Westinghouse

Westinghouse Electric Company
Nuclear Plant Projects
P.O. Box 355
Pittsburgh, Pennsylvania 15230-0355
USA

U.S. Nuclear Regulatory Commission
Document Control Desk
Washington, D.C. 20555

Direct tel: 412-374-4728
Direct fax: 412-374-5005
e-mail: vijukrp@westinghouse.com

Your ref: Docket No. 52-006
Our ref: DCP/NRC1639

October 16, 2003

SUBJECT: Transmittal of Programmatic Level Description of the AP1000 Human Factors Verification and Validation Plan

Enclosed please find Revision 2 of WCAP-15860, "Programmatic Level Description of the AP1000 Human Factors Verification and Validation Plan," dated October 2003. This revision incorporates changes previously identified in Westinghouse responses to DSER Open Items as follows:

| DSER Open Item | Westinghouse Letter | Date |
|---|---|---|
| 14.3.3-14 | DCP/NRC1600 | July 1, 2003 |
| 14.3.3-15 | DCP/NRC1600 | July 1, 2003 |
| 14.3.3-16 | DCP/NRC1600 | July 1, 2003 |
| 18.11.3.5-2 | DCP/NRC1600 | July 1, 2003 |
| 18.11.3.5-3 | DCP/NRC1600 | July 1, 2003 |
| 18.11.3.5-4 | DCP/NRC1600 | July 1, 2003 |

This reports contains no Westinghouse proprietary information.

Please contact me at 412-374-4728 if you have any questions concerning this submittal.

Very truly yours,

R. P. Vijuk, Manager
Passive Plant Engineering
AP600 & AP1000 Projects

/Enclosure
1. WCAP-15860, Revision 2, "Programmatic Level Description of the AP1000 Human Factors Verification and Validation Plan," dated October 2003

D063

DCP/NRC1639

October 16, 2003

**Enclosure 1**

WCAP-15860, Revision 2

"Programmatic Level Description of the AP1000 Human Factors Verification and Validation Plan,"

dated October 2003

Westinghouse Non-Proprietary Class 3

WCAP-15860
Revision 2

October 2003

# Programmatic Level Description of the AP1000 Human Factors Verification and Validation Plan

Westinghouse

# AP1000 DOCUMENT COVER SHEET

TDC: _____ Permanent File: _____ S _____

RFS#: _____ RFS ITEM #: _____

| AP1000 DOCUMENT NO. | REVISION NO. | | ASSIGNED TO |
|---|---|---|---|
| APP-OCS-GEH-020 | 2 | Page 1 of 21 | W–Winters |

ALTERNATE DOCUMENT NUMBER: WCAP-15860, Revision 2 WORK BREAKDOWN #: OCS

ORIGINATING ORGANIZATION: Westinghouse Electric Company LLC

TITLE: **Programmatic Level Description of the AP1000 Human Factors Verification and Validation Plan**

| ATTACHMENTS: | DCP #/REV. INCORPORATED IN THIS DOCUMENT REVISION: |
|---|---|
| CALCULATION/ANALYSIS REFERENCE: NA | Class 3 change to incorporate Draft Safety Evaluation Report Open Item Responses 14.3.3-14, 14.3.3-15, 18.11.3.5-2, 18.11.3.5-3, and 18.11.3.5-4. |

| ELECTRONIC FILENAME | ELECTRONIC FILE FORMAT | ELECTRONIC FILE DESCRIPTION |
|---|---|---|
| 5921r2.doc | Microsoft Word | NA |

**(C) WESTINGHOUSE ELECTRIC COMPANY LLC - 2003**

☐ WESTINGHOUSE PROPRIETARY CLASS 2

This document is the property of and contains Proprietary Information owned by Westinghouse Electric Company LLC and/or its subcontractors and suppliers. It is transmitted to you in confidence and trust, and you agree to treat this document in strict accordance with the terms and conditions of the agreement under which it was provided to you.

☒ WESTINGHOUSE CLASS 3 (NON PROPRIETARY)

| ORIGINATOR | SIGNATURE/DATE | |
|---|---|---|
| T. P. Hayes | T. P. Hayes 10/3/03 | |
| REVIEWERS | SIGNATURE/DATE | |
| | | |
| | | |
| | | |
| INDEPENDENT VERIFIER | SIGNATURE/DATE | VERIFICATION METHOD |
| M. M. Corletti | M. M. Corletti 10/3/03 | |
| AP1000 RESPONSIBLE MANAGER | SIGNATURE* | APPROVAL DATE |
| J. W. Winters | J. W. Winters | 10/7/03 |

*Approval of the responsible manager signifies that document is complete, all required reviews are complete, electronic file is attached and document is released for use.

