**Human Factors Engineering
Criteria and Design for the
Hanford Waste Vitrification Plant
Preliminary Safety Analysis Report**

**J. A. Wise
A. Schur
J. C. L. Stitzel**

September 1993

**Prepared for the U.S. Department of Energy
under Contract DE-AC06-76RLO 1830**

**Pacific Northwest Laboratory
Operated for the U.S. Department of Energy
by Battelle Memorial Institute**

**RECEIVED
OCT 14 1993
OSTI**

PNL-8700

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights.** Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST LABORATORY
operated by
BATTELLE MEMORIAL INSTITUTE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC06-76RLO 1830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information, P.O. Box 62, Oak Ridge, TN 37831;
prices available from (615) 576-8401. FTS 626-8401.

Available to the public from the National Technical Information Service,
U.S. Department of Commerce, 5285 Port Royal Rd., Springfield, VA 22161.

**Human Factors Engineering Criteria and
Design for the Hanford Waste Vitrification
Plant Preliminary Safety Analysis Report**

J. A. Wise
A. Schur
J. C. L. Stitzel

September 1993

Prepared for
the U.S. Department of Energy
under Contract DE-AC06-76RLO 1830

Pacific Northwest Laboratory
Richland, Washington 99352

MASTER

ds
DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

Summary

This report provides a rationale and systematic methodology for bringing Human Factors into the safety design and operations of the Hanford Waste Vitrification Plant (HWVP). Human Factors focuses on how people perform work with tools and machine systems in designed settings. When the design of machine systems and settings take into account the capabilities and limitations of the individuals who use them, human performance can be enhanced while protecting against susceptibility to human error. The inclusion of Human Factors in the safety design of the HWVP is an essential ingredient to safe operation of the facility.

Previous U.S. Department of Energy (DOE) guidance for incorporating Human Factors into facility operations has been mostly concerned with extant nuclear reactors and related structures. The HWVP is a new construction, nonreactor nuclear facility designed to process radioactive wastes held in underground storage tanks into glass logs for permanent disposal. Its design and mission offer new opportunities for implementing Human Factors while requiring some means for ensuring that the Human Factors assessments are sound, comprehensive, and appropriately directed.

Building upon the intent and structure of previous DOE guidance, this report proposes an approach to HWVP Human Factors safety design and operation that utilizes cross-impact matrices to relevance test Human Factors elements organized in a structural tree against ways in which accidents, abnormal, or anomalous operations can occur in the HWVP. This provides a systematic assessment process that efficiently outlines those areas that would most benefit from Human Factors attention, while revealing non-obvious sources of potential human error that can initiate, assist, or magnify the development of accident situations. The cross-impact matrices become an accounting tool that help ask the right questions about the relevant characteristics of human-machine-building interactions throughout the range of safety situations.

Using the matrices methodology is an iterative procedure that begins with the Preliminary Safety Analysis Review and continues with successive cycles of Safety Analysis Reviews throughout HWVP design development. Both the structure of Human Factors elements and the operational scenarios for potential safety risks, as used in the matrices, can be refined and employed at lower levels of implementation as more detailed analysis of the facility design and the processes it employs becomes available.

Acronyms

CCTV	Closed-Circuit Television
CFAs	Control Function Allocations
DBA	Design Basis Accidents
HF	Human Factors
HMI	Human-Machine Interface
HWVP	Hanford Waste Vitrification
PSAR	Preliminary Safety Analysis Report
SAR	Safety Analysis Report

Contents

Summary	iii
Acronyms	v
1.0 Introduction	1.1
2.0 Human Factors in the HWVP	2.1
3.0 The Process of Human Factors in Safety Analysis	3.1
3.1 Design Basis Accidents	3.1
3.2 Abnormal Operations	3.1
3.3 Anomalous Operations	3.2
4.0 The Cross-Impacts Matrix: A Systematic Application on Human Factors to SAR	4.1
5.0 An Example and Conclusions	5.1
6.0 Conclusion	6.1
7.0 Bibliography/References	7.1
8.0 Acronyms	8.1

Tables

1	Staffing	4.2
2	Human-Machine Interface - Workplace Environment	4.3
3	Human-Machine Interface - Communications and Alarm Warning System	4.4
4	Human-Machine Interface - Controls, Displays, and Labels & Location Aids	4.6
5	Human-Machine Interface - Computers	4.8
6	Human-Machine Interface - Panel Layout and Control Display Integration	4.10

Figures

1	Structural Diagram of HF Elements as Applied to the HWVP	2.4
---	--	-----

1.0 Introduction

This document introduces the background rationale and application concepts that could be used to bring Human Factors (HF) into the safety design and operations of the Hanford Waste Vitrification Plant (HWVP). HF is the collective noun that describes the study of human performance in designed systems and how it can be enhanced while protecting against the sources of human error. The HWVP is a new, nonreactor nuclear facility that is being designed to convert the Hanford radioactive wastes, held in underground storage tanks, into glass logs for permanent disposal. The Safety Analysis Report (SAR) of the HWVP serves to define and control the safety basis for the design, procurement, construction and operation of the facility. U.S. Department of Energy Order Number 5480.23 (DOE 5480.23 4-10-92) applies to the HWVP and mandates that HF considerations will be a component of the SAR. This document includes a brief summary of DOE guidance on HF, sources of relevant HF standards, and an example system for structured HF inquiry into the safety design of the HWVP. It also has examples of how HF input to the design of the HWVP can help prevent and recover from various potential accidents, abnormal occurrences, and anomalous operations. This document provides input to the Preliminary SAR (PSAR) of the HWVP to demonstrate acknowledgement of HF criteria in the SAR, their understanding for this specific facility design, and their implementation into the ongoing safety design process.

A formal HF component to the SAR process was added in 1992. It is the outcome of the DOE "lessons learned" throughout the engineering world in response to accidents with technological systems such as Bhopal, the Challenger, Chernobyl, the Exxon Valdez, the Piper Alpha platform, and Three Mile Island, where events went tragically wrong. In all of these cases, human error made fundamental contributions to the pattern of circumstances, either in the cascade of influences precipitating the core incident, or in the failure to engage proper mitigating actions to minimize the consequences.

