


Westinghouse Class 3

WCAP-10170
Supp. 4-NP
Revision 0

Westinghouse Technical Support Complex
Design and V&V Process for
the Donald C. Cook Nuclear Plant

By:

C. L. Werner

Approved: 
for E. P. Rahe, Jr., Manager
Nuclear Safety Department

Westinghouse Water Reactors Division

February 1985

8504100353 850403
PDR ADOCK 05000315
F PDR

WESTINGHOUSE CLASS 3

NOTE: Sections of this document that differ from WCAP-10170 are delineated with an asterick (*) in the margin.

WESTINGHOUSE CLASS 3

Westinghouse Technical Support Complex Design and V&V Process for the
D. C. Cook Nuclear Station

<u>Section</u>	<u>Title</u>	<u>Page</u>
1.0	Introduction	2
1.1	Objective of Report	3
1.2	Chronology of Events	3
2.0	System Design Process	5
2.1	Project Organization	5
2.2	Design Process	6
2.2.1	Development of SPDS Design Bases and Functional Requirements	6
2.3	Design Bases Document	17
2.4	Functional Requirements	18
2.5	SPDS Design Specification	19
2.5.1	Hardware Design	21
2.5.2	Software Design	23
2.5.3	Systems Integration and Factory Acceptance Tests	25
2.5.4	Test Plan and Procedures Acceptance Criteria	25
3.0	NRC Verification and Validation Process	28
3.1	Verification of System Design Requirements	28
3.2	Validation of Integrated System	28
3.3	Verification of Installed System	30
4.0	Documentation	31
4.1	Design Bases	31
4.2	Functional Requirements	31
4.3	Design Specifications	31
5.0	References	32
6.0	Appendices	33

1.0 INTRODUCTION

Investigations of the accident at Three Mile Island identified the need for improving the presentation of data to both plant operating and technical support personnel. This need was described in two NUREG reports; NUREG 0578 (TMI-2 Lessons Learned Task Force Status Report and Short-Term Recommendations), July, 1979 and NUREG 0585 (TMI-2 Lessons Learned Task Force Final Report), October, 1979. In response to that need and subsequent requirements from the Nuclear Regulatory Commission (NRC), Westinghouse developed a Technical Support Complex. The Westinghouse Technical Support Complex (TSC) addresses the NRC's requirements for the:

1. Safety Parameter Display System (SPDS) and the
2. Onsite Technical Support Center (OTSC)

In addition the Westinghouse Technical Support Complex includes a Bypass and Inoperable Status Indication system which is in response to the Task Force recommendation that automatic status monitoring be required by a decision to backfit Regulatory Guide 1.47. *

In October, 1982 the NRC conducted a design verification audit of the generic WSPDS. The 'Emergency Response Facility Design and V&V Process' (WCAP-10170) and its subsequent appendices (A through E) document the WSPDS design and verification processes in a 'forward-fit' manner with respect to the design/implementation of the D. C. Cook TSC system. Because of the parallel activities that took place after May, 1980, namely the design/implementation of the D. C. Cook TSC and the generic WSPDS design and verification activities, it is not possible to directly apply WCAP-10170, the October 1982 NRC audit and the February 1984 NRC Safety Evaluation Report to the D. C. Cook TSC. However, most of the activities described in WCAP-10170 were applied to the D. C. Cook design. This report, a modified version of WCAP-10170, provides an overview of the design process used for the D. C. Cook SPDS. Sections of this document that differ from WCAP-10170 are delineated with an asterisk (*) in the margin. *

The report also presents a summary of the review process used in the conceptual design of the SPDS and the verification and validation (V&V) processes that were used in the system design and system integration of the D. C. Cook SPDS. *

1.1 Objective of Report

Because the SPDS is not part of the safety system, that is, it is not a Class 1E device, the quality of verification and validation need not meet the same rigid requirements as for the automatic protection system. The intent of this report is to describe a design process and V&V program which is consistent with the availability needs of a system that, while it is important to safety, only provides information to the operator and does not perform any automatic control or actuation functions.

The overall objective of this report is to provide a document that describes the D. C. Cook TSC design and design verification activities while, at the same time, highlighting activities identical to those given in WCAP-10170. By doing this the utility, the NRC and Westinghouse can apply relevant review activities from the generic design directly to the D. C. Cook design. *

1.2 Chronology of Events

The Westinghouse activities for the conceptual design of the Plant Safety Status Display (PSSD) were initiated in the latter part of 1979 based on input from the NRC TMI-2 Lessons Learned Task Force Report, NUREG 0585, and the work that Westinghouse had underway on an EPRI Research Project (RP 891-3), Scoping and Feasibility Study for Plant Wide Distribution Analysis and Surveillance System (DASS). The Westinghouse work for the display system, named the PSSD, was initiated prior to the labeling of the device by the NRC as an SPDS. Therefore, Westinghouse documentation for this device carries the PSSD label. In this report for the NRC both the PSSD and SPDS labels are used. The chronology of events by both the NRC and Westinghouse for the PSSD/SPDS and related items is summarized below.

WESTINGHOUSE CLASS 3

TIME TABLE OF EVENTS FOLLOWING TMI

<u>NRC</u>	<u>WESTINGHOUSE</u>
July 1979 NUREG 0578	Oct. 1979, Technical Work on TSC initiated
Oct. 1979 NUREG 0585	Oct. 1979, Technical Work on EPRI DASS Project initiated
July 1980 (Draft) NUREG 1580 (Control Room Eval.)	May 1980 W Equipment Sales Receive order for D. C. Cook TSC
Nov. 1980 TMI Action Plan	June 1980 WCAP 9725
Dec. 1980 RG 1.97 Rev. 2	Dec. 1980 Technical work on EPRI DASS Project completed.
Feb. 1981 NUREG 0696 (ERF's)	Jan. 1981, W requests NRC preimplementation review of Generic SPDS
Mar. 1981 (Draft) NUREG-0659 (Control Room Eval.)	
May 1981 Submit Conceptual Design	May 1981 RG 1.97 Design Basis issued
Aug. 1981 NUREG 0814 (ERF's)	Sep. 1981 W Owners Group Procedures
Oct. 1981 NUREG 0700 (Control Room Design)	Oct. 1981 WCAP 9725 Supp 1 Issued
Oct. 1981 (Draft) NUREG 0835 (SPDS)	
	April 1982, WCAP-10170 (draft)-ERF Design and V&V Processes submitted to NRC
	Oct. 1982, NRC conducts design verification audit of WSPDS
	Jan. 1983, WCAP-10170 Appendices A through D submitted to NRC
	June 1983, WCAP-10170 Appendix E submitted to NRC
	Feb. 1984, NRC issues SER for WSPDS design & design verification activities

WESTINGHOUSE CLASS 3

2.0 SYSTEM DESIGN PROCESS

2.1 PROJECT ORGANIZATION

In January, 1980 Westinghouse formed a dedicated functional group (Control Room & Computer Development) to develop the Westinghouse product which has become known as the Technical Support Complex. This product addresses the requirements for the Onsite Technical Support Center (OTSC), the Plant Safety Status Display (PSSD) and Bypassed and Inoperable Status Indicator (BISI). This group was also the focus for Westinghouse efforts relative to the Disturbance Analysis and Surveillance System (DASS).

Because of the short implementation schedule originally expressed by the NRC, this dedicated group of personnel was given the responsibility to expeditiously develop, market, design and procure the Technical Support Complex product. The group was multidisciplinary in nature, staffed with engineering personnel with functional analysis, process control and plant computer experience in order to effectively carry out this project from start to finish. Another dedicated group (Software Development) was formed with responsibility for development of computer software. While the design and development work was carried out largely within these two functional groups, close contact was maintained with the Westinghouse Nuclear Safety Department and the two supplier divisions to ensure that the design met the NRC requirements at the time of sale and that the design was compatible with existing computer technology. In addition, personnel from the Westinghouse R&D Human Sciences Department were an essential part of the product design team throughout the development and design process to ensure that human factors considerations were effectively incorporated into the product design.

In the initial phases of the design activity it was necessary for the development, design and procurement processes to proceed simultaneously in order to ensure an integrated high quality product consistent with the implementation scheduler requirements then defined. This necessitated continuous interaction between requirements development and system design rather than a serial progression from requirements definition to system implementation.

WESTINGHOUSE CLASS 3

Westinghouse organizational changes subsequent to completion of the major development effort and basic system design have resulted in the following groups with responsibilities relative to the Technical Support Complex:

1. Electrical Systems Integration with responsibility for the functional design of the Technical Support Complex.
2. System Configuration & Test with responsibility for the design and procurement of the Technical Support Complex. | *
3. Software Development with responsibility for development of digital computer software required for the Technical Support Complex.
4. Westinghouse R&D Human Sciences Department to provide human factors and cognitive psychology input into the design.
5. Nuclear Safety Department to ensure that design meets current NRC requirements and maintain open communications with the NRC.

2.2 DESIGN PROCESS

The overall design process used for the Technical Support Complex is shown in Figure 1. Table 1 identifies support documentation for each process given in Figure 1. Subsequent subsections discuss each one of the major activities identified in this figure. | *

Of particular interest for the SPDS is the design process used to develop the design basis and functional requirements for the system. This process is described in the next section. It must be remembered that this work was initiated in the fall of 1979, more than a year in advance of the completion of NUREG-0696.

2.2.1 Development of SPDS Design Bases and Functional Requirements

Since the SPDS would perform a vital function in the man-machine interface, a unique design approach was developed to incorporate human engineering principles

from the onset of the engineering design. The design approach is divided into three major phases: concept, development, and implementation.

The conceptual phase is comprised of two parts: human factors analysis and functional analysis. The development stage consists of the integration of the human factors and functional analyses into a design specification from which the individual efforts for equipment design, software design and the man-machine interface design can proceed. The combined results of these efforts then undergo a test and evaluation process before proceeding with implementation. The implementation phase considers the utility's integration of the SPDS into the total plant operation; not only the installation of equipment into the plant, but also the incorporation of the system's derived benefits in terms of revised operator training methods and procedures. This subsection deals with the activities which resulted in the design bases and functional requirements. |*

a) Functional Analysis

The functional analysis efforts consist of setting key design requirements for the SPDS design in the areas of:

1. Adequacy of input data base
2. System operational goals
3. Operational flexibility

Input Data Base

To define input data, the data set must be sufficient to permit the evaluation of the safety state of the plant for all possible transients, including those which might not be postulated.

