Three principles of human-system integration

ALAN HOBBS
SJSU Foundation/NASA Ames Research Center

BERNARD ADELSTEIN
NASA Ames Research Center

JOHN O'HARA
Brookhaven National Laboratory

CYNTHIA NULL
NASA Langley Research Center

Introduction

Early spacecraft such as Gemini and Apollo were developed at a time when the field of human factors was still in its adolescence. Nevertheless, human factors design principles were applied to controls and displays. In recent years, human factors considerations were key determinants of planned upgrades to the avionics of the space shuttle. The field of human factors has matured significantly since the first days of manned spaceflight. It is reasonable to expect that the profession can now make a greater contribution to the design and construction of complex equipment than was the case 40 years ago.

NASA has announced that the space shuttle fleet will be retired in 2010 and will be replaced by a new launch vehicle "Orion" to enter service in 2015. As NASA embarks on the development of the new space transport system, it must evaluate whether the design optimizes human-system integration.

Inadequate human system integration has costs not only in terms of safety and mission effectiveness, but also increases the overall complexity of the system, increases the time needed to perform tasks, complicates training and maintenance, while decreasing the capabilities of the system.

In 2006, the Astronaut Office at NASA Johnson Space Center (JSC) requested the NASA Engineering and Safety Center (NESC) to assess best practices for developing a crewed space vehicle that is both reliable and robust. The NESC defined reliability as being "free of failures throughout its mission" and robustness as "tolerant of unexpected conditions should they arise". Groups were assigned to the range of spacecraft subsystems including propulsion, structures, avionics, software, and the human element, and in each case consider how reliability and robustness can be achieved. The conclusions of the human factors group are briefly summarized in this paper. The full report can be found in Adelstein, Hobbs, O'Hara & Null (2006).

Although the terms reliability and robustness are widely used, it is no simple matter for a customer to evaluate whether a system has been designed to maximize these characteristics. A common pattern in many industries is for human factors expertise to be called in once the system design has been finalized, either to help solve problems stemming from poor design, or to certify that the system meets requirements. This paper, in contrast, is about the involvement of human factors at all stages of the design and construction process, from concept development, through to operation.

Booher (2003) distinguishes between six levels of complexity in socio-technical systems, ranging from very highly complex systems that often operate in unpredictable environments (Level A) through to devices and parts that serve limited functions in more predictable environments (Level F), see Table 1. Human/system interactions occur at all levels of the hierarchy. Good human/system interface of subsystems and parts at the D-F level is a necessary pre-condition for satisfactory system performance at higher levels, but in no way guarantees the effectiveness of the overall system.

The safety performance of complex systems is a growing area of research (see Hollnagel, Woods and Leveson, 2006). While acknowledging the need to understand the performance of complex organizations, our focus in this report was on how the human-system interfaces at the D-F level on board the Orion crew vehicle could be designed to maximize reliability and robustness. Many thousands of people perform key roles in the operation of a space transport system, from managers to control room operators. In this document however, we deal with the human factors associated with direct physical contact with the Orion vehicle during construction, testing, operation and maintenance.

Table 1. Levels of Complexity of Sociotechnical Systems (Adapted from Booher, 2003)

Sociotechnical System	Mission Area		
	Health care	**Transportation**	**Energy**
A. Very highly complex organizations	National Health System	NASA	US Department of Energy
B. Highly complex organizations	Hospital	National Airspace System	Nuclear Regulatory Commission
C. Complex organizations	Emergency department	Airline	Nuclear Power Plant
D. Major technological systems	MRI machine	ATC control Centre	Control room
E. Critical technological subsystems	Display monitor	ATC Console	Control/display
F. Devices and system parts	Catheter	Flight strip	Feed water pump

A great deal of guidance material has been produced by NASA, the US Department of Defense, and other agencies specifying in great detail human factors design standards and best practices. This material ranges from micro-level recommendations of the amount of force required to press a button, to macro-level considerations on the management of technological systems whose complexity approaches that of living things. United States Military Standard 1472 (US Department of Defense, 1999) is an example of a widely-used design standard containing human factors recommendations. The NASA System Engineering Handbook (NASA, 2007), on the other hand, overviews best practices for human factors in design. Our intention was not to re-write or replace existing standards, but to consider fundamental design characteristics that have the potential to affect the reliability and robustness of systems.

