INL/CON-14-32524
PREPRINT

HUMAN FACTORS DESIGN, VERIFICATION, AND VALIDATION FOR TWO TYPES OF CONTROL ROOM UPGRADES AT A NUCLEAR POWER PLANT

Proceedings of the Human Factors and Ergonomics Society Annual Meeting 2014

Ronald Laurids Boring

October 2014

The INL is a
U.S. Department of Energy
National Laboratory
operated by
Battelle Energy Alliance

uman Factors Design, Verification, and Validation for Two Types of Control Room Upgrades at a Nuclea Power Plant

Ronald Laurids Boring

Proceedings of the Human Factors and Ergonomics Society Annual Meeting 2014 58: 2295
DOI: 10.1177/1541931214581478

HUMAN FACTORS DESIGN, VERIFICATION, AND VALIDATION FOR TWO TYPES OF CONTROL ROOM UPGRADES AT A NUCLEAR POWER PLANT

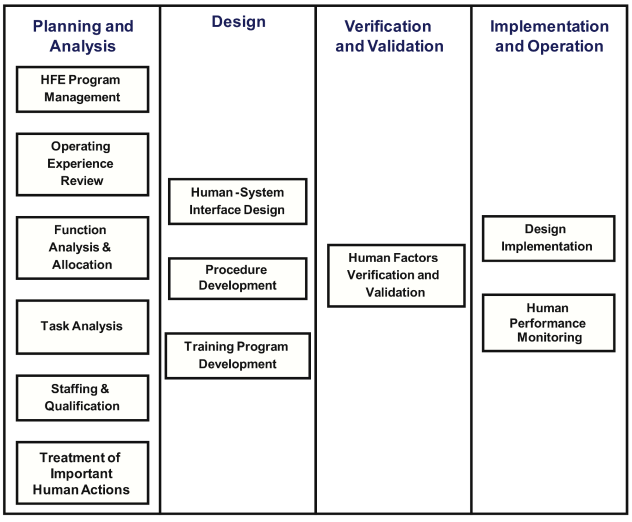
Ronald Laurids Boring
Idaho National Laboratory, Idaho Falls, Idaho, 83415, USA

This paper describes the NUREG-0711 based human factors engineering (HFE) phases and associated elements required to support design, verification and validation (V&V), and implementation of a new plant process computer (PPC) and turbine control system (TCS) at a representative nuclear power plant. This paper reviews ways to take a human-system interface (HSI) specification and use it when migrating legacy PPC displays or designing displays with new functionality. These displays undergo iterative usability testing during the design phase and then undergo an integrated system validation (ISV) in a full scope control room training simulator. Following the successful demonstration of operator performance with the systems during the ISV, the new system is implemented at the plant, first in the training simulator and then in the main control room.

INTRODUCTION

This paper describes the human factors engineering (HFE) phases and associated elements required to support design, verification and validation (V&V), and implementation of a new plant process computer (PPC) and turbine control system (TCS) at a nuclear power plant. The HFE phases discussed in this document are described in the U.S. Nuclear Regulatory Commission's (NRC) *Human Factors Engineering Program Review Model*, NUREG-0711, Rev. 3 (O'Hara et al, 2012). Each phase consists of one or more elements (see Table 1). Each element contains a description of the review criteria applied by the NRC HFE staff to assess the acceptability of an applicant's upgrade submittal regarding safe plant operation.

Table 1. HFE Phases Covered in NUREG-0711.



DESIGN ELEMENT ACTIVITIES

As described in NUREG-0711, Rev. 3, "The [human-system interface (HSI)] design process represents the translation of function and task requirements into HSI characteristics and functions." This section explains how previous work performed in the Planning and Analysis phase feeds into the actual design of an HSI at a representative U.S. nuclear power plant that is undertaking control room modernization. This section also illustrates the process by which existing PPC displays may be migrated to the new distributed control system (DCS) platform as well as the process by which new functionality can be introduced to the control room. In addition, the TCS an existing analog system on the panel is being converted to a DCS, and this section contains guidance to ensure the new design is successful.