To meet this criterion, the concept of key safety goals is utilized. The ultimate safety goal is to prevent the uncontrolled release of radioactivity to the environment. The barriers which prevent the release of radioactivity to the environment are the fuel cladding, the reactor coolant system and finally the reactor containment structure. The integrity of the barriers is maintained by monitoring and controlling the parameters which define the

Figure 1. EMERGENCY RESPONSE FACILITIES DESIGN PROCESS

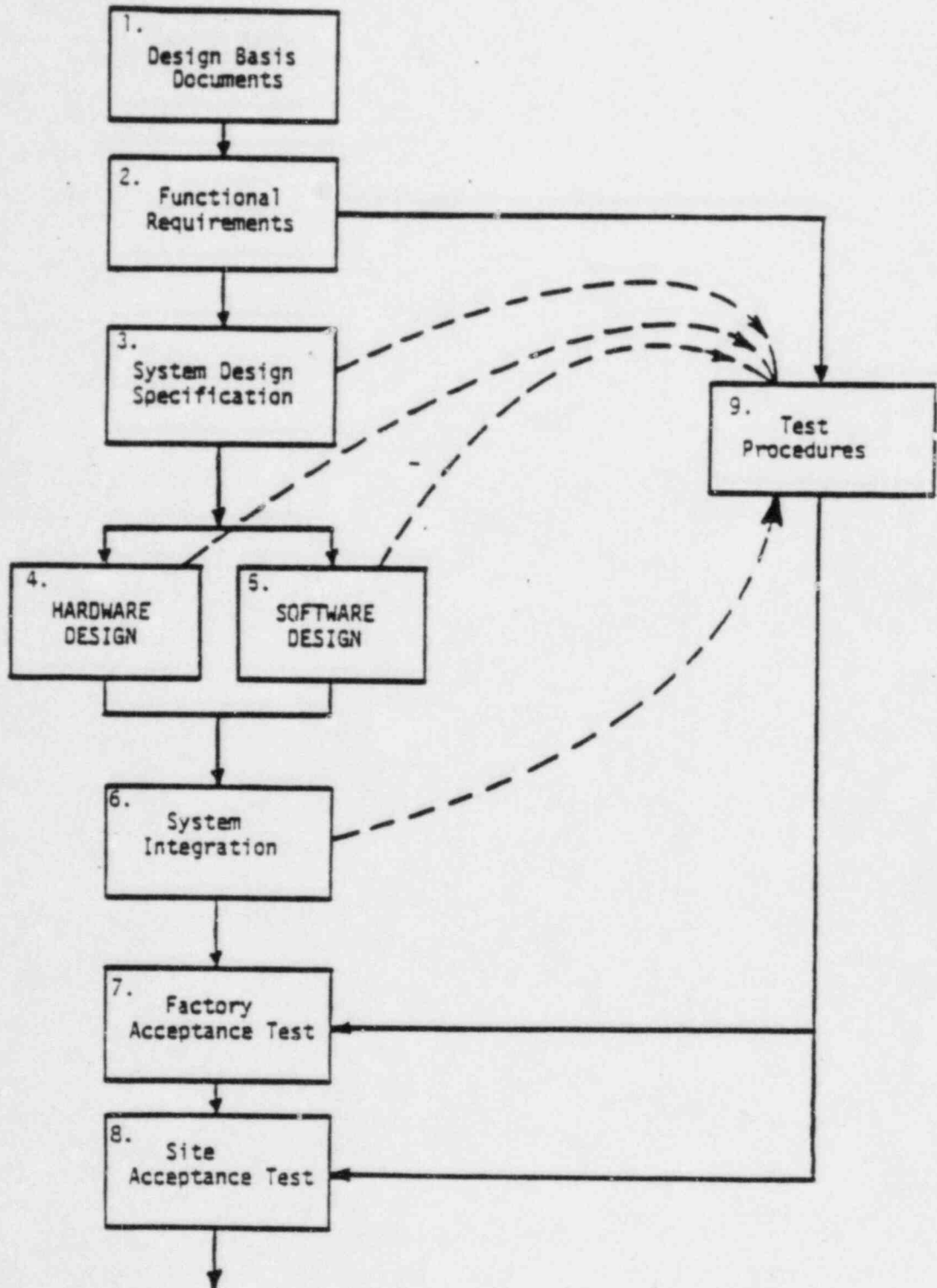


TABLE 1
D. C. COOK TSC DOCUMENTATION
(As Related to Figure 1 Processes)

(1) Design Basis Documents

The Design Basis Documents for the PSSD, is ESD-CR&CD-105 and the OTSC is ESD-CR&CD-109.

(2) Functional Requirements

'Functional Requirements for the TSC' is ESD-CR&CD-94.

(3) System Design Specification

The design specifications for the D. C. Cook TSC are as follows:

<u>Description</u>	Unit 1 <u>Spec #</u>	Unit 2 <u>Spec #</u>
Standard TSC	955286	955286
PSSD/OTSC	955393	955484
BISI	955413	955413

(4) Hardware Design

The hardware design is specified in E-Spec 955286 Rev 1 as identified in the D. C. Cook Master Index List under Item 10, Spin #TSELCC. Also identified in the Master Index List are all the equipment design drawings which have been transmitted to AEP.

TABLE 1 (Cont)
D. C. COOK TSC DOCUMENTATION
(As Related to Figure 1 Processes)

(5) Software Design

The software design is specified in D-Specs 955393 and 955413 (unit 1) and 955484 and 955413 (unit 2) as identified in the AEP Master Index List under Item 10, Spin #TSELCC. Other documents related to the design are the TSC Programmer's Manual and the Program Listings are also listed under item 10.

(6) System Integration

System Integration is a process of configuration control. The software is integrated into the configured system by the W Software Team from the Source Stored on protected files on the IBM and Data General machines.

(7) Factory Acceptance Test

Factory Acceptance Testing (F.A.T) is executed at Westinghouse's facility on a prototype computer to insure that the software operates in accordance with the software specifications. The test is given in the Test Procedure document (see Item 10.) A signed-off copy of the test results are maintained as part of the W Files.

(8) Site Acceptance Test

Site Acceptance Testing (S.A.T.) is executed at the D. C. Cook site. The Test Procedures used for F.A.T. are also executed during S.A.T. This test is to insure that the 'as delivered' software operates at the site as it did on the Westinghouse prototype system. A signed-off copy of the Test Procedures, as applied during S.A.T., will be transmitted to AEP.

TABLE 1 (Cont)
D. C. COOK TSC DOCUMENTATION
(As Related to Figure 1 Processes)

(9) Test Procedures

As S.A.T progresses, signed-off copies of the Test Procedures are retained at the D. C. Cook site. After 'system acceptance' by AEP, signed-off copies of the Test Procedure sign-off sheet will be officially transmitted.

WESTINGHOUSE CLASS 3

operational limits: reactor flux, reactor coolant system pressure, temperature, inventory and containment pressure. Hence the function of the SPDS is to monitor the plant process in terms of satisfying the key safety goals and thereby the question of unanticipated events or scenarios is addressed.

Operational Goals

To adequately address the spectrum of safety concerns associated with abnormal events, two operational modes for the system were established as follows:

1. Provide the capability for the operator to monitor the state of the plant and detect any abnormalities for which corrective action might be taken to terminate the event prior to the initiation of automatic reactor trip and/or safeguards functions.
2. In the case of events which the operator does not detect or cannot terminate, enable the operator to assess the safety state of the plant and verify proper safeguards function to mitigate the consequences of the event.

Operational Flexibility

The design of the SPDS should accommodate operational flexibility, i.e., the capability of the SPDS to be incorporated into normal control room functions. The capability provided by the addition of a CRT display system could enhance control operations to improve plant availability as well as plant safety. By providing a system that is utilized in normal daily operations, familiarity with the system is automatically assured when the function must be relied upon in an off-normal situation.

b) Human Factor Analysis

Human engineering is a design approach which takes into consideration the user's characteristics in meeting the user's needs. For the SPDS design the human factors analysis efforts focused on three areas:

1. The user as an element in the control loop.

2. The perceptual and mental processing characteristics of the user.
3. The tasks and decisions facing the user during abnormal plant conditions.

The User

Research by Rasmussen and others at RISØ National Laboratories in Denmark has resulted in a model which is useful in describing various types of human behavior for human data processing.

According to Rasmussen these are three basic types of behavior:

1. Skill-based behavior - automatic actions are performed without conscious control.
2. Rule-based behavior - actions are dictated by a stored set of rules, either written or memorized.
3. Knowledge-based behavior - identification of task and development of a strategy consistent with desired goals.

Associated with each behavior type are three distinct phases; detection, association of the problem with actions, and the execution of the actions.

Perceptual and Mental Characteristics

In terms of perceptual and mental characteristics one very important characteristic is the need to match the field of attention with the level of abstraction in data presentations.

For example, the field of attention for a plant operator depends upon the task and can range from the status of the overall plant to the position of a specific valve. As the field of attention varies so must the level of abstraction; a wide field of attention requires a high level of abstraction. Level of abstraction varies from a low level, one of physical form and

function (e.g., how does this valve operate?) to a high level of functional (e.g., what is the purpose of the containment spray system?).

Many other perceptual and mental characteristics were factored into the analysis process and are reflected in visibility and legibility requirements such as display resolution, character size, screen refresh rate, and others.

Operator Tasks and Decisions

The third area focused upon in the analysis was the definition of the control room operator's role during abnormal events.

Guidance for the definition of the role of the control room operator was taken from the many investigations and studies performed after TMI, in particular the Three Mile Island Special Inquiry Group and the Lessons Learned Task Force Final Report. NUREG/CR 1270 presented the central man-machine concept that the operators function in two roles during abnormal conditions;

1. The system manager role where the operator is concerned with the prompt recognition of abnormal occurrences, the control and monitoring of plant process resources, and the evaluation of alternative courses of action.
2. The maintenance or equipment operator role which is essentially a procedure following role, that is the operator proceeds from known problems (with conforming symptoms) to preventive and corrective actions.

The Task report identified two operational safety goals:

- a. Reduce challenges to the plant safety systems by recognizing precursors to off-normal situations and neutralize them before they develop into direct challenges to the safety systems.
- b. Provide maximum capability to mitigate the challenges that inevitably occur.

Based upon the above and a task analysis of emergency operating procedures, an operator response model was developed to describe the operator's expected tasks during abnormal events.

The tasks are divided into four distinct phases: detection or discrimination, verification, diagnosis and corrective action, and finally, feedback.

c) Development

Having discussed the functional and human factors analysis efforts that form the design bases, the next phase in the design process is the development of the man-machine interface functional requirements.

Historically, the principles and concepts previously discussed were not addressed directly in nuclear plant control room design. With the advent of CRT display technology, CRT systems have gradually been incorporated into plant control rooms, but they contain many deficiencies. Display selection is often a slow and tedious process requiring an operator to remember or look up in a reference a mnemonic for a particular parameter or display. Displays are often dense and overcrowded with no means for highlighting important parameters. Displays are often programmed from process and instrumentation drawings originally intended for construction purposes. As a result, display systems are sometimes comprised of independent, isolated displays with important interface relationships missing.

With these deficiencies in mind, a display development methodology was established.

The first step in the process is to define a purpose for the data structure in the display system. Display hierarchy and individual task descriptions are written.¹

1. These documents are retained by Westinghouse as part of the development files.

*

Secondly, the criteria developed in the task descriptions are used to define data content, format and organization for each display necessary to support the purpose or function of each display.

Human factors guidelines are utilized at each stage of the process in terms of display format best suited for the particular task, methods for highlighting critical data, and improving operator search.

The keystone of display development is the preparation of a task description. As an aid to developing task descriptions for the SPDS, a checklist was developed.

The concepts of operator mental models and displays forming perceptual maps were incorporated into the design to produce a well-integrated display system. Mental models are used to ensure that the particular display represents the dynamics of the process, including important interface relationships. For example, a mental model of the reactor coolant system not only includes the reactor coolant system status but also the status and performance indicators of systems affecting the state of other reactor systems (the steam generators, the reactor coolant makeup system, etc), and the storage and transport of materials and energy.

Organizing displays into a perceptual structure aids information integration across displays. The important system relationships which are within the operator's mental model become a visible part of the display structure. The perceptual organization and display overlap aids the user in moving between displays and in locating data.

The display hierarchy developed for the SPDS is comprised of:

1. Top level summary of plant health.
2. Second level graphic display of overall plant status.
3. Third level graphic displays of plant systems.
4. Fourth level alphanumeric format displays of sensor data.

