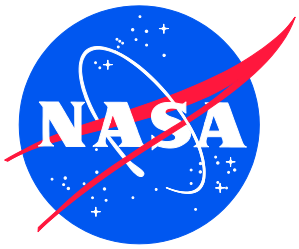
NASA/TM–2020-20205001486
NESC-NPP-18-01368



Guidance for Human Error Analysis (HEA)

Cynthia H. Null/NESC
Langley Research Center, Hampton, Virginia

Alan Hobbs
San Jose State University Research Foundation, San Jose, California

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

Charles Dischinger
Marshall Space Flight Center, Huntsville, Alabama

April 2020

NASA STI Program . . . 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 plays a key part in helping NASA maintain this important role.

The NASA STI program operates under the auspices of the Agency Chief Information Officer. It collects, organizes, provides for archiving, and disseminates NASA's STI. The NASA STI program provides access to the NTRS Registered and its public interface, the NASA Technical Reports Server, thus providing one of the largest collections of aeronautical and space science STI in the world. Results are published in both non-NASA channels and 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 counter-part of peer-reviewed formal professional papers but has 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 also include organizing and publishing research results, distributing specialized research announcements and feeds, providing information desk and personal search support, and enabling data exchange services.

For more information about the NASA STI program, see the following:

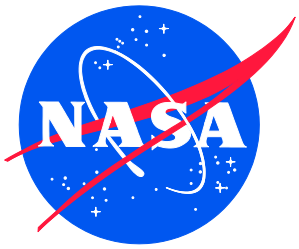
- Access the NASA STI program home page at *http://www.sti.nasa.gov*

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

- Phone the NASA STI Information Desk at 757-864-9658

- Write to:
  NASA STI Information Desk
  Mail Stop 148
  NASA Langley Research Center
  Hampton, VA 23681-2199

NASA/TM–2019-20205001486
NESC-NPP-18-01368



Guidance for Human Error Analysis (HEA)

Cynthia H. Null/NESC
Langley Research Center, Hampton, Virginia

Alan Hobbs
San Jose State University Research Foundation, San Jose, California

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

Charles Dischinger
Marshall Space Flight Center, Huntsville, Alabama

National Aeronautics and
Space Administration

Langley Research Center
Hampton, Virginia 23681-2199

April 2020

Available from:

NASA STI Program / Mail Stop 148
NASA Langley Research Center
Hampton, VA 23681-2199
Fax: 757-864-6500

NASA Engineering and Safety Center
Position Paper

Guidance for Human Error Analysis (HEA)

November 21, 2019

Report Approval and Revision History

NOTE: This document was approved at the November 21, 2019, NRB. This document was submitted to the NESC Director on December 3, 2019, for configuration control.

Approved:	*Original Signature on File*	12/3/19
	NESC Director	Date

Version	Description of Revision	Office of Primary Responsibility	Effective Date
1.0	Initial Release	Dr. Cynthia H. Null, NASA Technical Fellow for Human Factors, ARC	November 21, 2019

Table of Contents

List of Figures

List of Tables

1.0 Purpose of this Document

NASA's Human-Rating Requirements for Space Systems in NASA Procedural Requirements (NPR) 8705.2C requires Program Managers to conduct a human error analysis (HEA) for all mission phases. The purpose of the HEA is to enable programs to understand and manage potential catastrophic hazards that could be caused by human error, understand the relative risks and uncertainties within the system design, and influence decisions throughout the system lifecycle.

This document provides guidance to NASA civil servants and contractors on how the Agency's HEA requirement can be fulfilled. It is intended to assist with the planning and conduct of the HEA, the preparation of the HEA report, and the evaluation of the HEA adequacy. This document presents approaches and methods that can be used to meet the intent of NPR 8705.2C, but does not preclude the use of alternative approaches.

2.0 Signature Page

Submitted by:

Team Signature Page on File - 12/5/19

Dr. Cynthia H. Null Date

Significant Contributors:

Alan Hobbs Date
San Jose State University Research Foundation
alan.hobbs@nasa.gov

John O'Hara Date
Brookhaven National Laboratory
ohara@bnl.gov

Charles Dischinger Date

Signatories declare the contents are factually based from data extracted from program/project documents, contractor reports, and open literature, and/or generated from independently conducted tests, analyses, and inspections.

3.0 Introduction

Operational personnel make a vital contribution to system safety, especially in novel situations where human intelligence and adaptability can help manage and mitigate unforeseen circumstances. However, despite positive human contributions to system operations and maintenance, human errors sometimes occur. When they do, they can pose a threat to system safety and performance.

NPR 8705.2C, Human-Rating Requirements for Space Systems, Appendix A, defines human error as: "Either an action that is not intended or desired by the human or a failure on the part of the human to perform a prescribed action within specified limits of accuracy, sequence, or time that fails to produce the expected result and has led or has the potential to lead to an unwanted consequence" [ref. 1, p. 49].

A requirement to perform an HEA is contained in NPR 8705.2C, as follows:

2.3.11.1 The Program Manager shall conduct a human error analysis for all mission phases to include operations planned for response to system failures.

2.3.11.2 At PDR [Preliminary Design Review], the Program Manager shall summarize, in the HRCP [Human Rating Certification Package], and present how the human error analysis (to date) was used to: (This is updated at CDR [Critical Design Review] and ORR [Operational Readiness Review].)

a. Understand and manage potential catastrophic hazards which could be caused by human errors.

b. Understand the relative risks and uncertainties within the system design.

c. Influence decisions related to the system design, operational use, and application of testing. (p.29)

A requirement to consider human error is also included in NASA's General Safety Program Requirements (NPR 8715.3D, §1.7.3.1), which state that managers must ensure that designs include considerations for the possibility of human errors [ref. 2].

Because HEA is performed as part of the system development process, it is a projective approach requiring the analyst to identify, conceive of, and predict scenarios where human actions could contribute to a catastrophic outcome. HEA is required for all mission phases, including ground processing, launch preparation, and recovery/disposal operations, in addition to flight operations. Each group of personnel and their interactions may involve different types of HEA issues. Ground processing, for example, may involve an emphasis on interactions with hardware under 1 g, but may also involve the preparation of software and data entry. An analysis of in-flight operations is likely to emphasize interactions with controls and displays under 0 g, or microgravity.

NPR 8705.2C defines HEA as: "A systematic approach to evaluate human actions, identify potential human error, model human performance, and qualitatively characterize how human error affects a system. HEA provides an evaluation of human actions and error in an effort to generate system improvements that reduce the frequency of error and minimize the negative effects on the system. HEA is the first step in Human Risk Assessment and is often referred to as qualitative Human Risk Assessment."

While the NASA Engineering and Safety Center's (NESC) focus is the use of HEA to support design improvements, the results of HEA can also inform probabilistic risk assessments (PRA) as required by NPR 8705.5A. Conversely, HEA can draw on data collected to support probabilistic analyses of human reliability. For a review of probabilistic approaches to human error, see NASA/SP-2011-3421 and Chandler, et al [refs. 3, 4].

The health and safety of ground personnel is not within the scope of NPR 8705.2C or this guidance document. Ground personnel health and safety is covered by Occupational Safety and Health Administration regulations (29 Code of Federal Regulations) [ref. 5] and NPR 8715.3.

The requirement for system developers to consider possible human errors is not unique to NASA. The need for such an analysis has been recognized in other safety-critical contexts, including aviation, maritime, military, and nuclear applications (see Appendix A for an overview of the use of HEA in other domains).

3.1 Human Error and Error Traps

Human errors frequently occur because a person falls into an "error trap." These errors are sometimes referred to as "design-induced errors." An "error trap" is a set of specific circumstances that can provoke similar mistakes, regardless of the people involved [ref. 6]. Error traps can take the form of hardware, software, procedures, training, or other aspects of system design and operation with the potential to increase the likelihood of human error. Examples are plugs that can be mated to the wrong connections; procedures that require a level of precision or strength that cannot be reliably delivered under the work conditions; and tasks that impose unreasonable cognitive demands.

