



April 12, 1991
LD-91-016

Project No. 675

U. S. Nuclear Regulatory Commission
Attn: Document Control Desk
Washington, DC 20555

Subject: Response to NRC Requests for Additional
Information

Reference: NRC Letter, I&C and Human Factors RAIs,
D. M. Crutchfield (NRC) to S. T. Brewer (C-E),
dated December 21, 1990

Dear Sirs:

The reference requested additional information for the NRC
staff review of the Combustion Engineering Standard Safety
Analysis Report - Design Certification (CESSAR-DC).
Enclosure I to this letter provides our responses.

Should you have any questions on the enclosed material,
please contact me or Mr. S. E. Ritterbusch or my staff at
(203) 285-5206.

Very truly yours,

COMBUSTION ENGINEERING, INC.

E. H. Kennedy
Manager
Nuclear Systems Licensing

EHK:lw

Enclosure: As Stated

cc: P. Lang (DOE - Germantown)
J. Trotter (EPRI)
T. Wambach (NRC)

ABB Combustion Engineering Nuclear Power

Combustion Engineering, Inc.

1000 Prospect Hill Road
Post Office Box 500
Windsor, Connecticut 06095-0500

Telephone (203) 688-1911
Fax (203) 285-9512
Telex 99297 COMBEN WSOR

9104190057 910412
PDR PROJ
675A PDR

DO32
11

RESPONSE TO NRC REQUEST FOR ADDITIONAL INFORMATION
I & C AND HUMAN FACTORS BRANCHES

Number: 420.4 (7)

Question: This question requests C-E to provide design details so that the staff can evaluate the system/equipment design with respect to all appropriate regulations and standards. C-E is requested to provide examples which address most of the Instrumentation and Control (I&C) equipment. The first example requested is the Core Protection Calculator. The staff is relatively familiar with this equipment and C-E has a current complete design available from which an appropriate level of detail could be provided.

The second example requested is equipment which is in the C-E scope but has not been completely designed, or selected and may not be finalized until after design certification. Possible examples could be the programmable logic controllers for the Emergency Safety Features Actuation System (ESFAS) or the Integrated Process Status Overview (IPSO) panel.

The third example requested is for equipment outside of the C-E scope for which interface requirements are to be established. As identified in the DC (7.1.1.4.L), the Heating, Ventilation and Air Conditioning (HVAC) systems are to be supplied by others. Since the HVAC is important as an I&C support system, the staff must make a determination that the design is acceptable and the necessary level of design detail (or requirements) is included or referenced in the DC.

Response: Example 1:

CESSAR-DC Section 7.1.2 "Identification of Safety Criteria" describes compliance with applicable standards and regulations and/or references to other parts of CESSAR-DC where the design's compliance is discussed further.

The Core Protection Calculators are discussed in Section 7.2.1.1.2.5. Initiation logic, bypasses, interlocks, testing and analysis are described in the applicable sections of 7.2. This information is consistent with that supplied for staff review in other recent FSARs.

Additional Core Protection Calculator documentation can be found in C-E document NPX80-IC-SD570*, Rev. 00, "System Description for Core Protection Calculators for Nuplex 80+."

*This document is considered proprietary to Combustion Engineering, Inc. Access to this document will be provided to facilitate NRC staff review of CESSAR-DC. Information from this document determined to be necessary to support the staff's safety finding will be placed in CESSAR-DC in a future amendment.

There are three basic changes to the CPC from System 80:

1. The data links between the CEA input multiplexors and the calculator have been extended so that the multiplexors can be located remotely (i.e., near the containment penetrations).
2. The data links between CPC channels have been extended so the channels can be located in geographically separate rooms.
3. A rod motion block signal and reactor power cutback initiation signal have been added to limit the effects of CEA related events. These signals interface to the Power Control System via the PPS Interface and Test Processor.

Example 2:

Additional design details describing the programmable logic controllers for the Engineered Safety Features Actuation System (ESFAS) are provided in the following documents:

- o NPX80-IC-SD640*, System Description for Component Control Systems (CCS) for Nuplex 80+
- o NPX80-IC-DP640-01*, Design Procedures for Component Control System Component Functional Grouping for Nuplex 80+

The Integrated Process Status Overview (IPSO) panel is described in CESSAR-DC Section 7.7.1.5.2. Additional design details describing the IPSO panel are provided in the following document:

- o NPX80-IC-SD791-01*, System Description for Control Complex Information System for Nuplex 80+

The information contained in these documents is representative of the information provided in system descriptions of all other Nuplex 80+ instrumentation and control systems. C-E considers this information final in that it is suitable for procurement of implementation hardware. Information determined to be necessary for the staff's safety finding will be included in CESSAR-DC.

Example 3:

The Emergency Operations Facility, Operational Support Center and the Laboratory Facilities, are examples of items outside the scope of System 80+. Consistent with 10 CFR Part 52, conceptual descriptions for these facilities are provided in CESSAR-DC (see the response to RAI 810.1 provided in C-E letter LD-91-013, March 15, 1991).

*This document is considered proprietary to Combustion Engineering, Inc. Access to this document will be provided to facilitate NRC staff review of CESSAR-DC. Information from this document determined to be necessary to support the staff's safety finding will be placed in CESSAR-DC in a future amendment.

Number: 420.5 (7)

Question: This question refers to the EPRI Utility Requirements Documents (URD), Chapter 10. In the LRB, C-E provides a listing of the differences between the C-E DC document and the EPRI RD. One area identified is the Advanced Control Complex. This question is a general question related to the many items listed in the EPRI RD for which the Plant Designer has a task to perform. Some of the tasks have been performed by C-E already, such as the basic system functional descriptions. Some of the tasks, such as use of simulators and selection of specific wireless communications frequency allocations, may not have been completed. This question requests C-E to address the EPRI requirements in detail and provide a listing of the tasks that have been performed or will be performed prior to design certification and identify the tasks and the interface requirements which will not be completed until after design certification.