**WCAP-15860**
**Revision 2**

# Programmatic Level Description of the AP1000 Human Factors Verification and Validation Plan

**S. P. Kerch**
**T. P. Hayes**

**October 2003**

**AP1000 Document: APP-OCS-GEH-020, Revision 2**

Westinghouse Electric Company LLC
P.O. Box 355
Pittsburgh, PA 15230-0355

© 2003 Westinghouse Electric Company LLC
All Rights Reserved

# TABLE OF CONTENTS

LIST OF FIGURES ..... iii

LIST OF ACRONYMS AND ABBREVIATIONS ..... iv

1 INTRODUCTION ..... 1-1
- 1.1 AP1000 V&V ACTIVITIES AND OBJECTIVES ..... 1-1
- 1.2 GENERAL SCOPE OF AP1000 V&V ..... 1-3
- 1.3 GUIDANCE DOCUMENTS FOR DEVELOPMENT OF V&V IMPLEMENTATION PLANS ..... 1-4

2 HSI TASK SUPPORT VERIFICATION ..... 2-1

3 HFE DESIGN VERIFICATION ..... 3-1

4 INTEGRATED SYSTEM VALIDATION ..... 4-1
- 4.1 METHODOLOGY ..... 4-1
- 4.2 TOOLS USED FOR EVALUATING DYNAMIC TASK PERFORMANCE ..... 4-1
- 4.3 INTEGRATED SYSTEM VALIDATION EVALUATIONS ..... 4-1
- 4.4 RISK-IMPORTANT TASKS ..... 4-2
- 4.5 COMPLIANCE WITH REGULATORY GUIDE 1.33 ..... 4-2
- 4.6 CRITERIA FOR SELECTION OF TEST SCENARIOS FOR DYNAMIC EVALUATIONS ..... 4-2
- 4.7 REALISTIC VALIDATION SCENARIOS ..... 4-4
- 4.8 PERFORMANCE MEASURES AND ACCEPTANCE CRITERIA ..... 4-4
- 4.9 SUBJECTS ..... 4-5
- 4.10 VALIDATION TEST DESIGN ..... 4-5
- 4.11 DATA ANALYSIS ..... 4-6
- 4.12 RESULTS AND DOCUMENTATION ..... 4-6

5 ISSUE RESOLUTION VERIFICATION ..... 5-1

6 PLANT HFE/HSI VERIFICATION ..... 6-1

7 REFERENCES ..... 7-1

# LIST OF FIGURES

Figure 1-1 AP1000 Verification and Validation Activities ..... 1-2

## LIST OF ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| EOP | emergency operating procedures |
| HED | human engineering discrepancies |
| HFE | human factors engineering |
| HRA | human reliability analysis |
| HSI | human system interface |
| HSID | human system interface design |
| NPP | nuclear power plant |
| PRA | probabilistic risk assessment |
| PRM | program review model |
| RTS | representative test set |
| TSC | technical support center |
| V&V | verification and validation |

# 1 INTRODUCTION

This document provides a programmatic level description of the AP1000 Human Factors Verification and Validation (V&V) plan. It specifies at a high-level the activities to be performed as part of the AP1000 V&V. Individual implementation plans that provide more detailed descriptions of the tests to be performed, and acceptance criteria to be used, will be developed for each V&V activity specified in this report. Individual V&V implementation plans will be developed after design certification.

## 1.1 AP1000 V&V ACTIVITIES AND OBJECTIVES

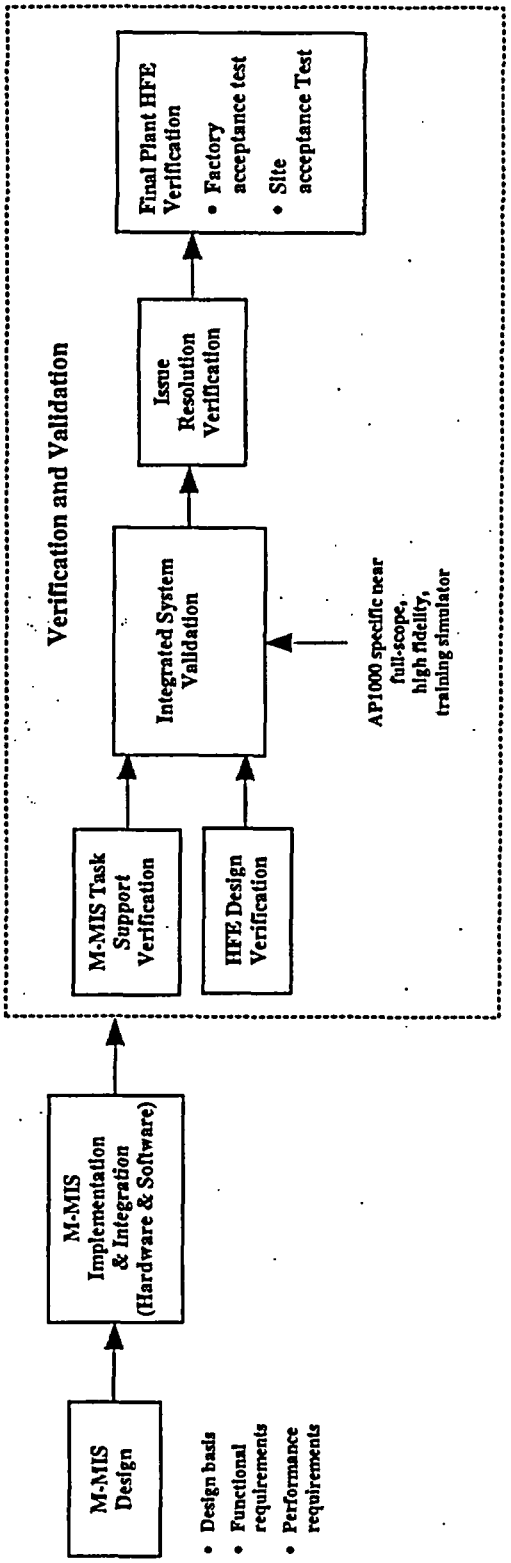
The Human Factors Engineering (HFE) Program Review Model (PRM) developed under the sponsorship of the U. S. NRC (NUREG-0711) specifies that an HFE V&V program should include five activities with the following objectives:

| | | |
|---|---|---|
| 1. | Task Support Verification: | Verifies that the human system interface (HSI) design provides all necessary alarms, displays, and controls to support plant personnel tasks |
| 2. | HFE Design Verification: | Verifies that the HSI design conforms to HFE principles, guidelines, and standards |
| 3. | Integrated System Validation: | Validates that the HSI design can be effectively operated by personnel within all performance requirements |
| 4. | Issue Resolution Verification: | Verifies that the HSI design resolves all identified HFE issues in the tracking system |
| 5. | Final Plant HFE Verification: | Verifies that the plant HFE/HSI (as designed at the time of plant startup) conforms to the verified and validated design that resulted from the HSI design process |

The AP1000 V&V will include all five of these activities. Figure 1-1 presents the following AP1000 V&V activities:

1. HSI Task Support Verification
2. HFE Design Verification
3. Integrated System Validation
4. Issue Resolution Verification
5. Plant HFE/HSI (as designed at the time of plant startup) Verification

As shown in Figure 1-1, the HSI Task Support Verification and HFE Design Verification may be conducted as parallel activities. It is also possible for the Issue Resolution Verification to be completed in parallel with other V&V activities.




Note: The Issue Resolution Verification may be performed in parallel with other V&V activities.

**Figure 1-1 AP1000 Verification and Validation Activities**

## 1.2 GENERAL SCOPE OF AP1000 V&V

The AP1000 V&V scope is defined with respect to HSI resources included in the V&V. The PRM scope description includes trained personnel and communication. Personnel training requirements and communication requirements will be addressed in the integrated system validation.

The scope of the AP1000 V&V will include:

- HSI hardware
- HSI software
- Procedures
- Workstation and console configurations
- Design of the overall work environment

Specifically included in the AP1000 V&V is verification and validation of the AP1000 Emergency Operating Procedures (EOPs). The implementation plan for the HFE Design Verification will address the verification of EOP format. The implementation plan for the Integrated System Validation will address the validation of the EOPs and associated HSI.

The AP1000 EOPs will be computerized. A backup will be available to handle the unlikely situation where the Computerized Procedure System is lost. Verification and validation will be conducted primarily on the computerized procedures. The backup will be evaluated as part of the integrated system validation by including test scenarios that examine the use of the backup following the simulated loss of the Computerized Procedure System.

Tasks for inclusion in the task analysis and V&V will be identified based on consideration of the importance of human actions for function achievement, and the impact of task failure on safety. Tasks in the areas of maintenance, test, inspection, and surveillance will be limited to those determined to be *risk-important* based on the probabilistic risk assessment (PRA) threshold criteria specified in the Implementation Plan for Integration of Human Reliability Analysis (HRA) and HFE Design.

Operational sequences will cover the full range of plant operating modes, including:

- Startup
- Normal operations
- Abnormal and emergency operations
- Transient conditions
- Low-power
- Shutdown conditions

The V&V scope will be limited to those facilities required for scenario evaluation that involve *risk-important tasks*, as defined by the PRA threshold criteria. Facilities included in the V&V scope are:

- Main control room
- Remote shutdown workstation
- Technical support center (TSC)

The AP1000 design does not require *risk-important* actions to be taken from local control stations, so local control stations are not included in the V&V scope. If, as a result of further analysis, *risk-important* tasks or critical actions are identified at local control stations, those stations, with respect to the identified tasks or actions, will be included in the V&V.