The inclusion of HF broadens the SAR to include the ways that facility and equipment engineering design, staff characteristics and capabilities, and operational procedures all combine to strengthen and enhance human performance while protecting against susceptibility to human error. This represents a new "systems" contribution to safety analysis. HF in safety analysis focuses on the interaction of design, work, and technology management to improve operational safety by revealing and rectifying problems that are not apparent from single discipline perspectives. HF is not an "add-on". It makes cross-cutting impacts on potentially all aspects of safety design and operations.

DOE 5480.23 (4-10-92) on Nuclear Safety Analysis Reports and the accompanying Guidance for Preparation of Safety Analysis Reports (1992) clarify the importance of HF in the SAR process. They also note that the failures to include adequate HF safety design contributed substantially to the most spectacular nuclear and nonnuclear engineering failures of the last few decades. All of those technological systems had safety devices in place that were either misinterpreted, misused, or overlooked in operator and staff activities that led to the incident or cause of the failure to adequately recover from it. Because HF cuts across all other aspects of safety design and operations, because errors can reoccur in backup components that are supposed to offer additional safety protection, and because they can initiate the contributions of all other safety components if not able to be properly used, HF should be seen as one of the most important additions to the HWVP PSAR.

The Bibliography/Reference section of this document is divided into two groups. The first are standard resources that form much of the basis for HF inputs into the HWVP. The second are additional resources that contain additional information for particular types of issues and circumstances not covered in the standard resources (e.g., teleoperation, remote handling).

2.0 Human Factors in the HWVP

DOE has called for increased attention and incorporation of HF into its new and existing facilities. However, the current DOE guidance for implementing HF in the SAR (Clayton memorandum 1992),^(a) does not apply, as written, to new facility designs because the specific checklists used rely on an experience and operational history with a facility. However, by addressing the specific HF concerns identified in the DOE checklists and the intent that these manifest, existing DOE guidance is useful for planning HF inquiries into the safety design of the HWVP.

While the HWVP is both a new facility and a new type of facility conducting the largest scale vitrification process ever planned for high level radioactive wastes, it encloses and supports safety in human activities in much the same ways as other processing plants, laboratories, and control rooms. In the absence of a history of experience with this type of facility, HF standards can be most effectively and efficiently employed by engaging a three-pronged strategy.

Work from DOE HF guidance already in place for nuclear and other DOE facilities. One of the best classic documents is the *Human Factors Guide for Nuclear Power Plant Control Room Development* (EPRI 1984). Another source in widespread use by DOE is *Human Engineering Design Criteria for Military Systems, Equipment, and Facilities* (DOD 1989). DOE 5480.23 (4-10-92) also recommends the *IEEE Recommended Practice for Graphical User Interface Drivability* (IEEE 1992). DOE is also reviewing a new HF standard, *Human Factors Engineering Design Criteria: Volume 1 General Criteria*, (DOE 1993) that summarizes much of the relevant basic HF practices.

Work from HF criteria employed in similar or analogical processes and facilities. NASA has prepared extensive HF standards for telerobotics stations and remote handling operations that can be profitably employed in the HWVP. Also, as a nonreactor nuclear facility, the HWVP appears to have more in common with chemical processing plants than with nuclear plants. HF standards developed for application in the chemical processing industry may be valuably employed in the design and operation of the HWVP. The additional resources portion of the references lists the applicable documents.

Work by engaging a systematic matrix process designed to reveal the impacts HF can have in potential accident scenarios and abnormal and anomalous operations for the HWVP. This provides a customized, facility specific approach that allows us to incorporate the analysts' experience base and the results of the first two approaches to identify unique HF safety contributions at this site.

The in-place DOE guidance (Clayton Memorandum 1992)^(a) specifies elements HF is to consider,

(a) Memorandum from Richard A. Clayton to Distribution dated October 16, 1992.

although it does not structure these elements for HWVP application, nor show how they are to be employed toward new facilities. The five elements of HF are: Procedures, Qualifications and Training, Staffing, Human-Machine Interface (HMI), and Allocation of Control Functions.

Procedures are steps taken in a definite order as a way of accomplishing something. HF considerations ensure that these steps are logical and can actually be performed under the operational circumstances, and that each step can be verified as it is accomplished.

Qualifications and Training describe the skills and standards that must be met for particular job positions, and the method for attaining and maintaining those skills and standards. HF considerations ensure that staff are able to perform the work demanded of them. They include the design of adequate training programs with inclusion of end-users in the procedure writing process to gain input from practical experience, and regular training updates as procedures and equipment change. HF refers training programs to a job or task analysis, using severity, frequency, and experience with the task to determine the level of training required. Instructors must be technically qualified to understand the subjects they teach, and capable of designing lesson plans which incorporate real tasks.

Staffing describes the number of personnel and the physical and technical skills needed to accomplish a mission or operate a facility. Unlike nuclear reactor facilities, staffing requirements for nonreactor nuclear facilities have not been determined. HF considerations derive safety relevant staffing requirements from task analyses of requirements for operating a facility under emergency situations, or to handle abnormal circumstances.

Human-Machine Interface is concerned with how people utilize equipment and furnishings, and how habitable interior working conditions are maintained in the facility. HMI HF ensures that safety relevant actions by staff that depend on equipment and sustained environmental conditions will be effective and accurate under emergency or abnormal conditions. They also ensure that the kinds of human errors likely to create anomalous conditions will not occur, while identifying links to machinery and key influences in the work environment that may enable the formation of an incident or hinder the recovery from one.

Allocation of Control Functions determines how work will be divided between humans and machines. Tasks, functions, and responsibilities are assigned to either individuals, semi-automated, or automated devices. Proper allocation of control functions for safety operations ensures that tradeoffs between the limits and capabilities of humans and machines will be optimal, that the workload under emergency and abnormal conditions will not exceed the operators' capacity to deal with it, and that appropriate control responses to conditions will be made within time-critical windows of opportunity.