Response: C-E has used the EPRI ALWR-URD, Chapter 10, as a basis for the design process and design of Nuplex 80+. C-E is familiar with the requirements because of its continuous participation in the development of Chapter 10. Since EPRI ALWR-URD goals, which go beyond a safety determination, shall not be imposed as regulatory requirements for individual designs (Staff Requirements Memorandum for SECY-89-311, dated December 15, 1989), we do not intend to provide a requirement-by-requirement listing of the status of Nuplex 80+ with respect to Chapter 10. We will, however, keep the NRC staff informed about the comparison of System 80+ with the EPRI URD. The key differences in the design philosophy of Nuplex 80+ compared to the EPRI design requirements were transmitted to NRC on December 21, 1990 via letter LD-90-097. In terms of the design process, C-E views conformance to Chapter 10 as an ongoing process which does not end until after plant commissioning.

Number: 420.6 (7.1.2.10)

Question: The staff agrees that fiber-optic technology provides inherent electrical fault isolation. Though the independence and separation provided by the fiber-optics will satisfy the Regulator Guide 1.75, the DC claims that the fiber-optic technology will ensure that no single credible event can propagate. Single credible events can include random bit errors or power supply loss which are not unique to fiber-optics but should still be addressed. This question requests C-E to clarify that other features are required to make a system single failure proof or that the single failure that is being addressed is limited to electrical faults.

Response: C-E agrees with NRC assessment and will reword the sentence to "no single credible electrical fault" in place of "no single credible event".

Other single credible events involving fiber-optic interconnects, such as those pointed out in the question; random bit errors, erroneous data or power supply loss are addressed in the protection system design. For example, the loss of a power supply at either end of the fiber-optic interconnect will result in the receiving end defaulting to the safe state as is the case for detectable random bit errors.

Erroneous data is addressed by the selection of bounding failure assumptions in the FMEA. Features to address multiple channel failures from data link communication errors are also addressed in responses to NRC Questions 420.17, 41, 48 and 58.

Number: 420.7 (7.1.2.10)

Question: This section states that systems are "generally" designed to fail safe for the conditions listed. Provide a list of systems or parts of systems which do not meet this philosophy.

Response: All I&C systems fail "safe" (i.e., the response to a failure does not exacerbate the event), there are no exceptions. The Plant Protection System fails in a tripped and actuated condition on a per channel basis. The Component Control Systems (Process-CCS and ESF-CCS) fail in a manner that will drive their controlled components to states that are consistent with the mechanical systems design. That is solenoid valves are driven to their de-energized position, Motor operated valves and circuit breaker operated components will remain "as-is". Contactor operated devices are driven to a deenergized state. I&C systems fail consistent with failure modes of conventional I&C systems. The word "generally" will be deleted. This subject is also discussed in response to Question 420.41.

Number: 420.8 (7.1.2.16.C.1)

- Question: (1) This section states that test modes are designed such that they do not prevent system actuation. Does this include automatic as well as manual actuation? Are operator actions required to reset from test mode to allow automatic signals to actuate safety equipment? List any exceptions.
- (2) Are there any test modes during refueling outages which require systems to be locked out for equipment or personnel protection?
- (3) Provide a detailed explanation of the test and maintenance philosophy for the I&C design with respect to minimizing the potential for human errors and spurious actions.

Response: (1) The testing functions of the PPS cannot prevent safety system actuation regardless of the method in which the actuation was created, manually or automatically. C-E response to NRC Question 420.42 describes the automatic testing process.

The bistable function analog input check, a manual test, requires operator/maintenance personnel actions. To run this test, the operator/maintenance personnel must bypass the desired trip channel. Interlocks ensure the other three redundant channels cannot be in bypass. Because the analog input test can be run-conservative, the same operator/maintenance personnel action that applies the test analog input to the selected bistable also forces the bistable output to be tripped. This protection to ensure that system actuation cannot be blocked is in addition to the single channel bypass interlock described above. Termination of the operator/maintenance personnel test action removes the forced trip and the test analog input. Removal of the forced trip and the test input would also result from the loss of the trip channel bypass or selection of a different bistable test function.

During this test, the coincidence logics (one in each of the four redundant channels) for this process trip are operating in a 2 out of 3 coincidence mode. Initiation of reactor trip or safeguard functions are not effected.

- (2) There is no I&C equipment that must be locked out during refueling; however, it is anticipated that electro-mechanical devices such as breakers will require lock-out. All lock-outs that render a safety system inoperable will be accompanied by a "system inoperable" alarm in the main control room. In accordance with Reg. Guide 1.47, this alarm will be automatically generated for all lock-outs that are expected more frequently than once per year.

- (3) The safety systems I&C design utilizes built-in automatic testing that verifies most hardware functionality without operator intervention. Failures are brought to the operator's attention via alarms by the DPS with details provided by the safety system's operator's module. Hardware not easily tested automatically, such as process instrumentation, reactor trip switchgear and safeguard actuated components, are tested by written test procedures to minimize human error. The DPS contains an application program called Computer Aided Testing (COMAT) that can be used by operator/maintenance personnel to assist in testing safeguard actuated components. COMAT records and verifies:

- Pre-test component line-ups
- Actuated component positions and response time
- Post-test restored line-ups

See CESSAR-DC Sections 7.2.1.1.9 and 7.3.1.1.8 for additional discussions regarding testing safety system I&C.

Number: 420.9 (7.1.2.16.D.1)

Question: If the non-Class 1E Data Processing System is used to monitor the critical safety system setpoints describe how the information is to be verified or validated.

Response: PPS fixed trip setpoints, or constants used in the calculation of variable trip setpoints are checked by the PPS Interface and Test Processors (ITP). Verification and Validation of ITP software is discussed in response to question 420.24. The trip setpoints are also sent to the DPS as an added defense against undesired setpoint changes.

