 1792 (2006), the US Nuclear Regulatory Commission (NRC) has provided an overview of good practices for HRA that can be used as overall guidance. Generally speaking, HRA analyses should be tailored to the level of the overall analysis, should address dependency, uncertainty, and performance shaping factors, should be based upon a generally accepted error taxonomy, and should reference an underlying model of human performance. A benefit of the use of risk models is that they provide the capability to perform sensitivity analyses to determine the relative importance of various human and machine failures, in isolation or in combination.

2. Augment Task Descriptions – Once important personnel tasks are identified, they are analyzed in detail, with a focus on error-forcing situations and contexts. An error-forcing context represents the combined effect of performance shaping factors (PSFs) and system conditions that create a situation in which the probability of human error is high. Generally, PSFs are factors that influence human performance including such things as the availability of procedures, time available to perform, task complexity, training, HSI design features, and stress. For non-ground based operations, such as EVA, influencing factors associated with bioastronautics should also be identified.

The tasks descriptions developed in task analyses can be used as the starting place for this analysis. The descriptions should be augmented with details concerning how error might occur, circumstances that predispose toward (or mitigate against) errors, and pertinent characteristics of

the HSI, if available at the time of the analysis. Augmenting the task descriptions will require subject matter experts; at a minimum, personnel who are expected to perform the tasks should be consulted. Table HF-3 contains examples of the questions that can be asked of personnel in the course of reviewing or talking through the task to be analyzed.

Table HF-3. Sample Questions for Human Error Analysis

- Are there any reasonable and credible adverse conditions, occurring either coincidentally with the event or in a casual relationship to it (e.g. a loss of some instrumentation due to a senor failure) which could affect the level of performance significantly?
- How stressful do you think the scenario would be for the operating team? Have you been in any events like this one, or in any other emergencies/abnormalities? Would you anticipate this being more or less stressful?
- What do you believe would be the most credible way in which this task could fail?
- Can you think of any errors or unintended actions that could delay the task's completion or jeopardize it entirely?
- Are there any problems if this task is interrupted prior to completion?
- Are there any steps in performing the task that may be confusing, and in which errors may occur?
- Is adequate and understandable information available at each step of the task to support decision-making and selection of appropriate response actions?
- Is access to any control, or possible confusion between different controls, a possible problem that could cause an error?
- Is task execution either dependent upon or subject to influence from different organizations such as task sharing between the flight crew and Mission Control? If so, what is the resource allocation?

3. Identify Potential Errors and Management Approaches – Once the human error considerations have been added to the selected tasks descriptions, the tasks should be reviewed to explicitly identify potential errors and changes to the task that might reduce the likelihood of errors or mitigate their consequences.

Finally, it is noted that human performance variability is a well-recognized threat to the reliability of all systems that require humans to perform critical tasks. Experience in a range of industries such as nuclear power and aviation has demonstrated that for continued system reliability, it is necessary to have a non-punitive incident reporting system that focuses on human error. For such as system to function, personnel must be encouraged to report errors and other operational problems, and the reported incidents must be analyzed to identify necessary corrective actions. The Columbia Accident Investigation Board (NASA CAIB, 2003) noted that NASA has historically had difficulty making use of incident data.

Additional information on Human Error and Reliability Analysis can be found in the following sources.

NPR 8705.2A, Appendix C.6.7
NPR 7120.5C Sec 3.2.5.2d
NPR 8000.4
NASA/OSMA Technical Report (December 2006) Human Reliability Analysis Methods Selection Guidance for NASA
DoD (1998) MIL-H-46855B
EPRI (1999) SHARP1
EPRI (2005)
Fields et al. (1997)
Forester et al. (2006)
Gertman & Blackman (1994)
Hollnagel (1998)
IEEE STD 1082 (1997) Human Action Reliability Procedure
JSC 29867 (2002)
Kirwan, B. (1994)
Kolaczkowski et al. (2005)
O'Hara et al (2004)
Reason, J. (1990)
Woods, et al. (1994)

3.7 Human-System Interface and Procedure Design

NPR8705.2A Section 3.2 requires that the crew of space systems be provided with interfaces to monitor and control critical functions as well as receive feedback for all commands for critical functions. Similar requirements for Ground Control are found in NPR8705.2A Section 3.3. The HSI provides the resources needed by personnel to interact with the systems. HSIs include alarms, displays, controls, decision support aids, and their integration into workstations and control centers. HSI also includes elements of the system with which personnel (beyond flight crew) interact during construction, test and maintenance, such as connectors, fasteners and test systems. A well-designed HSI has the characteristics outlined in Table HF-4.

Table HF-4. General Characteristics of a Well-Designed HSI

Accurately represents the system
Meets user expectations
Supports situation awareness and crew task performance
Minimizes secondary tasks and distractions
Balances workload
Is compatible with users' cognitive and physical characteristics
Is tolerant to error
Is simple to use (simplest design possible)
Is standardized and consistent throughout
Provides information and feedback in a timely way
Provides a means to obtain explanations where needed
Provides guidance and help
Provides appropriate flexibility so it can be adapted to unique situations and personal preferences

Key methodological elements are:

1. Identify HFE Design Requirements – The analyses discussed in previous sections result in requirements for the HSI and procedures. For example, the staffing analysis identified the crew size and the roles and responsibilities of various crewmembers. The task analyses identify the detailed requirements for performing tasks. Human error analysis identifies requirements where error tolerance is needed.

There are other requirements for designing the workspace and environment based on the overall concept of operations, e.g., shirt-sleeve versus extravehicular activity (EVA) pressure suit environment. Other engineering requirements exist that also impact the design of the HSI, such as available space, anticipated power, etc. Together, these requirements provide a framework within which the HSIs can be designed.

Human factors standards such as MIL STD 1472 and NASA STD 3000 specify good practices for the design of equipment, not only for operability but also for maintainability. Examples of good practices for maintainability are given in Table HF-5.