HSI Specification

Each HSI display specification should include a general name of the display (corresponding to plant naming and numbering conventions), a description of the function of the display, a description of the placement of the display (e.g., some displays may be statically located, while others may be pulled up from any DCS display), assumptions regarding the hardware (e.g., size and resolution of display), information about the control mechanism (e.g., soft controls using a touchscreen vs. mouse or keypad control), and version information. Additionally, the specification should address the required information found in Figure 1, namely the relationship between operator/system inputs, the program logic, and the operator/system outputs. The system inputs (e.g., temperature at a certain sensor point) and outputs (e.g., valve close signal) may not in all cases be displayed to the operator, but their background use should be clearly documented in the specification. The specification should also feature documentation about any design considerations from the Planning and Analysis phases that influenced the design. The design background information may become crucial should later design modifications or license review be required.

Figure 1. Required Information for Display Specification. Migrating an Existing HSI Display.

A number of displays at the plant—most notably the Emergency Response Facility Information System (ERFIS) or Safety Parameter Display System (SPDS)—are slated for migration from the existing platforms to the new DCS platform. These displays have proven to be instrumental to operators, and it is desirable to carry these displays forward to the new DCS HSI. While no new functionality is required for these legacy displays, an effective migration needs to consider the characteristics of the DCS vs. the predecessor system. Relevant factors include:

- *Navigation*—if the DCS has a standardized navigation scheme, the legacy displays may not conform to that standard. For example, legacy ERFIS displays may feature primarily command-line execution, whereas the navigation of the new DCS is mainly menu driven. This disparity must be reconciled. Fortunately, the decision how to handle navigation is a one-time decision that can be applied across the entire suite of ERFIS displays, not piecemeal for individual ERFIS displays. The general navigation solution should be complemented by a display-specific navigation, e.g., where the display fits in menus or navigation groupings.
- *Display characteristics*—the DCS displays will likely be higher resolution than the predecessor systems, which may require some scaling conventions. Moreover, the DCS may feature reserved areas (e.g., designated alarm areas or navigation panes) that may not conform to the layout of the existing displays. The legacy displays may require additional updates to conform to the current HSI style guide. These display characteristics will need to be considered for each legacy display, although a few general display migration rules should suffice for the majority of displays.
- *Additional functionality*—for most purposes, the addition of features to legacy displays should be minimized. However, there may be some features that are required for continuity with newer DCS displays. For example, alarm functionality not found in the legacy displays may be desirable or even expected to harmonize the look and feel of the displays. The decision must be made to what extent the legacy displays look or behave differently than newer DCS displays. It is preferable not to have multiple conventions and styles within the DCS. However, the cost of adding or harmonizing features to legacy displays must be considered. Note that operators will tend to prefer displays with which they are familiar. An initial preference to retain the look and feel of legacy displays should be reevaluated after operators have opportunity to gain experience with the new DCS. Also, core functionality of a legacy HSI display should in most cases remain the same despite any aesthetic upgrades.

Table 2 provides a step-by-step list of questions to consider in the migration of legacy display to the new DCS display.

Table 2. HSI Design Migration Checklist.

1. Do any lessons learned from the Operational Experience Review apply to this display, and are any changes required as a result?
    a. If YES, what changes are required? If significant changes are required, follow the process outlined on designing new HSI displays.
2. Is any additional functionality suggested by the Functional Requirements Analysis or Function Allocation?
    a. If YES, what changes are required? Should the changes be made to this display, or should a new display be created? Follow the process outlined on designing new HSI displays.
3. Is all required information identified in the Task Analysis present in the display to support task execution?
    a. If YES, what changes are required? If significant changes are required, follow the process outlined on designing new HSI displays.
4. Does the existing display adhere to the present HSI Style Guide?
    a. If NO, what changes are required? Do the graphics translate or scale to the new DCS displays? Does navigation require updates? Are there conflicts (e.g., reserved areas on the DCS displays) between the existing display and the DCS? If significant changes are required, follow the process outlined on designing new HSI displays.
5. Are any required changes to the existing displays universal? In other words, can changes made to one legacy display be used as a template for other displays?
    a. If YES, document these changes (e.g., how to switch from command-line navigation to menu navigation) as an addendum to the HSI Style Guide, specifically as an HSI Migration Style Guide. This should eliminate the need to redesign each legacy display according to the process outlined on designing new HSI displays.
    b. If an HSI Migration Style Guide is available, follow it. If there are any required exceptions to this style guide, note them.