ESF-CCS process control setpoints are periodically verified during selection group testing described Section 7.3.1.1.8.6 of CESSAR-DC. These setpoints are also sent to the DPS as an added defense against undesired setpoint changes.

Number: 420.10 (7.1.2.17.C)

- Question:
- (1) This section states that all bypasses are at the channel level. The staff understands this to mean that all intentional bypasses are input at the local coincidence logic processors. Is this correct?
 - (2) Can the process sensors, transmitters, fiber-optic links or initiation logic be bypassed individually?
 - (3) If an initiation circuit fails, is that circuit placed in trip or bypass?

Response:

- (1) No, that is not correct. The sense and command sections of all safety systems are configured as four redundant safety channels. Within a safety channel, there are multiple trip channels. A trip channel consists of a process sensor, transmitter, setpoint comparator function and the trip signal which is generated by the bistable processor and is sent to a local coincidence logic processor in each of the four redundant safety channels. The Plant Protection System portion of the sense and command section provides two methods to bypass the function of the trip channel. The two methods are referred to as "trip channel bypass" and "operating bypass". See Sections 7.2.1.1.5 and 7.3.1.1.3 of CESSAR-DC for a description and application of the two bypass methods. In summary, the operating bypass is input to the bistable processor to block generation of the bistable's trip signal output. The trip channel bypass is input to the local coincidence processor to put the processor in a 2-out-of-3 coincidence mode, thereby ignoring the bypassed trip signal input. All bypasses are input manually at the PPS operators module(s) and interface to the bistable or coincidence processor via the interface and test processors. It is noted that the functional operation of these bypasses is the same as in other C-E designs in currently operating plants.

- (2) Process sensors or transmitters can be bypassed using the trip channel bypass discussed above. If the sensor is used in more than one bistable function (i.e., high trip and low trip), each function must be bypassed to fully bypass that sensor. Like functions may be bypassed in only one channel at a time.

Fiber optic links transmitting bistable trip signals between channels cannot be bypassed directly. However, in theory a total data link can be bypassed by individually initiating trip channel bypasses for all functions in one channel (i.e., 16 trip functions). This can only be done if there are no trip channel bypasses in any other channel.

Initiation logic cannot be bypassed in any channel, in any channel.

- (3) If an initiation circuit fails it should fail-safe (i.e., in a trip condition). This will result in a partial trip (1 of 4) in the selective 2-out-of-4 ESFAS actuation logic or reactor trip breaker arrangement. The partial trip will be alarmed the same as a full ESF trip and actuation and indicated by the DIAS and DPS; the partial trip cannot be bypassed. If the initiation circuit fails in an undesired condition the failure will be promptly detected and alarmed via the automatic test function. Since the actuation functions in the RSTG and ESF-CCS work in a selective coincidence logic, this is considered a degraded condition and a technical specification LCO will apply.

Number: 420.11 (7.1.2.17.C, Figure 7.2-1)

Question: If Channel A is bypassed which sensor is bypassed, if any?

Response: As explained in response to Question 420.10, a trip channel bypass created in PPS safety Channel A is associated with one bistable trip function; not an entire safety channel, nor all functions from one sensor. For example, Channel A RPS steam generator low level trip has a Channel A RPS steam generator low level trip bypass. When this bypass is activated it blocks only the Channel A RPS steam generator low level trip signal in the RPS steam generator low level coincidence function located in each of the four redundant safety channels. It is noted that at any instant only one trip channel can be blocked, therefore, if A is blocked, B, C, and D must be active and the coincidence logics will continue to function in a two-out-of-three configuration. For the example chosen, the same steam generator low level sensor is also used for initiating the Emergency Feedwater System via an EFAS steam generator low level trip. The bypass explained above would have no impact on this trip function. This trip function would need a EFAS steam generator low level trip bypass to block its effect on the EFAS steam generator low level coincidence functions.

In summary, a sensor can only be considered fully bypassed if all trip functions associated with that sensor are each bypassed. A safety channel can only be considered bypassed if all trip functions for that safety channel are each individually bypassed.

Additional design information is found in CESSAR-DC, Sections 7.2.1.1.3 and 7.3.1.1.2.2.

Number: 420.12 (7.1.2.21.2)

Question: For this section and several others the statement is made that a function is manually initiated. This question requests C-E to clarify the intention of manual actions. These actions can range from touching an interactive display screen to physically turning valve stem wheels.

Response: The term "manually initiated" is used to indicate human intervention only. It is not intended to refer to any specific interaction mechanism. The specific subsection cited is discussing the PPS trip channel bypass indication as regards Regulatory Guide 1.47. The indication (light/no light) condition results from the bypass being manually initiated or removed (i.e., human interactions with a touch screen select device that results in the function (signal) true or false, state). For example, if the PPS-A high pressurizer pressure trip channel bypass touch target (part of the PPS-A remote operator modules and the local maintenance and test panel) is touched a true PPS-A high pressurizer pressure trip bypass signal is created and the PPS-A high pressurizer pressure trip bypass indication (part of each redundant channels' remote operator's modules and local maintenance and test panel) is turned on.

Manual initiation of reactor trip and engineered safeguards, required by IEEE-603 are discussed in the response to Q420.13.

Further discussion of human interactions with electro-mechanical or electronic devices that result in manually initiated functions (variable trip setpoint reset, operating bypass enable, safeguard system component position, etc.) are found in CESSAR-DC Sections 7.2 and 7.3 as well as C-E documents NPX80-IC-SD560* "System Description for Plant Protection System for Nuplex 80+" and NPX80-IC-SD640* "System Description for Component Control Systems for Nuplex 80+.

*This document is considered proprietary to Combustion Engineering, Inc. Access to this document will be provided to facilitate NRC staff review of CESSAR-DC. Information from this document determined to be necessary to support the staff's safety finding will be placed in CESSAR-DC in a future amendment.