Table HF-5. Examples of Good Practices for Equipment Design

Equipment that has the same form and function shall be interchangeable throughout a system and related systems. If equipment is not interchangeable functionally, it shall not be interchangeable physically. MIL STD 1472 5.9.1.7
Connectors serving the same or similar functions shall be designed to preclude mismatching and/or misalignment. MIL STD 1472 5.9.1.7
Susceptibility to abuse. Cables shall be routed or protected to preclude mechanical damage and abuse, including damage by doors, lids, use as steps or hand holds, or being bent or twisted sharply or repeatedly. MIL STD 1472 5.9.13.6

2. Develop and Select Concept Design – Alternative ways of meeting the requirements should be identified or developed. The reason that alternatives are recommended in this guidance is that they provide an opportunity to explore tradeoffs between different approaches. Evaluating alternative designs and getting personnel feedback on them can help the identification of the best solution. Evaluation methods can include:

   - trade-off evaluations
   - personnel opinions and usability evaluations
   - performance-based tests and evaluations

3. Style Guide Development – Once a concept design is selected, a style guide is developed. A system-specific style guide defines the detailed characteristics and functions of the HSI elements. HSI design guidance exists at different levels of specificity. Industry guidelines and standards, such as NASA-STD-3000 (and its successors for the Constellation program), generally provide high-level guidance. However, high-level guidance cannot be used as is for design. The guidance must be made more specific and precise, which is the role of a style guide. A style guide provides detailed specifications or rules that describe the characteristics and functions of a specific system's HSI, such as overall cockpit layout, display screen organization, the way system features and functions are presented to personnel, display navigational features and functions, and specific design features such as display fonts and use of color. Thus, for example, a general HSI guideline may state the "A standard display screen organization should be evident for the location of various HSI functions (such as a data display zone, control zone, or message zone) from one display to another" (NRC, 2002, guideline 1.5-1). A system-specific style guide can implement this guideline as follows: "Each screen will be divided into four zones: an upper zone providing label and identifying information; a left zone providing navigation controls; a lower zone providing alarm, status, and message information; and a large center zone displaying user selected information."

Use of a style guide leads to consistency across the HSI design, even though the design may be developed by different design teams. In addition, use of HFE guidelines helps the design to be

compatible with human physiological and cognitive characteristics. Users bring their physiological and cognitive characteristics to their interaction with HSIs. The HSI must accommodate human visual, auditory, and haptic perception, information processing characteristics, physical size, and strength. Fortunately, the design engineers do not have to determine these characteristics for each project. Many physiological and cognitive characteristics that are important to HSI design are already reflected in the HFE guidelines.

4. Detailed Design – With the selected concept design and style guide, the detailed design of the HSIs and procedures can be completed. There are usually additional considerations that have to be addressed in the detailed design, such as:
    - Differing levels of automation
    - Supporting teamwork
    - Long-Term HSI use
    - HSI use under varying environmental conditions
    - HSI test, inspect, and maintenance
    - Coping with HSI and instrumentation and control degradation and failure

Designing for error tolerance is a significant consideration in detailed design. This means designing HSIs to:

- minimize the occurrence of user errors
- provide a means for users to detect errors when they are made
- provide means to gracefully correct errors

While it is a good practice to make HSIs tolerant to all errors, it is especially significant when addressing important human tasks—i.e., those with potentially significant impact on mission success, safety, and equipment and personnel protection.

The first step is to ensure that a complete HFE analysis exists. Designing for error tolerance begins with the earlier HFE analyses, specifically:

- identification of operating experience related to the important human action
- consideration of the level of automation of the important human action
- task analysis of the important human action
- analysis of human errors associated with the important human action
- analysis of the staffing and qualifications associated with the human action

These analyses should have already been performed. However, if they have not, then they should be performed at this point so that the task requirements of the action are known.

A general approach to making an HSI more error tolerant is to ensure that the primary task is supported. Primary tasks are those directly related to system operations, including monitoring, detection, situation assessment, response planning, and response implementation. To make sure

the primary task is supported, the key task elements have to be identified and explicitly addressed in the design. Table HF-3 identifies these key elements.

Next, secondary tasks should be minimized. Secondary tasks are those performed when interfacing with the system, but are not directed to the primary task. They may include: navigating through and paging displays, searching for data, and making decisions regarding how to configure the interface. Minimizing these tasks helps prevent error because it leaves more attention and cognitive resources available for the primary tasks. The existence of secondary tasks, such as display navigation, should be examined and minimized to the extent possible. The use of several of the HSI design techniques identified above, such as a task-based display or a computer-based procedure, can help to minimize secondary tasks. Modern display navigation techniques can also help. For example, a mouse click on a sensor symbol for a controlled process variable can result in the display of the related process control system and related HSI in addition to obtaining a trend plot of the controlled variable.

The analysis of human error (see Section 3.6) may have identified specific mechanisms for human error along with suggested design features to consider adding to the design to help manage or mitigate the errors. For example, if two or more situations are very similar yet require different responses, mistaking one situation for the other is an error. Designing HSI features to support personnel in discriminating between the situations can minimize this type of error. This can involve something as simple as providing information on a display that identifies the key parameters that distinguish situation A from B and the current status of each. This will aid personnel to evaluate the current conditions and identify which situation exists. A more sophisticated solution is to develop a decision aid that automatically analyzes the conditions and identifies the correct situation.

Finally, performance of important tasks can also be supported with procedures and specific training to provide the familiarization necessary to perform the tasks properly. Training can identify specific task performance criteria, the mastery of which can be assessed as a normal part of the training program. Training can also explicitly address potentially critical errors identified by the human error analysis or by the design team.

It is also worth noting here that “Design for Maintainability” issues, which pertain to onboard maintenance activities both in shirtsleeve and EVA pressure suit work environments and are associated with ergonomic and anthropomorphic factors (NASA-STD-3000, sections 11 and 14), also impact design reliability in other spacecraft system domains such as mechanisms, avionics, GN&C.

Additional information on HSI and procedure design can be found in the following sources.