An important contribution of the HEA is to identify error traps, or other circumstances where human error could lead to catastrophic outcomes. This information is then used to influence decisions related to design, operations, and testing to manage the threat.

The term "human error," as used in everyday speech, sometimes carries connotations of judgment or blame. The purpose of examining human error in complex human-machine systems is to identify and mitigate problems at an integrated system level, including hardware, software, personnel, facilities, processes, and procedures. It is not about finding fault with individuals.

3.2 Relation to other HSI Requirements in NPR 8705.2C

HEA is not the only human systems integration (HSI) activity called for in NPR 8705.2C. The document requires the establishment of a HSI team and the creation of a HSI plan to ensure that the system design accommodates human capabilities and limitations. The NPR also requires the Program Manager to:

- Comply with NASA Space Flight Human-System Standard 3001 [ref. 7] (2.2.5 a, b).
- Comply with Federal Aviation Administration (FAA) Human Factors Design Standard (HFDS) [ref. 8] (2.2.5c).
- Evaluate crew and ground control workload (2.3.9).
- Conduct human-in-the-loop usability evaluations for critical operations involving crew and ground control personnel (2.3.10).
- Include in the HRCP a "description of a process for identifying hazards, understanding risk implications of the hazards" (Appendix D).

HEA builds on these activities. The HEA and the results of these interrelated analyses will then be documented as part of the HRCP.

3.3 General HEA Principles

The HEA process should be guided by the general principles listed in Table 3-1.

Table 3-1. General HEA Principles

General Principle	
1. The goal of HEA is to enhance system reliability and safety	HEA enhances system reliability and safety by identifying where significant human errors could occur, the conditions that could provoke these errors (error traps), and means to mitigate them.
2. HEA is an iterative process	Analysis of potential human errors should occur throughout all phases of the design process.
3. HEA is directed at the entire system, not people alone	HEA identifies problems with the total system, including hardware, software, equipment, facilities, processes, and procedures. HEA is not about finding fault with people or attributing blame.
4. HEA cannot be applied in detail to every HSI	Mission success relies on thousands of human tasks performed by operational personnel on the ground and in flight. It is impossible to analyze all of them. Screening is necessary to identify those which, if performed incorrectly, would pose the greatest risk to mission success and safety.
5. HEA must consider tasks in context	Tasks are not performed in isolation, but occur in the context of a workflow. Potential interactions between tasks must be considered.
6. HEA must consider work as actually performed	HEA must consider the full range of possible HSI, including interactions not envisioned by designers or covered by formal procedures.
7. HEA should be integrated with other analyses	HEA should use information from available analyses, such as hazard and task analyses, and provide input to other analyses, such as risk analyses.
8. HEA benefits from independent perspectives	HEA should provide a perspective that is independent from the design team.
9. HEA should be performed by a multidisciplinary team	It is best performed by a team that includes personnel trained in HEA, as well as subject matter experts (SMEs) and design engineers familiar with the systems being evaluated.
10. HEA requires input from operational personnel	Analysis of system demands and tasks should include input from personnel who perform the tasks in question. Even when a task is new, or associated with a new system design, input from personnel who have performed similar tasks can provide valuable insights.
11. HEA requires imagination	HEA requires careful thought and imagination to identify vulnerabilities where human performance could pose a threat to the mission. It should not be a “box checking” exercise.
12. There is no single correct approach to HEA	HEA can use a variety of methods, including evaluations by SMEs, the application of engineering judgment, task analysis, and formal analyses such as human reliability analysis (HRA).

3.4 HEA Throughout the Project Lifecycle

HEA should be performed throughout the project lifecycle. As the technology moves towards operational readiness, more information on human interactions will become available, as design, procedures, and mission operating environments are further defined. NPR 8705.2C, Section 2.3.11.2, specifies that HEA should be presented at PDR, then updated at CDR and ORR.

In the early stages of concept development, it may be appropriate to perform the HEA at a broad level of granularity at the level of high-level tasks. Such an analysis may describe errors in terms of the outward behavior that would, in theory, be observable by a hypothetical objective viewer. Examples are: "Task not performed" or "Task performed incorrectly." Table 3-2 provides a hypothetical example of an early-stage HEA that occurs at a broad level.

Table 3-2. Hypothetical Example of an Early-stage HEA

Prior to the PDR, a general list of functions that may require human input during flight is obtained by the HEA team. A detailed list of crew tasks is not yet available, but the HEA team identifies that crew members will be involved in certain critical functions during the initial ascent, which will require them to interact with screen displays. The HEA team identifies that vibration during ascent stage could lead to crew errors when reading text on screen displays as conceived in the initial concept. The HEA team reviews existing research on the topic and recommends the adoption of a larger font size.

Early HEAs are critically important, as they have the potential to identify problems that can be addressed at a time when design changes are least disruptive (see Figure 3-1). As the design process proceeds, human actions will become progressively more defined and more fine-grained HEA will be possible. This may require a two-stage approach, with an analysis at the level of outward behavior, followed by a cognitive analysis.

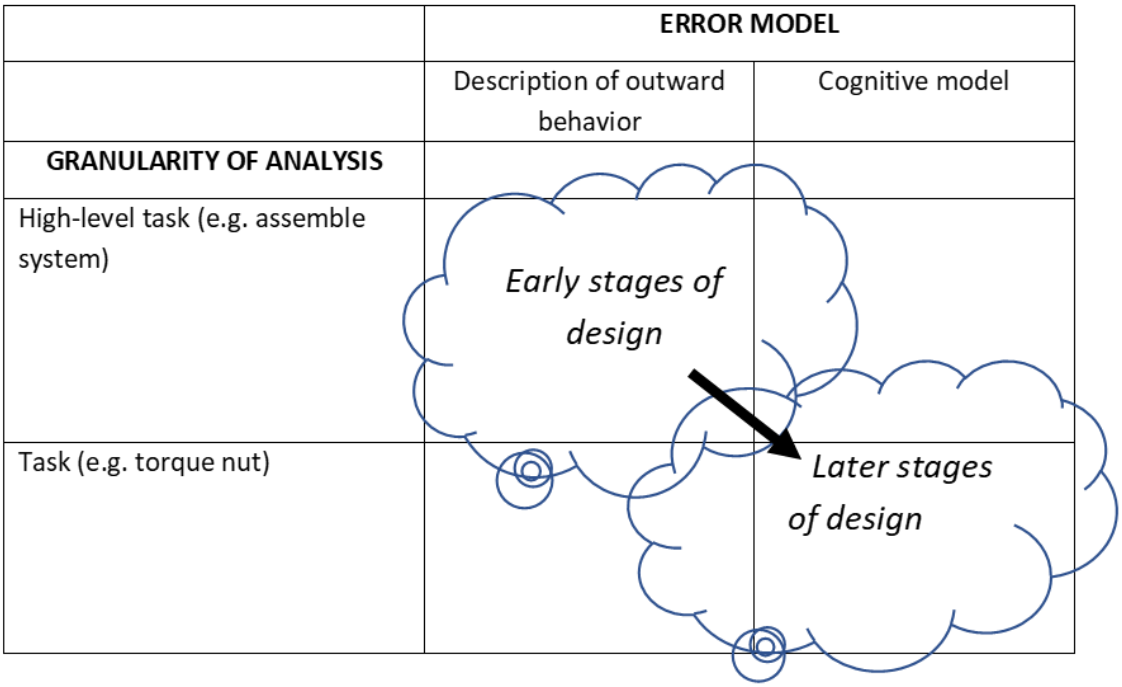


Figure 3-1. HEA Specificity May Increase as Design Process Progresses

HSI is an essential aspect of system development. At each stage of development, system designers will have already taken human performance into consideration. Therefore, many of the most obvious human errors should have been identified and addressed. It is appropriate for the HEA analysts to review and collate the HSI activities that have occurred during system development; however, their most important role is to seek overlooked vulnerabilities where human performance could pose a threat to the mission. Therefore, HEA requires careful thought and imagination and should not be considered a "box checking" exercise.