In addition to the five major HF categories, the *Guidelines for Control Room Design Reviews* (NRC 1981) further divided the HMI element into nine subcategories: Workspace Environment, Communications, Annunciator warning systems, Controls, Displays, Labels and Location Aids, Computers, Panel Layout, and Control-Display Integration.

Workspace Environment describes how to recognize and avoid or mitigate environmental conditions that may degrade the reliability or effectiveness of staff under emergency, abnormal, or anomalous conditions.

Communications describes how information exchange both on and offsite will satisfy requirements to keep or return the facility to safe operating conditions.

Annunciator warning systems ensure that emergency signals and notifications of off-nominal conditions are prioritized, grouped appropriately, and presented so as to allow a timely and accurate response.

Controls enable human and machine safety relevant actions to be made effectively and accurately.

Displays present needed safety relevant information in an easily noticed, interpreted, and integrated manner to form a true "situational awareness" of the facility operations and conditions.

Labels and location aids ensure that safety equipment and features are consistently designated and easily found and interpreted under all operating and emergency conditions.

Computers have their own special display and control devices which should remain operable under highly degraded facility conditions.

Panel Layout determines how controls and displays are designed, arranged, and integrated to support effective operations under all conditions.

Control-Display Integration describes the degree to which controls and displays are compatible in their use and interpretation. Compatibilities should occur in the timed feedback, and the position, direction, and magnitude of control-display motions.

We have arranged the five higher level elements and the NUREG categories into a structural tree (Figure 1). This tree is an interpretive structural diagram illustrating how HF elements are applied to the HWVP. In the tree, each of the original elements and categories have been further divided into subcategories that each specify a focus of HF safety issues for the HWVP.

The structural tree is a basic tool that constitutes a formal outline for investigative HF analysis. It can be developed to any level of detail desired to structure and apply HF to safety issues. At the level of the PSAR, the present level of detail suffices. Through subsequent analysis, lower levels of detail may become appropriate as facility design advances or new results of relevant studies become available.

The high level element of Control Function Allocations (CFAs) connects (dotted lines) to the elements of Staffing and HMI. This shows that the same lower level branches of the tree under those elements also occur under CFAs which deal with the division of tasks between humans and machines, or among different levels and types of personnel. These allocations determine what should be automated or semi-automated, and how.

Figure 1. Structural Diagram of HF Elements as Applied to the HWVP

3.0 The Process of Human Factors in Safety Analysis

HF is applied to safety analysis in the design of the HWVP by taking the HF elements in any level of the structural tree and relevance testing them against the ways in which accidents, abnormal operations, or anomalous operations can occur at different levels of detail. The level of detail is carried as far as needed to specify the source of an incident and its seriousness. The following discussion provides examples of how HF evaluations contribute to the review of facility design and safety analyses of different events.

3.1 Design Basis Accidents

The PSAR identifies thirteen potential Design Basis Accidents (DBA) associated with nuclear release, explosion, fire, or design-basis natural phenomena that may cause significant offsite consequences (Severity/hazard category 1). This represents the highest level of resolution for HF applications. Each of the DBAs include opportunities where HF considerations can help mitigate the consequences and aid recovery from the DBA. The HF significant aspects of the event are revealed by relevance testing the HF elements of the structural tree in the context of the proposed chain of events in the DBA.

In the DBA of "Earthquake", maximum consequences are likely to be created if the melter feed pump continues to operate and pump glass frit and waste slurry into the hot melter vessel, which may be broken or overflowing onto the spill pan. Under HMI for this DBA, operators need to receive rapid warning of this condition from multiple sensing systems that cannot be rendered inoperable at that location. This consideration is listed under Alarms and Warning Systems in the tree. Operators also need to have backup means of shutting down the melter feed pump that are not susceptible to a common mode failure, and a display that shows the action was successful. These HF considerations are listed under the subcategories Controls and Control Display Integration.

HF evaluation can be extended to even greater levels of detail. If a manual turnoff for the melter feed pump is feasible, its location and method of operation can also be "human factored" to ensure accessibility and operability. This graded approach to applying HF at greater levels of detail is determined by the severity of consequences in the DBA.

3.2 Abnormal Operations

The next level of resolution for HF applications is Abnormal Operations (classified as Severity/hazard level 2) and carry significant onsite consequences. Seven types of Abnormal Operations are identified in the PSAR. Again, the characteristics of each of these can be relevance tested against the operational HF elements to reveal a specific concern or event and suggest potential HF contributions.

For example, in the case of a potential airflow reversal of the HWVP ventilation system, personnel are to evacuate the contaminated area or don respirators. Immediate HF contributions listed under Workplace Environment-Wayfinding would ensure that evacuation routes are short, located in the most advantageous parts of the building, and large enough to accommodate the expected

number of people. If transit through double airlock doors of the facility is required, there will be safeguards against blocking both doors open under an egress load, which would compromise the facility even further. In addition, the distribution of emergency use respirators throughout potentially afflicted areas can conform to the personnel distribution, thus minimizing the time and effort to don one. This would be listed under Workplace Environment-Layout contributions.

Analogous HF contributions are to be made to the pressure differential alarms installed to detect airflow reversal, and to the operator controls needed to respond to this abnormal operating condition.

3.3 Anomalous Operations

We have added a level of Anomalous Operations to the above two levels of analysis in the PSAR to allow considerations of conditions that, while not abnormal in themselves, may be part of a cascade of occurrences, or multiple unrelated occurrences, that creates an abnormal operating condition. The lessons learned from prior failures in other complex engineered systems show that anomalous operations can be the critical events in a series of actions that either allow an abnormal condition to develop further once underway, or hinder recovery. Consideration of anomalous operating conditions introduces a preventative tool that HF brings to safety analysis.