## 1.3 GUIDANCE DOCUMENTS FOR DEVELOPMENT OF V&V IMPLEMENTATION PLANS

Implementation plans providing detailed test procedures and acceptance criteria will be developed for each of the five V&V activities identified in Figure 1-1.

V&V implementation plans will be developed using accepted industry standards, guidelines, and practices. Documentation to develop the V&V implementation plans will include:

- CEI/IEC 964 "Design for Control Rooms of Nuclear Power Plants," International Electrotechnical Commission, 1989.
- IEEE Std. 845-1999 "IEEE Guide for the Evaluation of Human-System Performance in Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 1999.
- IEEE Std. 1023 "Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 1988.
- NUREG-0899 "Guidelines for the Preparation of Emergency Operating Procedures," U.S. Nuclear Regulatory Commission, Washington, D.C., August 1982.
- NUREG-1358 "Lessons Learned from the Special Inspection Program for Emergency," U.S. Nuclear Regulatory Commission, Washington, D.C., April 1989.
- NUREG-0711 "Human Factors Engineering Program Review Model," U.S. Nuclear Regulatory Commission, Washington, D.C., July 1994.
- NUREG-0700 "Human-System Interface Design Review Guideline," Rev. 1, U.S. Nuclear Regulatory Commission, Washington, D.C., June 1996.
- Regulatory Guide 1.33, "Quality Assurance Program Requirements," Rev. 2, U.S. Nuclear Regulatory Commission, Washington, D.C.

# 2 HSI TASK SUPPORT VERIFICATION

An implementation plan will be developed specifying a methodology for HSI task support verification. The HSI task support verification objective will be to verify all aspects of the HSI design (for example, controls, displays, alarms, procedures, and data processing) that are required to accomplish personnel tasks and actions as defined by task analyses, EOPs, and *risk-important* human tasks identified by the PRA.

The HSI Task Support Verification implementation plan will include a methodology description by which the HSI design will be checked against the information and control requirements identified by:

- Function-based task analyses
- Operational sequence task analyses performed for important and representative tasks as defined in Element 4 (Task Analysis)
- Operational sequence task analyses performed for *risk-important* personnel tasks as defined by the PRA
- Operational sequence task analyses performed for the complete set of EOPs
- Required minimum inventory of alarms, displays, and controls
- Required federally mandated (10CFR50.34) indication and control features

The HSI Task Support Verification methodology will describe how, in each case, the HSI resources will be verified to ensure that all alarms, displays, controls, procedures, and data-processing required for task performance are available, and that the characteristics of the HSI (for example, units of measure, accuracy, precision, and dynamic response) match task requirements.

The HSI Task Support Verification implementation plan will also describe a process by which the HSI design will be verified to ensure that the HSI does not include information, displays, or controls that do not support operator tasks. The information and controls provided on the HSI resources will be checked against display and control requirements generated from the function-based and operational sequence task analyses. Any information, display, or control appearing on an HSI resource not identified as required by any of the task analyses, will be flagged, requiring further analysis and review. If the information, display, or control is shown to be necessary to support operator performance, it will be documented, and the task analyses will be revised accordingly. If, after review, no explanation can be found for how the information, display, or control supports operator performance, it will be removed and the documentation will be revised accordingly.

# 3 HFE DESIGN VERIFICATION

An implementation plan that specifies a methodology for HFE design verification will be developed. The objective of the HFE design verification will be to verify that all aspects of the HSI (for example, controls, displays, procedures, and data processing) are consistent with accepted HFE guidelines, standards, and principles.

The HFE design verification implementation plan will specify a process by which deviations from accepted HFE guidelines, standards, and principles will be identified and acceptably justified based on a documented rationale, such as trade study results, literature-based evaluations, demonstrated operational experience, and tests or experiments.

The HFE design verification will include all HSI in the control room, remote shutdown workstations, and the TSC. Local control stations will be reviewed to the extent that they are required for *risk-important* human actions as defined by the PRA.

The HFE design verification specification plan will describe a procedure by which HSI resources will be verified, ensuring conformance to AP1000-specific HSI standards and convention guideline documents that will be prepared to cover all HSI resources and their integration. The AP1000-specific standards and convention guidelines will include:

- Alarm guidelines
- Display guidelines
- Controls guidelines
- Computerized procedures guidelines
- Anthropometric guidelines

The AP1000-specific HSI standards and convention guidelines will provide:

- Specification of accepted HFE guidelines, standards, and principles to which the HSI will conform

- Specification of particular design conventions (e.g., particular coding conventions) to which the HSI will conform

- Documentation of any deviations from accepted HFE guidelines, standards, and principles; and justification based on documented rationale such as trade study results, literature-based evaluations, demonstrated operational experience, and tests and experiments

An illustrative subset of accepted HFE guideline documents that will be used in compiling accepted HFE guidelines, standards, and principles to be included in the AP1000-specific standards and convention guideline documents are:

- American National Standards Institute, ANSI HFS-100-1988, "American Standard for Human Factors Engineering of Visual Display Terminal Workstations," Santa Monica, California, 1988.