In reviewing the existing design guidance on human system integration, it became apparent that best practices for system design can be placed in two broad categories, the attributes of the *product*, and the *processes* used to develop the product. In the sections below, we consider attributes of the product that contribute to reliability and robustness. In later pages we consider the characteristics of processes.

Human Factors and Product Attributes

The "product" includes hardware, software, systems documentation, training systems, and procedures. Human factors relate to all aspects of the system life, i.e., build, test, operate and maintain, across the spectrum of operating conditions (normal and emergency). Human factors also apply to all people who come into contact with the product, including design and construction personnel, test and verification personnel, operators and maintainers.

A reliable and robust design is one that addresses the following three questions of human/system integration. First, are the task demands compatible with human capabilities and characteristics? Second, has the system been designed to cope with the inevitability of human error? Third, does the system take advantage of unique human capabilities? We consider each of these three questions below.

Question 1: Are task demands compatible with human capabilities and characteristics?

A robust and reliable system is one in which the tasks demanded of people can be performed reliably, under normal and contingency conditions. Ensuring that task demands are within the mental and physical capabilities of the user has been a central concern over the entire history of the human factors field. Examples of contraventions of this principle are displays that cannot be read under expected conditions of vibration, controls that cannot be moved with sufficient precision, or task steps that invite procedural non-compliance. In large part, design standards such as Military Standard 1472 (US Department of Defense, 1999) contain guidance on the matching of task demands to human capabilities.

The following case illustrates a mismatch between operational demands and human capabilities.

> *Salyut 11 Decompression*
>
> On June 30, 1971, the Soyuz 11 capsule was returning to earth with three crewmembers onboard. 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).

Question 2: Has the system been designed to cope with the inevitability of human error?

The observance of good design principles can decrease the probability of undesired human actions such as human error, but can never completely eliminate such actions. Robust and reliable systems are designed to tolerate and recover from human-induced disturbances. The principle of "two-fault tolerance" is one strategy to address the threat of human error. For example, the NASA Safety Manual (NASA NPR 8715.3, requires sufficient system redundancy to tolerate two failures or two human operator errors when loss of life (i.e., crew or vehicle) or mission-critical events could occur, but permits one-failure tolerance in cases where the lesser consequences of mission loss or damage or personal injury could occur. The two-failure tolerance concept is also referred to in US Military Standards (US Department of Defense, 2000) and NASA's Human-Rating Requirements for Space Systems (NASA 2005).

Error tolerance can be achieved in three ways:

(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. Examples of such features are: button/switch covers to prevent inadvertent activation, keyed connectors to prevent incompatible connections, and machine guards to prevent person entering unsafe area.

(b) Errors that are not blocked can be detected and recovered from, such as through features that permit the detection and correction of erroneous actions. Examples of error detection and correction features are: a checklist to detect an incomplete task, functional checks after maintenance, features that enable an action or command to be "undone".

(c) Undesired deviations that are not blocked, detected, or corrected, will have consequences that are minimized wherever possible. Such barriers often prevent an incident from escalating into an accident, or prevent a minor accident from developing into a major accident. Examples of consequence-limiting features are: maintenance procedures that prevent the simultaneous maintenance of parallel systems thereby quarantining the effects of errors, redundant systems, and crashworthy seats.

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).

Question 3: Does the system take advantage of unique human capabilities?

Robust systems allow human capabilities to be brought to bear on non-routine, unanticipated problems. The human performance literature has traditionally focused on the human role in system failures. As a result, the indexes of human factors texts are sometimes little more than lists of afflictions and limitations that characterize humans as creators of disturbances and generators of errors.

The positive contribution of human performance to mission success is so commonplace that we often take it for granted. In aircraft maintenance for example, fatigue cracks are often found by maintenance technicians who were not specifically looking for damage. The intelligent adaptation of humans to unanticipated situations can significantly contribute to mission success in the face of situations that were not anticipated when the system was designed. A robust system keeps the operating crew and other personnel in the loop and enables them to take action when novel situations arise. The response to the Apollo 13 emergency in 1970 is an example of how human intervention can enable systems to recover from unanticipated conditions.

Apollo 13 (Example of human capabilities in a non-routine operational situation)

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).