NASA STD-3000 Volumes I and II.
NPR 8705.2A Section 3, and Appendix C.7-,C.8,C.9
MIL-STD-1472
O’Hara et al. (2002) NUREG-0711 rev 2
O’Hara et al. (2005) EPRI 1010042

3.8 Training Program Design

Personnel training is an important factor in ensuring safe and reliable system operation and maintenance. The objective of a training program is to provide personnel with the skills, knowledge, and abilities to properly perform their roles and responsibilities.

Key methodological elements are:

1. General Considerations – The training program should be based on a "systems approach to training" methodology. The overall scope of training should be defined including the following:

    - categories of personnel to be trained (e.g., flight crew, ground support)
    - categories of training (e.g., initial, refresher, just-in-time)
    - specific conditions (e.g., normal, contingency, emergency)
    - specific operational activities (e.g., maintenance)

The roles of all organizations involved in the development of training should be identified and the qualifications of organizations and personnel involved in the development and conduct of training should be defined.

2. Analyze Tasks and Identify Learning Objectives – Training programs should be based on the systematic analysis of job and task requirements. This analysis should include the results from other HFE activities. Learning objectives should be derived from an analysis of desired performance following training. Learning objectives should address the knowledge and skill attributes associated with all relevant dimensions of the trainee's job, such as interactions with the system, the HSIs, and other personnel.

3. Develop the Content – The design of the training program should be defined to specify how learning objectives will be conveyed to the trainee. The definition should include:

    - The use of media such as lecture, simulation, and on-the-job training to convey particular categories of learning objectives
    - Specific conditions and scenarios to be used
    - Training implementation considerations such as the temporal order and schedule of training segments

Factual knowledge should be taught within the context of actual tasks so that personnel learn to apply it in the work environment. The context of the job should be defined, and it should be represented meaningfully to help trainees link knowledge to the job's requirements.

Training programs for developing skills should be structured so that the training environment is consistent with the level of skill being taught. It should support skill acquisition and long-term retention by allowing trainees to manage cognitive demands. For example, trainees should not

be placed in environments that teach high-level skills, such as coordinating control actions among crewmembers, before they have mastered requisite, low-level skills, such as how to manipulate control devices.

Training should address strategies for decision-making related to subsystems, HSIs, and procedures. It should include rules for accessing and interpreting information and heuristics for interpreting symptoms of failures of systems, HSIs, and procedures.

4. Training Facilities and Resources – Facilities and resources such as full-mission simulators, part-task training simulators, mockups, equipment replicas, and classrooms needed to satisfy training design requirements should be defined.

5. Implement Training – Implementation of training based on the learning objectives and prepared course content.

6. Evaluate and Modify the Training Program – Methods for evaluating the overall effectiveness of the training programs and trainee mastery of training objectives should be defined, including written and oral tests and review of personnel performance during walkthroughs, simulator exercises, and on-the-job. Evaluation criteria for training objectives should be defined for individual training modules. Evaluation and revision of the training based on the performance of trained personnel in the job setting should be built into the program.

Methods for verifying the accuracy and completeness of training course materials should be defined as well. Procedures for refining and updating the content and conduct of training should be established, including procedures for tracking training course modifications.

7. Provide Periodic Refresher – Personnel should undergo periodic refresher training. Any changes or increases in refresher training should be evaluated.

Additional information on Training Programs can be found in the following sources.

NPR 7120.5C.
U.S. Marine Corps. (2004)
O'Hara et al (2004)

3.9 HFE Verification and Validation

V&V evaluations comprehensively determine that the design conforms to HFE principles and that it enables personnel to successfully perform their tasks to achieve system safety and operational goals. The HFE aspects of V&V help to ensures that:

- HSIs and procedures support task requirements
- HSIs and procedures are designed to accommodate human capabilities and limitations
- The integrated system design (i.e., hardware, software, and personnel elements) meets mission objectives and performance requirements

Key methodological elements are:

1. HSI Task Support Verification – This is an evaluation to verify that the HSI and procedures support personnel task requirements, e.g., that all alarms, information, and control capabilities required for personnel tasks are provided, and that task requirements are defined by the task analyses. The design is examined to verify that identified requirements are available in the design.

2. HFE Design Verification – This is an evaluation to verify that the HSI is designed to accommodate human capabilities and limitations as reflected in HFE guidelines. The design should be evaluated to ensure its conformance with HFE guideline, such as those provided in NASA-STD-3000 (and its successors for the Constellation program) or a system style guide (see Section 3.8).

3. Integrated System Validation – This is an evaluation using performance-based tests to determine whether an integrated system design (i.e., hardware, software, and personnel elements) meets performance requirements and supports safe and reliable operation of the system. NPR8702.5 Section 1.6.6 mandates human-in-the-loop testing involving flight, ground processing, and mission support crews "to verify that the system design meets the human performance requirements during system operation and in-flight maintenance consistent with the anticipated mission operations concept and anticipated mission duration" (Requirement 34253). This type of evaluation is also referred to as "operational testing" (Meister 1986). This assessment will often be made using a high-fidelity simulator because it is often impractical to test how well the integrated system responds to design basis events with the actual system in the field.

These evaluations identify potential design problems that should be assessed for importance and corrected if necessary.

Additional information on V&V can be found in the following sources.

NASA (2005) NPR8705.2A, Sec 1.6.6
Charlton & O'Brien, (2002).
DoD. (1998).
Meister (1986).
O'Hara, et al. (1997).
Wise et al. (1993).

3.10 In-Service Monitoring

System evaluation should not end once a system is deployed in the field. This activity is performed to identify and address issues and lessons learned that arise once a new system is in operation. Examples include an incorrect label on a process display, an HSI function that behaves differently in the simulator than in the operational environment, and a change in the way a task is performed that creates unanticipated difficulties. Treating these types of issues in a formal program can help to systematically identify and address issues, rather than depending upon anecdotal information and ad hoc fixes.

Key methodological elements are:

1. Planning and Administration – Specific planning for the in-service monitoring activity is essential. Resources and personnel are needed to support the monitoring activities. Even though only modest effort will be required for most in-service monitoring, if no effort or funds are explicitly allocated to support it, it will not be done.