Supplementing the display hierarchy is a reactor coolant system pressure-temperature operating limit curve, and trend and history plots.

The SPDS display hierarchy and the operator role are matched in terms of levels of abstraction and field of attention, behavior type, and task as specified during the human analysis stage of the design process.

The top level of the display hierarchy consists of two polar graphics or iconic displays to support the discrimination phase by providing a concise summary of plant health.

The two iconic displays were developed to support the "terminate" and "mitigate" operational goals defined in the functional analysis. The terminate (narrow range) display is primarily intended for use at conditions between zero and full hot power conditions. The mitigate (wide range) display is intended for use over the full operational range of the plant from cold shutdown to full power.

A unique attribute of this display is that it is a robust mechanism for information presentation. The display supports skill and rule-based activities but can also support the knowledge-based activities identified in Rasmussen's model. The skill-based and rule-based activities are supported by the association of the shape of the figure with a procedure or action. The knowledge-based activities of identification of state, strategy setting using goals to decide actions, is supported by a concise set of parameters indicating the state of plant safety functions.

2.3 DESIGN BASIS DOCUMENT

The purpose of the design basis document is to expressly state the baseline criteria for the system design. These criteria include the statement of the functional purpose that the system is to support, the general design approach to be followed, and the considerations and reasons for elements of the conceptual design. Included in this document are:

1. Baseline criteria for the system and its components
2. Baseline design principles to be addressed
3. Operational modes the system is to support
4. Requirements to be met in defining an adequate data base
5. Requirements for data validation and information coding.

The design basis document states the missions of the system, basic criteria to be followed, and basic system requirements for key elements of the conceptual design so that the more detailed design specification process can proceed. With the design basis documented, the definition of detailed functional requirements and system design specifications can be developed in a consistent manner with each other and with the missions of the systems.

The Plant Safety Status Display Design Basis Document is documented by ESC-CR&CD-105 (Rev. 1, dated 7/10/81).

2.4 FUNCTIONAL REQUIREMENTS

The functional requirements address the specific design and performance requirements for the various components of the system and its interface with the plant. The system functional requirements are the translation of the criteria and general design requirements defined in the system design basis document into more detailed specific requirements for the system. In addition to specifically addressing the missions set forth in the design basis document, the functional requirements also address other issues concerning the installation, operation, and interface of the system in the plant. Included in the functional requirements are the following issues:

1. Regulatory criteria
2. Availability
3. Environmental considerations
4. Data processing requirements
5. Time response
6. Test and calibration requirements
7. System performance requirements
8. Display requirements
9. Interfaces with associated equipment

The Functional Requirements together with the Design Basis Document provide a documented basis for development of specific system and software design specifications.

The functional requirements for the Plant Safety Status Display are contained in the document, Functional Requirements for the Technical Support Complex, ESD-CR&CD-94 (Rev. 1, dated 7/14/81).

2.5 SPDS DESIGN SPECIFICATION

The Safety Parameter Display System (SPDS) Design Specification is a document which combines and translates the functional requirements, human factors guidelines, regulatory requirements, and plant specific (or generic plant) design information into a form which allows procurement of hardware systems, sub-systems, or components which satisfy the overall system requirements.

In addition, conceptual or preliminary software Design Specification information is used in the preparation of the Design Specification to ensure that the equipment specified therein has sufficient capacity and size to execute and perform the required function.

The SPDS Hardware System performs three major functions:

1. Data Acquisition
2. Data Processing and Application Program Computations
3. Man-Machine Interface

The Design Specification defines both general and function-unique requirements for hardware that is required to perform these functions.

The Design Specification documents the following general requirements for all SPDS hardware components for sub-systems:

- a) General material requirements: prohibited materials, type and size of wire, paint requirements, etc.
- b) Definition of responsibilities among vendor, Westinghouse, sub-vendors, and customer/utility/architect engineer as appropriate
- c) Accuracy requirements

WESTINGHOUSE CLASS 3

- d) Availability requirements
- e) Environmental qualification and seismic requirements
- f) Acceptance criteria for specified equipment
- g) Interface to other equipment
- h) Tests to be performed by supplier
- i) QA requirements
- j) Applicable standards and codes
- k) Packaging and shipping requirements
- l) Equipment arrangement and mounting requirements.

The Specific Hardware requirements defined in the Design Specification for each of the Major System Functions are as follows:

Data Acquisition based on functional requirements, customer requirements, and plant fluid system diagrams and system descriptions, the Design Specification defines:

- a) The type of I/O (remote, local, multiplexer)
- b) The scan rate requirements
- c) Signal processing requirements
- d) Signal distribution (number of points by signal type, distribution of points in I/O cabinets, and number of cabinets required)
- e) Redundancy requirements and method of failover
- f) Error detection requirements (on-line diagnostics).

Data Processing and Application Program Computations

Past experience, preliminary modeling, preliminary Software Design Specification and plant specific database information is used to specify the processing portion of the SPDS hardware.

This information is used to estimate the system throughput, memory storage and computational requirements.

The resulting definition of required computer resources is combined with the interface requirements of the I/O and MMI to form specifications for the computer systems.

Man-Machine Interface

During the specification, particular emphasis is given to the functional requirements, human factor guidelines, Vendor Technical bulletins and customer/plant requirements in order to specify CRT's and keyboards that include the required characteristics. For example, the characteristics of CRT's relative to color, character size, screen size, resolution, refresh rate, flicker, graphic capability, etc. are specified relative to the keyboard. The Design Specification defines the requirements for the keys, i.e. functions, engraving, coding conventions, physical arrangement, and number.

2.5.1 HARDWARE DESIGN

The SPDS Design Specification functionally defines the required performance of the hardware in three major areas:

1. Data Acquisition
2. Data Processing and Application Program Computations
3. Man-Machine Interface

The design and implementation of the hardware proceeds as follows. Cognizant system design activity develops a conceptual hardware configuration based upon the functional requirements as the SPDS Design Specification is being formulated. This allows the advance ordering of long lead-time components.

The hardware design cannot be finalized until the Software Design Specification (SDS) is generated. The data acquisition hardware is dependent upon the number and type of plant instrument channels required to support the display system as defined in the SDS. Similarly, the data processing and man-machine interface hardware may be impacted by the requirements in the SDS.

Design control is imposed upon the hardware. The SPDS Design Specification functionally defines the required performance of the hardware, but system drawings and component specifications (where required) are generated from the Design Specification to explicitly define the hardware. This hardware design package is controlled by established QA procedures (Reference section 5, items 6 and 7) and maintained throughout the life cycle of the project. | *

Applicable portions of the hardware design package become part of the procurement package. Procurement control is exerted on component suppliers. Supplier qualification is surveyed in advance and may be periodically verified via audit. Purchase order and change notice documentation impose in contractual terms the requirements for the hardware. Quality release is required for selected components prior to shipment to Westinghouse for staging.

Materials control procedures are established for the hardware. These include receipt inspection and testing, traceability of components, shipping, handling, and storage procedures.

Maintenance and testing of the hardware during the staging period at Westinghouse is in accordance with prescribed procedures. Component and system diagnostic routines are executed to troubleshoot hardware problems and to verify proper operation. These hardware diagnostic routines are to be successfully executed during the preliminary phases of both the factory acceptance test and the site acceptance test. Hardware trouble reports are submitted by testing personnel or other system users to identify problems

during staging. These trouble reports are collected and resolved by the cognizant organization, which maintains traceable records of hardware problems.

2.5.2 Software Design

a) Software Design Specification

Using the System Design Specification as a reference point, the plant specific algorithms needed to implement each applications function are generated and collated into the SDS. The plant I/O list is integrated into the generic algorithms and displays, producing the following contents:

- 1) A) PSSD CRT Coding Sheets - giving the diagram layouts for each display page in the system
 - B) PSSD CRT Updatable Parameter Sheets - defining all updatable parameters for each page
 - C) PSSD CRT Coding Conventions - defining the graphics coding of display elements
 - D) PSSD Hierarchy/Paging Definitions - giving the inter-connections among all displays
 - E) PSSD Poke Field Definition
- 2) A) PSSD Algorithms - giving for each:
 - i) Abstract
 - ii) Functional description
 - iii) Flow chart (or equivalent) of algorithm
- B) PSSD Algorithm Data Sheets - addresses inputs, outputs, constants, units, sorted by algorithm name
- C) PSSD Calculated Value - Addressable Constant Data Sheets - tabulating all calculated values and addressable constants

The SDS is machine-independent, giving only the formal specifications for each algorithm.

Software Design Procedures

b) Software Design

The controlling inputs for this phase of the project are the software design specification, the plant-specific database and the programmer's manuals for the computer operating system. In the generation of the D. C. Cook Technical Support Complex, the computer operating system was sub-contracted to the Westinghouse Instrumentation & Electronic Division, and their quality assurance and design procedures were used in the development of the operating system software. *

The design process includes the programming and integration of all software modules into the hardware and database systems of the vendors. Concurrent with these processes is the development of all test procedures except the factory acceptance tests and the initial documentation of all program modules and systems.

Working from the design documents, initial sizing and timing requirements for the various subsystems are established, while the I/O list is used as the basis for the entire system database. Each module has at any one time a single source file and binary to match. When changes are ~~to~~ made the entire system is rebuilt from the binary and source file that exist. This procedure insures that the latest software is always in the system. *

The database and graphics subsystem are added as the final stage of system integration. Each stage has a mechanism for software trouble reporting, allowing the programmer or systems integrator to drop back to the appropriate level, re-program, test and integrate in a controlled fashion. Configuration control from the release point ensures the orderly progression of these changes. The process is repeated on an increasingly larger scale until the system is ready for test as a system.

2.5.3 Systems Integration and Factory Acceptance Test

The software and hardware systems have, by this stage, been thoroughly tested separately and have in fact, been used to a large degree to test each other. The hardware system may now begin to be exercised through simulation to provide loading information on both hardware and software. The simulation will also test the interfaces between the data acquisition, computation and graphics display systems, and errors will be corrected, re-implemented and re-tested as described above.

As each of the systems comes to maturity, portions of the factory acceptance test may be used to test performance, for informational purposes only. The systems thus come to a formal state of acceptance by all parties involved. This state is then frozen, as the factory acceptance test commences.

The factory acceptance test is run on this frozen system, each test continuing until completion or until such deficiencies occur as to make it impossible to continue beyond that point in a section of the tests. All errors are reported, but no corrective action is taken to disturb the particular configuration of the system. Any deficiencies in the system performance are noted as all the specified capabilities are tested.

If a series of correctable errors are discovered through the factory acceptance test, then, at test's end, the errors are corrected, and those subsystems subjected to the same set of factory tests. A sampling of other tests are also performed to insure against the inadvertent creation of one set of errors by correction of any other set. As this is completed, the proper QA procedures are verified to allow shipment of the system to the plant site.

2.5.4 Test Procedures

The purpose of the test procedures is to ensure that the delivered Technical Support Complex satisfies the system design requirements.

The procedures are reviewed towards determining the acceptable range of response for each function in the system, including responses to out-of-range or incorrect inputs. From these ranges for the data acquisition keyboard, algorithm and display systems, a discrete set is established to exercise the system with respect to the range of inputs and outputs, and with respect also to other combinations of functions occurring simultaneously within the system. A set of tests is established with output criteria separated into acceptable and unacceptable responses as explicitly as possible. The key point is to gather into a repeatable format those combinations which will subject the system to the widest range of possible uses during any time in its life. It is this ultimate test of functional response that is the cornerstone of the test philosophy.