- CEI/IEC 964 "Design for Control Rooms of Nuclear Power Plants," International Electrotechnical Commission, Geneva, Switzerland, 1989.

- NUREG-0899 "Guidelines for the Preparation of Emergency Operating Procedures," U.S. Nuclear Regulator Commission, Washington, D.C., August 1982.

- NUREG-1358 "Lessons Learned from the Special Inspection Program for Emergency," U.S. Nuclear Regulatory Commission, Washington, D.C., April 1989.

- NUREG-0700 "Human-System Interface Design Review Guideline, Rev. 1," U.S. Nuclear Regulatory Commission, Washington, D.C., June 1996.

- NUREG/CR-6501 "Human Factors Engineering Guidelines for the Review of Advanced Alarm Systems," U.S. Nuclear Regulatory Commission, Washington, D.C., September 1994.

- U.S. Department of Defense, DOD-HDBK-761A, "Human Engineering Guidelines for Management Information Systems," Office of Management and Budget, Washington, D.C., 1990.

- MIL-Std 1472F, "Human Engineering Design Criteria for Military Systems, Equipment and Facilities."

All aspects of the HSI – including information, displays, controls, data processing, navigation mechanisms, and workstation and console configurations – will be verified against the standards and conventions specified in the applicable AP1000-specific guideline documents.

The HFE Design Verification implementation plan will address the verification of EOP format and compliance with the respective procedure writer's guide.

The HFE Design Verification implementation plan will specify procedures for identifying, reviewing, and addressing deviations from the standards and conventions specified in the guideline documents. Included in the scope of the HFE design verification will be the identification of nonfunctional decorative details (borders and shadowing on graphic displays) not specified in the guideline documents that do not support operator task performance.

All deviations from standards and conventions specified in the guideline documents will be flagged for review. If there is adequate justification for the deviation, the justification will be documented. Otherwise, a change will be made to bring the HSI resource into compliance with the guideline documents.

# 4 INTEGRATED SYSTEM VALIDATION

An implementation plan will be developed specifying a methodology for integrated system validation. The objective of integrated system validation is to ensure that the functions and tasks allocated to the plant personnel can be accomplished with the HSI design implementation. Explicitly included in the integrated system validation is validation of the AP1000 EOPs.

## 4.1 METHODOLOGY

The integrated system validation implementation plan will include a methodology section that addresses:

- Objectives
- Personnel performance issues
- Test methodology and procedures
- Test participants
- Test conditions (including plant conditions, operating sequences, and accident scenarios)
- HSI description
- Performance measures
- Data analysis
- Acceptance criteria
- Process by which results will be used to determine whether changes to the HSI are required, and the process by which change requirements are tracked and verified

## 4.2 TOOLS USED FOR EVALUATING DYNAMIC TASK PERFORMANCE

Integrated system validation will be performed using an AP1000-specific, near full-scope, high-fidelity, simulator facility that satisfies the general requirements of Sections 3 and 4 of ANSI/ANS-3.5-1993. The near full-scope, high-fidelity simulator of the AP1000 control room will display high physical fidelity (the testbed will physically resemble the actual hardware to be implemented in the AP1000 control room), as well as high-fidelity with respect to information content (containing AP1000-specific displays and controls), and underlying process dynamics (it will be driven by an AP1000-specific plant simulation). The adverb *near* is used to indicate that features of the simulation not relevant to the test being made may not be full-fidelity.

Operator actions at non-control room facilities, such as remote shutdown panels and the TSC, may be evaluated using static mockups, or prototypes.

## 4.3 INTEGRATED SYSTEM VALIDATION EVALUATIONS

The implementation plan will specify the objectives of the integrated system validation to:

- Establish the adequacy of the integrated HSI for achieving HFE program goals
- Confirm allocation of function and the structure of tasks assigned to personnel
- Validate the EOPs and associated HSI
- Confirm the dynamic aspects of the HSI for task accomplishment

- Evaluate and demonstrate error tolerance to human and system failures
- Establish the adequacy of staffing and the HSI to support staff to accomplish their tasks

The implementation plan will specify how the integrated system validation will fulfill these evaluation objectives.