2. Establish a Team –To carry out effective in-service monitoring, it will be necessary to establish an In-Service Monitoring Team to be responsible for each portion of the activity. Over the monitoring period, the team will be responsible for:

    - collecting information
    - accessing individuals as necessary based on specialized expertise
    - analyzing and resolving identified issues
    - documenting the results of the in-service monitoring program and preparing brief summaries of the monitoring effort and the conclusions reached

3. Collect Data – Methods must be in place to enable personnel to not only identify problems that are observed, but also capture useful positive feedback. Some of the methods used include: problem reporting sheets users can use to record issues that arise, user interviews, and observation of work practices (where possible). Ultimately, such information should contribute to an active "Lessons Learned" database.

4. Screen Issues for Importance – Issues identified should be evaluated by the team to determine their importance.

5. Develop and Implement Solutions – For significant issues, solutions need to be developed, tested, and implemented.

Additional information on In-Service Monitoring can be found in the following sources:

NPR 8705.2A Sec 1.6.6
EPRI (2005)

3.11 Test and Evaluation

This activity is an integral part of the entire HFE process and spans the full design life cycle. For example, tests and evaluations can be performed to resolve a tradeoff (i.e., whether to use touch screen or mouse input), obtain design information (i.e., determine the meaning of a set of icons), or to try out a new approach (i.e., web-like monitoring and control of remote equipment). Information from users also supports performing evaluations, for example, to evaluate whether the design meets performance requirements. Tests and evaluations also provide a valuable means of obtaining information and feedback from users.

Test and evaluation methods include:

- Interviews of users
- Surveys, questionnaires, and rating scales
- Focus groups
- Observational studies
- Walk-throughs using drawings, mockups, or prototypes
- Performance-based tests, such as can be conducted on a full-mission simulator
- Computer modeling

Each has key methodological considerations that include the selection of participants, selection of test bed(s), scenario selection and design, test design, selection of performance measures and criteria for evaluation, and data analysis. How each of these is addressed depends on the type of test/evaluation being performed and when it is performed (early versus late in the design process).

Additional information on Test and Evaluation can be found in the following sources:

NPR 8705.2A Sec 1.6.6
Charlton & O'Brien, (2002).
EPRI (2005)
Meister (1986)
O'Hara, et al. (1997).

4.0 Historical Perspective and Past Performance

4.1 Historical Perspective

HFE, often termed "human engineering" in heritage NASA systems, was recognized for its specific role in aspects of spacecraft systems that were in direct contact with the flight crew. These aspects include only several of the contemporary HFE activities listed above in Section 3.5. Predominant among heritage HFE system activities were those associated with HSI and procedure design. Other HFE spacecraft system DDT&E activities listed in Section 1.3, such as function analysis, task analysis, and risk analysis, were traditionally carried out within other organizations such as Systems Engineering (Goodman, 1972), often without the participation of formally trained HFE experts. A series of 114 NASA Technical Notes[4], published in the early and mid-1970's, discusses design and development history of the various Apollo spacecraft systems. Five of these Apollo experience reports associated with crew station integration are overtly in the purview of traditional human engineering (Allen & Nussman, 1976; Landoc & Nussman, 1975; Wittler, 1975; Hix, 1973; Wheelwright, 1973). A much greater number of these Apollo experience reports describe HFE-like and HFE-related activities that were carried out by other organizations as part of development of their respective system elements. (e.g., Hyle,

[4]Available at http://ntrs.nasa.gov/. Search the archive for the term "Apollo experience report", including the quotation marks.

Foggatt, & Weber, 1972; Burtzlaff, 1972; Graves & Harpold, 1972; Hyle & Lunde, 1972; and many others)

Prominent among heritage space system HSI responsibilities were the design, development, test, and evaluation of "active" interfaces (i.e., display and controls—D&C) to monitor and operate the spacecraft, as well as the "passive" crew-vehicle interface elements such as seating, handholds, windows, and lighting. Associated with both active and passive interface elements was the need to ensure that the crew could safely, effectively, and *reliably* use these space system components given the rigors of the space environment. Thus, the role of human engineering was historically not only to develop and apply requirements for flight crew anthropometry (i.e., reach envelopes and force capabilities) and perceptual capacity (e.g., vision and audition), but also to attend to environment factors (e.g., hyper- and micro-gravity, vibration, atmosphere, thermal, radiation) ensuring that they were physiologically tolerable (i.e., habitable) and would not unacceptably impede crew task performance. Ensuring that the spacecraft environment met human engineering habitability requirements was, in part, the responsibility of Environment Control and Life Support Systems.

Critical human engineering data employed in the design of early NASA systems to ensure successful performance by the flight crew (including the impact of the space environment on habitability) were initially collected from early (post World War II) aerospace flight experience and associated laboratory studies into the Bioastronautics Data Books (NASA SP-3006, Edition 1, 1964; Edition 2, 1973). These early data along with interface design experience from Apollo and Skylab systems were ultimately consolidated into the Man-Systems Integration Standards (NASA-STD-3000, 1987; Rev B, 1995).

Trends in human interface procedures and D&C design practices for crewed NASA systems are traceable back to the experimental aircraft of the 1950s, through sub-orbital, orbital (Mercury and Gemini) and lunar flight (Apollo). The introduction and growth of onboard computer capabilities during the Apollo and later in the Shuttle programs first raised a still ongoing discussion of the roles of automated and manual systems and the relative allocation of control functions between the two. Certain mission functions such as lunar landing were considered too critical to *not* be principally reliant upon direct manual control with through the window (plus other on-board instrument) feedback. In general, automatic elements were designed to allow manual override in contingency operation (Landoc & Nussman, 1975).

Initial research studies in spacecraft simulators of human performance as a quantitative indicator of system reliability, essentially a precursor to current human reliability analysis (HRA), started during the Gemini and Apollo programs. (Grodsky & Flaherty, 1965) The general design philosophies that governed human interface design for Apollo Lunar Module (LM) and Command Module (CM) as listed by Landoc and Nussman (1975) are captured verbatim in Table HF-6. Embodying what Landoc and Nussman term the "most fundamental and influential" requirements for D&C design and use, these philosophies followed principles from previous aerospace systems and actually preceded Apollo D&C development. Recognizable in this list are antecedents that underlie many of the human system integration principles for robustness, redundancy, and reliability in the current NPR 8705.2A and NASA-STD-3000, and that are the foundation for HSIR and other CARD requirements presently in development. Of

note, Landoc and Nussman's list only provides single fault (i.e., "arm-fire") as opposed to two-fault (i.e., "ready-arm-fire" or "arm-arm-fire") resistance to inadvertent human action.