Identified types of anomalous operations are: 1) omission of information, 2) omission of action, 3) inadvertent actuation, 4) misunderstood condition, 5) inappropriate action, 6) deviation from procedure, and 7) access difficulty. Each of these can be interacted with HF elements on whatever level of detail necessary to help ensure that, during normal HWVP operations any one or combination of these potential anomalies does not contribute to the development of an abnormal operating condition. The places to look for possible anomalous influences on safety are in the designs of facility systems and subsystems that have already been identified in DBAs and abnormal operations.

4.0 The Cross-Impacts Matrix: A Systematic Application of Human Factors to SAR

Tables 1 through 6 are cross-impact matrices that determine HF inputs to the SAR process. Across the top of the matrices are the lowest level elements from structuring the HF categories. These columns express, at a current level of operational detail, the specific concerns within each of the major HF categories.

The side (rows) of the matrices denote, in three decreasing orders of specificity and consequentiality, the various types of scenarios that could produce safety problems at the HWVP, as discussed in the previous section. These range from DBAs, through abnormal operations, to anomalous operations.

The matrices are used by selecting a row and interacting its entry with each of the operational HF elements in the successive columns. This reveals the different HF implications incorporated within the scenario. Working across the matrices in this fashion guarantees a rather exhaustive look at how HF can contribute to ensuring safety in each of the relevant situations. The matrices are filled in only a few places to demonstrate the process.

Many of these entries are in the form of questions or suggest non-specific interventions because the preliminary design of the facility is either not at the stage of detail needed or because the scenario in the SAR is undeveloped to that point. The value of the matrices process, then, is in how they focus HF questions within thinking about safety design and operations. Where a question would not be answered through regular design development, the use of a more specific HF tool is indicated (e.g., a task analysis would answer some of the safety issues about qualifications and staffing listed under some of the DBAs).

During the SAR process, an HF matrix analysis, as described, can be used to guide both thinking about incident scenarios and detailed design development. As it becomes more complete, it also acquires analytic value of its own in revealing the more critical areas of HF safety, as well as likely sources of safety problems in plant design and operations.

For example, looking down a column of a matrix would reveal which of the HF impact areas appear to have the most questions or concerns connected to them, which helps guide the next round of inquiries. Looking across a row helps determine which of the incident scenarios appear most problematic in their range of HF impacts. This suggests which of the possible problem areas deserve further design or operations treatment. In this way, a matrix becomes a tool that can be used iteratively to bring HF into the successive planning and design of the HWVP, which is where it needs to be if it is to make its most successful safety contributions.

Table 1. Staffing

<u>Context</u>	<u>Qualification & Training General Job Specific</u>	<u>Emergency Team</u>	<u>Procedures Changes/Updates Accuracy</u>	<u>Qualification of Writers</u>
DBA				
Earthquake			✓(a)	
Aircraft Crash			✓(a)	
Train Impact			✓(a)	
Extreme Winds			✓(a)	
Ash Fall			✓(a)	
Stream Explosion in Melter			✓(a)	
Formic Acid Fire			✓(a)	
Inadvertent Chemical Mix			✓(a)	
Cold Chemical Tank Breach			✓(a)	
Hydrogen Explosion/Receipt			✓(a)	
Tank				
Tank Bump			✓(a)	
Waste Hold Tank Breach			✓(a)	
Transfer Line Brk/Soil			✓(a)	
Abnormal Operations				
Tank Press. in Process Cell			✓(a)	
Overflow of Liquid Tank			✓(a)	
Exposure to Rad Source			✓(a)	
Mix of Caustic/Acid Tank			✓(a)	
Crane/Lift Drop			✓(a)	
Airflow Reversal on HVAC			✓(a)	
Small Glass Spill			✓(a)	
Anomalous Operations				
Omission of Information			✓(a)	
Omission of Action			✓(a)	
Inadvertent Actuation			✓(a)	
Misunderstood condition			✓(a)	
Inappropriate Action			✓(a)	
Deviation from Procedure			✓(a)	
Access Difficulty			✓(a)	

- (a) *Communication—Timeliness.* When an anomaly is detected, timely communication of the condition to the appropriate party may be critical. Ease of access to communication devices to report conditions is critical for timely response. For example, the report of an overflow of liquid tanks. The report of any leaks from hoses transporting the liquid should be prompt. Another example is anomalous pressure conditions in tanks.

Table 2. Human-Machine Interface - Workplace Environment

<u>Context</u>	<u>Control Room</u>	<u>Anthro Access</u>	<u>Wayfinding</u>		<u>Ambient Conditions</u>	
			<u>Air</u>	<u>Temp</u>	<u>Light</u>	<u>Sound</u>
DBA						
Earthquake						
Aircraft Crash						
Train Impact						
Extreme Winds			✓(b)	✓(b)	✓(b)	✓(b)
Ash Fall						
Stream Explosion in Melter						
Formic Acid Fire						
Inadvertent Chemical Mix						
Cold Chemical Tank Breach						
Hydrogen Explosion/Recpt Tank						
Tank Bump						
Waste Hold Tank Breach						
Transfer Line Brk/Soil						
Abnormal Operations						
Tank Press in Process Cell						
Overflow of Liquid Tank						
Exposure to Rad Source		✓(a)				
Mix of Caustic/Acid Tank						
Crane/Lift Drop						
Airflow Reversal on HVAC						
Small Glass Spill						
Anomalous Operations						
Omission of Information						
Omission of Action						
Inadvertent Actuation						
Misunderstood condition						
Inappropriate Action						
Deviation from Procedure						
Access Difficulty						

- (a) *Labels--Access, Legibility, and Meaning.* When labels are not used or are unclearly marked, and operator can misinterpret the information displayed, which can cause an inappropriate or delay of response to the up-set condition. Alarms and Warnings displays should have labels that indicate the type of upset condition, such as the alarm severity (warning condition, alarm condition), and the problem, such as the non functioning of the automatic shut-off to the tank pressure chemical process cell.
- Quick egress of a given area in emergency conditions could be hindered by poor visual access of EXIT signs, perhaps due to poor placement and lighting of these signs. Illuminated exit lines on floors and kickout pass-through panels in lower areas of the doors are both safety features that allow rapid egress in case of fire with thick interior smoke.
- (b) *Ambient Conditions--Air, Temperature, Light, and Sound.* Control room design should consider that the breach of control rooms by wind borne missiles through glazing (broken windows) could occur with extreme winds. Control room design should preclude the occurrence of this event.