Number: 420.13 (7.1.2.22)

Question: As described in this section the amount of equipment common to automatic and manual initiation is to be minimized. Describe the equipment which is common. Are there any common hardware or software modules?

Response: The amount of equipment common to automatic and manual initiation is minimized.

Manual initiation of reactor trip and engineered safety features is shown in the simplified block diagram, Figure 420.13.

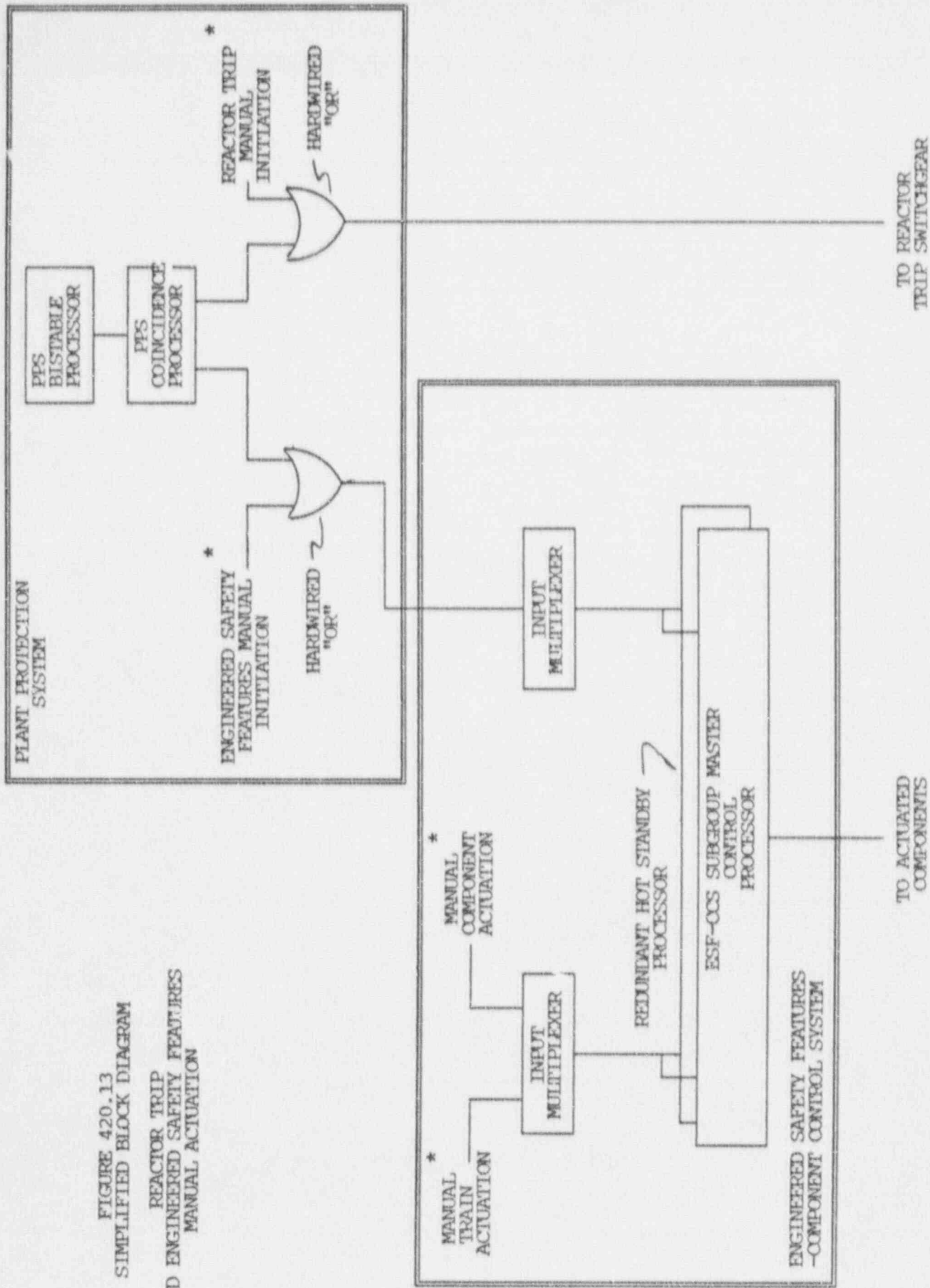
Reactor trip manual initiation is a hardwired function which interfaces with the reactor trip switchgear through hardwired circuits in the PPS cabinet. This manual initiation function does not rely on the use of computers to operate. The details of this circuit are shown in CESSAR-DC Figure 7.2-12 and Figure 7 of Appendix A of the PPS System Description, NPX80-IC-SD560*.

Similarly the ESFAS manual initiation interfaces to the ESF-CCS through hardwired circuits in the PPS cabinet. The engineered safety features manual initiation function bypasses all computers used for automatic initiation of engineered safety features (i.e., PPS Bistable and Coincidence Processors). Within the ESF-CCS one input multiplexer is common to system level manual and automatic initiation of engineered safety features. Another input multiplexer accepts manual train actuation and manual component actuation signals from the operators module and component control switches, respectively. These ESF-CCS multiplexers are independent to the extent that credible single failures will impact one multiplexer only.

The only equipment common to all engineered safety feature initiation (automatic and manual) is the subgroup master control processor. This processor utilizes a redundant hot standby processor for increased reliability. To enhance software diversity train actuation (manual and automatic) and manual component actuation signals are processed in the software logic at different levels as shown in CESSAR-DC Figure 7.3-2.

*This document is considered proprietary to Combustion Engineering, Inc. Access to this document will be provided to facilitate NRC staff review of CESSAR-DC. Information from this document determined to be necessary to support the staff's safety finding will be placed in CESSAR-DC in a future amendment.