Table HF-6. Fundamental and Influential Requirements for Apollo D&C Systems (Landoc & Nussman, 1975). Associated NASA NPR8705.2A requirements are shown in red.

1. No single display or control failure would jeopardize the safety of the flight crew or be cause for an abort. [cf. NPR8705.2A, Req 34422]
2. The D&C design would allow a single crewman to fly either the CM or the LM to safety (i.e., the LM to lunar orbit or the CM to Earth).
3. Displays and controls would be provided to enable the flight crew to control the vehicle and to manage the subsystems during all mission phases. [cf. NPR8705.2A, Req 34483, Req 34495]
4. Information would be presented so as to permit rapid assessment of critical system status without resorting to extensive troubleshooting procedures to identify malfunctions.
5. Normal subsystem operation would not require continuous monitoring or control by the crewmen.
6. Displays and controls that were susceptible to damage or to inadvertent actuation as a result of normal crew operations would be guarded appropriately. [cf. NPR8705.2A, Req 34426, Figure 5]
7. Existing proven design concepts would be used as much as practical.
8. The D&C of the CM and the LM would be standardized to improve crew efficiency by the elimination of conflicting designs.
9. All D&C would be designed for satisfactory operation by a pressure-suited crewman, and all D&C used during accelerated flight would be designed for operation by a pressure-suited, fully restrained crewman.
10. Primary command would be onboard the spacecraft. The capability would exist to perform the mission without dependence on ground-based information; however, the use of ground-based information to increase reliability, accuracy, or performance would not be precluded. [cf. NPR8705.2A, Req 34463, Req 34481]
11. Automatic systems would be used to obtain precision, to speed response, or to relieve the crewmen of tedious tasks; but all automatic control modes would have a manual backup.
12. Initiation of any abort would be onboard, and the crewmen would have the primary responsibility. [cf. NPR8705.2A, Req 34481, Req 34487, Req 34488]
13. Annunciator displays would be provided to indicate critical malfunctions of onboard systems. Activation of these displays would be announced to the crewmen by both visible and audible master alarm signals.
14. Displays and controls would be furnished to provide the LM with the capability for a visual or an instrument landing.
15. Crew launch-abort initiation would be based on at least two cues. Within the aforementioned general philosophies, detailed design practices were established.

4.2 Past Performance

4.2.1 Failures and Successes

The Shuttle Independent Assessment Team Report (NASA SIAT, 2000) identified a series of human factors problems in the Shuttle program and proposed a number of recommendations to alleviate them. Central to these were workforce and human error management issues that will also need to be considered in future missions. Key themes were the need for communication between workforce, engineering, and management, in order to foster cooperation and maintain

workforce trust and loyalty. Workforce transitions and downsizing were observed to result in a loss of corporate technical and process knowledge and in stretching the workforce too thin. Importantly, the SIAT Report identified the need to incorporate human factors in decision processes as a means to eliminate the potential for single- and multiple-point failures. Additionally, the report recommended that human error management and safety metric development "should be supported aggressively and implemented program-wide."

Problem and error tracking is essential to gauging human error and safety performance. NASA currently operates several PRACA databases, although additional incident information may also be stored in databases kept by contractors. NASA's system of reporting and storing incident information was criticized by the Columbia Accident Investigation Board under the heading of "dysfunctional databases." In 2000, the Shuttle Independent Assessment Team report also identified problems with the gathering, storage, and analysis of PRACA data within NASA. Key findings were that the PRACA system:

- Does not provide information needed by decision makers
- Suffers from missing data and inconsistent treatment of events
- Lacks sophisticated analysis tools
- Is fragmented
- Requires specific expertise and experience to extract incident information

The SIAT team made several recommendations concerning problem reporting and tracking within NASA. A key recommendation was that the PRACA system should be revised using state-of-the-art database design and information management techniques.

4.2.2 Examples of Human Factors Failures and Successes

Human-induced threats can occur at all stages of the system life cycle through Design, Manufacture, Test, Operate, and Maintain. At each of these stages, human capabilities can also enable systems to recover from, or contain the effects of, non-routine events. The 1997 collision of a Progress vehicle with the Mir space station and the consequent Spektr depressurization serves to illustrate this point. A variety of human factors failures from perceptual-motor performance, fatigue, and training currency, through to more global, ground-based organizational policy and international political issues can be seen as contributors to the accident. At the same time, the on-board crew contributed the resilience in recovering from the emergency that ultimately prevented loss of life and loss of the vehicle. (Ellis, 2000).

The following four case studies further illustrate how human performance can degrade or support system reliability. In the first two cases, the systems did not perform reliably because the design of the system was not well matched to human performance. The last two case studies illustrate how human intervention can enable a system to recover from an undesirable and unplanned-for condition.

Salyut 11 Decompression (Example of mismatch between operational demands and human capabilities)
On June 30, 1971, the Soyuz 11 capsule was returning to earth with three crewmembers on board. At an altitude of 168 km, as the capsule separated from the orbital module, misfiring pyrotechnic devices caused a pressure equalization valve to open prematurely. The valve began to vent the capsule atmosphere, a process that took between 30-50 seconds. There is evidence that the crew responded to the emergency by attempting to manually close the valve. The procedure to close the valve would have taken the crew around 60 seconds to perform, and the cosmonauts perished before the valve was half-closed. It appears that system designers did not take into account the speed with which a human operator could operate the control. (Newkirk, 1990; Johnson, 1980).