## 4.4 RISK-IMPORTANT TASKS

The integrated system validation will include test scenarios designed to validate the adequacy of staffing and the HSI to support personnel performance for:

- Important and representative tasks as defined in Element 4 (Task Analysis)
- Risk-important tasks as defined by the PRA threshold criteria
- Design-basis and beyond-design-basis accident scenarios covered by the EOPs

## 4.5 COMPLIANCE WITH REGULATORY GUIDE 1.33

Regulatory Guide 1.33, Appendix A, lists categories of activities that should be covered by written procedures, such as administrative procedures, general plant operating procedures, procedures for control of measuring and test equipment and for surveillance, procedures for performing maintenance, and chemistry and radiochemical control procedures. As indicated in Regulatory Guide 1.33, the procedures may be combined, separated, or deleted to conform to procedure plans.

Complete validation of all classes of procedures identified in Regulatory Guide 1.33 is beyond the scope of the integrated system validation. As stated in subsection 1.2, the V&V scope in the areas of maintenance, test, inspection, and surveillance will be limited to tasks determined as risk-important based on PRA threshold criteria

Integrated validation will include test scenarios simulating situations governed by sample procedures from selected Regulatory Guide 1.33 categories, for the purposes of increased realism, and to ensure that the AP1000 control room design, in conjunction with such procedures, can achieve their intended functions without interfering with plant operations. Test scenarios will be developed that include select maintenance, test, and surveillance activities conducted in the main control room while the plant is being operated to show that these tasks can be accomplished without interfering with operator tasks necessary for monitoring and controlling the plant

## 4.6 CRITERIA FOR SELECTION OF TEST SCENARIOS FOR DYNAMIC EVALUATIONS

A multi-dimensional set of criteria will be used to define a set of test scenarios to be included in the integrated system validation. Dimensions to be considered will include covering:

- Range of operational modes including normal plant evolutions (startup, full power, and shutdown)

- Transients (reactor trip and turbine trip)

- Design-basis and beyond design-basis accidents covered by the EOPs
- AP1000-specific design features (the Automatic Depressurization System and the Diverse Actuation System)
- Scenarios that include human performance actions identified to be *risk-important* by the PRA
- Instrument failures
- HSI equipment and processing failures, including failure of the computerized procedure system, establishing the ability to use the backup
- Reactor shutdown and cooldown from the remote shutdown panel
- Situations that produce cognitive challenges, including situations that complicate:
  - Situation assessment by providing degraded or conflicting plant state information
  - Response (require balancing of multiple goals and require manual takeover of automatic systems)
  - Performance by increasing personnel communication/coordination requirements

  or

  - Increase workload by introducing additional tasks or distractions (Sections 4.5 and 4.7)

The set of test scenarios specified will be sufficient to validate the EOPs as implemented in computerized procedures or by an alternative procedure implementation method.

They will also include scenarios to validate key HRA modeling assumptions for event sequences that involve *risk-important* human actions. Examples of assumptions to be confirmed are that particular human actions that need to be performed are satisfactorily completed within the time-window specified in the PRA.

The set of test scenarios included in integrated system validation will be defined by a multi-disciplinary team that includes input from EOP developers, HSI designers, human factors specialists, and human reliability analysis/PRA analysts. The test scenarios listed below will be included in the complete list of scenarios identified by the multi-disciplinary team: (Each of these scenarios satisfies one or more of the selection criteria described above.)

- Normal plant heatup and startup to 100-percent power
- Normal plant shutdown and cooldown to cold shutdown
- Transients – reactor trip and turbine trip

- Accidents
  - Small-break loss of coolant accident
  - Large-break loss of coolant accident
  - Steam line break
  - Feedwater line break
  - Steam generator tube rupture

The Representative Test Set (RTS) must be selected from the universe of conceivable scenarios based on an ad hoc technical understanding of the plant system and its credible failure modes. The bases for the selected events must justify that the RTS is reasonably conservative in its coverage of credible challenges to system safety. The basis for the RTS is a principle justification for the sufficiency of validation testing.

## 4.7 REALISTIC VALIDATION SCENARIOS

The implementation plan will specify how test scenarios will be realistic with respect to plant conditions that are likely to hold for the situations being represented (number of personnel in the control room, communication requirements with personnel outside the control room, requirements for notification to outside organizations, noise level, and temperature).

Selected scenarios will include environmental conditions, such as noise and distractions, which may affect human performance in an actual nuclear power plant.

For actions outside the control room that are within the scope of the integrated system validation, performance impacts of potentially harsh environments that require additional time will be realistically simulated (for example, time to don protective clothing and access hot areas).

## 4.8 PERFORMANCE MEASURES AND ACCEPTANCE CRITERIA

The implementation plan will specify performance measures used to establish that mission goals and operator performance requirements are achieved. Performance measures will include:

- System measures relevant to plant safety
- Personnel primary task performance
- Personnel errors
- Situation awareness
- Workload
- Personnel communications and coordination
- Dynamic anthropometry evaluations (such as reach and dexterity)
- Physical positioning and interaction with HSI

For each measure, the availability of practical tools will be evaluated. Where valid cost-effective tools are identified, the measurements approach and tools to be used will be specified and objective acceptance criteria will be defined. The acceptance criteria will focus on acceptable operation of the plant and the HSI. Additional measures may be used in a diagnostic or exploratory fashion; that is, where basis for valid acceptance criteria is lacking. Measurement approaches may range from objective measures of

crew performance to subjective measures of performance obtained through post-scenario questionnaires and rating forms administered to test participants, to evaluations made by an evaluation team participating in the validation exercises as expert observers.