4.0 HEA Steps

The HEA process is shown in Figure 4-1. The HEA process consists of seven steps, each of which is described in the following subsections.

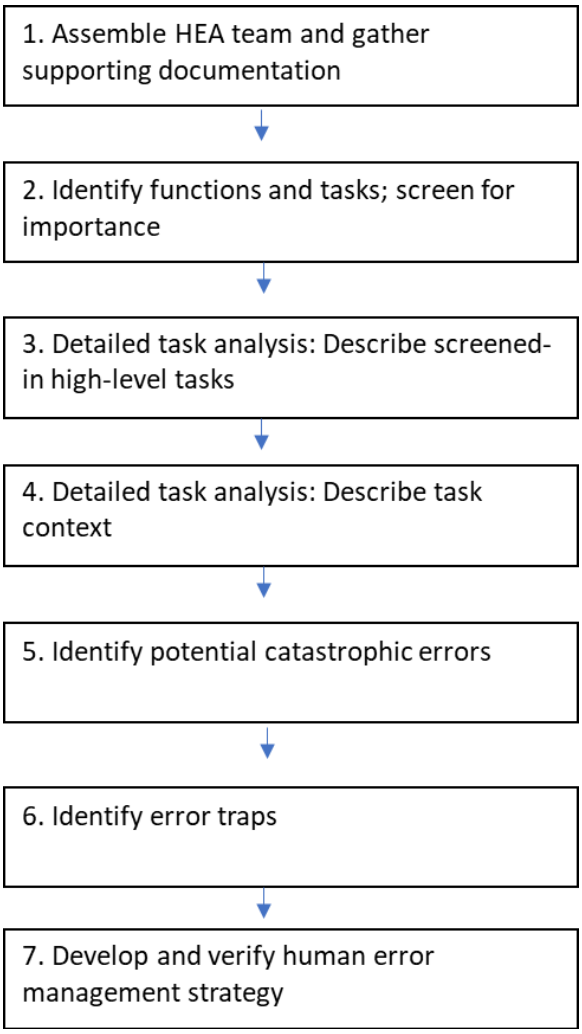


Figure 4-1. The HEA Process

4.1 Assemble HEA Team and Supporting Documentation

The HEA should be conducted by a team comprising diverse, multidisciplinary expertise, experience, and perspectives. Typically, this will be the HSI team, as specified in NPR 8705.2C, Section 2.3.8. In addition to the human factors specialist, the team should include SMEs from the system's user community who will be familiar with the systems and tasks. For example, if the HEA is considering a ground processing task, the HEA team may comprise a Human Factors specialist and design engineers as well as experienced ground processing personnel. Even when the tasks are new and associated with new system designs, personnel who have performed similar tasks with predecessor systems are likely to provide valuable insights. The HEA team also should have access to the design team members needed to understand the design and resolve questions.

The HEA team should maintain close bi-directional communication with the design team throughout the design process, and should be ready to provide assistance when needed to identify and address potential human errors. However, because it can be difficult for designers to recognize human error traps in their own designs, the HEA team also provide an assessment of the system independent of the design team. The HEA team should have access to design

documentation as well as evaluations and analyses that can help identify functions that rely on human performance and tasks during which human errors could occur.

4.2 Identify Functions and Tasks, and Screen for Importance

The purpose of this step is to (1) identify critical functions that, if lost, could lead to catastrophic events, and (2) identify the high-level tasks that must be performed to accomplish the critical functions.

Systems accomplish their missions through a set of functions. Functions are described in terms of high-level goals, without reference to how they are accomplished. For example, a crewed-spacecraft function is "maintain cabin habitability." As the design develops, functions are further decomposed into the systems and actions needed to accomplish the function. This is part of the systems engineering functional decomposition process [ref. 9]. Functions may be accomplished by machine actions (e.g., automatic systems), human actions (e.g., tasks performed by personnel) (see Figure 4-2), or through a combination of human and machine actions. Collectively, human actions define the roles and responsibilities of personnel in the system. The allocation of functions to machines or humans should be defined in a system's Concept of Operations (ConOps) document. According to NASA's Systems Engineering Handbook [ref. 9]:

> *"The operational concept must include scenarios for all significant operational situations, including known off-nominal situations. To develop a useful and complete set of scenarios, important malfunctions and degraded-mode operational situations must be considered." (p. 10)*
>
> *"Operational scenarios are used extensively to ensure that the mission system (or collections of systems) will successfully execute mission requirements. Operational scenarios are a step-by-step description of how the system should operate and interact with its users and its external interfaces (e.g., other systems). Scenarios should be described in a manner that allows engineers to walk through them and gain an understanding of how all the various parts of the system should function and interact as well as verify that the system will satisfy the user's goals and expectations. ... Operational scenarios should be described for all operational modes, mission phases (e.g., installation, startup, typical examples of normal and contingency operations, shutdown, and maintenance), and critical sequences of activities for all classes of users identified. Each scenario should include events, actions, stimuli, information, and interactions as appropriate to provide a comprehensive understanding of the operational aspects of the system." (p.95)*

Thus, if available, the HEA team should consult the systems engineering activities already performed to identify the system functions, allocation of those function to human and machine agents, and key scenarios.

In addition to the system descriptions and ConOps documentation identified above, the HEA analyst may also obtain information on system functions and tasks from other sources, including:

- System operations documentation.
- Input from SMEs, including operations and maintenance personnel.
- Analysis of procedures, where available.
- Crew Master Task List.

- Task analyses conducted as part of other HSI activities.
- Analysis of similar systems (e.g., operational experience review of prior similar systems).

Several scenarios should be identified for each function to be used in the evaluations to follow. This is because the types of tasks and the demands they pose can differ across scenarios for the same function. A representative set of scenarios for each function will provide the HEA analyst with the ability to evaluate the task and demand differences across them.

At this step, the HEA analyst should have a description of the high-level tasks personnel must perform in support of the scenarios related to those functions. By high-level tasks, what is intended is a description of what the task should accomplish, but not necessarily the detailed physical and cognitive actions necessary. That is part of the detailed task description that can be developed in the next HEA step. The tasks include fully manual actions (no machine involvement) as well as those where interaction between personnel and machines are necessary. In addition, the machine actions should be identified as well as the role of personnel in monitoring and managing automatic machine actions. The HEA analyst should note the role of automation in function accomplishment. The responsibilities of personnel in the monitoring and management of automation is often overlooked when human roles are analyzed, yet failure to do so can have catastrophic results.

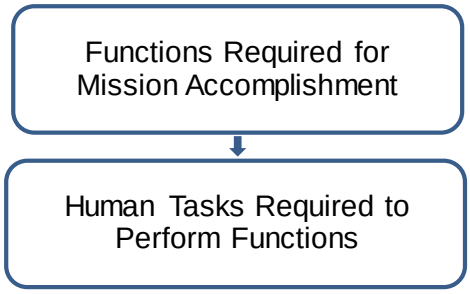


Figure 4-2. Functions and Tasks

The number of tasks associated with a system's construction, operation, and maintenance can be immense. Therefore, HEA should focus on those tasks that are most important to mission success, starting with those that could result in catastrophic failure. This is accomplished by a screening process. Screening requires the identification of critical functions and tasks by determining whether a catastrophic outcome could result from failure to perform a task or from errors during task performance.

Functions and associated tasks not determined to be critical can generally be screened out and not considered further. For critical functions, the analyst should determine which of the identified high-level tasks are necessary for function accomplishment. Those that are necessary are screened in for further analysis. Those that are not necessary are screened out from further analysis.

Each HEA team must develop its own internal guidelines to determine which tasks should be screened in for analysis, although the team should retain the flexibility to examine additional tasks if judged necessary. For example, the team may decide to screen in the following situations and tasks:

- Situations where a catastrophic outcome could result from a single inadvertent operator action (as specified in 8705.2C, Section 3.2.5), including responses to system failures or emergency conditions.
- The large number of ground processing operations presents an additional challenge for the HEA team, as every human interaction with flight hardware cannot possibly be subject to a thorough HEA.