Genesis spacecraft G switches (Example of lack of test procedure to detect a human deviation)
A critical element of the Genesis spacecraft was a set of G switches designed to trigger the deployment of the spacecraft's parachutes. Due to errors in assembly drawings, the sensors were installed upside down. As a result, parachutes did not deploy when the spacecraft returned to earth. A centrifuge test that would have detected the error was deleted due to schedule pressure. In this sense, system reliability was degraded because of the absence of a "safety net" that would have captured a human error (Kerr, 2004; NASA, 2006).

FOD in Orbiter (Example of utilization of human capabilities in a non-routine maintenance situation—"diving catch")
An example of a "diving catch" provided by the Shuttle Independent Assessment Team Report is of maintenance personnel finding a lint-free pad stuffed in a tube prior to brazing a water line in the forward compartment (NASA SIAT, 2000). Maintenance personnel caught the problem outside of normal procedures. This case illustrates how unplanned human interventions during ground processing can contribute to the reliability of a system. Numerous other examples of "diving catches" are cited in Appendix 3 of the SIAT report.

A "lessons learned" appendix in the SIAT report lists a series of commercial aviation accidents in which causes ascribed to mechanical failure fundamentally were a consequence of human performance errors during maintenance. Many of the occupational stress contributors in these aviation accidents could also be observed in the Shuttle program at the time. Proposed measures to alleviate the potential for errors include use of human error management techniques and the incorporation of safety tracking metrics.

Apollo 13 (Example of use of human capabilities in a non-routine operational situation)
The example of Apollo 13 is given here as an example of how human intervention can enable systems to recover from unanticipated emergencies. After an explosion in a liquid oxygen tank damaged the service module of Apollo 13, the crew flew part of their return to earth with the unused lunar module still attached to the command module. This configuration, which had never been flown before, allowed the Apollo 13 crew to use the lunar module as a temporary "lifeboat". The safe return of the crew required problem-solving and creative thinking by mission control personnel and astronauts. A frequently cited example of this is the creation of a jury-rigged carbon dioxide scrubber that prevented CO2 from reaching dangerous levels. While

it is not possible to predict and plan for every conceivable emergency, reliable systems provide operators with the opportunity to apply creativity and flexibility to unanticipated problems. (Shayler, 2000)

5.0 Summary/"Best Practices" Indicators

Human-system interaction occurs in all phases of system development and operation of spacecraft systems. These phases include 1) design, 2) fabrication (build), 3) testing, 4) operation, and 5) maintenance. Therefore all of the indicators/questions listed below need to be evaluated for each phase of the spacecraft lifespan.

5.1 System Attributes

Considering system attributes that would accommodate and promote effective, safe, reliable and robust human interaction with spacecraft systems asks the following questions.

- Are system demands compatible with human limitations? Do they capitalize on human capabilities?
- Can the tasks demanded of people be performed reliably including under adverse conditions?
- Can the system can tolerate and recover from human-induced deviations?
- Has two-failure tolerance been built into the system wherever feasible?
- Can the system enable human capabilities to be brought to bear on non-routine, unanticipated problems?
- Does the system keep humans in the loop and enable humans to take action in situations that cannot be handled by automation?

5.2 Program Attributes

The HFE program is undertaken to achieve HFE goals and key product attributes for system reliability and robustness. The general characteristics of an HFE program for high-reliability systems should have the following key attributes:

1. Is the HFE program fully integrated into the overall engineering process from the outset?
2. Are the HFE aspects of a system should be developed, designed, and evaluated on the basis of a systems analysis that uses a "top-down" approach? Top-down refers to an approach starting at the "top" of the hierarchy with the system's high-level mission and goals. The detailed design (of the interfaces, support systems, procedures, and training) is the "bottom" of the top-down process.
3. Is HFE considered to span the full life cycle; i.e., from concept planning through operations and ultimately decommissioning/disposal?

4. Are HFE activities graded to focus the level of HFE design to where it will have greatest need in the design process?

5.3 Core HFE Activities

The HFE program comprises eleven core activities that need to be performed by the organizations (NASA, primary contractors, subcontractor) involved in the design and evaluation process. Associated with each of the eleven core HFE activities are a number of best practices to be evaluated.

1. HFE Program Planning

Does the HFE Program identify:

- general HFE program goals and scope?
- high-level concept of operations for the new system?
- HFE design team skills necessary to conduct subsequent HFE activities?
- engineering procedures (such as QA and use of an issues tracking system) to be followed?
- description of HFE products and documentation of analysis and results?
- key milestones and scheduled to ensure the timely completion of HFE products?

Are the results of the planning activity documented in a human factors program plan that can be used to manage the overall HFE effort?

2. Operating Experience Review and Lessons Learned

Are Operating Experience Review (OER) and Lessons Learned documents maintained and readily accessible to the design team? Do they provide a clear indication of issues identified, the design activities to which they are relevant, and their importance?

3. Function Analysis and Allocation

Have the various functions needed to achieve the mission been described? Has the allocation of responsibility for conducting functions, or parts of functions, to personnel, to automatic systems, or to some combination of the two been made? Is the allocation made on the basis of a function analysis to determine what is required to perform the function? Have the roles and responsibilities of personnel and automation in the performance of system functions, including how they may be changed as a result of various types of failure conditions?

4. Task Analysis

Do the task analyses specify the requirements for successful task performance, e.g., what alarms, information, controls, communications, and procedures are needed?

5. Staffing, Qualifications, and Integrated Work Design

Has it been determined how those tasks should be assigned to crewmembers and what overall staffing levels are required? In particular, has the analysis (1) allocated human tasks to individual crewmembers, (2) evaluated the qualifications need for crewmember positions to accomplish their assigned tasks, and (3) evaluated the overall impact of all tasks when they are considered in an integrated fashion?

6. Human Error and Reliability Analysis

Have significant personnel tasks (i.e., those that impact mission success, the safety of system operations, and where personnel safety is an issue) been identified and analyzed in detail? Have these been evaluated with sufficient detail so that error tolerant design strategies (minimize personnel errors, allow their detection, and provide recovery capability) can be applied to manage them, e.g., through the design of Human-System Interfaces, procedures, training, and automation?