Table 3. Human-Machine Interface - Communications and Alarm Warning System

<u>Context</u>	<u>Communications</u>			<u>Alarm Warning System</u>		
	<u>Access</u>	<u>Intelligibility</u>	<u>Operations</u>	<u>Access</u>	<u>Identify</u>	<u>Intelligibility</u> <u>Operations</u>
DBA						
Earthquake						
Aircraft Crash						
Train Impact						
Extreme Winds						
Ash Fall						
Stream Explosion in						
Melter						
Formic Acid Fire						
Inadvertent Chemical						
Mix						
Cold Chemical Tank						
Breach						
Hydrogen Explosion/						
Recpt Tank						
Tank Bump						
Waste Hold Tank Breach						
Transfer Line Brk/Soil						
Abnormal Operations						
Tank Press in Process						
Cell	✓(a)	✓(b)		✓(c)	✓(c)	✓(c)
Overflow of Liquid Tank	✓(a)	✓(b)		✓(c)	✓(c)	✓(c)
Exposure to Rad Source						
Mix of Caustic/Acid						
Tank				✓(c)	✓(c)	✓(c)
Crane/Lift Drop						
Airflow Reversal on						
HVAC						
Small Glass Spill						
Anomalous Operations						
Omission of Information						
Omission of Action						
Inadvertent Actuation						
Misunderstood condition						

Table 3. (contd)

<u>Context</u>	<u>Communications</u>			<u>Alarm Warning System</u>		
	<u>Access</u>	<u>Intelligibility</u>	<u>Operations</u>	<u>Access</u>	<u>Identify</u>	<u>Intelligibility</u> <u>Operations</u>
Inappropriate Action						
Deviation from Procedure						
Access Difficulty						
<hr/>						
(a) <i>Communication--Timeliness.</i> When an anomaly is detected, timely communication of the condition to the appropriate party may be critical. Ease of access to communication devices to report conditions is critical for timely response. For example, the report of an overflow of liquid tanks. The report of any leaks from hoses transporting the liquid should be prompt. Another example is anomalous pressure conditions in tanks.						
(b) <i>Communication--Intelligibility.</i> Communications type and quality is key to successful mitigation and recovery from an incident. When an emergency condition is being reported, it is important that the message be transmitted as clearly and accurately as possible. Unclear message transmissions can lead to misinterpretation of the type of emergency response activities. It may also be difficult for individuals to understand instructions to litigate an emergency, thereby increasing the response time to an emergency.						
(c) <i>Alarm Warning System--Access, Identify, and Intelligibility.</i> Due to the complexity of the HWVP plant, different types of up-set conditions are possible. Alerts and alarms should clearly communicate these conditions. The HF design of the alarm warning system has a major impact on early detection, prevention, and mitigation of an up-set condition. The operator, at all times, should have access to alerts that are presented to the appropriate sensor. If the alert is sonic, an operator should be certain of hearing it if noise is part of the event.						
Unintentional barriers, such as a console blocking a seated operator's field of view, can prevent the operator from seeing a presented alert and hence detecting it (e.g., an alert displayed on an annunciator panel indicating tank pressure has reached a critical value). If an operator, from a remote location, is expected to detect alarm conditions by observations such as detecting leaks in the hose conveying formic acid between a tank and a tanker truck, the image (perhaps by between a tank and a tanker truck, the image (perhaps by closed circuit television [CCTV]) should present a comprehensive view to ensure that no aspect of the hose is hidden from sight. Similarly, if a computer monitor is used to present an alert, the system may actually be sending an alert signal to the operator but the HMI design may preclude the operator from viewing the alert or having their attention drawn to it. This could degrade response to anomalous pressure conditions in tanks and/or response to improper mixing of caustic and acid chemicals. Another example is the detection of an upset pressure condition in tank process cells.						

Table 4. Human-Machine Interface - Controls, Displays, and Labels & Location Aids

<u>Context</u>	<u>Controls</u>			<u>Displays</u>			<u>Labels & Location Aids</u>		
	<u>Access</u>	<u>Location</u>	<u>Operations</u>	<u>Locate</u>	<u>Read</u>	<u>Meaning</u>	<u>Access</u>	<u>Legibility</u>	<u>Meaning</u>
DBA									
Earthquake									
Aircraft Crash									
Train Impact									
Extreme Winds									
Ash Fall									
Stream Explosion in Melter									
Formic Acid Fire									
Inadvertent Chemical Mix									
Cold Chemical Tank Breach									
Hydrogen Explosion/ Recept Tank									
Tank Bump									
Waste Hold Tank Breach									
Transfer Line Brk/Soil									
Abnormal Operations									
Tank Press in Process Cell	✓ ^(a)	✓ ^(a)						✓ ^(b)	
Overflow of Liquid Tank									
Exposure to Rad Source									
Mix of Caustic/Acid Tank									
Crane/Lift Drop	✓ ^(c)	✓ ^(c)	✓ ^(d)						
Airflow Reversal on HVAC									
Small Glass Spill									
Anomalous Operations									
Omission of Information									
Omission of Action									
Inadvertent Actuation									
Misunderstood condition									
Inappropriate Action									
Deviation from Procedure									

Table 4. (contd)