Table 2 illustrates how each of the three principles described in the previous sections can be applied throughout the system life cycle. Note that the table provides illustrations rather than definitions.

Human Factors Process Attributes

Up to this point, we have considered characteristics of the product that are associated with robustness and reliability. Before accepting a new product however, the user must also be assured that human factors were appropriately considered throughout the development process, and were not merely treated as an add-on at the end of the design process.

Figure 1 shows an idealized product development process, proceeding from initial concept development on the left of the figure to operational introduction of the product on the right.

Planning for the Human Factors Engineering (HFE) program begins at the start of the design process, and sets in train a series of critical activities, including analysis of the tasks that must be performed by humans, the design of the Human System Interface (HSI), culminating in in-service

monitoring. These processes of course, do not guarantee adequate human system integration, yet in their absence, problems with HSI are virtually assured.

Table 2. Three design principles and examples of their application during 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-motor envelope.	Human-system interface are consistent with human performance standards.	Maintenance tasks are within human capabilities.
System can tolerate and recover from human errors. Undesired errors are blocked. Detect and recover from errors. Minimize consequences of uncorrected errors.	Components designed to make incorrect assembly difficult.	Test and verification tasks are not performed by the same staff who manufactured the system being tested.	Appropriate interlocks, make it difficult to do dangerous things.	Avoiding simultaneous maintenance of redundant systems.
System enables utilization of human capabilities in non-routine and unpredicted situations.	Construction personnel are able to identify and log problems.	Output of test results are sufficiently detailed to enable identification of abnormal states.	System keeps human operators in the loop and permits humans to take control in the event of unexpected events.	If necessary, non-routine trouble-shooting and system repair is possible.

A comprehensive coverage of these activities can be found in O'Hara et al (2004), and Adelstein, Hobbs, O'Hara & Null (2006). Human Systems Integration activities are also covered in US Navy Human Systems Integration Guide (US Navy, 2005) and Defense Acquisition Guidebook (US Department of Defense, 2006). In the following pages, we illustrate by focusing on three key human factor activities.

Operational Experience Review (OER) 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.

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

Task analysis

Task analysis provides detailed information about what is needed to perform tasks. Generally, the term "task" is used to refer to a group of activities that have a common purpose.

Task analysis is actually a family of techniques. For example, Kirwan and Ainsworth (1992) list over 40 tasks analysis techniques, each of which is suited to a particular situation or objective.

Task analysis information has many uses in subsequent analyses, including: staffing, procedure design, training, and human error and reliability analysis.