7. Human-System Interface and Procedure Design

Does the HSI provide the resources needed by personnel to interact with the systems? Do HSIs and procedures that (1) reflect the system's functional and physical design, (2) meet personnel task requirements, (3) exhibit the general characteristics of well-designed HSI and procedures, and (4) are easy to learn and use?

8. Training Program Design

Does the training program provide personnel with the skills, knowledge, and abilities to properly perform their roles and responsibilities? Is the training program should be based on a systems approach, including the identification of learning objectives, development the course content, implementation of training, evaluation and modification of the training program, and periodic refresher training?

9. HFE Verification and Validation

Do the V&V evaluations comprehensively determine that the design conforms to HFE principles and that it enables personnel to successfully perform their tasks to achieve system safety and operational goals? Do the HFE aspects of V&V help ensure that HSIs and procedures support task requirements, HSIs and procedures are designed to accommodate human capabilities and limitations, and that the integrated system design (i.e., hardware, software, and personnel elements) meets mission objectives and performance requirements?

10. In-Service Monitoring

Does system evaluation continue once the system is deployed in the field? Does this activity identify and address issues and lessons learned that arise once a new system is in operation?

11. Test and Evaluation

Is this activity an integral part of the entire HFE process and does it span the design life-cycle?

References

Allen, L.D. & Nussman, D.A. (1976) *Apollo experience report: Crew station integration. Volume 1: Crew station design and development*. NASA-TN-D-8178

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

Burtzlaff, I.J. (1972) *Apollo experience report: Acceptance checkout equipment for the Apollo spacecraft*. NASA-TN-D-6736

Chandler, F. et al, NASA (2006). NASA/OSMA Technical Report (December 2006) Human Reliability Analysis Methods Selection Guidance for NASA.

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

Crandall, B., Klein, G., & Hoffman, R. (expected 2006). Working Minds : A Practitioner's Guide to Cognitive Task Analysis. Cambridge: MIT Press.

Diaper, D., & Stanton, N.A. (Eds.) (2004). *The Handbook of Task Analysis for Human-Computer Interaction*. Mahwah, NJ: Lawrence Erlbaum Associates.

DoD (2000) Standard Practice for System Safety (MIL-STD-882C).

DoD. (1998). Human Engineering Requirements for Military Systems, Equipment and Facilities (MIL-H-46855B). Washington, D.C.: Office of Management and Budget.

Ellis, S.R. (2000). Collision in space. *Ergonomics in Design*, *8*(1) 4-9.

EPRI (1999). SHARP1--A Revised Systematic Human Action Reliability Procedure (NP-7183-SL). Palo Alto, CA: Electric Power Research Institute.

Fields, B., Harrison, M., & Wright, P. (1997). THEA: Human Error Analysis for Requirements Definition. Technical Report YCS 294. Department of Computer Science, University of York, York O10 5DD, UK.

Forester, J., Kolaczkowski, A., Lois, E. (2006) Evaluation of Human Reliability Analysis Methods Against Good Practices (NUREG-1842). Washington, D.C.: U.S. Nuclear Regulatory Commission.

Gertman, D.I., & Blackman, H.S.(1994) Human reliability and Safety Analysis Data Handbook. New York: Wiley.

Goodman, J.R. (1972) *Crew Station Aspects of Manned Spacecraft Design.* Unpublished MS Thesis. Department of Industrial Engineering, University of Illinois, Urbana-Champaign

Graves, C.A., & Harpold, J.C. (1972) *Apollo experience report: Mission planning for Apollo entry*. NASA-TN-D-6725.

Grodsky, M.A. & Flaherty, T.M. (1965). Crew reliability during simulated space flight. AIAA/AFLC/ASD Support for Manned Space flight Conference, Dayton, OH April 21-23. AIAA Paper 65-275.

Hix, M.W (1973) *Apollo experience report: Crew station integration. Volume 4: Stowage and the support team concept.* NASA-TN-D-7434.

Hollnagel E. (1998). *Cognitive Reliability and Error Analysis Method (CREAM).* Oxford UK: Elsevier Science.

Hyle, C.T. & Lunde, A.N. (1972) *Apollo experience report: The application of a computerized visualization capability to lunar missions.* NASA-TN-D-6853

Hyle, C.T., Foggatt, C.E., & Weber, B.D. (1972) *Apollo experience report: Abort planning.* NASA-TN-D-6847.

IEEE (1997) IEEE Guide for Incorporating Human Action Reliability Analysis for Nuclear Power Generating Stations. Standard 1082. New York: Institute of Electrical and Electronics Engineers.
IEEE (1998) Systems Engineering Standard 1220. New York: Institute of Electrical and Electronics Engineers.
Johnson, N. J. (1980). Handbook of Soviet Manned Space Flight. San Diego: Univelt.
JSC (2002). Human Reliability Analysis (HRA) Final Report. Volume VII: Human Error Analysis Methodology. JSC report 29867.
Kerr, R. A. (2004, 22 October). *Flipped Switch Sealed Fate of Genesis Spacecraft*. Science, 5696, p 587.
Kirwan, B. & Ainsworth, L.K. (1992). *A Guide to Task Analysis*. London: Taylor and Francis.
Kirwan, B. (1994). *A Guide to Practical Human Reliability Assessment*. London: Taylor & Francis.
Kolaczkowski, A., Forester J., Lois, E., & Cooper, S. (2005). Good Practices for Implementing Human Reliability Analysis (HRA) (NUREG-1792). Washington: U.S. Nuclear Regulatory Commission.
Landoc, W.A. & Nussman, D.A. (1975). Apollo experience report: Crew station integration. Volume 2: Crew station displays and controls. NASA-TN-D-7919.
Meister, D. (1986). *Human factors in testing and evaluation*. Amsterdam: Elsevier.
NASA (1964). *Bioastronautics Data Book*. SP-3006. (2nd Edition, 1973)
NASA (1987). *Manned-Systems Integration Standard*. NASA-STD-3000. (Rev B, 1995).
NASA (1995). *Systems Engineering Handbook*. SP-6105.
NASA (2006). *Genesis Mishap Investigation Board Report. Vol. 1*.
NASA NPR 7120.5C (2005). *Program and Project Management Processes and Requirements*.
NASA NPR 8000.4 (2002). *Risk Management Procedural Requirements*.
NASA NPR8702.5A (2005). *Human-Rating Requirements for Space Systems*.
NASA SIAT (2000) Shuttle Independent Assessment Team Report.
NASA CAIB (2003) Columbia Accident Investigation Board Report.
NESC RP-06-104, Design, Development, Test, and Evaluation Considerations for Robust and Reliable Human Rated Spacecraft Systems, NESC SEO Office, December 2006.
Newkirk, D. (1990). *Almanac of Soviet Manned Spaceflight*. Houston, TX: Gulf Publishing.
O'Hara, J., Brown, W., Lewis, P. & Persensky, J. (2002). Human-system interface design review guideline (NUREG-0700, Rev 2). Washington: U.S. Nuclear Regulatory Commission.
O'Hara, J., Fink, R., Hill, D., & Naser, J. (2005). Human Factors Guidance for Control Room and Digital Human-System Interface Design and Modification: Guidelines for Planning, Specification, Design, Licensing, Implementation, Training, Operation, and Maintenance (EPRI 1010042). Palo Alto, CA: Electric Power Research Institute.
O'Hara, J., Higgins, J., Persensky, J., Lewis, P., & Bongarra, J. (2004). Human factors engineering program review model (NUREG-0711, Rev. 2). U.S. Nuclear Regulatory Commission, Washington, D.C.
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.
Reason, J. (1990). *Human error*. New York, NY: Cambridge University Press.
Shayler, D. (1990). *Disasters and accidents in manned spaceflig*ht. New York: Springer.