FIGURE 420.13
SIMPLIFIED BLOCK DIAGRAM
REACTOR TRIP
AND ENGINEERED SAFETY FEATURES
MANUAL ACTIVATION



* LOCATED ON MAIN CONTROL PANEL
AND REMOTE SHUTDOWN PANEL

Number: 420.14 (7.1.2.25.A)

Question: The staff requests C-E to avoid the use of the caveat "to the extent practicable" in this section or others. With the design certification format this would be a difficult item to verify during construction as to the original scope and intent of the requirement. The staff does not disagree with the statement about subcomponents but is simply attempting to understand the design more accurately and to minimize future disagreements. What is the intent of this caveat and how would it be standardized?

Response: In Amendment I, C-E has minimized the use of the phrase "to the extent practicable" in this and other sections of CESSAR-DC. Instead, where all encompassing statements cannot be made, the specific exceptions are cited. The use of "to the extent practicable" in CESSAR-DC Section 7.1.25.A results from paraphrasing the words of Regulatory Guide 1.73, Section C.1, which states: "To the extent practicable, auxiliary equipment (e.g., limit switches) that is not integral with the valve operator mechanism but will be part of the installed valve operator assembly should be tested in accordance with the subject standard." The intent of this specific caveat is to allow the use of valves which have been qualified and used in previously licensed applications and which have subcomponents which are integrated with the valve operator.

Number: 420.15 (7.1.2.32)

Question: Describe the software verification and validation to be used for the non-Class 1E systems.

Response: The software verification and validation to be used for the non-Class 1E systems is described in the Nuplex 80+ V&V plan, document NPX80-IC-VP-790-00*. The major difference between safety systems and non-safety systems V&V is the degree to which the personnel conducting the V&V activities are independent from those personnel who are actually generating the design. This level of independence is shown in Figure 2-0 of the Nuplex 80+ V&V plan. This figure has been corrected from its original issue. A corrected copy is included herein as Figure 420.15. In summary, for non-safety systems, some V&V activities may be conducted by members of the system design team (although not the specific designers that generated the work). For safety systems all V&V activities are conducted by persons not on the design team; the designers and verifiers report to different first line managers.

*This document is considered proprietary to Combustion Engineering, Inc. Access to this document will be provided to facilitate NRC staff review of CESSAR-DC. Information from this document determined to be necessary to support the staff's safety finding will be placed in CESSAR-DC in a future amendment.

Figure 420.15

V&V Reviewers

	<u>Non-Safety</u>	<u>Important to Safety or Availability</u>	<u>Safety</u>
Functional Requirements	RT/DT or DT/VT	RT/DT or RT/VT	RT/DT&VT
System/Software Description	DT/RT or DT/VT	DT/RT or DT/VT	DT/RT&VT
System/Software Specifications	DT/DT	DT/RT or DT/VT	DT/VT
System/Software Implementation	DT/DT	DT/VT	DT/VT
Module Test Procedure	DT/DT	DT/VT	DT/VT
Module Testing	DT/DT	DT/VT	DT/VT
System Test Procedure	DT/VT or DT/RT	DT/VT or DT/RT	RT/VT
System Testing	RT/DT or VT/DT	RT/DT or VT/DT	RT/VT

Key XX/YY: XX = Originator
 YY = Reviewer

DT = Design Team
 RT = Requirement Team
 VT = V&V Team

System Sys: PPS, E-CCS, PAMI
 Important Sys: DIAS, P-CCS, PCS
 Non-Safety: DPS, NIMS, SOE

Number: 420.16 (7.1.3)

Question: This section address stable and noise free power to the I&C equipment. Are any specific standards to be referenced? What are the requirements for electromagnetic and radio frequency interference?

Response: Vital Instrumentation and Control Power Systems are addressed in CESSAR-DC, chapter 8, section 8.3. Vital Instrumentation and Control Power Systems power stability specifications are 120VAC \pm 2% regulation at full rated load and 60Hz \pm 0.5Hz, total harmonic distortion not to exceed 5% RMS, with no more than 3% distortion in any single harmonic. Typical I&C equipment specifications require 120VAC \pm 10%, 60HZ \pm 3HZ and 5% minimum harmonic distortion. For the 125VDC vital power supplies voltage regulation is required to be between 105VDC-140VDC.

Electromagnetic and radio frequency interference requirements to which I&C equipment is designed are addressed in NPX80-IC-QC790-00*, "Qualification Guidelines for Instrumentation and Controls Equipment for NUPLEX 80+" which references MIL-STD-461C, "Electromagnetic Emission and Susceptibility Requirements for the Control of Electromagnetic Interference" (sections RS03, RS02, CS01, CS02 and CS06).

*This document is considered proprietary to Combustion Engineering, Inc. Access to this document will be provided to facilitate NRC staff review of CESSAR-DC. Information from this document determined to be necessary to support the staff's safety finding will be placed in CESSAR-DC in a future amendment.

Number: 420.17 (7.1.3.E)

Question: Describe the tests and/or analyses that will be used to demonstrate that failures in non-Class 1E will not degrade the Class 1E circuits.

Response: A fault isolation qualification program is described in the following document:

- o NPX80-IC-QG790-00*, Qualification Guidelines for Instrumentation and Controls Equipment for Nuplex 80+.

The qualification program as described will be applied to demonstrate that electrical faults that might occur in non-Class 1E equipment will not propagate to potentially degrade the Class 1E circuits. Fault isolation qualification will be conducted in accordance with IEEE Std. 384-1981 as augmented by Reg. Guide 1.75 using test signal levels representative of worst case credible fault exposure levels. Testing will not be applied for fiber optic cable which inherently provides requisite electrical fault isolation.

It should be noted that, in the Nuplex 80+ designs, dataflow is unidirectional from Class 1E systems to non-class 1E systems. Separate communication processors are utilized to protect the Class 1E functional processors from handshaking and data communication errors.