Each test description includes the specific requirements stated first with the appropriate design document reference, followed by the required method of test. The state of the system is listed at the beginning of each test, together with a staged description of every action required by the tester and the acceptable system state following the action. Signature blanks are provided as an attachment to the test procedures. The engineer/technician performing the test signs the blanks only if the test results are unambiguously acceptable.

Unacceptable test results are numbered and documented, with each specific trouble area uniquely identified on separate TSC Error Reports (TER). TER's are closed only upon satisfactory completion of the specific test in which the trouble was discovered.

The test procedures detail:

- 1) test equipment requirements
- 2) prerequisites

WESTINGHOUSE CLASS 3

Each subsystem will be tested, including

- 1) keyboard functions - display, selection, control common to all systems as well as system specific functions such as transform, history, trends and change status
- 2) input processing functions - scan rates, processing capability, sensor out-of-range, transforms, process inhibiting
- 3) algorithms - iconics, redundant sensor, startup, valve position, op-limits, reactor trip, mathematical
- 4) display coding - headings, alphanumeric, graphics, poke fields, data quality plots
- 5) systems - power fail/startup, CPU and disk failures, system failure alarms

3.0 NRC VERIFICATION AND VALIDATION PROCESS

The activities that were proposed to be the subject of NRC audits for Verification and Validation of the ERF design process are shown in Figure 2. The particular NRC audit activities shown in this figure are

1. Verification of the design bases and functional requirements.
This was a technical audit by the NRC.
2. Validation of the integrated system.
This would be a procedural audit by the NRC; that is a QA audit.
3. Verification of the installed system.
This would be a procedural audit by the NRC; that is a QA audit.

Each of these steps in the V&V process is discussed in more detail in the following subsections.

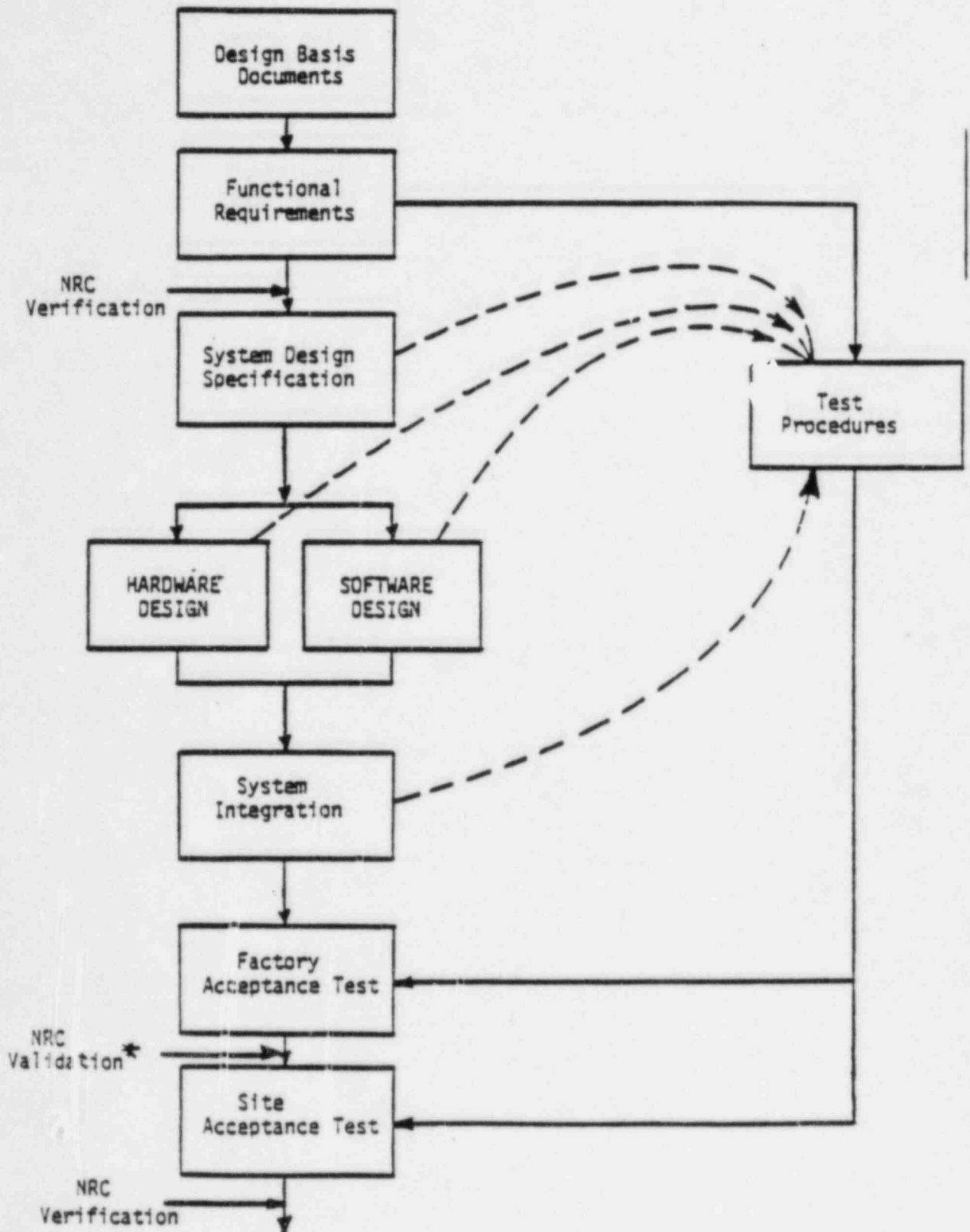
3.1 VERIFICATION OF THE SYSTEM REQUIREMENTS

This step in the NRC V&V process checks the design basis and the functional requirements of the system against the functional design criteria recommended by the NRC as modified by the exceptions to those recommendations which were taken by the design organization.

In the case of the SPDS the functional design criteria recommended by the NRC are primarily those given in NUREG 0696, Sections 5.1 and 5.5.

3.2 VALIDATION OF THE INTEGRATED SYSTEM

This step of the NRC V&V process addresses the demonstration of the performance of the integrated system against the system requirements as established in the design basis and functional requirements for the system. Included in this step is the evaluation of the adequacy of the test plan for



the system integration test and the adequacy of the design QA program which controlled the development of the system design specification and the design of the software and the hardware.

In the case of the SPDS this step includes the design criteria recommended in NUREG-0696, Section 5.6 as modified by the exception to those recommendations which were taken by the design organization.

3.3 VERIFICATION OF THE CORRECT INSTALLATION OF THE EQUIPMENT

Most of this is normally outside Westinghouse scope except where Westinghouse specified installation requirements for proper performance of the equipment. These requirements then become a section of the basis for the verification of the installation and are included in the list plan and procedures for the on-site acceptance lists.

4.0 DOCUMENTATION

Each phase of the design process is documented such that the equipment and design interfaces are unambiguously defined. The relevant design documents for the SPDS are identified in the following paragraphs.

4.1 Design Bases

The Design Bases for the SPDS were developed from a combination of NRC and internal Westinghouse requirements. The Design Bases are documented in References 1 and 2. | *

4.2 Functional Requirements

These requirements quantify the design and performance requirements for the components and interface of the system; they are developed from the design bases. The Functional Requirements are documented in Reference 3. | *

4.3 Design Specifications

For a computer system the design specifications support two parallel efforts: 1) the hardware specification and procurement, and 2) the software specification and procurement. The documentation supporting these efforts are found in References 4 and 5, respectively. | *

5.0 REFERENCES

1. Design Basis Document - Plant Safety Status Display, ESD-CR&CD-105 (Rev. 1, July 10, 1981)
2. Design Basis Document - Onsite Technical Support Center, ESD-CR&CD-109 (Rev. 1, July 9, 1981)
3. Functional Requirements - Technical Support Complex, ESD-CR&CD-94 (Rev. 1, July 14, 1981)
4. Standard Technical Support Complex, D-Spec. 955286.
5. Standard Software Design Specification - PSSD/OTSC, D-Spec. 955393.
6. QCS-2 Rev. 1, Quality Systems Requirements
7. QPS-319-2 Rev. 2, Quality Procurement Specification for WESD Supplied Technical Support Complex.
8. WCAP-10170, Emergency Response Facilities Design and V&V Process (April 29, 1982), Appendices A through D (Jan. 13, 1983), Appendix E (June 8, 1983)

*

*

APPENDICES

Appendix

- A.0 Introduction

- B.0 SPDS Development Process
 - B.1 Chronological Sequence
 - B.2 Westinghouse Verification and Validation Program
 - B.2.1 Verification of the design Bases and Functional Requirements
 - B.2.2 Verification of Hardware and Software system
 - B.2.3 Factory Acceptance Tests
 - B.3 Verification of the Installed SPDS

- C.0 Key Safety Parameter Selection

- D.0 Bibliography
 - D.1 Design Basis
 - D.2 Functional Requirements
 - D.3 Verification
 - D.4 Information Documents

- E.0 Application of Safety Parameter Display Evaluation Project to Design of WSPDS.

*

WESTINGHOUSE CLASS 3

A.0 INTRODUCTION

In late October 1982, the NRC met with Westinghouse to conduct an on-site technical audit of the Design Basis and Functional Requirements for the Safety Parameter Display System. At the conclusion of this audit the staff requested documentation to clarify the activities associated with the design process, the documents developed from these activities, and the effects upon iteration of these activities back into the principal design documents. Also, the NRC staff requested a mapping of the measured parameters fed into the SPDS onto the parameters required for an SPDS as stated in SECY 82-111.

Appendix B of this document responds to the same questions raised on the generic design process but responds specifically for the D. C. Cook Nuclear Plant TSC design. Appendix C provides the mapping of D. C. Cook's measured parameters into the SECY 82-111 parameters. The bibliography is given in Appendix D. Appendix E documents the manner in which man-in-the-loop testing was factored into the development of the design basis and functional requirements of the Westinghouse SPDS.