The decision process behind these questions should be documented with the display specification. The checklist should be used to help finalize the design specification for each migrated HSI display. Following development of the

specification, the HSI displays should be prototyped to verify appearance, functionality, and completeness. Each new HSI display should be reviewed by operators prior to performing the formal V&V activity. Designs that do not meet initial operator satisfaction should be iterated to improve the design. Documentation of the migrated design should explain how changes are consistent with earlier HSIs and the plant's Safety Analysis Report to aid regulatory licensing.

Designing New HSI Displays

New features should be developed in accordance with a standard user-centered design method such as ISO 9241-210 (2010), *Ergonomics of Human-System Interaction—Part 210: Human Centred Design for Interactive Systems*, and ISO 9241-11 (1998), *Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs)—Part 11: Guidance on Usability.* An example approach tailored for DCS display design can be found in Figure 2. The approach has five basic steps:

1. Identify the desired features and functions of the DCS display—whereby insights are extracted from the Operational Experience Review (to the extent there may be deficits in the existing HSI), the Functional Requirements Analysis and Function Allocation, and the Task Analysis conducted in the Planning and Analysis phase of NUREG-0711. There should be a clearly documented need for the new functionality as demonstrated by an existing performance deficit (e.g., a cumbersome or error-inducing HSI) or the opportunity for operator performance improvement (e.g., increased reliability through automation or improved operator response time). While operators' desires for new features may be considered, the basis for new features and functions should remain grounded in opportunities for improved reliability, safety, and performance.
2. The desired features and functions are turned into a specification. The HSI display specification should conform to the requirements outlined earlier in this paper. This display specification should conform to the plant's HSI style guide for DCS displays.
3. The specification is prototyped to a degree suitable for evaluation. The prototype can be as simple as a line sketch of the interface or involve using the DCS graphics development tools to create an early version of the final implemented DCS display. The prototype should contain sufficient fidelity such that dimensions and colors can be depicted accurately. If the native DCS environment is used for the prototype, it is not necessary to enable all functionality. The prototype will be evaluated, and it is important that the prototyping phase not be considered the end development and deployment stage. The prototype may be discarded in favor of better designs, once the usability testing is complete.
4. The prototype undergoes usability testing. Usability testing is the process of assessing the degree to which the designed system can be used effectively by the target user. Success metrics range from user satisfaction to user performance. In the case of the usability evaluation of the DCS displays, the foremost goal is to ensure that operators understand the HSI elements and also can operate the HSI, from navigating between different displays in the DCS to controlling parts of the plant using the DCS. The usability evaluation is ideally *formative*, meaning it is used not only to verify the usability of the designed system but also to help specify the design in an iterative fashion. There are two accepted ways of usability testing:
   - *Expert review*—in which subject matter experts in human factors, nuclear operations, or control systems review the HSI. This review may follow specific usability criteria called heuristics or provide an overall impression of how the HSI would be used and any deficiencies they might note. Expert reviews are especially useful early in the design phase, when a full-scale V&V will be conducted later in the development cycle.
   - *Operator testing*—which can range from walkthroughs with nonfunctional mockups to scenario testing using fully functional prototypes. The level of fidelity and functionality is a product of the resources of the design team and the degree to which the new functionality diverges from current plant operations. Note that operator testing at this stage will typically focus on the DCS HSI alone and not in the overall context of the control room. Integrated system validation (ISV)—testing of the new DCS with the full control room—occurs at the V&V phase.

   Results from the usability testing phase should be used to refine the design. If there are design deficiencies, the design should be revised and the process iterated starting at Step 2.
5. The design is finalized. Once the prototype has been evaluated and it has been determined that the HSI can be used successfully and safely by operators in the control room, the design specification and supporting documentation are assembled. This information is used as the basis of implementation and should be retained for licensing support. Additionally, it is anticipated that new HSI functionality incorporated into the control room would require a change in plant operating procedures. As the design is finalized, the adequacy of existing procedures should be documented.
6. The finalized design will be used in the V&V phase, which is documented in the next section.