## 4.9 SUBJECTS

In actual operation, the AP1000 main control room and associated human system interface design (HSID) features will be used only by highly trained, qualified commercial nuclear power plant (NPP) operating crews. The hypothetical group of all such qualified crew members is referred to here as the "target user population." To ensure that test subjects will represent this population, validation crews will consist of currently qualified operating crews, as adjusted in number to man the AP1000 control room for conditions of minimum and maximum staffing. This excludes, by definition, members of the design organization.

The target users can be subdivided on the basis of qualification and experience. For AP1000, two subgroups of interest are referred to here as "operators" and "supervisors." Supervisors by definition have longer experience and higher qualifications. To ensure a conservative test, steps will be taken to identify and select test subjects from crews with less experience or unexceptional performance. This may be difficult to achieve for several reasons, including the sensitivity of being identified as average or below. However, test subjects will in no case be selected for their superior skills or experience.

A key question is the number of subjects to be used in each test (that is, sample size = n). Several authors have examined the mathematical models that underlie descriptive usability evaluations. Plotting the proportion of usability problems detected as a function of number of test participants, the relation can be modeled as a simple Poisson process. In essence, each successive test subject tends to reveal fewer findings. Reference [13] continues in this vein to suggest that five test subjects are typically enough to detect 70 to 90 percent of major usability problems in a prototype. Thus, a minimum of n = 6 subjects (3 crews) is proposed as sufficient for validation tests.

Prior to testing, subjects will receive a week of training on the testbed. Training content will exclude actual scenarios used for validation testing. Training should be sufficient to prepare subjects for the demands of the planned tests. However, since the training is relatively brief, it is not expected to produce test subjects for the new design quite equal to the fully qualified and experienced crew of an existing plant. As a result, inexperience still tends to weigh against favorable validation results, but as a conservative error, this is acceptable.

## 4.10 VALIDATION TEST DESIGN

The basic design of validation tests is to administer the representative test set to multiple subject crews, for a minimum of 3 runs on each scenario in the test set. Because the number of crews is likely to be much fewer than the number of scenarios, no formal balancing strategy is needed other than random assignment of scenario order. The representative test set will be defined later as described in Section 4.6.

It is not actually necessary for each crew to perform each scenario, as long as each scenario in the set is exercised three or more times. For one thing, there is no basic concern with controlling for subject variance in validation tests, other than by proper selection and training (see Section 4.9). The point of the test is to demonstrate that any passably trained crew can at least operate safely; hence, validation failure is

possible with each individual test run, and differences between crews are of no interest. This is advantageous because, particularly if the test set is long, it may be necessary to begin with one crew, and finish with another. It also allows for lost test runs to be made up by a different crew, if a restart of the scenario is unreasonable (e.g., because the scenario has progressed far enough to invalidate the test). In fact, though added diversity among the crews is less efficient (due to added training overhead) but it will tend to create a more demanding test, since every crew will be less experienced at the conclusion of testing, and each added crew stands to be the best (or worst) yet. If the added crew happens to be the worst, then validation failure becomes more likely.

Pilot testing of each scenario should be performed at least once to ensure that the test procedures are sufficient, that test personnel are sufficiently trained, that the scenario provides an effective test, that the scenario behaves as expected on the simulator, that the evaluation tools have been properly tailored, and so forth. Pilot testing is performed for the benefit of the test developers. Actual test subjects are not used.

## 4.11 DATA ANALYSIS

The following performance measures will be collected and used as a basis for generating results from the test trials:

- Questionnaires (self-assessment, issue assessments, HSI ratings, raw Task Load Index/workload)
- Observer checklists (Operator Performance Assessment System-style milestones, completeness)
- Debriefing (questions, comments and discussion)
- Time history (speed)
- Action history (actions, usage, errors, accuracy)
- Plant performance (applicable margins and behavior)
- Video tape

Overall, the measures produce data that are either objective, (defined as observable and verifiable), or subjective (defined as inherently meaningful responses from knowledgeable participants). Whether quantitative or qualitative, data will primarily be treated as descriptive. That is, use of inferential hypothesis testing for validation tests will be limited to statistical comparisons deemed of interest, and will not be used to implement validation criteria. Data measures that do not fit these definitions, or that are otherwise not cost-effective to collect and process, will be avoided. Examples of typical measurement tools, data, and analysis techniques used by Westinghouse are identified in WCAP-14396.