*

B.0 SPDS DEVELOPMENT PROCESS

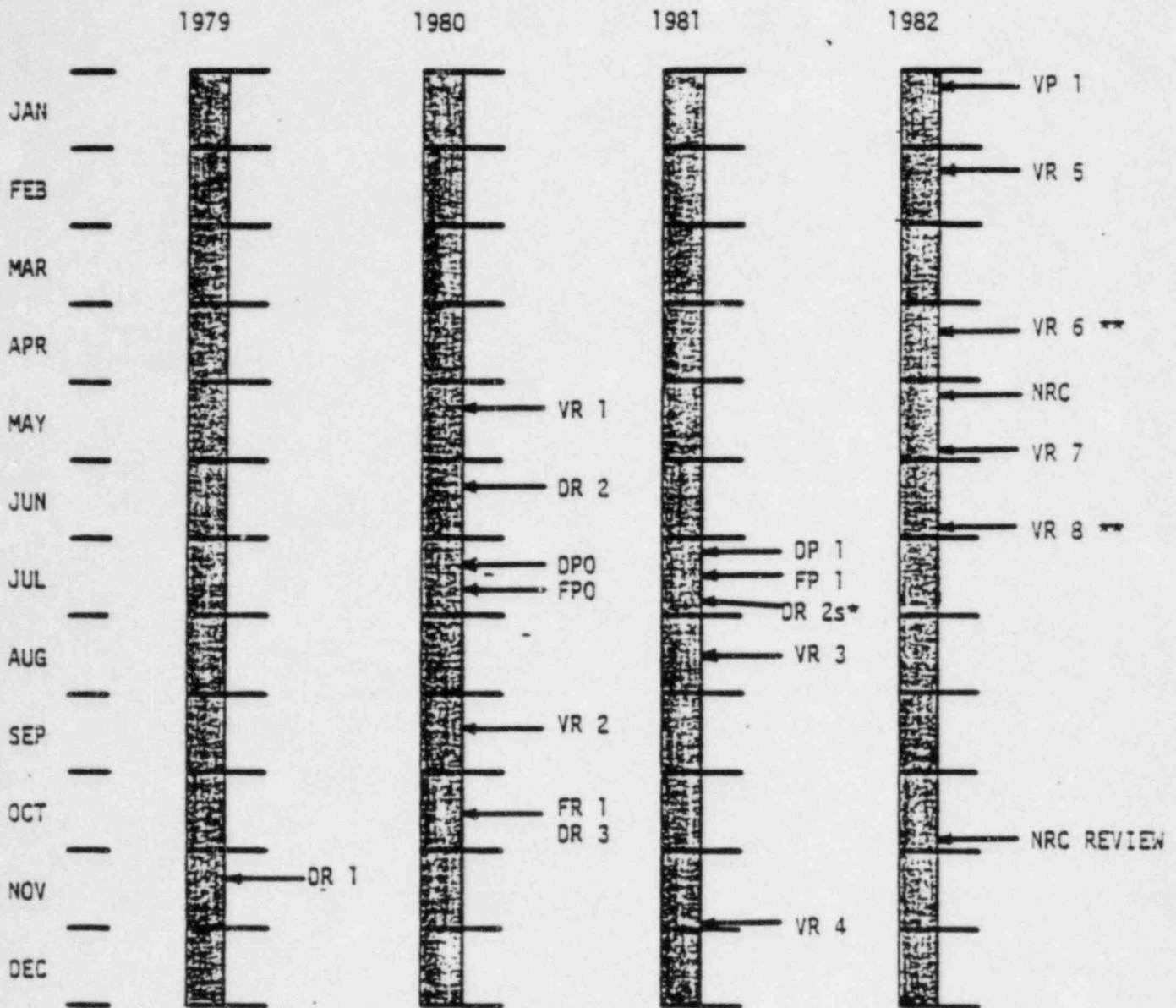
The process for developing the Design Bases, and Functional Requirements documents for the Safety Parameter Display System (SPDS) was evolutionary and iterative in nature because the development, design and verification activities for the SPDS were carried out in parallel. Figure B.1 has been developed to clarify the subject matter and temporal relationship of the documents produced throughout the time period of these activities.

In what follows the design bases and functional requirements documents are referred to as principal documents and are labeled on Figure B.1 as DP and FP, respectively. Reference documents are documents produced to support the information given in the principal documents. Reference documents are labeled DR or FR on Figure B.1 for the design bases and functional requirements, respectively. The terminology of principal and reference documents is also used for documents produced for the verification activity. These documents are labeled VP and VR on Figure B.1. Appendix D is the bibliography. The references given in the bibliography are ordered consistently with the format used in figure B.1.

B.1 CHRONOLOGICAL SEQUENCE

The development of the SPDS began in late 1979. The first document - DR1, proprietary, November, 1981 - provides a comparative evaluation of iconic displays. The next document - VR1, proprietary, May, 1980 - is a human factors verification of a draft of the functional requirements. VR1 is an informal, internal, dated and typed memo. DR2 - June, 1980 - provides a functional and technical description of the Westinghouse Technical Support Complex.

In July 1980, Rev. 0 of the Design Basis and Functional Requirements documents was issued. These documents were followed in September 1980 by VR2, proprietary, a verification of display prototypes by Human Factors specialists and utility operators, and DR3, proprietary - also listed as FR1 - a reference document for both the Design Basis and Functional Requirements, which presents Human Factors criteria for the development of information coding schemes.



*Supplement 1 to DR2

**These responses did not affect the bases or functional requirements

- DP Principal Design Basis Document
- DR Reference Design Basis Document
- FP Principal Functional Requirements Document
- FR Reference Functional Requirements Document
- VP Principal Verification Document
- VR Reference Verification Document

Figure B.1 The Chronological Sequence of Documents Produced for the Development of the Design Basis and Functional Requirements for the SPDS.

WESTINGHOUSE CLASS 3

In July, 1981, Rev. 1 of the Design Basis and Functional Requirements documents, both proprietary, and Supplement 1 to DR2, shown as DR2S on Figure 1, were issued. The former documents were the principal documents provided for NRC review at the October audit meeting; the latter document was a comparison of the design of the Westinghouse Technical Support Complex against the guidance given for Emergency Response Facilities in NUREG 0696. The third reference document for verification, VR3, was issued in August, 1981. This document provided an analysis of critical operator decisions in the context of four, recent, off-normal events occurring during normal power plant operations. In November 1981, the fourth reference verification document was issued, VR4. This document provided an evaluation of two experimental concepts for a Safety Parameters Display System.

The principal verification document, VP1, proprietary, was issued in January, 1982. This document presents the methods and results of a Human Factors review of the displays used in the Westinghouse Technical Support Complex. Verification of the SPDS design concept continued in 1982 and a series of review documents appeared describing the results of verification activities and the responses of the SPDS designers to the recommendations of the verifier. The verifier documents are VR5 and VR7, and the designer documents are VR6 and VR8. The last four verification documents, VR5 through VR8, are all proprietary documents.

B.2 WESTINGHOUSE VERIFICATION AND VALIDATION PROGRAM

The Westinghouse Verification and Validation activities for the development and construction of the SPDS are carried-out in three distinct phases. Phase I activities are those activities carried-out to verify the SPDS concept; these activities were discussed above. The results of these activities are reflected in the Design Basis and Functional Requirements documents. Phase II activities are those activities carried-out to verify the design of the equipment and software for the SPDS. The results of these activities are documented in the component acceptance tests, conducted by the vendors at their factory site, and again by Westinghouse upon delivery of the hardware from the vendors, and in the software verification test reports. The Phase III activity is the factory acceptance test, conducted by Westinghouse at the

Westinghouse site, to demonstrate the performance of the integrated hardware/software system. A subset of the factory acceptance test is the validation test which demonstrates the integrated system performs to the requirements called-out in the Design Basis and Functional Requirements documents.

The design process and verification activities are shown in Figure B.2.

B.2.1 Verification of the Design Bases and Functional Requirements

These activities were described in chronological detail in section B.1. The activities consisted of a review by Human Factors specialists of the displays in the Westinghouse Technical Support Complex, VP1; an evaluation of the functional requirements, VR1; an evaluation of displays for the SPDS, VR2; an evaluation of control room improvements, VR3; and an evaluation of SPDS concepts, VR4. Additional reviews, VR5 and VR6, were obtained from simulator trials using an operational SPDS. The documentation from these reviews is described in the Bibliography, Appendix D.

B.2.2 Verification of Hardware and Software System

The design of the SPDS system proceeds from the functional requirements to the development of the system design specification which establishes the basis for the decomposition of the SPDS into hardware and software design requirements.

Hardware Verification

The design for the hardware system evolves from the System Design Specification, and is documented in the equipment specification. A purchase requisition, based on the equipment specification, is used to order components from Westinghouse approved vendors.

Factory acceptance test procedures are prepared by the vendor and approved by Westinghouse. The tests are conducted at the vendor site and repeated by Westinghouse after delivery of the components. The two sets of results are compared to assure no components are damaged during shipment.

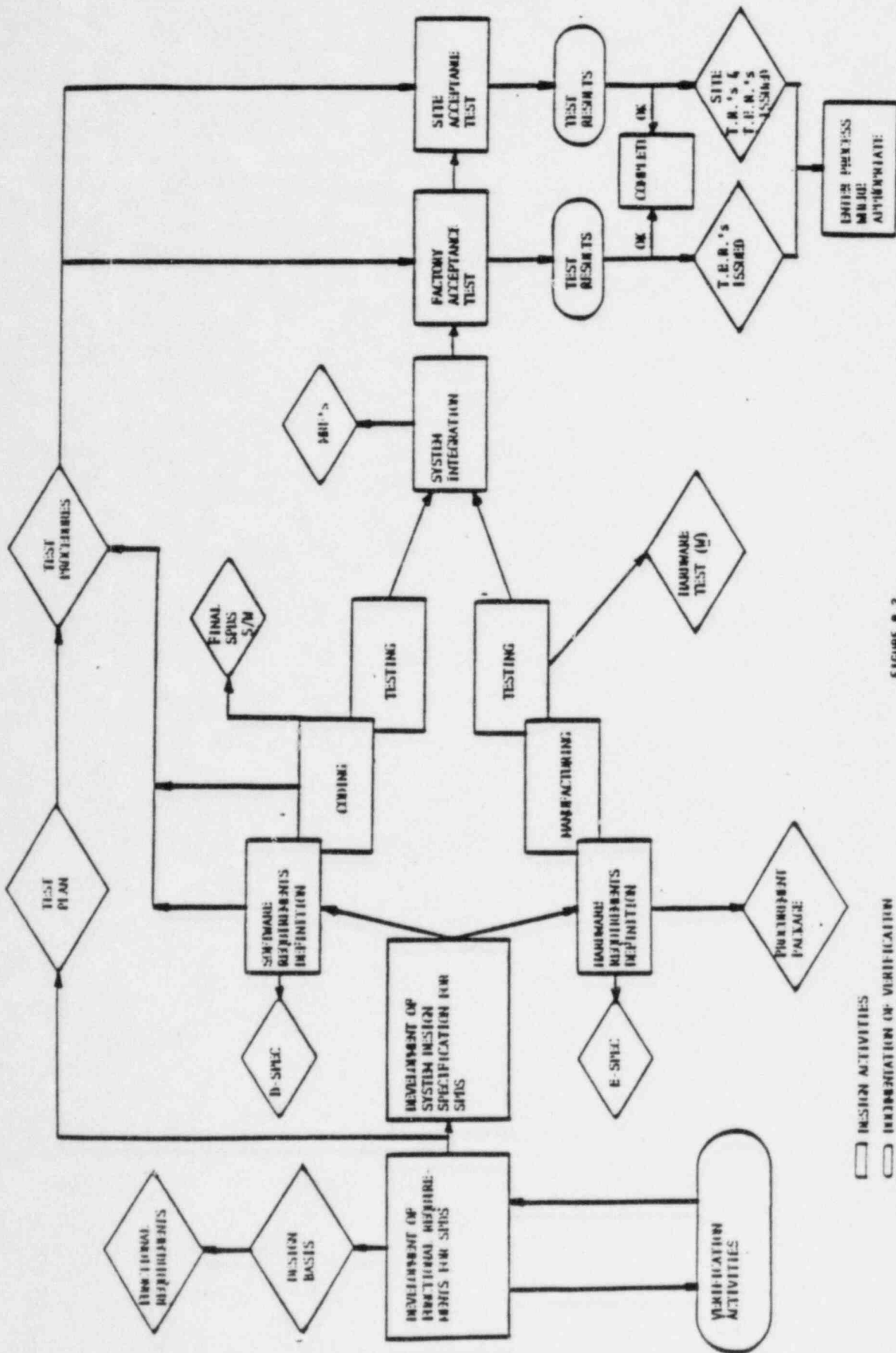


FIGURE B.2
DESIGN PROCESS AND VERIFICATION ACTIVITIES
FOR THE DEVELOPMENT OF THE WESTINGHOUSE SPIS
FOR THE D. C. COOK NUCLEAR STATION

□ DESIGN ACTIVITIES
 ○ INITIATION OF VERIFICATION
 ◇ INITIATION FOR REVIEW

Software Verification

B.2.3 Factory Acceptance Test

The test plan and test procedures for testing the integrated system are developed throughout the design process. All functions of the SPDS are exercised and measured against the acceptance criteria given in the test procedures. A portion of these tests validates the performance of the integrated system against the Design Basis and Functional Requirements documents.