Qualification for the potential effect on Class 1E systems of communication errors caused by hardware failure or software error originating in non-Class 1E systems is an integral part of software verification and validation for all Class 1E systems. Validation test methods are developed on a case by case basis and are based on the software, hardware and data protocols in use. The V&V program is described in NPX80-IC-VP790-00*, Verification and Validation Plan for Nuplex 80+.

*This document is considered proprietary to Combustion Engineering, Inc. Access to this document will be provided to facilitate NRC staff review of CESSAR-DC. Information from this document determined to be necessary to support the staff's safety finding will be placed in CESSAR-DC in a future amendment.

Number: 420.18 (7.1.3.H)

Question: Describe the difference between "deliberately made inoperable" and bypassed. Would different operator actions or technical specifications be required?

Response: In the context of Section 7.1.3.H, the terminology "deliberately made inoperable" and "bypassed" are synonymous. Both phrases imply degraded system operability. The extent of operator actions required or technical specification limitations are dependent on the extent of system degradation. For example, the bypass of a single channel of a 2-out-of-4 logic function (placing it in a 2-out-of-3 condition) would not impose a technical specification limitation, since the remaining configuration still meets the design basis single failure criteria. However, reduced functional operability such as the disabling of one train of a two-train system (i.e., Containment Spray System) would impose technical specification limitations, since the remaining configuration does not meet the design basis single failure criteria.

Number: 420.19 (Figure 7.1-4)

Question: Provide a description or drawing which shows the extent of shared taps, lines, and reference legs. Provide justification for any sharing proposed in the design.

Response: All Nuplex 80+ sensor taps, lines and reference legs are designed to meet Reg. Guide 1.151. Redundant safety channels are independent and control channels are independent of safety channels.

For the non-safety-related Alternate Protection System (APS) taps, lines and reference legs are shared with safety-related sensors. This is acceptable in accordance with Reg. Guide 1.151, since a failure in the APS or its sensing lines will not cause a plant condition requiring protective action. This is also acceptable per 10CFR50.62, since sensors are allowed to be shared between primary and back-up protection systems. This sensor arrangement is shown in the following Piping and Instrument Diagrams (P&IDs):

- o CESSAR-DC Figure 5.1.2-3, Pressurizer and Safety Depressurization System P&I Diagram.
- o CESSAR-DC Figure 10.1-2, Main Steam and Feedwater System Flow Diagram.

It is noted that in several cases, safety-related sensors are used for control through the application of electrical isolation and signal validation. This design approach has eliminated shared sensing lines between control and protection sensors that exist on previous C-E plants. This is addressed in the response to Question 420.38.

Number: 420.20 (Figure 7.1-4C)

Question: This drawing shows the Supplementary Protection System (SPS). Section 7.1.1.7 states that the SPS is being replaced with the Alternate Protection System (APS). By which name is the system to be named? Also, this drawing shows the system to be Class 1E while Section 7.7.1.1.11 shows the APS to be a non-Class 1E system. Is the system 1E or non-1E?

Response: Figure 7.1-4C depicting the Supplementary Protection System (SPS) was removed from CESSAR-DC in an earlier amendment. Section 7.1.1.7 correctly states that the SPS, a Class 1E system, is replaced by the non-1E Alternate Protection System (APS) in the Nuplex 80+ design. The APS, described in Section 7.7.1.1.11, is a non-1E system as allowed by 10CFR50.62. The correct name given to the "ATWS system" in the Nuplex 80+ design is the Alternate Protection System (APS).

Number: 420.21 (7.2.1.1)

Question: The second paragraph contains the statement that the fourth channel is provided as a spare and allows bypassing of one channel while maintaining a two-out-of-three system. Is C-E's intention to license the plant as a two-out-of-four plant in which case a bypass would be a technical specification limiting condition for operation with a time limit or is the intent to obtain the design certification based on a two-out-of-three design that would allow indefinite bypass of the spare channel? How would this be evaluated in the PRA?

Response: C-E's intention is to license the System 80+ plant for two-out-of-three trip channel operation with a fourth trip channel included as an installed spare. This approach allows indefinite bypass of any one of four trip channels without imposing technical specification limiting conditions for operation.

The PRA evaluation for the System 80+ design is based on typical plant operating modes with consideration given to the minimum number of trip channels operable. For this design, the typical number of operating trip channels is four while the minimum number of operable channels is three.

Number: 420.22 (7.2.1.1.3)

Question: The system described is a two-out-of-four system which can have one channel in bypass. This leaves a two-out-of-three configuration which allows any single failure and would still complete the logic. Provide a comparison of this design with Section 8.3.2.4 of the EPRI URD Chapter 10. This section of the EPRI document requires the reactor protection system to withstand two single failures and still perform its function. Bypass capability is not addressed. Provide a summary list of all I&C areas that differ from the EPRI URD.

Response: The RPS design of Chapter 7.2 of CESSAR-DC meets the requirements of EPRI URD Chapter 10, Section 8.3.4.2, "Effects of Failures in RPS on Protective Action." While C-E agrees that bypass capability is not addressed here, C-E believes that EPRI did not intend to preclude bypass capability. They do discuss bypass capability elsewhere in their document (Section 3). C-E believes that EPRI did not intend that two failures be accommodated with a channel in bypass.

A list and discussion of key differences between the EPRI ALWR-URD and the System 80+ standard design were transmitted to NRC on December 21, 1990 (via letter LD-90-097). That transmittal provides the key differences in the entire System 80+ design. Please see the Response 420.5 for additional information.