The HEA team may choose to use additional screening guidelines similar to the following examples:

- Screen in assembly, test, and integration tasks that occur at the launch facility.
- Screen in tasks at the level of interactions with line replaceable units (LRUs).
- Screen out most interactions with components or parts.
- Screen out ground processing actions followed by a full functional test prior to launch.
- Screen out ground processing actions if failure to perform correctly would be obvious and correctable prior to launch.

4.3 Detailed Task Analysis

In the next HEA step, those human tasks identified as critical, are analyzed in greater detail. This is accomplished by performing a detailed task analysis. Detailed task analysis continues the decomposition process that started with functions. High-level tasks are decomposed into subtasks so task requirements can be identified (see Figure 4-3).

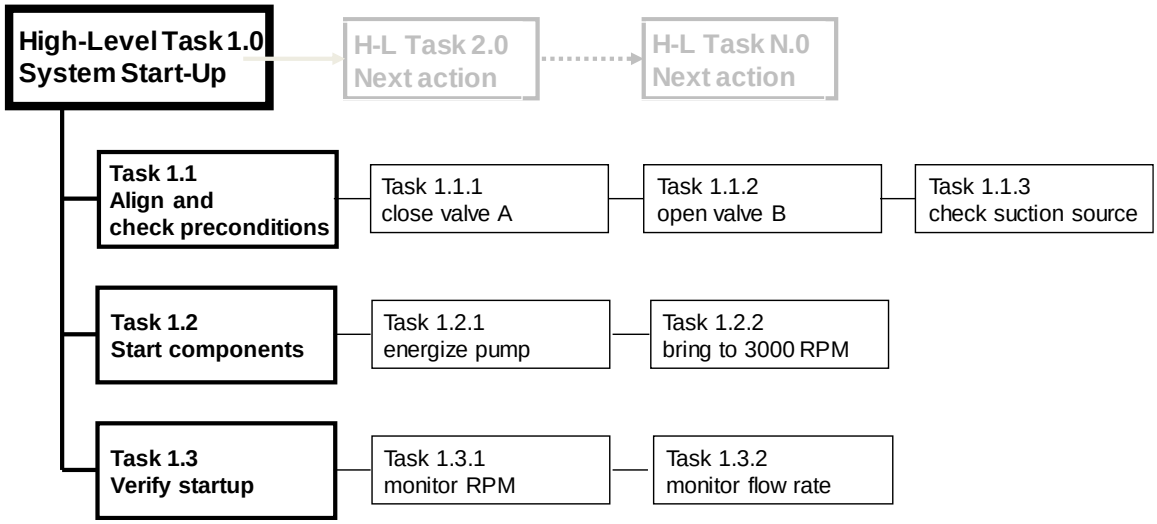


Figure 4-3. Decomposing High-level Tasks into Detailed Tasks

The analyst may not have to conduct the task analysis as part of the HEA if task analyses have been performed as part of other HSI activities, such as the Master Task List for in-flight activities, the Human-Centered Task Analysis required by NASA-STD-3001, or the task analysis created for a HRA, as described in NASA/SP-2011-3421. The initial steps of HRA are similar to the steps required for HEA. In each case, the tasks assigned to humans are defined, and then potential errors are identified. However, while HRA moves on to assign probabilities to errors,

HEA remains a qualitative analysis focused on identifying and responding to the threat posed by specific errors.

Augmenting the task descriptions will require the involvement of SMEs. At a minimum, personnel who are expected to perform the tasks should be consulted.

Since the user-system interface design details have a major influence on error, available results of testing of the pertinent interfaces or prototypes should be consulted, and operational personnel should be interviewed about their use of user interfaces to perform the task. Those soliciting this information should keep in mind that personnel might take interfaces for granted. They may routinely work around existing deficiencies or may uncritically accept new interfaces as better. Among the many issues to be considered are anthropometrics, consistency of controls and displays, human computer interfaces, and design for maintainability.

If detailed task analyses are not available, they should be conducted to support the HEA. This may particularly be the case for ground operations. Task analysis refers to a broad family of techniques used to characterize and understand human interactions with systems and the detailed requirements needed to accomplish human responsibilities. The methods can range from formal analysis methods, such as hierarchical task analysis, to less formal methods like walk-throughs of tasks by operations personnel. Task analysis provides a robust context to understand how human tasks are performed and, potentially, what conditions may lead to human errors.

The task analyst must consider not only the ways tasks should be performed, but also how work might actually be performed under the demands of the work environment. At times, operational personnel will interact with systems in ways that were not intended or foreseen by system designers, procedure developers, and trainers. For example, objects that have the shape of a handle will sometimes be misused as a handhold, even when this was not intended by the designer. For this reason, HEA must also consider some HSIs not linked to specific tasks, including cases of foreseeable misuse (see Glossary, Section 7.0).

Many traditional task analysis methods focus on outward behaviors (i.e., physically observable actions). For a description of traditional task analysis methods, see Kirwan and Ainsworth [ref. 10]. However, all tasks involve cognitive activities, and as operations become more automated, the role of personnel is becoming less activity-oriented and more reliant on cognitive activities that must be inferred by the task analyst rather than observed directly.

If the task is determined to be critical (i.e., if an error during the task could result in a catastrophic event), it may be necessary to analyze the task further using cognitive task analysis techniques.

Cognitive tasks analysis methods are directed at identifying the unobservable, but crucial, mental processes involved in task performance. This need not be overly complicated, and may involve identifying (1) the sources of information relied on by the task performer, (2) the mental processes, memory demands, and decisions made during task performance, and (3) the actions required to accomplish goals. A summary of applied cognitive tasks analysis methods can be found in Seamster and Redding [ref. 11].

In addition to task analysis, other sources of information can be used to assess critical tasks. This information can provide task step details, illustrate how work is actually performed in the field, highlight factors that impact task performance, and provide insights into how task errors

can occur and be prevented. A variety of methods are available to collect this information, including:

- Surveys, questionnaires, and rating scales
- Interviews
- Observational studies
- Walk-throughs
- Performance-based tests
- Computer models

A brief description of each of these methods is given in Appendix B.

4.4 Describe the Task Context

Once the detailed descriptions are available for each critical task, the HEA analyst should consider aspects of the task context that could increase the likelihood of error.

For the purposes of this document, these contextual factors will be referred to as error-producing conditions (EPCs). Some of these are internal to the person at the time (e.g., fatigue, skill level, or stress). Others exist external to the person (e.g., environment, task, equipment). Over a century of human factors research has contributed to a vast literature on these conditions, and the human factors SMEs will be familiar with the state of knowledge in this field.

It is helpful to distinguish between EPCs and error traps. An EPC is a general condition that can increase the likelihood of error across a range of tasks. An error trap is a set of circumstances that can provoke a specific error on a specific task. Many EPCs, such as human fatigue, can never be eliminated entirely. However, in most cases, error traps can be eliminated with appropriate design.

The presence of significant EPCs can be a sign to the HEA team that the task requires close examination for potential errors. For example, recovery tasks that could be performed at sea in challenging sea states may have a heightened overall chance of error, and may therefore require more analysis than tasks performed in more forgiving conditions.

The human factors literature contains numerous lists and taxonomies of EPCs, and the intent is not to provide detailed information in this document. Table 4-1 contains sample questions concerning error-producing conditions that can be asked of personnel while reviewing or talking through the task to be analyzed.

Table 4-1. Sample Questions to Identify EPCs

- Is there anything about the human-system interface or equipment that could increase the likelihood of error on this task? If so, describe.
- Are there task demands, either physical or cognitive, that could increase the likelihood of error (e.g., required physical strength or reach, or cognitive demands such as reliance on memory or attention)? If so, describe.
- Could any of the procedures for this task potentially confuse the operator or otherwise lead to an error? If so, describe.
- Could the environment in which the task is performed increase the likelihood of error? If so, describe.
- Are there coordination, teamwork, or communication issues that could increase the likelihood of error on this task? If so, describe.