B.3 VERIFICATION OF THE INSTALLED SPDS

The plant site tests to assure that the SPDS software and computer hardware¹ are correctly installed are the responsibility of Westinghouse. However, a portion of these verification tests (site acceptance tests) repeat the factory acceptance tests.

1 Verification of inputs (field sensor wiring) is the responsibility of the utility. (ie - all required inputs are provided and properly terminated and calibrated)

WESTINGHOUSE CLASS 3

C.O KEY SAFETY PARAMETERS

The goal of a safety parameter display system is to decrease the potential for operator cognitive errors by aiding operators in detecting deviations from safe plant conditions. An understanding of the task of detection is required in order to design an effective SPDS. From a simplistic view point detection usually refers to the initial detection of a plant abnormality. In terms of operator detection needs, detection also refers to the subsequent detections, in the sense of feedback, i.e., verification that operator actions are achieving safety goals and intended operator actions are successfully executed. In the sense of multiple failure emergencies detection also means detecting a second, third, etc., failure after initial detection of the first.

The detection process can be broken into stages:

- Activation - the operators determine that some abnormal condition exists that demands further investigation.
- Observation/data collection - data are collected, from control room instruments or other sources, to help investigate the nature of the abnormal condition.
- Recognition - recognize plant state in terms of a familiar pattern; usually leads directly to selection of a sequence of actions.
- Identification of system state - the data previously collected are abstracted into a coherent representation of the current state of the plant; at this point, the crew will identify what is wrong, but not why or how the abnormal conditions developed.

These stages cover the operators detection process from the initial activation that an abnormal condition exists to his resulting knowledge of what is wrong in terms of his understanding of the state of the plant.

In other words the role of concept-driven observation must be recognized in the detection process. This means that, once activated, observation is a

guided process -- looking for something. The quality of operator observations then depends on his recognition or identification of plant state.

The result is that to support the operator's ability to detect departures from safe plant conditions, an SPDS should support: (a) subsequent as well as initial detections of abnormal conditions; (b) feedback to the operator on the success of actions both in terms of successful action execution and in goal achievement; (c) observation, recognition and identification of plant state; and (d) guidance to the operator for further data collection activities (concept-driven observation).

The two top level displays (the Terminate Mode Iconic and the Mitigate Mode Iconic) are intended to aid the operator in the activation step of the detection process by making the operator aware that some abnormal condition exists that demands further investigation. The parameters used on these two top level displays are placed in the five safety functions itemized in NUREG-0737, Supplement 1 in Tables C-1 and C-2, respectively.

The second level display aids the operator in the observation/data collection and recognition stages of the detection process and focuses his data collection activities into the appropriate plant system so that he might accomplish the identification of system state step in this detection process. These steps in the detection process effectively translate the abstract issues of safety functions and the awareness that some abnormal conditions exists into the practical language of plant operations, i.e., from safety functions to pressures, temperatures, levels, etc. This display provides more detailed information on the entire plant.

The identification of system state step is accomplished by the use of the individual system displays. The systems that are depicted in these displays are mapped into the safety functions itemized in NUREG-0737, Supplement 1 in Table C-3.

To complete the mapping, all of the parameters that appear in the Westinghouse SPDS are individually mapped into the NUREG-0737, Supplement 1 safety functions in Table C-4.

TABLE C.1

D. C. Cook Top Level (Terminate Mode) WSPDS Variables
Mapped into NRC Safety Functions (NUREG-0737, Supplement 1) to Aid the
Activation Step in the Counting Process of Detection

Reactivity Control

Power Mismatch (Nuclear-Turbine)

Reactor Core Cooling & Heat Removal From the Primary System

Pressurizer Pressure

RCS T_{avg}

Steam Generator Level (Narrow Range)

Reactor Coolant Integrity

Pressurizer Level

Net Charging Flow

Radiation Monitoring

Containment Monitoring

Radioactivity Control

Radiation Monitoring

Containment Condition

Containment Monitoring (Temp, Press., Sump Level)

Radiation Monitoring

*

*

TABLE C.2

D. C. Cook Top Level (Mitigate Mode) WSPDS Variables
Mapped into NRC Safety Functions (NUREG-0737, Supplement 1) to Aid the
Activation Step in the Cognitive Process of Detection

Reactivity Control

Start-Up Rate

Reactor Core Cooling & Heat Removal From the Primary System

RCS Pressure

Core Exit Temperature

Steam Generator Level (Wide Range)

Reactor Coolant Inventory

Pressurizer Level

Reactor Vessel Level

Containment Pressure

Radiation Monitoring

Radioactivity Control

Radiation Monitoring

Containment Conditions

Containment Pressure

Radiation Monitoring

TABLE C.3 (cont)

*

Westinghouse PWR System Appearing in the D. C. Cook
WSPDS Mapped into NRC Safety Functions (NUREG-0737, Supplement 1) to
Aid the Identification of System State Step
in the Cognitive Process of Detection

Reactor Coolant Integrity

Reactor Coolant
Chemical and Volume Control
Residual Heat Removal
Safety Injection
Containment Monitoring
Radiation Monitoring

Radioactivity

Radiation Monitoring
Containment Isolation

Containment Conditions

Containment Monitoring
Containment Spray
Hydrogen Recombiners
Radiation Monitoring

*

TABLE C.4

D. C. Cook Unit 1
SPDS Safety Concern Variables
Mapped into NRC Safety Functions (NUREG-0737 Supplement 1)

b,c

*

TABLE C.4 (cont)

b,c

*

TABLE C.4 (cont)

b,c *

TABLE C.4 (cont)

b, c

*

TABLE C.4 (cont)

b,c

*

WESTINGHOUSE CLASS 3

TABLE C.4 (cont)

b,c

*

TABLE C.4 (cont)

b, c

*

WESTINGHOUSE CLASS 3

TABLE C.4 (cont)

b,c

*

--	--

WESTINGHOUSE CLASS 3

TABLE C.4 (cont)

b,c

*

TABLE C.4 (cont)

b,c *

TABLE C.4 (cont)

b, c

*

WESTINGHOUSE CLASS 3

TABLE C.4 (cont)

b,c

*

TABLE C.4 (cont)

b,c

*

WESTINGHOUSE CLASS 3

TABLE C.4 (cont)

b, c

*

TABLE C.4 (cont)

b,c

*

TABLE C.4 (cont)

b,c

*

TABLE C.4 (cont)

b,c

*

TABLE C.4 (cont)

b,c

*

--	--

WESTINGHOUSE CLASS 3

TABLE C.4 (cont)

b,c

*

WESTINGHOUSE CLASS 3

TABLE C.4 (cont)

b, c

*

WESTINGHOUSE CLASS 3

TABLE C.4 (cont)

b, c

*

WESTINGHOUSE CLASS 3

TABLE C.4 (cont)

b, c

*

TABLE C.4 (cont)

b,c

*

WESTINGHOUSE CLASS 3

TABLE C.4 (cont)

b,c

*

WESTINGHOUSE CLASS 3

The following addendum describe only the differences in Table C.4 for Unit 2.
All other variables including plant I.D. numbers are identical to Unit 1.

*

WESTINGHOUSE CLASS 3

TABLE C.4

D. C. Cook Unit 2 Addendum
SPDS Safety Concern Variables
Mapped into NRC Safety Functions (NUREG-0737 Supplement 1)

b, c

*

WESTINGHOUSE CLASS 3

TABLE C.4 (cont)

b, c

*

WESTINGHOUSE CLASS 3

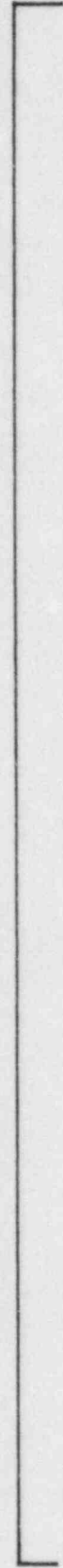
TABLE C.4 (cont)

b, c *

TABLE C.4 (cont)

b,c

*



D.0 BIBLIOGRAPHY

The bibliography is divided into four sections: Design Basis, Functional Requirements, Verification, and Information Documents. Except for the section on Information Documents, each section is sub-divided into principal and reference documents; and the documents are numbered as described in Appendix B and as presented on Figure B.1.

D.1 DESIGN BASIS

Principal Document

- DP1. J. L. Little, W. F. Schaefer, "Design Basis Document - Plant Safety Status Display, Revision 1", SA&I-ESI-078, July 10, 1981, Proprietary Class II.

Reference Design Documents

- DR1. J. F. Obrien, "Evaluation of Iconic Displays for Application in Nuclear Power Plant Control", Research Report 79-IC57-CONRM-R1, Nov. 8, 1979, Proprietary Class II.

This report describes a controlled experiment that was conducted to evaluate the feasibility of a graphic display concept, iconic displays, for presentation of information used to identify leaks in a nuclear power plant. Results indicated that iconic displays were superior to standard meter type displays for identifying leaks that were unfamiliar to the training center instructors who participated in the study. Meter type displays were slightly superior to iconic presentations for more familiar events. Based on these findings, it was recommended that developmental work on iconic displays proceed. Training related implications of the study findings were also discussed.

- DR2. D. V. Gennaro et al, "Westinghouse Technical Support Complex", WCAP-9725, June 1980, Suppl. 1, July 1981

WESTINGHOUSE CLASS 3

This report provides the functional and technical descriptions of the Westinghouse TSC that will enable, in normal as well as abnormal operations, the collection, processing, display, and transmission of plant status information. These data are provided to aid the plant operator and technical support personnel in limiting the consequences of abnormal events. The TSC reflects the results of an intensive Westinghouse study of the plant from the perspective of the recommendations given by the NRC Lessons Learned Task Force. The concepts and implementation methods discussed in this report are the results of the Westinghouse study and provide the basis for potential longer-term requirements in this area.

- DR3. D. D. Woods and S. Eckert, "Man-Machine Interface Design Basis Document: Information coding for Computer Display Systems, Rev. 0", ESD&E-CR&CD-224, October 20, 1980.

This document presents Human Factors criteria for the development of information coding schemes in computer display systems.

D.2 FUNCTIONAL REQUIREMENTS

Principal Document

- FP1. W. F. Schaefer & J. L. Little, "Functional Requirements - Technical Support Complex - Revision 1", SA&I-ESI-079, July 14, 1981, Proprietary Class II.

Reference Documents

- FR1. D. D. Woods and S. Eckert, "Man-Machine Interface Design Basis Document: Information Coding for Computer Display Systems, Rev. 0", ESD&D-CR&CD-224, October 20, 1980, Proprietary Class II.

This document presents Human Factors criteria for the development of information coding schemes in computer display systems.

D.3 VERIFICATION

Principal Document

- VP1. D. D. Woods, & M. C. Eastman, "Human Factors Evaluation of the Technical Support Complex Display Systems: Vol. 1-Text - Vol. 2-Appendices", Research Report 81-ICE7-CONRM-R1, January 12, 1982, Proprietary Class II.