<u>Context</u>	<u>Controls</u>			<u>Displays</u>			<u>Labels & Location Aids</u>		
	<u>Access</u>	<u>Location</u>	<u>Operations</u>	<u>Locate</u>	<u>Read</u>	<u>Meaning</u>	<u>Access</u>	<u>Legibility</u>	<u>Meaning</u>
Access Difficulty									
<p>(a) <i>Controls and Panel Layout—Access, Operations, Location.</i> Controls that affect emergency shut-offs (e.g., shut-off of the feed to a tank) should be designed to easily enable, yet be protected from, inadvertent actuation. These controls should also be operable by individuals wearing protective clothing and should be located so that the individual activating the control does not obstruct the egress traffic flow. To ensure appropriate responses, the emergency consoles should have the same arrangement as consoles for general operations.</p> <p>(b) <i>Labels—Access, Legibility, and Meaning.</i> When labels are not used or are unclearly marked, and operator can misinterpret the information displayed, which can cause an inappropriate or delay of response to the up-set condition. Alarms and Warnings displays should have labels that indicate the type of upset condition, such as the alarm severity (warning condition, alarm condition), and the problem, such as the non functioning of the automatic shut-off to the tank pressure chemical process cell.</p> <p>Quick egress of a given area in emergency conditions could be hindered by poor visual access of EXIT signs, perhaps due to poor placement and lighting of these signs. Illuminated exit lines on floors and kickout pass-through panels in lower areas of the doors are both safety features that allow rapid egress in case of fire with thick interior smoke.</p> <p>(c) <i>Controls—Access and Location.</i> The general term for remote human control and sensing from a distance is <i>teleoperation</i>. The HWVP will employ many remote operating devices, like the control cranes, that will be teleoperated. The main bridge crane will be designed to facilitate repair or replacement of all major vessels and components in the process cells, to remove and replace cell covers, and to perform other lifting functions on lighter-weight supporting components. During any of the teleoperations, the possibility of dropping or in appropriately wedging objects must be considered. Poor access and location of the telemanipulator controls by the operator can cause them to adopt operating postures that are awkward and hinder dexterity thus causing undesirable actions such as dropping a captured components. Effective performance of teleoperation activities can be greatly improved by incorporation HF principles in to the design of telemanipulator controls.</p> <p>(d) <i>Controls—Operations.</i> The type of sensory-motor feedback the operator receives while performing a given telemanipulator activity can determine the accuracy (i.e., avoidance of unwanted collisions, repetitive bumping of equipment, and "letting go" of objects) and timeliness of operations. Poor sensory-motor feedback of the crane controls could result in an undesirable incident, such as a breach in one of the process tanks or the inadvertent drip of a cover block, thus slowing recovery from an identified up-set condition.</p>									

Table 5. Human-Machine Interface - Computers

<u>Context</u>	<u>Computer Monitors</u>	<u>Controls & Input Devices</u>
DBA		
Earthquake		
Aircraft Crash		
Train Impact		
Extreme Winds		
Ash Fall		
Steam Explosion in Melter		
Formic Acid Fire		
Inadvertent Chemical Mix		
Cold Chemical Tank Breach		
Hydrogen Explosion/Recpt Tank		
Tank Bump		
Waste Hold Tank Breach		
Transfer Line Brk/Soil		
Abnormal Operations		
Tank Press in Process Cell	✓(a)	✓(a)
Overflow of Liquid Tank	✓(a)	✓(a)
Exposure to Rad Source		
Mix of Caustic/Acid Tank	✓(a)	✓(a)
Crane/Lift Drop		
Airflow Reversal on HVAC	✓(a)	✓(a)
Small Glass Spill		
Anomalous Operations		
Omission of Information	✓(a)	✓(a)
Omission of Action	✓(a)	✓(a)
Inadvertent Actuation	✓(a)	✓(a)
Misunderstood condition	✓(a)	✓(a)
Inappropriate Action	✓(a)	✓(a)

Table 5. (contd)

<u>Context</u>	<u>Computer Monitors</u>	<u>Controls & Input Devices</u>
Deviation from Procedure	✓(a)	✓(a)
Access Difficulty	✓(a)	✓(a)

-
- (a) **Computers—Computer Monitors and Controls & Input Devices.** Many processes in the HWVP will be automated. Historically, many systems are developed where the automated system(s) and operator cannot operate in a coordinated manner. The results of this working environment is that the operator can easily, inadvertently initiate a chain of events which can cause unsafe conditions, can fail to detect unsafe conditions, and can respond inappropriately to emergency conditions. For example, the events that occurred at Three Mile Island. To avoid both anomalous operations and conditions, and to enable safe, timely responses to anomalous events it is critical that the operator be provided with active supervisory control and monitoring of the automated systems. Such an approach creates a design philosophy which is operated by centered automation, and thereby, places the operator in a position of total system control at all times. The avoidance of anomalous conditions, detection, and/or examples where active supervisory control and monitoring can have a positive impact on the safe operations of these processes. Operator intervention to shut off a feed to a tank or the initiation and transfer of mixing caustic and acid chemicals in a neutralization tank, could be performed manually by an operator issuing a command by computer. In these circumstances, the controls(s) used to initiate this action should be properly protected and appropriate feedback should be provided in a timely manner to indicate the status of the action initiated by the operator. Inappropriate protection and feedback of an initiated control could result in inadvertent and/or continued initiation of the action.

Table 6. Human-Machine Interface - Panel Layout and Control Display Integration

<u>Context</u>	<u>Panel Layout</u>				<u>Control Display Integration</u>			
	<u>Access</u>	<u>Identify</u>	<u>Intelligibility</u>	<u>Operations</u>	<u>Interactive Control</u>	<u>Sys Feedback</u>	<u>Data Protection Control</u>	<u>Sys Layout</u>
DBA								
Earthquake								
Aircraft Crash								
Train Impact								
Extreme Winds								
Ash Fall								
Stream Explosion in Melter								
Formic Acid Fire								
Inadvertent Chemical Mix								
Cold Chemical Tank Breach								
Hydrogen Explosion/Recpt Tank								
Tank Bump								
Waste Hold Tank Breach								
Transfer Line Brk/Soil								
Abnormal Operations								
Tank Press in Process Cell		✓(a)		✓(a)				
Overflow of Liquid Tank								
Exposure to Rad Source								
Mix of Caustic/Acid Tank								
Crane/Lift Drop					✓(b)	✓(b)		
Airflow Reversal on HVAC								
Small Glass Spill								
Anomalous Operations								
Omission of Information								
Omission of Action								
Inadvertent Actuation								
Misunderstood condition								
Inappropriate Action								
Deviation from Procedure								