VERIFICATION AND VALIDATION OF THE HSI

The HSI design process described in the previous section encompasses many of the HSI testing requirements for V&V outlined in NUREG-0711. In fact, this approach is explicitly

endorsed in Chapter 11 of NUREG-0711, Rev. 3. The specific phase of V&V that must be conducted independent of usability testing is integrated system validation (ISV). The steps for an ISV on the modified or new HSIs for PPC and TCS encompass the following steps:

1. The prototyped system is implemented in a fully functional variant in the full-scope control room simulator. The actual DCS display should be imbedded

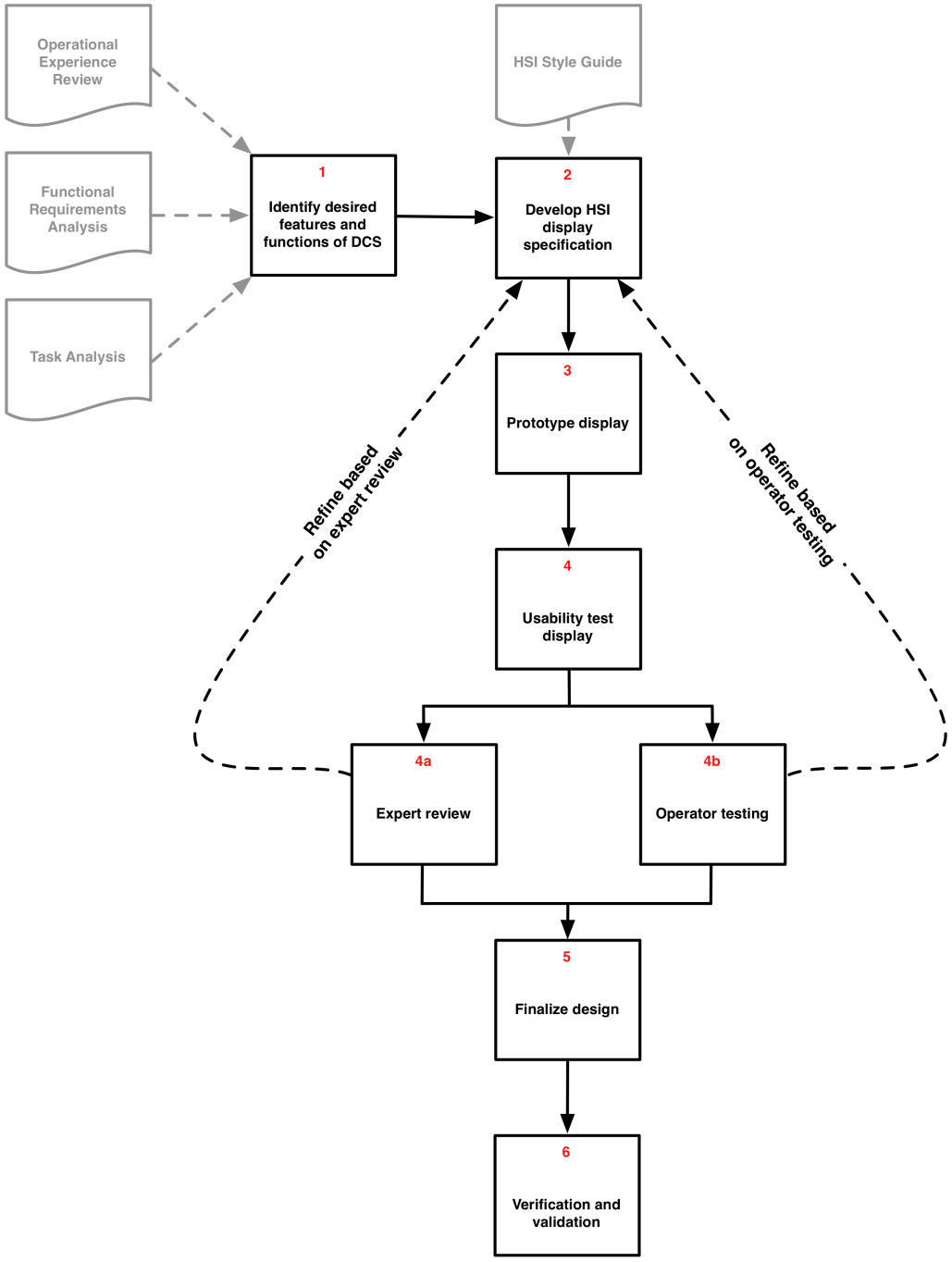


Figure 2. Flow Diagram for Developing New HSI Displays for DCS.

in the simulator to minimize the need for later detailed analysis of the tested vs. deployed system. As such, the DCS should follow careful software and hardware quality assurance requirements as part of the ISV. Note that a glasstop simulator using the underlying plant model from the training simulator may serve as a surrogate for the actual plant training simulator. This process can avoid the need to physically modify the training simulator (e.g., change hard panels to introduce displays) until the implementation phase. This avoids potential conflicts between training for the plant as is vs. the plant as it will be once modified.