Shraagen, J., Chipman, S., & Shalin, V. (2000). *Cognitive Task Analysis*. Mahwah, NJ: Lawrence Erlbaum Associates.
U.S. Marine Corps. (2004) Systems Approach to Training (SAT) Manual
Vicente, K., (1999). Cognitive Work Analysis. Toward Safe, Productive, and Healthy Computer-Based Work. New Jersey: Lawrence Erlbaum Associates.
Wheelwright, C.D. (1973) *Apollo experience report: Crew station integration. Volume 5: Lighting considerations.* NASA-TN-D-7290.
Wise, J., Hopkin, D., & Stager, P. (1993). *Verification and validation of complex systems: Human factors issues* (NATO ASI Series F, Vol. 110). Berlin: Springer-Verlag.
Wittler, F.E. (1975) *Apollo experience report: Crew station integration. Volume 3: Spacecraft hand controller development*. NASA-TN-D-7884.
Woods, D., Johannesen, L., Cook, R., & Sarter, N. (1994). Behind human error: Cognitive systems, computers, and hindsight (CSERIAC SOAR 94-01). Crew Systems Ergonomics Information Analysis Center, Wright Patterson Air Force Base, OH.

Bibliography

Boff, K., & Lincoln, J. (1988). *Engineering Data Compendium.* (Published by the US Air Force).
Boff, K. (ed.) (1986). *Handbook of Perception and Human Performance* (Multiple volumes). New York: Wiley-Interscience.
Helander, M., Landauer, T., Prabhu, P., (eds.), *Handbook of Human-Computer Interaction (2nd edition)*, Elsevier Science Publishers, Amsterdam, 1998.
International Organization for Standardization, International Standard: Ergonomic Design of Control Centres (ISO 11064). Geneva, Switzerland: ISO.
International Organization for Standardization, International Standard: Human-Centred Design Process for Interactive Systems (ISO 13407) Geneva, Switzerland: ISO.
Meister, D., *Conceptual Aspects of Human Factors*, The Johns Hopkins University Press, Baltimore, 1989.
NASA NIAT (2000) *Enhancing Mission Success—A Framework for the Future*. NASA Chief Engineer and NASA Integrated Action Team Report.
Salvendy,G. (Ed.). (2006) *Handbook of Human Factors (Third Edition)*. New York: Wiley.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
01- 12 - 2006	Technical Memorandum	July 2006- December 2006

4. TITLE AND SUBTITLE

NASA Engineering and Safety Center's Super Problem Resolution Human Factors Team Report - Design, Development, Testing, and Evaluation: Human Factors Engineering

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Adelstein, Bernard; Hobbs, Alan; O'Hara, John; and Null, Cynthia

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

843515.02.01.07.03.01.04

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

NASA Langley Research Center
Hampton, VA 23681-2199

8. PERFORMING ORGANIZATION REPORT NUMBER

L-19317 NESC-RP-06-108/05-173-E

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

National Aeronautics and Space Administration
Washington, DC 20546-0001

10. SPONSOR/MONITOR'S ACRONYM(S)

NASA

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

NASA/TM-2006-214535

12. DISTRIBUTION/AVAILABILITY STATEMENT

Unclassified - Unlimited
Subject Category 18
Availability: NASA CASI (301) 621-0390

13. SUPPLEMENTARY NOTES

An electronic version can be found at http://ntrs.nasa.gov

14. ABSTRACT

While human-system interaction occurs in all phases of system development and operation, this chapter on Human Factors in the DDT&E for Reliable Spacecraft Systems is restricted to the elements that involve “direct contact” with spacecraft systems. Such interactions will encompass all phases of human activity during the design, fabrication, testing, operation, and maintenance phases of the spacecraft lifespan. This section will therefore consider practices that would accommodate and promote effective, safe, reliable, and robust human interaction with spacecraft systems. By restricting this chapter to what the team terms “direct contact” with the spacecraft, “remote” factors not directly involved in the development and operation of the vehicle, such as management and organizational issues, have been purposely excluded. However, the design of vehicle elements that enable and promote ground control activities such as monitoring, feedback, correction and reversal (override) of on-board human and automation process are considered as per NPR8705.2A, Section 3.3.

15. SUBJECT TERMS

NESC; Spacecraft systems; Human factors; Human factors engineering (HFE); DDT&E; Life cycle; Robustness; Reliability

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			STI Help Desk (email: help@sti.nasa.gov)
					19b. TELEPHONE NUMBER *(Include area code)*
U	U	U	UU	52	(301) 621-0390