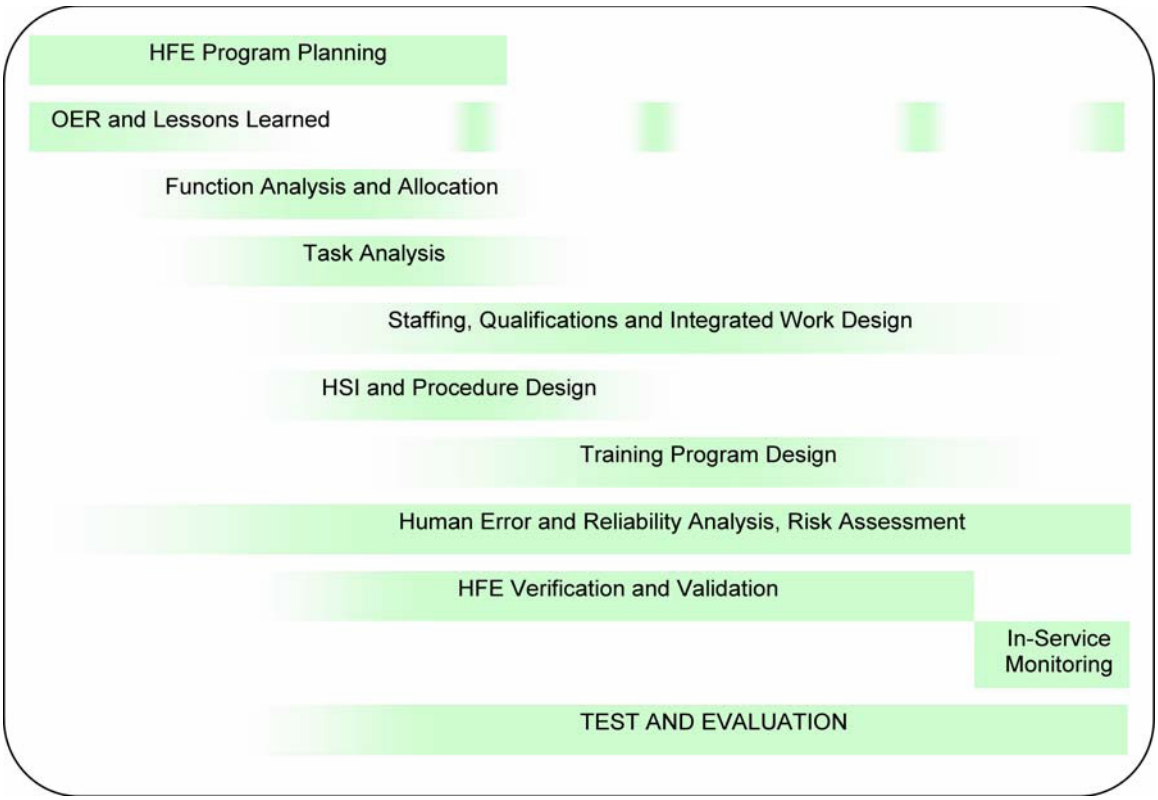

Figure 1. Human Factor Activities as part of the design program

Human Error and Reliability Analysis

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 during the design process. As the project progresses through analysis to definition and design, iterative analyses will identify potential human errors and human factor risks in progressively finer levels of detail.

The aims of a human error analysis are to identify critical areas where system demands may be incompatible with human capabilities, and identify critical areas where the system is vulnerable to human error, 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 and a broad level of granularity.

The initial human error analysis would consider normal as well as non-normal operations in all stages of the system life cycle, from design, construction, operation and maintenance.

The initial human error hazard analysis would draw on information from operational experience reviews, incident and accident databases, and relevant experience from other industries and settings.

Two analysis techniques guide the human error hazard analysis.

1. Fault Tree Analysis (FTA) is a top-down approach, starting with a list of potential catastrophic scenarios and then working down to identify how these could occur. During the human error analysis, the emphasis is naturally placed on the human actions that could jeopardize a mission or lead to loss of life. Although probability estimates are commonly inserted into fault trees, even without this level of detail, fault trees can help the analyst identify situations where the system is vulnerable to human error, 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 (NASA, 2002).The two approaches of FTA and HFPFMEA are complementary and information from one approach is used to refine and guide the other. The relation between the two approaches is depicted schematically in Figure 2.