2. A representative sample of scenarios is selected to walk through the new DCS HSIs with operators. These scenarios should encompass actual use of the DCS , test operator knowledge, test operator interactions with each other in the control room, and represent potential accident sequences. Note that the scenarios previously used in the Functional Requirements Analsysis/Function Allocation and Task Analysis workshops fulfill these criteria. The same scenarios that were run previously can be run during the V&V phase. These scenarios thereby also serve to benchmark operator performance before and after the new DCS HSI.
3. The DCS display should be pilot tested with a group of operator or qualified personnel (e.g., not-yet-licensed reactor operators, qualified trainers, recently retired reactor operators) to ensure the proper functioning of the system.
4. Operators are trained on the use of the new DCS HSIs. A stand-alone training program will be developed in cooperation with the training organization. In addition, the scenarios will be reviewed by trainers and procedure writers to ensure that the operating procedures do not require modifications as used in conjunction with the new DCS display.
5. Operators perform the selected scenarios using the new DCS HSI for PPC and TCS. A combination of systems engineering, HFE, and training personnel oversee the scenario walkthroughs to ensure:
   - The DCS implementation functions per the design specification.
   - The operators are able to complete the scenario tasks successfully (i.e., correctly, completely, within time requirements, and without confusion or misunderstandings) using the new DCS display. HFE personnel will assess situation awareness and workload to ensure these are within acceptable bounds.

   More than one set of operators should walk through the scenarios, and the order of the scenarios should be randomized to ensure performance on particular scenarios doesn't reflect learning effects.

The results of the ISV should be documented. Any deficiencies (e.g., human engineering discrepancies) should be resolved, and that resolution should be documented. Significant deficiencies should result in re-entering the HSI design process described earlier, although in most cases, a repeat of the entire ISV may not be necessary assuming usability testing of any redesigned HSIs is conducted.

DISCUSSION

As outlined in the previous section, the DCS is actually completed and tested as part of the ISV process. A final phase involves installing the new DCS and HSI. There are several stages to this installation:

1. The underlying DCS is installed in the plant simulator and plant.
2. The DCS HSI for PPC and TCS is deployed in the control room simulator for training purposes.
3. Operators are trained on the DCS HSI for the PPC and TCS.
4. The PPC and TCS DCS HSI are deployed in the main control room.

With separate DCS backbone and DCS HSI deployments, the deployment of the DCS would logically span a period between two scheduled outages at the plant. It is, however, possible to compress this cycle. The DCS, including both the backbone and the HSI, may be deployed in a single setting. Alternately, portions of the DCS backbone may be installed piecemeal, without major obstruction to regular plant operations.

The process outlined in this paper provides supplemental guidance to NUREG-0711 and ensures that control room modernization involving either a migrated HSI or a new HSI is successful. This process is currently being implemented at a U.S. nuclear utility with four plants slated for control room modernization. Additional details and lessons learned from those implementations will be published in future papers.

DISCLAIMER

This work of authorship 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 any of their employees makes any warranty, express 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. Idaho National Laboratory is a multi-program laboratory operated by Battelle Energy Alliance LLC, for the United States Department of Energy under Contract DE-AC07-05ID14517.

REFERENCES

International Standards Organization. (1998). *Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs)—Part 11: Guidance on Usability, ISO 9241-11.* Geneva: International Standards Organization.

International Standards Organization. (2010). *Ergonomics of Human-System Interaction—Part 210: Human Centred Design for Interactive Systems, ISO 9241-210.* Geneva: International Standards Organization.

O'Hara, J.M., Higgins, J.C., Fleger, S.A., and Pieringer, P.A. (2012). *Human Factors Engineering Program Review Model, NUREG-0711, Rev. 3.* Washington, DC: U.S. Nuclear Regulatory Commission.