This report presents the method and results of a Human Factor review of the Westinghouse Technical Support Complex display systems.

There are three sets of displays in the Technical Support Complex: (1) the basic display set called the Plant Safety Status Displays (or PSSD) designed to aid operators in emergency operations, (2) additional displays for the Onsite Technical Support Center (or UTSC) to aid accident recovery, and (3) the Bypass and Inoperable Status Indication Displays (or BISI) to cover pre-accident operability of safeguards systems.

The evaluation was based on two sources of input: (1) task descriptions (e.g., what should the display do for the user?) for the display systems that were developed as part of the conceptual analysis portion of the design process, and (2) human factors principles for enhanced information transfer from display to user. The input from these two sources formed the basis for a checklist, customized to this application, which was the evaluation mechanism. Feedback from the checklist evaluations was provided to the display designers to enhance the quality of the display systems. Examples of the major kinds of revisions are included in the report as well as a complete catalogue of initial displays and revised displays.

Reference Documents

- VR1. S. Eckert & D. Woods, "Review of Functional Requirements", Private Communication, May 1980, Proprietary Class II.

WESTINGHOUSE CLASS 3

This informal document provides paragraph by paragraph "Human Factors" Comments on the system Functional Requirements,"

- VR2. D. D. Woods, "Evaluation of Technical Support Complex Polar Graphic Display Prototypes", Research Report 80-IC57-CONRM-R3, December 8, 1980, Proprietary Class II.

This report presents both Human Factors specialists and utility operators comments on the Polar Graphic display prototypes. The evaluation materials consisted of actual, dynamic CRT displays driven by simulated power plant transients or video tapes of the same dynamic displays supplemented by photographs. The Polar Graphic display concept was evaluated as an effective tool for the presentation of multiparameter data. However, some areas of potential improvement and some areas for further research and analysis were identified.

- VR3. R. W. Pew, D. C. Miller, and C. E. Feeher, "Evaluation of Control Room Improvements Through Analysis of Critical Operator Decisions", EPRI NP-1982, August 1981.

Decision making by nuclear power plant operators was studied in the context of four recent off-normal events in order to assess the potential impact of various control room improvements and innovations. Categories of improvements considered in the study included proposed changes in staff organization and training, controls and displays, and computerized support systems.

The evaluation methodology involved judgments by a panel of experts regarding the benefits of proposed improvements for specific operator decisions. It also included the explication of a model of operator decision making and an analysis in terms of this model of how each improvement could help prevent or resolve decision-making errors.

The results indicated that time stress on the crew played an appreciable role in performance failures. The report concludes that it is unrealistic to expect that further training improvements alone

can do much to address the multitude of potential situations that operators face. A combination of improvements will be necessary, integrated by a strong underlying operational concept that could be embodied in a computerized support system. The recommended approach would emphasize the detection and correction of errors when they occur, in addition to the prevention of errors.

- VR4. D. D. Woods, "Evaluation of Safety Parameter Display Concepts", Research Report 81-5657-HFSPE-R1-Vol. 1 and 2, October 30, 1981.

New control room equipment designed to improve operator performance must be evaluated before adoption and installation. Two experimental concepts for a Safety Parameters Display System (SPDS) were evaluated to assess benefits and potential problems associated with the SPDS concept and its integration into control room operations. Participants were licensed utility operators undergoing retraining on a nuclear power plant simulator. Both quantitative and qualitative data were collected and analyzed on crew response to seven simulated accident conditions.

Data on operator decisions and actions have been organized into timelines. Analysis of the timelines and observations collected during testing provide important insights about the potential impact of the SPDS concept on control room operations. The study demonstrates that 1) the safety panel prototypes can provide access to information needed to aid crew decision-making, but attention must be given to the integration of the panels with procedures, training, and conventional control room instrumentation; 2) the key decision analysis method simulator can be used during a normal training program to evaluate safety panel concepts.

- VR5. C. P. Roman, "TSC System Capabilities", TSC-82-25, February 9, 1982, Proprietary Class II. (Not incorporated into D. C. Cook WSPDS)
- VR6. J. L. Little, "SPDS Changes and Improvements", SA&I-ESI-227, April 15, 1982, Proprietary Class II. (Partially incorporated into D. C. Cook WSPDS)

WESTINGHOUSE CLASS 3

- VR7. C. P. Roman, "Comments on SPDS/OTSC Simulator," TS-82-98, May 27, 1982, Proprietary Class II.
- VR8. E. F. Kelly, "Changes/Enhancements to the TSC", SA&I-ESI-178, June 25, 1982, Proprietary Class II. (Not incorporated into D. C. Cook WSPDS)

This series of memos provide comments and design modifications as a result of those comments for the Safety Parameter Display System.

D.4 INFORMATION DOCUMENTS

J. L. Little & D. D. Woods, "A Design Methodology for the Man-Machine Interface for Nuclear Power Plant Emergency Response Facilities", Research Report 81-IC57-CONRM-P1.

D. D. Woods, "Visual Momentum: A Concept to Improve the Cognitive Coupling of Man and Machine", Research Report 82-IC57-CONRM-R3, April 23, 1982.

APPENDIX E (TO WCAP-10170) (NON-PROPRIETARY)

APPLICATION OF SAFETY PARAMETER DISPLAY EVALUATION
PROJECT TO DESIGN OF WSPDS

Prepared by: D. D. Woods

INTRODUCTION

Appendix E documents the manner in which man-in-the-loop testing was factored into the development of the design basis and functional requirements for the Westinghouse SPDS by application of the experience obtained from the EPRI project, "Evaluation of Safety Parameter Display Concepts", EPRI-NP-2239. Man-in-the-loop testing with regard to the design concept of the SPDS as an aid to the operator was completed in the EPRI project.

1. Role of Safety Parameter Display Evaluation Project in Westinghouse SPDS Design Process

The Safety Parameter Display Evaluation project examined operator performance in simulated accidents with 2 prototype safety panels (i.e., man-in-the-loop testing). Two kinds of results were derived from this study: the study showed that analysis of operator decision making was a useful tool to understand operator behavior; there were findings with respect to the concept of safety panels in general and the specific prototypes used, in particular. The study was done during the time when Westinghouse was in the process of developing a Safety Parameter Display System design (1980-1981).

A statistical comparison of crew performance with and without a safety panel available was not performed because of limitations imposed by the retraining program on the experimental design and because of variations in crew response strategies. To date there has been no quantitative evaluation of a control room modification on a full scale simulator. Instead the analysis of the data was based on decision process analysis. This technique reveals not just what actions a crew takes but also the decision process or context that led to the action. It is important to know why and how a crew action was ultimately

successful or not successful in order to identify the useful features of a new operator aid, design deficiencies, and boundary conditions (e.g., where will a new concept help and where is it unable to help the user's decision process).

The particular decision analysis performed in this study was derived from Rasmussen's (1979) model of operator behavior (Figure 1). The different stages of this model were grouped into four categories: detect, interpret, control, and feedback. The detect stage included alert, observation, recognition and identification activities; the interpretation stage concerned how the crew understood plant status including the implications of system status, relevant goals and strategy planning; the control category included action selection and execution, and the feedback stage concerned observation/data collection, recognition and identification as follow up to an operator action as opposed to the detect stage where these activities occur as a follow up to an alert. Effective feedback includes verifying that actions were implemented correctly, monitoring the effect of the action on plant state, and monitoring the effect of the action on reaching goals. (Note that the last two items imply a link between the feedback stage and the interpretation stage).

These categories were used to chart the decision process in each test event. The decision model provided a mechanism to generalize operator behavior and operator SPDS usage across particular tasks, events, and crews.

The decision analysis revealed, in the area of crew decision making, that operator problems did not occur in the detection of initial system failures, rather they occurred with subsequent problems, either operator error/miscontrol or subsequent system failures. These problems were associated with poor feedback about the results of control actions with respect to system state and recovery goals. The usefulness of the SPDS in alleviating problems with poor feedback is included in Section 2, which gives a detailed discussion of results from the Safety Parameter Display Evaluation project.

This result confirms part of the Westinghouse SPDS design basis (cf., Little & Woods, 1981, pg. 7), in particular, that displays should support operator roles in detection (both initial and subsequent detections) -- "is there a problem? where? what kind of problem? is the problem decreasing or

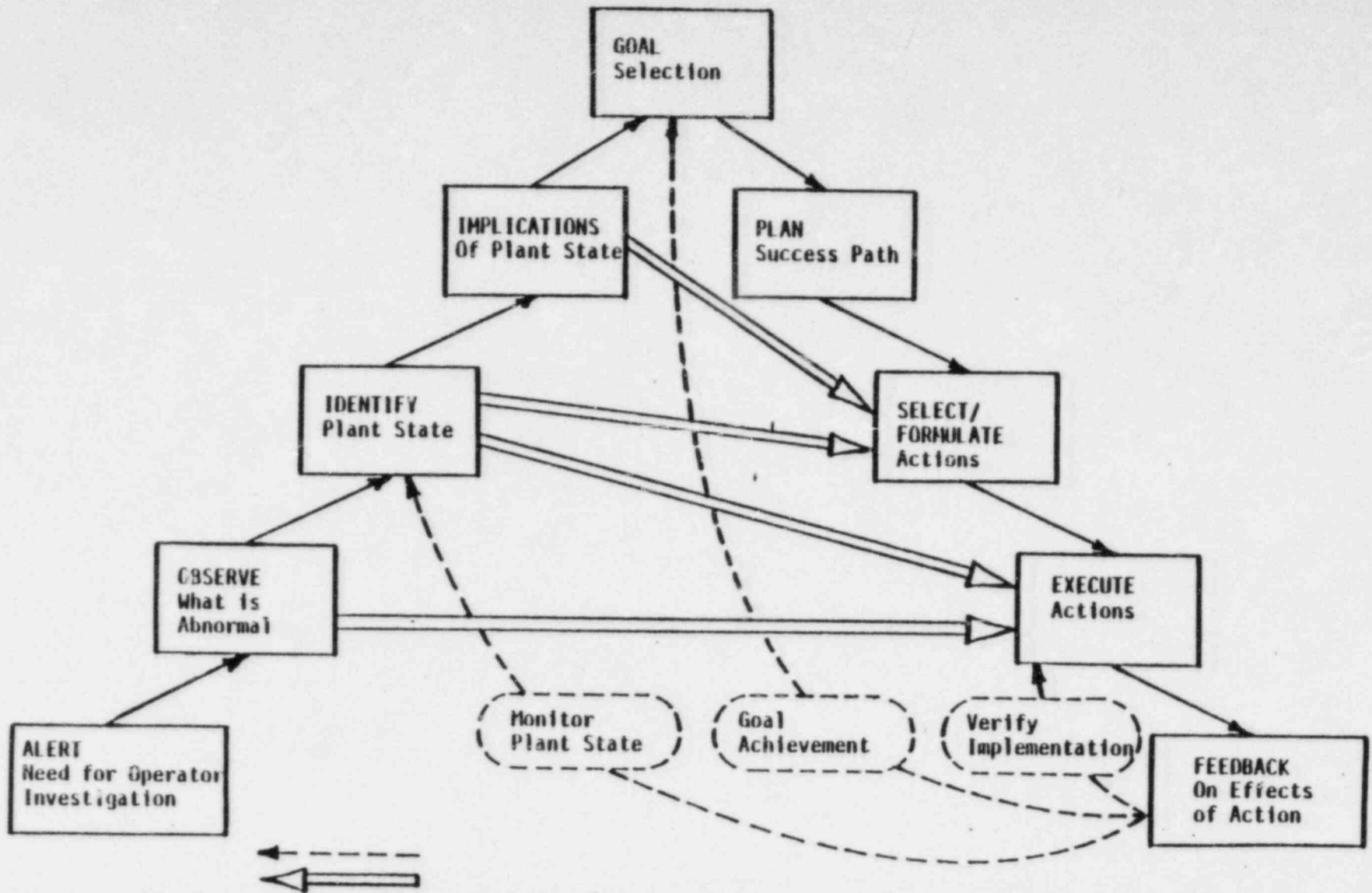


Figure 1. Decision-Making Model (Adapted from Rasmussen) Including Feedback

increasing in severity? -- and feedback (monitoring the effect of actions on plant state and monitoring the effect of actions on reaching goals) -- "are the actions taken successful? is the problem receding or expanding?" Furthermore, the safety panel usage data (in particular, the data from the prototype that was based on Westinghouse SPDS concepts) showed that an SPDS can serve as the source of improved feedback to operators. However, it should be noted that feedback associated with verifying that actions were implemented correctly is not part of the SPDS primary function and is performed by control board instrumentation, such as status lights for switches (although SPDS displays can support this function to the extent that component status is part of the data base).