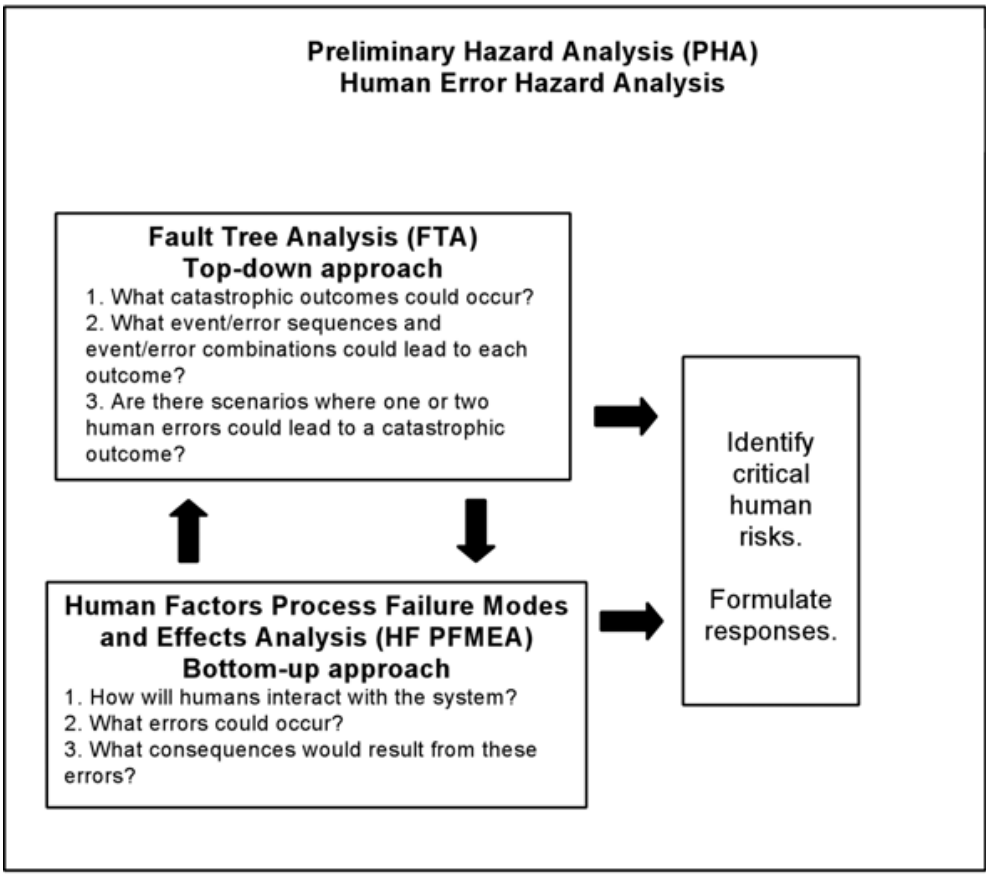

Figure 2. Two complementary approaches to the identification of human error hazards.

Conclusions

The work described in this paper was directed at design issues pertaining to a spacecraft, however the principles are applicable to a wide range of products and systems, ranging from simple household objects to advanced technological systems.

Careful attention to the design of human system interfaces can make a significant contribution to the overall performance of complex systems. It must be noted however that good design of subsystems or components does not guarantee the performance of the overall system. Furthermore, managing the performance of a highly complex system involves more than just ensuring adequate interface design, and we have not attempted here to deal with the organizational issues associated with the management of complexity.

The three principles of reliability and robustness introduced in this paper represent distinct but overlapping divisions in the field of human factors. Over the last half century, much attention has been directed at the first and second of these three principles. The third principle has received less attention, yet it is important to acknowledge the positive as well as the negative contributions that human performance contributes to system operation.

Ensuring effective human system integration requires the application of human factors principles early in the design process. A structured approach to human factors can save a great deal of trouble later in the life of the system in terms of re-design, training and safety incidents. There are of course, no guarantees that a formal consideration of human factors throughout the design process will identify

all the relevant human issues, however neglecting these areas is almost certain to result in a system lacking in reliability and robustness.

References

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

Booher, H. R. (Ed.). (2003). *Handbook of human systems integration*. New Jersey: Wiley.

Hollnagel, E., Woods, D, and Leveson, N. (2006). *Resilience engineering, concepts and precepts*. Aldershot: Ashgate.

Johnson, N. J. (1980). *Handbook of Soviet manned space flight*. San Diego: Univelt.

Kerr, R. A. (2004, 22 October). Flipped Switch Sealed Fate of Genesis Spacecraft. *Science, 5696,* 587.

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

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

NASA (2005). *Human-rating requirements for space systems*. (NASA Procedural Requirement 8702.5A). Washington DC: Author.

NASA. (2006*). Genesis mishap investigation board report. Vol. 1*. Washington DC: Author.

NASA. (2007). *System engineering handbook* (NASA/SP-2007-6105).Washington DC: Author.

NASA. (2007). *NASA general safety program requirements* (NPR 8715.3). Washington DC: Author.

Newkirk, D. (1990). *Almanac of Soviet manned spaceflight*. Houston, TX: Gulf Publishing

O'Hara, J., Higgins, J., Persensky, J., Lewis, P., & Bongarra, J. (2004). *Human factors engineering program review model* (NUREG-0711, Rev. 2). Washington, D.C.: U.S. Nuclear Regulatory Commission.

Shayler, D. (1990). *Disasters and accidents in manned spaceflight*. New York: Springer.

US Department of Defense. (2000). *Standard practice for system safety* (MIL-STD-882D). Washington DC: Author.

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

US Department of Defense. (1999). *Department of defense design criteria, standard human engineering* (MIL-STD-1472F). Washington DC: Author.

US Navy. (2005). *Human systems integration guide*. Washington DC: Author.