The following subsections provide examples of EPCs that might be considered in the course of the HEA. Note that the examples are far from comprehensive, and are intended merely to illustrate EPCs that might be found in the course of the HEA.

4.4.1 Human-System Interfaces

Human-system interfaces include displays, controls, alarms, and various support aids (e.g., decision aids) to enable personnel to perform their tasks under all operational conditions (e.g., normal, off-normal, and emergency situations).

Numerous standards provide guidance on the design of human-system interfaces, including electro-mechanical and computer interfaces (e.g., FAA HFDS, NASA-STD-3001, MIL-STD-1472). One way to identify EPCs in a human-system interface is to use an established design standard as a checklist to look for design features that could increase the probability of human error. For example, a review of a proposed design using NASA-STD-3001 might identify the EPCs such as those shown in the following list. Note that these are examples only, and the list is not comprehensive:

- Control systems that can be accidentally activated by bumping.
- Displays that are difficult to read by the crew from the crew's operating locations.
- Systems that provide no positive indication of a crew-initiated control activation (e.g., a physical detent, an audible click, an integral light).
- Controls that result in different outcomes that are difficult to distinguish from each other.

4.4.2 Task Characteristics

The following are examples of task characteristics that can increase the probability of error. Note that this is not a comprehensive list:

- Too little time is available.
- Task requires very precise timing or force.
- More than one task needs to be performed in parallel.

- Task creates high workload, creating overload of attention and memory.
- Task creates low workload, creating vigilance difficulties.
- Task requires long, sustained effort.
- Task is performed while wearing protective clothing, gloves, etc.
- Task is performed in a manner different from normal or habitual operations.
- Task is likely to be performed amid distracting conditions (e.g., during multiple system failures).

4.4.3 Human-Automation Integration

Automation can reduce human workload and enable processes to be controlled with a level of speed and reliability that could not be delivered by a human operator. However, inadequate consideration of human factors in the design of automated systems can increase the chance of automation-induced errors.

The FAA HFDS contains numerous design principles for automated systems that can be used to identify EPCs in automated systems and the interfaces between users and such systems. The following are examples of automation issues that can increase the probability of error. Note that this is not a comprehensive list:

- Automation that requires the human to act as a passive monitor.
- High false alarm rates that cause the user to disregard warnings.
- A reliance on manual data entry, such as the need to enter strings of digits.
- Excessive number of automation modes, increasing opportunities for error.

4.4.4 Hardware and Equipment

Hardware and equipment EPCs relate to physical objects, such as hatches, LRUs, seats, connectors, and handholds.

A review of items using the FAA HFDS and NASA-STD-3001 as checklists can help to identify hardware and equipment issues that may increase the probability of error. The following are examples of hardware and equipment issues that can increase the probability of error. Note that this is not a comprehensive list:

- Excessively heavy objects intended to be lifted by a single person during ground processing.
- Equipment positioned in a manner that prevents visual and physical access for operation or maintenance.
- Fasteners that are not captive used by the crew during maintenance.
- Physically interchangeable and similar items of hardware that perform different functions.

4.4.5 Procedures

Procedures include task instructions, checklists, emergency procedures, fault isolation guides, and other textual or graphical information intended to guide operators in performing a task. Procedures may be provided on paper or electronically as part of the human-system interface. They can also include text attached directly to items of equipment, in the form of labels or decals.

Many human errors have their origins in poorly designed procedures or documentation. Human factors guidelines for procedure design can help minimize the chances of procedure-related errors [ref. 12].

The following are examples of procedure factors that can increase the probability of error. Note that this is not a comprehensive list:

- Procedures that involve difficult cognitive operations (e.g., Boolean logic or high working memory demand).
- Procedures that have many branches, or numerous cross-references that direct the user to other sections of the procedure or other documents.
- Inconsistent or nonstandard terminology.
- Procedures that do not adhere to ergonomic principles, such as difficult-to-read typography, including the extensive use of CAPITALIZATION.

4.4.6 Environment

Environmental error-producing conditions relate to the physical conditions in which the task will be performed. The following are examples of environmental factors that can increase the probability of error. Note that this is not a comprehensive list:

- High levels of vibration.
- High acceleration.
- Reduced gravity conditions.
- Inadequate lighting for the task at hand.
- Temperature extremes.
- Excessive or distracting noise.
- Confined spaces.

4.4.7 Teamwork

Most tasks involve coordination, communication, and teamwork. Crew members may perform a task cooperatively from one location while, in other cases, team members will be in different locations. The following are examples of teamwork factors that can increase the probability of error. Note that this is not a comprehensive list:

- Complex crew coordination occurs across multiple locations.
- Crew communication is unstructured.

- Verbal communication occurs in a noisy environment.
- A partly completed task must be handed from one shift to another.

4.4.8 Individual Factors

Individual factors are internal to the human operator at the time of task performance. The following are examples of individual factors that can increase the probability of error. Note that this is not a comprehensive list:

- Sleep deprivation or circadian dysrhythmia.
- Stress.
- Unfamiliarity with task.
- Strength limitations.
- Reduced physical capabilities.
- Illness (e.g., motion sickness).
- Bodily dimensions (e.g., reach, height).

4.5 Identify Potential Catastrophic Errors

Section 4.4 describes tasks in detail and identifies contextual factors that could increase the likelihood of error. This section identifies potential catastrophic human errors that could occur on each task, resulting in catastrophic events. These could take the form of undesired human actions, failures to perform a prescribed action, or failures to perform a required action within specified limits of accuracy, sequence, or time. For the purpose of this analysis, a catastrophic error is defined as an error that has the potential to lead to a catastrophic event.

To identify potential errors, it can be helpful to ask questions such as:

- What is the most credible way in which this task could fail?
- What errors or unintended actions could occur while performing this task?

Guide words can help ensure that the full range of potential errors has been captured. Table 4-2 contains a generic list of errors expressed as outward behaviors, adapted from Hollnagel's Cognitive Reliability and Error Analysis Method (CREAM) [ref. 13]. Note that an error analysis at the level of outward behavior is concerned with what might happen, not with why a person might act in this way.

It is helpful to describe potential errors on a task precisely by referring to an actor, an action, and the object of the action. For example, "Technician (actor) applies excessive force to (action) bolt (object)" provides a more useful description of an event than vague descriptions such as "loss of situational awareness" or "inadequate performance."

Table 4-2. Guide Words to Assist in Identifying Potential Errors at Outward Behavior Level

General Effect	Specific Effect	Explanation
Action at wrong time	Too early	An action started too early, before a signal was given or the required conditions had been established
	Too late	An action started too late
	Omission	An action was not done at all
	Too long	An action continued beyond the point where it should have been stopped
	Too short	An action was stopped prematurely
	Repeated	An action was repeated
	Reversal	The order of two neighboring actions was reversed
Action of wrong type	Too little force	Insufficient force
	Too much force	Excessive force
	Too much distance/magnitude	Movement taken too far
	Too short distance/magnitude	Movement not taken far enough
	Too fast	Action performed too rapidly
	Too slow	Action performed slower than required
	Wrong direction	Movement in wrong direction (e.g., left instead of right)
	Wrong type of movement	e.g. pulling a knob instead of turning it
Action involves wrong object	Neighbor	The object acted upon is near the object that should have been acted upon
	Similar object	The object acted upon is similar in appearance to the object that should have been acted upon
	Unrelated object	Object was used in error, even though it has no obvious relation to the object that should have been used

(Adapted from Hollnagel, 1998)

In certain cases, it may be helpful to augment the outward description of the error using a cognitive model of error. Cognitive models categorize errors on the basis of their presumed cognitive origins (e.g., by describing an error as a memory lapse or a failure of problem-solving). Compared to outward descriptions, cognitive models can provide insight into error causation and therefore may be more helpful in identifying strategies to manage error. Errors with the same outward observable appearance may have markedly different cognitive origins. For example, an incorrect keyboard entry may require a different design response depending on whether the action is the result of a *skill-based slip* or results from a *knowledge-based mistake* (see Glossary, Section 7.0).