Number: 420.23 (7.2.1.1.8)

Question: This section states that the design will assure that predictable common mode failures do not exist. The staff agrees with this design goal but is also concerned with unpredictable common mode failures. 7.2.1.1.8.E discusses a degree of functional diversity. 7.2.1.1.8.G states that the Reactor Protection System (RPS) and Engineered Safety Features (ESF) systems use different design types which eliminate hardware and software design common cause failures. This question requests an elaboration of this statement. The staff considers software design errors to be a credible fault and, therefore, all modules which share common software design are subject to common mode failure. The information to be provided by C-E should specifically address the design features which either eliminate the potential for common mode failures between redundant channels of the safety systems or provide alternate, diverse means to accomplish the same task. One method that has been discussed is the non-safety systems which C-E has stated are designed with diverse equipment from the safety equipment. If this option is considered, C-E should address the possibility that the safety systems will not be utilized until the non-safety systems are already disabled and unable to provide a diverse method of providing a specific function. The staff notes that page A-102a A-47, "Safety Implications of Control Systems," of the DC states that non-safety grade control systems are not relied on to perform any safety functions.

Response: Section 7.2.1.1.8.G has been changed in Amendment I to state, the "Process-Component Control System and Power Control System utilize different diverse designs from the PPS and ESF-CCS." The PPS and ESF-CCS are of the same design type; similarly, the P-CCS and PCS are of the same design type. Common mode software failure concerns are addressed by the defense in depth approach described in response to Question 420.25. Specific segmentation included in the PPS and specific diversity features between control and protection systems are described below.

- (1) Segmentation Within the PPS - Whenever the reactor trip transient analysis indicates there are diverse sensors detecting the transient, the sensors are assigned to at least two different bistable and coincidence processors. In cases where there is only one sensor available to detect the event that sensor is also assigned to two processors to minimize the effects of single processor errors. This is shown in Table 1 of NPX80-IC-SD560*, Appendix A. The same approach is used for the engineered safeguard transient analysis. This is in Table 2 of NPX80-IC-SD560*, Appendix A.

*This document is considered proprietary to Combustion Engineering, Inc. Access to this document will be provided to facilitate NRC staff review of CESSAR-DC. Information from this document determined to be necessary to support the staff's safety finding will be placed in CESSAR-DC in a future amendment.

- (2) Diversity Between Control and Protection Systems - Nuplex 80+ includes diversity in the system designs as follows:

<u>Function</u>	<u>System Design Type 1</u>	<u>System Design Type 2</u>
Reactor Trip	Plant Protection System	Alternate Reactor Trip Within Process - CCS
Fluid System Controls	Emergency Success Paths (e.g., Emergency Feedwater) via ESF-CCS	Normal Success Paths (e.g., Main Feedwater via Process - CCS
Reactivity Controls	Emergency Boration via ESF-CCS	Normal CEA Control - via Power Control System
Alarm and Indication	Alarm Tiles and Discrete Indicators - via DIAS	CRT Displays - via DPS

To elaborate on this philosophy, Figure 420.23 defines all critical safety functions and identifies the plant systems available to maintain those functions (i.e., success paths) and the I&C systems that control them.

Regarding the philosophy to credit control systems for defense against common mode failures, C-E is following prior licensing precedence. The Plant Protection System and ESF-CCS in Nuplex 80+ design perform safety functions to mitigate design basis events. The ATWS rule, 10CFR50.62, set a precedence for dealing with common mode safety system failures by utilizing non-Class 1E systems to cope with beyond-design basis events. This precedence was followed in the System 80 design and is also followed in the Nuplex 80+ design as indicated in the above comparison.

It is noted that the availability of System 80+ non-safety systems is significantly improved when compared to previous licensed designs due to the addition of battery-backed power to all Nuplex 80+ control systems and the Alternate AC gas turbine generator to power the plant's non-safety mechanical systems.

C-E agrees that events can occur which would result in these non-safety systems being only partially effective. However, since these disabling events have a very low frequency of occurrence and a common mode protection system failure has a very low frequency of occurrence, the frequency of these occurring simultaneously is sufficiently low to be considered outside the design basis.

Control Function Success Path	Reactivity Control	Inventory Control	RCS Pressure Control	Core Heat Removal	RCS Heat Removal	GNMT Isolation	GNMT Environment	Indirect Radiation Release	Vital Auxiliaries
Normal Success Path (a)	1. CVCS (Boration) 2. CEA Drive Mechanism	CVCS	1. Pressurizer Heaters and Sprays 2. CVCS	RCPS	Main Feed	Control Valves	1. GNMT Fan Cooling 2. Hydrogen Recombiner	Monitoring Only	1. Nonvital AC from off site source 2. Alternate AC source 3. Nonsafety CCW
Alternate (Emergency or safety) Success Path (b)	1. RPS 2. Safety Injection	Safety Injection	1. Safety Injection 2. Safety Depressurization	1. Safety Injection 2. Shutdown Cooling	1. Emergency Feedwater 2. Atmospheric Dump Valves 3. Safety Depressurization	CIAS Actuation	GNMT Spray	Monitoring Only	1. Vital AC from off site source 2. Emergency Diesel Generators 3. Safety Related CCW

- (a) Type 2 Nuplex 80+ Systems - PCS or PCCS
(b) Type 1 Nuplex 80+ Systems - PPS or ESF-OCS

SYSTEM 80+ CRITICAL FUNCTION SUCCESS PATH DIVERSITY
FIG. 420.23

HWRFCUS.FRM
03/21/91

Number: 420.24 (7.2.1.1.9)

Question: This section states that the automatic testing does not degrade the ability of the RPS to perform its intended function. Describe the verification and validation of the testing software. Is the automatic test feature qualified as Class 1E?

Response: The RPS automatic testing is not considered a Class 1E function; however, the test software is designed, verified and validated in accordance with the same program as the RPS trip software which is Class 1E. This verification and validation program is described in the following document:

- o NPX80-IC-VP790-00*, Verification and Validation Plan for Nuplex 80+.

The RPS is qualified to ensure that the test software cannot impact RPS performance under valid trip conditions. The test system is designed to Class 1E requirements that include channel independence, seismic integrity and verification and validation. It is only demonstrated, however, that the test system will not impede RPS operation during design basis events. This approach is taken because historically, hardware supporting the RPS trip functions is considered Class 1E while hardware for RPS testing has not been considered Class 1E.