Table 6. (contd)

<u>Context</u>	<u>Panel Layout</u>				<u>Control Display Integration</u>			
	<u>Access</u>	<u>Identify</u>	<u>Intelligibility</u>	<u>Operations</u>	<u>Interactive</u>	<u>Sys</u>	<u>Data</u>	<u>Sys</u>
					<u>Control</u>	<u>Feedback</u>	<u>Protection</u>	<u>Layout</u>
Access Difficulty								

- (a) *Controls and Panel Layout—Access, Operations, Location.* Controls that affect emergency shut-offs (e.g., shut-off of the feed to a tank) should be designed to easily enable, yet be protected from, inadvertent actuation. These controls should also be operable by individuals wearing protective clothing and should be located so that the individual activating the control does not obstruct the egress traffic flow. To ensure appropriate responses, the emergency consoles should have the same arrangement as consoles for general operations.
- (b) *Control Display Integration—Interactive Control, System Feedback, Data Protection, and Control System Layout.* Remote operations of yokes and grapples will occur to affect repair or replacement of all major vessels. To perform these tasks, the integration of both the controls and displays will be necessary (e.g., obtaining an appropriate field of view with a telemanipulator controlled action). Often, a field of view may need to be changed to perform the necessary control action but the hands are busy using a telemanipulator. In these hands-busy eyes-busy situations, the voice commands allow the operator to obtain the appropriate views, as needed, or the inadvertent letting go of a component. In this example, the integration of voice and hand controls with the visual displays (CCTVs) must be seamless to minimize human error.

5.0 An Example and Conclusions

Looking across the DBAs, abnormal, and anomalous operations, it is apparent that many of the conditions would be detected and treated by operators through the use of remotely handled tools. Remote Closed-Circuit Television (CCTV) would be used to inspect suspected damage or imminent leaks. Cranes with a manipulator arm might be used to repair fittings or manually open and close valves that would normally be operated electrically. All of this points out the importance of HF in the HMIs that support teleoperation in the HWVP. (Teleoperation is used to describe the remote control of units which incorporate sensing and manipulating subsystems that extend the human operator's skills into a hostile or remote environment.) An HF engineer addressing teleoperator concerns looks for the following to be satisfied:

Coordination of visual and tactile/motor feedback. If feedback from any (e.g., the visual displays) of the components in the system is not coordinated with feedback from any of the others (e.g., handcontrollers) then the operator is forced to compensate. These compensations can lead to operator error such as inadvertently and frequently bumping into things, particularly when attempting to grab or "dock" with an object. This includes placing a lid on top of an opening or inserting fastener devices into their aperture. Another common symptom of poorly coordinated feedback is premature release of objects, or the continued torque of an object when no longer required. Premature release produces shocks to the object, while excessive torque can cause stress damage which can go undetected until the weakened part breaks under an added load.

Presence of necessary visual cues. The characteristics of the protective window or TV system where a remote operator views the results of their activities has the potential to distort details of the scene or cause them to be lost. This is particularly true with depth cues. Scene distortion and lack of depth cues make it difficult for the operator to accurately interpret the results of what they are doing. Poor or absent visual cues inevitably produce bumping or dropping of objects, along with failure to adequately complete a task.

The design of any remote viewing system must provide views of the actual scene that minimize scene distortion and maintain the depth or alternative cues needed to perform the manipulative tasks.

Workstation design that maintains task continuity (attention). The design of the telemanipulator workstation should allow the operator to have seamless access to the information needed without causing a break in telemanipulator actions. Discontinuity in a task sequence can cause an operator to lose track of the task resulting in an action that is unnecessarily repeated or skipped.

The sense of presence provided by proper visual access to a task is a critical factor in safe performance of a telerobotic activity. When CCTVs are used, the view obtained from a single camera is often insufficient to provide the operator with adequate views of the task site. This deficiency is typically compensated for by using a bank of images displaying different views of the site from multiple cameras. The design and location of this display bank impacts the task continuity for the operator. The operator should not have to move to see the various images, and should be able to see them in relation to each other, with their fields of view and detail selected to be congruent with a real

situational view as if the operator were actually present. This allows the operator's attention to be directed to the task demands, not to integrating disparate camera views.

Each of these concerns may be assessed and guaranteed to any limit of ability demanded, given the criteria of timeliness and severity of consequences that adroit teleoperations demand. Normal operations of the HWVP may suggest that a crane operator can work slowly and carefully, and therefore, does not need more elaborate views or controls. However, one or more of the DBAs and abnormal operations may place a high premium on completing remote actions quickly and accurately with the same control console. HF analysis can determine the minimum information and situational presence needed by an operator to perform safety relevant actions, and thereby set the human design requirements for the teleoperator system.

6.0 Conclusion

The range and depth of detail for HF considerations in safety design and operations of the HWVP is determined by combining the standards and analytical tools of HF with the situational demands that scenarios and foresight can devise. The cross-impact matrices are an accounting tool that helps ask the right questions throughout the total range of safety-relevant situations. HF inclusion in the SAR is not a list of standards or requirements. It is the establishment of a way of thinking about safety from the viewpoint of human demands and abilities, and the emplacement of a mechanism to ensure that subsequent safety analyses incorporate the power of this perspective into their results.

This successful incorporation of HF into safety analyses also provides the appropriate documentation needed to implement HF into safety designs. It brings together the human capabilities, design features, and the task context to determine the design basis of what is needed to meet the demands of safety in the facility. The present inclusion of HF in the PSAR of the HWVP and the mechanism for its continued application demonstrates that HF can be appropriately and effectively applied, in a timely manner, to affect all levels of facility and operational design.