Even if insufficient information is available to completely categorize the error with a cognitive model, a partial conclusion, such as determining whether the task would involve automatic or controlled processing, can be useful (see Glossary, Section 7.0).

In many cases, particular errors will be associated with specific contexts. For example, memory lapses are sometimes associated with isolated tasks steps and fatigue. Skill-based slips are frequently associated with tasks or interfaces that require the person to perform an action

contrary to a habitual pattern. Descriptions of cognitive models of error can be found in Hollnagel, Reason, and Null [refs. 13-15].

4.6 Identify Error Traps

After potential errors and their context have been described for each task, task-specific error traps may have become evident. In some cases, a single EPC can be considered to be an error trap—e.g., adjacent items of hardware that have compatible connectors enabling cross-connection. In other cases, an error trap will involve several factors that, in combination, can lead the operator to make a particular error—e.g., a difficult-to-reach non-captive fastener that must be tightened by a person wearing gloves who has no direct visual access to the fastener.

Because they apply to specific tasks, interfaces, and equipment, descriptions of error traps are likely to suggest possible solutions. Examples of error traps follow:

- In a particular procedure document, the first critical step that must be performed is listed as step 12.
- A warning in a procedure document appears after the procedural step to which it applies.
- Two components that are physically interchangeable but functionally different have similar labels or part numbers (e.g., NTS6132 and NTS1632).
- An input device provides no feedback to the operator that a command has been received, potentially leading to repetition of the command.
- A task requires the operator to perform an action opposite to habit, increasing the chance of a skill-based slip.
- Automation transitions from one mode to another without adequately informing the human operator.

4.7 Develop and Verify Human Error Management Strategy

For human errors that could result in catastrophic outcomes, a management strategy must be developed. The aim of human error management is not necessarily to remove human error by assigning functions and tasks to machines (although in some cases, that may be appropriate). In many cases, it will be appropriate to take steps to protect the system from human error, while retaining the positive contribution of the human to system performance.

The following human error management strategies are outlined in Section 2.3.12 of NPR 8705.2C, in order of precedence:

- Prevent human error.
- Reduce the likelihood of human error and provide the capability to detect and correct or recover from human error.
- Limit the negative effects of errors.

HEA management strategies can include a combination of such approaches.

Error management strategies can involve administrative or engineered countermeasures. Administrative countermeasures to error are “non-hardware” features of a system that rely on human behavior and compliance to prevent, detect, correct, and contain the effects of unwanted

behavior. They typically take the form of procedures, paperwork, work practices, training, and warning signs.

Engineered countermeasures to error are built into the system. They include physical features such as covers, interlocks, and tethers, as well as software features such as "undo" buttons and validation checks to capture data entry errors.

Issues to be considered include:

- Delayed vs. immediate consequences of error. If there is no delay between error and consequence, some interventions, such as secondary checks or inspections, may not be feasible. Some errors with delayed consequences will be immediately apparent and outwardly noticeable, whereas others will be latent (i.e., difficult to detect).
- Defense-in-depth. In some situations, it will be appropriate to have layers of defenses against a catastrophic error.
- Diversity of defenses. Adding diversity within the layer of defenses will generally provide more protection than simply repeating an existing defense (e.g., in some circumstances, an independent inspection *plus* a functional check may be more effective than two inspections or two functional checks).
- Matching countermeasures to errors. Ensuring that countermeasures are appropriate for the type of error. Different types of cognitive error (e.g., memory lapses vs. mistakes of controlled processing) require different interventions.
- Administrative vs. engineered countermeasures. Administrative defenses against error, such as procedures and warnings, typically rely on operator compliance and may not provide the same level of protection as engineered defenses, such as physical lockouts.

Proposed error management strategies should be verified to ensure they are effective in an operational context. The specific methods used for verification depend on the type of error management strategy. Verification methods include reviews by SMEs (including workers), comparison to requirements and human factors engineering (HFE) guidance, and performance testing.

5.0 Documenting the HEA

The HEA report should be seen as a living document that is first presented at the PDR, updated regularly, and presented again at the CDR and the ORR. At the PDR, the HEA report may examine potential errors at a relatively coarse level. However, as the design and development phase proceeds, it will be possible to identify potential errors with more granularity, and the HEA report should reflect this.

The report should consider all mission phases, including ground processing, launch, flight, mission control, and disposal/recovery.

The HEA team may choose to divide the report into two sections, as follows.

The first section of the HEA report should provide an overview of the activities outlined in the HSI plan, how they were used to identify potential human error, and the system improvements that resulted from these activities. This section will typically describe the application of human factors standards, crew workload evaluations, human-in-the-loop usability evaluations, and

hazard assessments. This section may refer to other activities, such as safety analyses, and may also contain:

- A review of relevant information from other analyses that were made available to the HEA team (e.g., PRA).
- A description of how the planned HSI and analysis activities enabled identification of potential catastrophic errors.
- A list of system improvements made to address human error.

The second section should describe the HEA approach taken to identify potentially catastrophic errors not captured by the activities outlined in the HSI plan, and the system improvements that occurred as a result of the HEA. System improvements may include changes to the design of hardware, procedures, or training. This section may contain:

- The screening approach used to identify areas for analysis.
- The method used to identify human tasks.
- The analysis methods used to analyze errors.
- A description of catastrophic errors identified during the HEA.
- System improvements made as a result of the HEA.

It may be useful to record the potential error and the related design response in a table or spreadsheet for ease of presentation and analysis. An example of a possible format is shown in Table 5-1.

Table 5-1. Example of Spreadsheet Presentation of HEA

	Task Descriptions		Task Context	Descriptions of Potential Errors		Error Traps	Proposed Error Management Strategy			
Scenario #	High-level task	Detailed task	Error-producing conditions (EPCs)	Outward description (guidewords may be used)	Cognitive description of error (if needed)	Error trap, if identified	Prevent error	Reduce likelihood of error	Enable detection and recovery from error	Limit conse-quences of error

6.0 Conclusion

There is no one way to conduct an HEA, and the team responsible must use judgment to identify the approach best suited to the systems being examined. HEA requires foresight to consider not only the human interactions that are expected to occur with systems, but also foreseeable but unplanned interactions that may ocur.

This document has described HEA as a series of sequential steps. However, in practice, the HEA process may not be entirely linear. Later steps in the process may bring to light information that requires earlier steps to be revisited. For example, when considering potential errors, it may become apparent that a task step has been overlooked in earlier task analyses.

HEA is not performed in isolation, but draws on other analyses, including hazard analysis and PRA. In addition, a thorough HEA will identify previously unidentified areas of concern that will need to be included in the other analyses.

The HEA team should be aware that interventions intended to manage the risk of human error could sometimes present hazards in themselves. Modifications for preventing or mitigating error should be re-evaluated to ensure that issues have been addressed and that no new error vulnerabilities have been introduced.

7.0 Glossary

Automatic processing	Human behavior or cognitive processes under the control of well-learned routines that can proceed without conscious thought.
Catastrophic error	An error with the potential to lead to a catastrophic event.
Catastrophic event	An event resulting in the death or permanent disability of a crew member or passenger, or an event resulting in the unplanned loss/destruction of a major element of the crewed space system during the mission that could potentially result in the death or permanent disability of a crew member or passenger.
Controlled processing	Human behavior or cognitive processes guided by conscious thought. In contrast to automatic processing, controlled processing is serial, slow, and effortful.
Critical action	An operator action required for mission success that, if performed in error during operations with zero failure, would result in a catastrophic event or an abort.
Critical function	A mission capability or system function that, if lost, would result in a catastrophic event or an abort.
Error	Either an action not intended or desired by a human or a failure on the part of the human to perform a prescribed action within specified limits of accuracy, sequence, or time that fails to produce the expected result and has led or has the potential to lead to an unwanted consequence.
Error-producing condition	A condition that can increase the likelihood of error across a range of tasks.
Error trap	A set of specific circumstances that can provoke similar errors, regardless of the people involved. Although factors internal to the person (e.g., fatigue or inexperience) may contribute to human error, the term “error trap” generally refers to a pre-existing aspect of procedures, human-system interfaces, and/or the task environment [ref. 6].
Foreseeable misuse	Undesired human interactions with an item of equipment that could have been reasonably predicted by the designers. (e.g., using a non-weight bearing structure as a foothold).
Knowledge-based error	An error in a situation that was unfamiliar or that presented new problems for the person, for which neither automatic mappings nor rules existed.