## 4.12 RESULTS AND DOCUMENTATION

Results will document the test design, the representative test set and its basis, and a summary of the data collected. All Human Engineering Discrepancies (HEDs) identified from the testing will be identified along with their resolution. The basis for concluding that the HSID is valid, i.e., that the integrated system performed acceptably during testing and that the HSID is safe and acceptably operable, will be documented. The inherent limitations of the validation paradigm will be reviewed.

# 5 ISSUE RESOLUTION VERIFICATION

An implementation plan will be developed specifying a methodology for human factors issues resolution verification.

The implementation plan will specify a procedure to ensure that all issues documented in the human factors issue tracking system are verified to be adequately addressed in the final HSI. The implementation plan will include a procedure for identifying and tracking human factors issues that cannot be resolved until a plant is built. The procedure will specify how verification of these human factors issues will be incorporated into the process for final plant HFE verification.

Among the potential human factors issues to be tracked and resolved are HEDs. HEDs occur when a human factors deficiency is formally identified in an otherwise completed design. A human factors deficiency is a failure of a complete design to meet design requirements or V&V criteria. The V&V processes defined in this document will cause human factors deficiencies to be identified and in turn formally documented as HEDs. HEDs will be thoroughly described, including their scope of occurrence and their expected impact. An assessment of safety- or risk-significance should be made such that risk-significant HEDs will receive high priority. As for other formally tracked HFE issues, all HEDs identified by Westinghouse are resolved prior to plant startup. After plant startup, human factors deficiencies and HEDs should be addressed similarly by the Combined License applicant.

# 6 PLANT HFE/HSI (as designed at the time of plant startup) VERIFICATION

An implementation plan will be developed specifying a methodology for verifying that the plant HFE/HSI (as designed at the time of plant startup) conforms to the HSI design that resulted from the HFE design process and V&V activities.

In the Westinghouse design process, mechanisms for ensuring that systems conform to the final functional requirements and design descriptions are: factory acceptance tests conducted on the actual system hardware at the factory, and the site acceptance test conducted after the hardware is installed at the plant site.

The implementation plan for the plant HFE/HSI verification will specify the verifications that will be conducted as part of the factory acceptance test, and site acceptance test, ensuring that the plant HFE/HSI (as designed at the time of plant startup) conforms to the HSI design that resulted from the HFE design process and V&V activities.

The implementation plan will include procedures for identifying aspects of the HSI that were not addressed in the design process V&V, and procedures for evaluating them using appropriate V&V methods. Aspects of the HSI design that fall in this category include design features that could not be evaluated in a simulator, and design modifications that occurred subsequent to the HSI design V&V, such as hardware upgrades.

# 7 REFERENCES

1. ANSI HFS-100-1988, "American Standard for Human Factors Engineering of Visual Display Terminal Workstations," American National Standards Institute, Santa Monica, California, 1988.

2. CEI/IEC 964 "Design for Control Rooms of Nuclear Power Plants," International Electrotechnical Commission, Geneva, Switzerland, 1989.

3. DOD-HDBK-761A "Human Engineering Guidelines for Management Information Systems," U.S. Department of Defense, Office of Management and Budget, Washington, D.C., 1990.

4. IEEE Std. 845-1999 "IEEE Guide for the Evaluation of Human-System Performance in Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 1999.

5. NUREG-0899 "Guidelines for the Preparation of Emergency Operating Procedures," U.S. Nuclear Regulatory Commission, Washington, D.C., August 1982.

6. NUREG-1358 "Lessons Learned from the Special Inspection Program for Emergency Operating Procedures," U.S. Nuclear Regulatory Commission, Washington, D.C., April 1989.

7. NUREG-0711 "Human Factors Engineering Program Review Model," U.S. Nuclear Regulatory Commission, Washington, D.C., July 1994.

8. NUREG-0700 "Human-System Interface Design Review Guideline," Rev. 1, U.S. Nuclear Regulatory Commission, Washington, D.C., June 1996.

9. NUREG/CR-5908 "Advanced Human-System Interface Design Guidelines," U.S. Nuclear Regulatory Commission, Washington, D.C., July 1994.

10. NUREG/CR-6501 "Human Factors Engineering Guidelines for the Review of Advanced Alarm Systems," U.S. Nuclear Regulatory Commission, Washington, D.C., September 1994.

11. Regulatory Guide 1.33, "Quality Assurance Program Requirements," Rev. 2, U.S. Nuclear Regulatory Commission, Washington, D.C.

12. ANSI/ANS-3.5-1993, "Nuclear Power Plant Simulators for Use in Operator Training and Examination," approved March 29, 1993.

13. Virzi, R. A. "Refining the test phase of usability evaluation: How many subjects is enough?," *Human Factors*, 34(4), 1992, 457-468.