7.0 Bibliography/References

Standard Resources

- Avery, L. W., R. V. Badalamente, S. E. Bowser, P. A. O'Mara, and S. E. Reynolds. 1990. *Human Factors Design Guidelines for the Army Tactical Command and Control System (ATCCS) Soldier-Computer Interface*. Pacific Northwest Laboratory, PNL-8272, Richland, Washington.
- Brookhaven National Laboratory. 1992. *Guidance for Preparation of Safety Analysis Reports*. (in press) Upton, New York.
- EPRI. 1984. *Human Factors Guide for Nuclear Power Plant Control Room Development, Final Report*. EPRI NP-3659, Essex Corporation, San Diego, California
- Farrell, R. J., and J. M. Booth. 1984. *Design Handbook for Imagery Interpretation and Equipment*. D180-19063, Boeing Aerospace Company, Seattle, Washington.
- Gilmore, W. E., D. I. Gertman, and H. S. Blackman. 1989. *User-Computer Interface In Progress Control, A Human Factor Engineering Handbook*. Academic Press, San Diego, California.
- IEEE. 1992. *IEEE Recommended Practice for Graphical User Interface Drivability*. IEEE P1201.2 Balloting Draft 1 May 1992, Institute of Electrical and Electronics Engineers, Inc., New York.
- NASA. 1989. *Man-Systems Integration Standards*, Vols 1-2. NASA-STD-3000, National Aeronautics and Space Administration, Washington, D.C.
- Poulton, E. C. 1974. *Tracking Skill and Manual Control*. Academic Press, Inc., New York.
- Smith, S. L., and J. N. Mosier. 1986. *Guidelines for Designing User Interface Software*. MITRE, Bedford, Massachusetts.
- U.S. Department of Defense (DOD). 1989. *Human Engineering Design Criteria for Military Systems, Equipment, and Facilities*. MIL-STD-1472D, Army Missile Command, Alabama.
- U. S. Department of Energy (DOE). 1992. *Nuclear Safety Analysis Reports*. DOE 5480.23, 4-10-92.
- U.S. Department of Energy (DOE). 1993. *Human Factors Engineering Program Requirements for Department of Energy (DOE) Nuclear Facilities*. DOE 5480.HFE (in press), Office of Nuclear Energy, Office of Nuclear Safety Policy and S, U.S. Standards, Washington, D.C.
- U.S. Department of Energy (DOE). 1993. *Human Factors Engineering Design Criteria: Volume 1 General Criteria*. DOE-XX-STD XXXX-1993 (in press), Project No. HFAC-0001, Office of Nuclear Energy, Office of Nuclear Safety Policy and S, U.S. Standards, Washington, D.C.
- U.S. Nuclear Regulatory Commission (NRC). 1981. *Guidelines for Control Room Design Reviews*.

NUREG-0700, Washington, D.C.

Woodson, W. E., B. Tillman, and P. Tillman. 1992. *Human Factors Design Handbook*. Second ed., McGraw-Hill, New York.

Additional Resources

Boff, K. R., and J. E. Lincoln. 1988. *Engineering Data Compendium: Human Perception and Performance, Vols. 1-3*. Harry G. Armstrong Aerospace Medical Research Laboratory, Wright Patterson Air Force Base, Ohio.

Davis, L. T., C. D. Gaddy, and J. R. Turney. 1985. *Approach to Team Skills Training of Nuclear Power Plant Control Room Crews*. NUREG/CR-4258, General Physics Corporation, Columbia, Maryland.

Dougherty, E. M. Jr., and J. R. Fragola. 1988. *Human Reliability Analysis: A Systems Engineering Approach with Nuclear Power Plant Applications*. John Wiley & Sons, Inc., New York.

Drury, C. G., and J. G. Fox. 1975. *Human Reliability in Quality Control*, Halsted Press, New York.

Mazour, T. J., and F. M. Ball. 1985. *Instructional Skills Evaluation in Nuclear Industry Training*. NUREG/CR-4344, Analysis and Technology, Inc., North Stonington, Connecticut.

Park, K. S. 1987. *Human Reliability: Analysis, Prediction, and Prevention and Human Errors*. Advances in Human Factors/Ergonomics, Vol. 7, Elsevier, New York.

Salvendy, G., ed. 1987. *Handbook of Human Factors*. John Wiley & Sons, Inc., New York.

Schur, A., S. T. Hunt, and D. J. Pond. 1991. *A Limited Human Factors Engineering Assessment of the 242-A Evaporator System: For Input to the Safety Class II Systems/Structure Assessment*. PNL-7806, Pacific Northwest Laboratory, Richland, Washington.

Swain, A. D., and Guttman, H. E. 1993. *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, Final Report*. NUREG/CR-1278, Sandia National Laboratories, Albuquerque, New Mexico.

U. S. Department of Defense (DOD). 1985. *Human Engineering Guidelines for Management Information Systems*. MIL-HDBK-761A (in press), Proposed Revision, U. S. Army Human Engineering Laboratory, Aberdeen Proving Ground, Maryland.

U. S. Department of Energy (DOE). 1991. *Personnel Selection, Qualification, Training, and Staffing at DOE Reactor and Non-Reactor Nuclear Facilities*. DOE 5480.20, 2-20-91.

U. S. Department of Energy (DOE). 1990. *Conduct of Operations Requirements for DOE Facilities*. DOE 5480.19, 7-9-90.

Distribution

**No. of
Copies**

**No. of
Copies**

OFFSITE

9 Pacific Northwest Laboratory

**2 DOE/Office of Scientific and Technical
Information**

**A. Schur K7-28
JCL Steitzel K6-65
J. A. Wise K6-66**

6 Westinghouse Hanford Company

**Publishing Coordination
Technical Report Files (5)**

D. F. Iwatate	G6-16
R. C. Brown	G6-06
B. W. Hall	G6-16
D. A. Smith	G6-16
D. I. Herborn	G6-16
D. G. Baide	G6-16

END

**DATE
FILMED**

12/16/93