"Safety panels were successfully used to aid in the problem recognition activity and for feedback during the control activity. (p. S-6).

The operators used the safety panels to obtain feedback about plant conditions following operator decisions or actions. Examples range from cases where operators used the safety panel prototypes to discover that the faulted steam generator had not been successfully isolated to cases where operators discovered that conditions in a hypothesized faulted steam generator did not match their diagnosis." (p. 4-25, 4-26).

The above example of results from the Safety Parameter Display Evaluation project shows that the decision analysis method derived from Rasmussen's model proved to be a useful tool to analyze operator behavior and to link that behavior to general and specific characteristics of potential SPDS designs.

As such, the study provided one basis, derived from the analysis of operator performance during transient testing rather than opinion, for the operator behavior concepts used in the Westinghouse SPDS design basis.

In addition to confirming design basis concepts, the Safety Parameter Display Evaluation study provided data on the two specific prototypes used in the test. The prototype based on Westinghouse SPDS concepts accounted for 63 percent of the total number of SPDS consultations (including both safety panel prototypes), over 80 percent of the total number of successful SPDS consultations, but only 6 percent of the unsuccessful ones (almost 30 percent of total

SPDS consultations were unsuccessful). In other words, an SPDS prototype based on Westinghouse concepts did provide operators with information needed during decision making. The specific deficiency related to the unsuccessful consultations were identified and the displays modified. In addition, display deficiencies identified for the other prototype were noted and the information used to avoid similar problems in Westinghouse SPDS displays that were not part of the Safety Parameter Display Evaluation test (Section 4.3.3 of the final report contains the particular deficiencies found).

In terms of the particular displays that made up the Westinghouse prototype safety panel (cf., p. S-8, S-9), the polargraphic display helped detect the onset of a problem; it was consulted to obtain an overview of plant status; the lack of operator familiarity reduced its usage; and the plant status display was the most frequently and effectively used display (primarily due to its data integration role) and was used by some SROs to carry out their system manager role.

2. Results With the Specific Safety Panel Prototypes

Human factors deficiencies in the Panel A concept greatly impaired the usability of these displays (Table 1). Some of these deficiencies were the result of implementation compromises rather than design features. Nevertheless, the low usage rate produced by these deficiencies obscured the potential usefulness of an SPDS designed along the Panel A concept. In particular, the trend displays on Panel A, as implemented, did not meet the operators' information needs (i.e., low usage rate), because these displays were not an effective real time monitoring tool (cf., pg S-8).

Sources of this result include:

- * Data update (30 seconds) was too slow (cf., pg I-9 for an example of unsuccessful usage due to this deficiency);
- * Data averaging time window was too large (30 seconds);
- * Display response time was too slow (10 seconds; implementation compromise);

WESTINGHOUSE CLASS 3

TABLE 1
SAFETY PANEL PROTOTYPE USAGE
(Each prototype was available in test events)

	Successful	Unsuccessful	Total
Panel A Concept	9	15	24
Westinghouse Concept	36	4	40
<hr/>			
Total	45	19	64

WESTINGHOUSE CLASS 3

- * The plots could have helped an operator identify past causes for current plant conditions (for example, is pressure dropping because a relief valve opened?) but did not because logarithmic scales obscured maxima, minima and rates of change information (cf., pg I-3 for examples);
- * In general, operators rarely used the trend portions of the displays, relying instead on the digital most recent value readout (cf., pg I-8 for an example).

NSAC has used the results of this evaluation to significantly modify their SPDS concepts, for example, by adding a top level display.

The Westinghouse prototype was used more frequently. Table 2 shows the frequency of successful/unsuccessful consultations as a function of crew. Only the Westinghouse prototype was used as an integrated part of the crew's recovery response. For example, in one trial (TR1-H), the shift supervisor effectively utilized the Westinghouse safety panel by stationing himself at the unit for virtually the entire first 18 minutes of the event. In two other trials (TR2-H and TR3-H), a different supervisor made use of the Westinghouse safety panel by referring to it frequently as he moved around the control room.

When a safety panel had a major impact on the evolution of a trial, the prototype was used to support the shift supervisor's system manager role.

For example, in TR2-H the supervisor used the Westinghouse safety panel to monitor and modify the BOP's control of the secondary system. In FW3-E he used the Panel A to monitor the evolution of his feed and bleed strategy. In events TR1-F and TR3-H, he used the Westinghouse safety panel to monitor RCS depressurization, directing operator actions as necessary to continue the depressurization.

The Westinghouse prototype safety panel was used successfully in several types of operational problems. First, it was used in the detection of initial problems (cf., pg I-2). Second, it was used to monitor plant status as an input to operator recovery decisions. This occurred both at the level of input

WESTINGHOUSE CLASS 3

TABLE 2
SUCCESSFUL/UNSUCCESSFUL CONSULTATIONS AS A FUNCTION OF CREW

<u>Crew</u>	<u>Safety Panel Concept</u>	<u>Number of Events SP Available</u>	<u>Successful Consultations</u>	<u>Unsuccessful Consultations</u>
A	Panel A	3	3	7
B	Panel A	2	2	1
C	Panel A	2	0	1
D	Panel A	1	1	2
E	Panel A	3	3	4
F	Westinghouse (Panel B)	4	12	3
G	Westinghouse (Panel B)	3	7	0
H	Westinghouse (Panel B)	4	17	1

WESTINGHOUSE CLASS 3

to strategic decisions, that is, choosing which maneuvers to execute, and at the level of tactical decisions, that is, decisions about how or when to execute planned actions.

Examples include:

- * In two events (FW2-G, FW3-G), a crew used Safety Panel B narrow range iconic and plant status displays to check that RCS conditions were stable and within safe bounds before it planned to establish a feedwater path through the condensate pumps as a solution to AFW problem.
- * In one event (FW3-G), before beginning to execute the condensate pump path, the BOP asked the RO what the status of the RCS was. The RO used Safety Panel B wide range iconic to check that RCS conditions were stable and within safe bounds.
- * A crew (PSI-F), knowing that low RCS pressure would initiate a SI signal and that there was no RCS leak, used Safety Panel B plant status display to check plant conditions, especially RCS subcooling, before deciding to block SI.
- * A crew (TR1-H) monitored a power reduction from Safety Panel B plant status display and performed a manual Rx trip when they detected nuclear power less than 10 percent.
- * A crew (TR1-F) consulted Safety Panel B plant status and RCS displays to check plant conditions as an input to the decision to begin to realign normal charging/letdown and to restart one RCP. The crew's goal was to use PRZR spray as a means of RCS depressurization.
- * The SRO in another event (FW1-G) asked the RO to call up and consult the Safety Panel B wide range iconic display to check plant status and PRZR level before the SRO decided whether or not to realign normal charging/letdown.

WESTINGHOUSE CLASS 3

A third area of results on safety panel utilization is feedback about the results of control actions, in particular, monitoring the effect of actions on plant state and monitoring the effect of actions on reaching goals. With respect to operator decision behavior, data on error correction reveal that operators can have problems with poor feedback about the effect of control actions on system state and recovery goals. In particular, when operators misidentified plant state or had execution difficulties, they generally failed to correct their understanding of plant state or to identify and correct execution problems within the duration of the test events (Table 3). When errors were corrected it was generally due to the intervention of external agents (i.e., the instructor) or took relatively long times (up to 8 minutes). The data in Table 3 does not include cases where operator problems were corrected with help from the Westinghouse safety panel, although it does include cases where Panel A did not provide necessary feedback.

The usage data with the Westinghouse prototype reveals several instances where this safety panel was successfully used to obtain feedback. Examples where feedback was obtained from the Westinghouse safety panel to correct problems include:

- * In event TR3-H the RO detected that the faulted SG level was within wide range instrumentation from Safety Panel B plant status and wide range iconic displays. The BOP had reported earlier that the faulted SG was empty by misreading narrow for wide range level from the control board.
- * The SRO (TR2-H) detected low SG levels in two unaffected SGs from Safety Panel B plant status display. (The BOP had been slow in re-establishing AFW flow to the unaffected SGs after stopping all AFW to aid in the SGTR diagnosis.) The SRO then directed the BOP to increase AFW flow to the unaffected SGs.
- * Safety Panel B plant status display helped the SRP detect that AFW had not been isolated completely from the faulted SG (TR2-H). The faulted SG had been isolated, but the BOP turned on the turbine driven AFW pump to increase unaffected SG levels. However, AFW flow also began to the faulted SG.

WESTINGHOUSE CLASS 3

TABLE 3
 ERROR CORRECTION RESULTS
 (Errors corrected with Westinghouse SPDS
 utilization are not included)

	<u>No Correction</u>	<u>External Correction</u>	<u>Correction</u>
Problems in State Identification	7	5	0
Problems in Execution	5	0	7
<hr/>			
Total	12	5	7

Other examples where operators used the Westinghouse prototype to obtain feedback on the results of control actions include:

- * In event TR2-H the SRO detected that only 2 of the 3 unaffected SGs were being used to cool the RCS from Safety Panel B plant status display. He directed the BOP to open the third SG PORV.
- * In another event (FW3-G), a crew detected that PRZR level was low and decreasing. The crew isolated letdown and then consulted Safety Panel B wide range iconic for feedback. The iconic display showed the crew that the PRZR level decrease halted.

These results suggest that SPDS concepts like those used in the Westinghouse prototype can aid operators to obtain better feedback on the results of control actions and therefore to provide a more error corrective man-machine system.

SUMMARY

There is a trade-off that occurs in tests of user performance with new aids: on one hand, the test can occur late in the design process when a rather refined design is available to test but where changes, especially fundamental ones, may be difficult to make; on the other hand, the test can occur early in the design process when there is the greatest opportunity for results to affect the design but where the test must be done with relatively cruder prototype systems. In this case, the Safety Parameter Display Evaluation project was performed early in the Westinghouse SPDS design process and served to help confirm (along with demonstrations of the concepts to operators) the Westinghouse design basis approach and provide guidance to the detailed design. In addition, man-in-the-loop testing was incorporated into the development of the design basis and functional requirements for the Westinghouse SPDS by application of the results from the Safety Parameter Display Evaluation Project.