Mission	A major activity required to accomplish an Agency goal or effectively pursue a scientific, technological, or engineering opportunity directly related to an Agency goal. Mission needs are independent of any particular system or technological solution [ref. 16].
Outward behavior	The outward form of a behavior that would be visible to an actual or hypothetical observer. Errors can be described in terms of outward behavior without specifying their cognitive origins.
Skill-based slip	The performance of a familiar skill-based action at a time when this action was not intended, or on an object that was not intended.
Task analysis	An analytical process for determining the specific human behaviors required to fulfill human roles and responsibilities in system construction, operation, and maintenance.

8.0 Acronyms and Abbreviations

CDR	Critical Design Review
CFR	Code of Federal Regulations
ConOps	Concept of Operations
CREAM	Cognitive Reliability and Error Analysis Method
EPC	Error-producing condition
FAA	Federal Aviation Administration
HEA	Human Error Analysis
HFDS	Human Factors Design Standard (published by the FAA)
HFE	Human Factors Engineering
HRA	Human Reliability Analysis
HRCP	Human Rating Certification Package
HSI	Human Systems Integration
LRU	Line Replaceable Unit
NPR	NASA Procedural Requirements
NRC	Nuclear Regulatory Commission
ORR	Operational Readiness Review
PDR	Preliminary Design Review
PRA	Probabilistic Risk Assessment
SME	Subject Matter Expert

9.0 References

1. NPR 8705.2C, Human-Rating Requirements for Space Systems.
2. NPR 8715.3, NASA General Safety Program Requirements.
3. NASA/SP-2011-3421, Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners (Second Edition).
4. Chandler, F.T.; Chang, Y.H.; Mosleh, A.; Marble, J.L.; Boring, R.L.; and Gertman, D.I. (2006) Human Reliability Analysis Methods. Selection Guidance for NASA. NASA/OSMA Technical Report.
5. Occupational Safety and Health Administration (OSHA) regulations (29 Code of Federal Regulations, https://www.osha.gov/laws-regs/regulations/standardnumber.
6. Reason, J. (2004). Beyond the organizational accident: the need for "error wisdom" on the frontline. BMJ Quality & Safety, 13 (suppl 2), ii28-ii33.
7. NASA-STD-3001, NASA Spaceflight Human-System Standard, Vols 1 & 2, Revision B.
8. FAA (2016) Human Factors Design Standard (HF-STD-001B). Atlantic City: FAA.
9. NASA (2016). NASA Systems Engineering Handbook (NASA SP-2016-6105 Rev2).
10. Kirwan, B., and Ainsworth, L.K. (1992). A guide to task analysis. London: Taylor and Francis.
11. Seamster, T.L., and Redding, R.E. (2017). Applied cognitive task analysis in aviation. London: Routledge.
12. AeroSpace and Defence Industries Association of Europe (2017). Simplified Technical English. Specification ASD-STE100. Brussels: ASD.
13. Hollnagel, E. (1998). Cognitive Reliability and Error Analysis Method (CREAM). New York: Elsevier.
14. Reason, J. (1990). Human Error. Cambridge, UK: Cambridge University Press.
15. Null, C. (2018). Human Error Taxonomies. In Kanki, B.; Clervoy, J.; and Sandal, G. (Eds). Space Safety and Human Performance (pp. 36-52). Oxford: Butterworth Heinemann.
16. NPR 7120.5E, NASA Space Flight Program and Project Management Requirements.
17. FAA Regulation 14 CFR § 25.1302, "Installed systems and equipment for use by the flight crew."
18. European Aviation Safety Agency, Certification Specifications for large Aeroplanes (CS 25.1302).
19. FAA Advisory Circular, "Installed systems and equipment for use by the flight crew," FAA AC 25.1302.
20. European Aviation Safety Agency, Acceptable Means of Compliance (AMC) for EASA 25.1302.
21. ASTM (2010). Standard Practice for Human Systems Integration Program Requirements for Ships and Marine Systems, Equipment, and Facilities. ASTM Standard F1337-10.

22. Department of Defense, Human Engineering Program Process and Procedures Handbook (HDBK-46855A).
23. O'Hara, J.; Higgins, J.; Fleger, S.; and Pieringer, P. (2012). Human Factors Engineering Program Review Model (NUREG-0711, Rev. 3). Washington, DC: U.S. Nuclear Regulatory Commission.
24. O'Hara, J.; and Fleger, S. (2019). Human-System Interface Design Review Guidelines (NUREG-0700, Rev 3). Washington, DC: U.S. Nuclear Regulatory Commission.

Appendices

A. HEA in Other Domains

B. General Approaches to Information Collection

Appendix A. HEA in Other Domains

A.1 Aviation

FAA regulation 14 CFR § 25.1302, "Installed systems and equipment for use by the flightcrew," and its European counterpart (CS 25.1302) require that cockpit equipment must be designed with explicit attention to error management [refs. 17, 18]. The regulations require that installed equipment must incorporate "means to enable the flight crew to manage errors resulting from the kinds of flight crew interactions with the equipment that can be reasonably expected in service." This requirement applies to normal and non-normal conditions, but does not apply to errors involving a lack of manual skill or actions arising from malice, recklessness, or criminal intent.

The associated advisory material [refs. 19, 20] makes it clear that when applying for certification of an aircraft, the applicant must show that they have considered the flight crew errors that could occur, and have incorporated design features to counteract these errors.

The advisory material acknowledges that in most cases, the probability of flight crew errors cannot be reliably predicted, therefore a qualitative approach to error management is necessary. The means of compliance with 25.1302 may differ from project to project, and can include evaluation using mock-ups, part-task simulations, or the application of data from previous research or tests.

A.2 Maritime

The standard for human-system integration in ships and marine systems requires that "Potential error-inducing equipment design features are eliminated, or at least minimized, and systems are designed to be error-tolerant" [ref. 21, § 6.1.9]. The standard provides no specific guidance on how to perform a HEA, but recommends several techniques, including a lessons learned analysis to identify functions that are error prone, the application of user interface principles to reduce human error, and usability testing.

A.3 Military

Department of Defense Handbook 46855A, "Human Engineering Program Process and Procedures," emphasizes the need to identify human errors as part of the system acquisition process [ref. 22]. The document refers to the need for task analysis and error analysis during testing and evaluation, leading to corrective actions to address the potential errors. The handbook, however, provides no detailed information on the performance of an error analysis.

A.4 Nuclear Energy

Identifying and managing potental human errors is at the core of the U.S. Nuclear Regulatory Commission's (NRC) safety review of the design and operation of nuclear power plants. The NRC's review method involves evaluating the applicant's/licensee's HFE program e.g., task analysis, and the products of the program, e.g., the main control room. Two key documents guide the safety review: The HFE Program Review Model (NUREG-0711) contains the detailed review criteria for evaluating an HFE program [ref. 23], and the Human System Interface Design Review Guidelines contains the detailed review criteria for evaluating the products of an HFE program [ref. 24]. Specific review criteria addressing human error are included in almost every

area of review in NUREG-0711, which includes both qualitative, deterministic analyses, and quantative (e.g., PRAs) evaluations of human errors. NUREG-0700 provides criteria for the review of user interfaces to verify that they are designed to accommodate human capabilities and limitations, and therefore, minimize the potential for design-induced human errors [ref. 24].

Appendix B. General Approaches to Information Collection

There are many ways to collect information from personnel in support of HEAs, including:

- Surveys, questionnaires, and rating scales
- Interviews
- Observational studies
- Walk-throughs
- Performance-based tests
- Computer models

These methods are often used together. For example, while questionnaires can be used alone, they may also be used in conjunction with performance-based testing to collect personnel opinions. Each is discussed below.

In this appendix, the term *personnel* is used to identify the individuals from whom information is being collected.

B.1 Surveys, Questionnaires, and Rating Scales

Questionnaires and surveys are structured lists of questions in written form. Rating scales are a structured means of obtaining personnel responses to questions. One value of these methods is that a lot of information can be collected quickly and inexpensively.

Questionnaires/surveys can address any aspect of task performance (e.g., how personnel use human-system interfaces to perform tasks). Questionnaires should include space for personnel to include comments explaining their ratings or provide suggestions and recommendations.

Rating scales are composed of a question or statement that personnel evaluate using a provided scale that usually offers a finite set of options along an underlying continuum.

The scales can force personnel to think critically about aspects of the design. Personnel often find it easier to provide ratings than to answer open-ended questions about the same topics; therefore, the time and effort involved in the evaluation is reduced. In addition, the structure imposed by the rating scale method of data collection can make responses easier to summarize and use.

The limitation of these methods is that actual performance is not measured, so there is a chance that personnel responses may not correlate with performance.

B.2 Interviews

Interviews are one of the best methods to solicit personnel comments and opinions. They can be used to determine the root causes of problems personnel encounter and how they can be mitigated. Interviews can be conducted with individuals or groups. The latter are sometimes referred to as focus groups. The value of group interviews is that personnel can be surveyed in a short time. Bringing personnel together has the potential to yield more information due to the added value of their interactions with each other (e.g., they can challenge others' assumptions or cite counterexamples). A potential limitation is group dynamics. Sometimes one or two

individuals emerge as “leaders” and dominate the discussion. This places a burden on the interviewer to make sure all participants have an opportunity to contribute.

There are two types of interviews: unstructured or structured (although they can be used in combination).

Unstructured Interviews

Unstructured interviews usually involve interactions with personnel that are not highly scripted. The analyst asks open-ended questions about personnel knowledge and experience. To conduct successful unstructured interviews, the analyst must have adequate technical knowledge of the subject; otherwise, important questions may not be asked. Initial unstructured interviews permit the analyst to gain some understanding of the jobs and tasks about which personnel have knowledge. As the interview progresses, the analyst can add more structure to the questions that are posed. The analyst can also use the responses to develop a set of specific follow-up questions to administer during a subsequent structured interview.

A potential limitation of unstructured interviews is that personnel may be sidetracked, providing information that is not pertinent to the goals of the interview. In that case, the analyst must steer personnel back to the topic of the interview.

Structured Interviews

Rather than exploring a topic generally and then delving into specific areas when the opportunity presents itself (as in an unstructured interview), a structured interview involves asking specific questions. Personnel may be asked about why they take (or do not take) certain actions, how they know that an action should be taken, how they know that an action has succeeded (or failed), and how they recognize and correct errors.

A potential limitation of structured interviews is that the structure itself can inhibit personnel from providing important clarifications or supplemental information. In addition, important aspects of the topic may not be addressed by the questions. Thus, opportunities must be built into the process to obtain this type of information.

B.3 Observational Studies

Observational studies involve personnel carrying out tasks in their actual work environment, such as a flight deck or control room, or representations thereof, such as a mock-up or training simulator. The analyst observes personnel activity as unobtrusively as possible and generally does not interact with them while they are working (there is usually opportunity after the observation session to interview personnel to obtain clarifications and additional information).

A limitation of this approach is that the analyst lacks control. That is, in observational studies, personnel are typically free to attend to whatever aspects of the situation they choose and perform functions by whatever means they deem appropriate. Thus, it is possible that little time may be spent in the types of interactions the analyst is most interested in.

B.4 Walk-throughs

In a walk-through, information is gained by walking through tasks with personnel, such as walking through a procedure. Walk-through techniques can use a variety of “testbeds.” Personnel can do a tabletop walk-through of the task with no props to aid in performing the task

flow. Walk-throughs also can use representations of the system on which the task is performed, such as engineering drawings, mockups, simulators, and the actual work environment.

Personnel perform selected activities and provide information to the analyst either in response to questions or as a narrative of their thought process as they carry out their actions. When personnel verbalize what they are thinking as they are performing the task or interact with the HSI, they may reveal the strategies they use and the resources needed to perform the task. The narrative will also draw attention to aspects of the design that do not complement personnel goals.

To supplement and better focus on the analysts' information needs, they may ask questions such as:

- Why do you do this?
- How do you do it?
- What are the preconditions for doing this?
- What information do you consult in doing this?
- What are the results of doing this?
- Do errors occur when doing this?
- How do you discover and correct these errors?

As the tasks are being described, the analyst should ask personnel to identify any especially positive or negative features of the design that may affect performance. Personnel can be asked to think of past experiences and any difficulties they have encountered. Personnel can be asked about the root causes of problems they identify.

B.5 Performance-based Tests

Performance-based tests involve having personnel perform tasks while measures of performance are obtained. The measures of performance can then be used to assess task performance and better understand the factors that affect it, such as situation awareness and workload. This type of test usually requires a controlled environment where the same scenarios can be repeated. Thus, they are typically performed using some type of simulation or engineering test facility.

There are many methodological considerations for conducting this type of test. These include selecting personnel to participate, developing scenarios, identifying an appropriate testbed, selecting measures of performance, and establishing criteria against which performance can be compared. Thus, this type of test can be resource intensive requiring test facilities and expertise in testing methodology.

B.6 Computer Models

As used in this context, modeling refers to modeling human performance. The other methods discussed thus far, the information was obtained from personnel. When modeling techniques are used, information is provided by the human behavior models, rather than personnel.

Modeling is increasingly being used in the design and evaluation of complex systems. By representing the behavior of the system and of the personnel that interact with it, it is possible, for example, to consider in iterative fashion the effects of design options on task performance,

including human errors. A value to modeling is that it does not require access to personnel or facilities, such as training simulators. Also, once developed, the models can be run over and over as modifications are made to the task and interface design.

A potential limitation is that human performance modelling typically requires time and specialized expertise to develop system and personnel models that are of high enough fidelity to produce data of use by HEA analysts.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
04/28/2020	Technical Memorandum	

4. TITLE AND SUBTITLE
Guidance for Human Error Analysis (HEA)

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Null, Cynthia H.; Hobbs, Alan; O'Hara, John; Dischinger, charles

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER
869021.03.07.01.04

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
NASA Langley Research Center
Hampton, VA 23681-2199

8. PERFORMING ORGANIZATION REPORT NUMBER
NESC-NPP-18-01368

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-2020-20205001486

12. DISTRIBUTION/AVAILABILITY STATEMENT
Unclassified - Unlimited
Subject Category Space Transportation and Safety
Availability: NASA STI Program (757) 864-9658

13. SUPPLEMENTARY NOTES

14. ABSTRACT
NASA's Human-Rating Requirements for Space Systems in NASA Procedural Requirements (NPR) 8705.2C requires Program Managers to conduct a human error analysis (HEA) for all mission phases. The purpose of the HEA is to enable programs to understand and manage potential catastrophic hazards that could be caused by human error, understand the relative risks and uncertainties within the system design, and influence decisions throughout the system lifecycle. This document provides guidance to NASA civil servants and contractors on how the Agency's HEA requirement can be fulfilled.

15. SUBJECT TERMS
Human Error Analysis; NASA Procedural Requirement; Human Error; Human Systems Integration

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)
U	U	U	UU	39	19b. TELEPHONE NUMBER *(Include area code)* (443) 757-5802