Periodic manual testing is used to confirm proper operation of the automatic test system for Nuplex 80+.

*This document is considered proprietary to Combustion Engineering, Inc. Access to this document will be provided to facilitate NRC staff review of CESSAR-DC. Information from this document determined to be necessary to support the staff's safety finding will be placed in CESSAR-DC in a future amendment.

Number: 420.25 (7.3.1.1.6)

Question: C-E is also requested to address in greater detail the design features that eliminate common mode software errors as a concern for the ESF I&C systems.

Response: C-E employs a defense in depth approach to eliminate common mode software errors as a concern for the Nuplex 80+ instrumentation and control systems. This approach is summarized as follows:

Deterministic Design - The algorithm execution in the Nuplex 80+ control and protection systems is deterministic. This means that all data is updated on a continuous cycle and all programs execute on a continuous basis, without interrupts. This approach makes the software easier to design, verify and validate. The potential for hidden errors is significantly lower than in other designs which include multi-tasking, event based execution, event based data communication, or interrupts. None of these non-deterministic features exists in the Nuplex 80+ control and protection systems.

Field Proven Products - Operating system software for Nuplex 80+ I&C systems is selected with three (3) years minimum of field experience in similar applications. These products are mature and, therefore, judged to be free of infant design errors.

Verification and Validation - For custom software generated by C-E, a comprehensive V&V program is employed, including independent document review and independent test. C-E has been using this approach to produce reliable, qualified Class 1E CPC software for more than fifteen (15) years. The V&V program for Nuplex 80+ is described in the following document:

- o NPX80-IC-VP790-00*, Verification and Validation Plan for Nuplex 80+.

Application software is subjected to the rigorous V&V program defined above. Independence is maintained between software development and verification personnel. Utility-Owner configuration controls are also imposed throughout the software life cycle. The V&V program minimizes the potential for introduction of common mode software errors during the design phase and during commissioned life of the system.

*This document is considered proprietary to Combustion Engineering, Inc. Access to this document will be provided to facilitate NRC staff review of CESSAR-DC. Information from this document determined to be necessary to support the staff's safety finding will be placed in CESSAR-DC in a future amendment.

Segmentation - Within all Nuplex 80+ systems, including the PPS ESF-CCS, and Process-CCS functions are divided into separate processors. Segmentation within each PPS channel ensures that two different trip functions are available in two separate processors for each design basis event. Similarly, within ESF-CCS Trains A and B, ESFAS functions such as SIAS and EFAS are distributed to separate control processors. Within the Process-CCS critical plant control functions, such as inventory control, heat removal, etc., are distributed to separate control processors. The potential for simultaneous errors in these multiple processors is minimized, since functional diversity is utilized and since software execution is asynchronous.

Diversity - Diversity offers the final defense against common mode failures. All critical safety functions, such as reactivity control, inventory control and heat removal, can be controlled by both the control systems and the protection systems. These systems are functionally diverse, as are the fluid/mechanical systems they control. In addition, to correspond with the hardware diversity of these fluid/mechanical systems, C-E employs both hardware and software diversity between control and protection I&C systems to eliminate the potential for common mode failures. This diversity exists in all software based aspects of these systems, including processors, multiplexers, communication networks and MMI devices. This same diversity philosophy is applied between DIAS and DPS to ensure availability of control room information. Additional diversity information is given in the response to NRC Question 420.37.

Number: 420.26 (7.4.1.1.9.3)

Question: The Safety Injection System (SIS) and Chemical and Volume Control System (CVCS) are diverse. Does this diversity include the I&C portions?

Response: Instrumentation and controls for the Safety Injection System (SIS) and Chemical and Volume Control System (CVCS) are diverse. The SIS is controlled by the Class 1E ESF-CCS while the CVCS is controlled by the non-Class 1E Process-CCS. These two I&C systems are diverse in both hardware and software. The diversity is applied in all software-dependent hardware elements such as CPU's, memory and datalinks. Diversity is not employed for components where extensive operating experience is known such as wire and switches.

Number: 420.27 (Table 7.5-3)

Question: The Reactor Coolant System (RCS) Boron Concentration is shown with a range of 0-5000 ppm. RG 1.97 has a range of 0-6000 ppm for this parameter. Exceptions from RG 1.97 guideline should be specifically noted and justified.

Response: 0-5000 ppm for the upper end of the boron concentration is consistent with C-E's System 80 design as implemented at Palo Verde. The diluted boron concentration for System 80+ for cold refueling conditions is 2150 ppm and SIS tank boron concentration is 2000-4400 ppm; therefore, the extended range to 6000 ppm is unnecessary and would not be utilized. Reducing the range to worst-case useful levels results in increased accuracy in concentration readings.

Number: 420.28 (7.7)

Question: Section 7.7.1 address the IPSO, Data Processing System (DPS), and Discrete Indication and Alarm System (DIAS) in the Advanced Control Complex. Section 7.7 is titled "Control Systems Not Required For Safety." This question requests C-E to provide a drawing or listing which clearly delineates the safety grade and non-safety grade displays and controls in the main control room.

Response: Each of the Nuplex 80+ system functions have been analyzed to determine the characteristics it must have to meet the required sections of regulatory guides and standards that apply to that system (Reg. Guide 1.97, NUREG-0696, NUREG-0737, IEEE-497, etc.) as well as desired reliability and performance characteristics. The following chart provides a definition of the key characteristics associated with the Nuplex 80+ indication and control systems:

Non-1E/Category I (PCS, Process-CCS, DPS)

- No Credited Redundancy
- Non-seismic (with exception of MCP/RSP mounted equipment)
- Joint Verification
- Joint Validation
- Multi-task CPUs
- Interrupt Driven (Process-CCS, DPS)
- Minimum Interrupts (PCS)
- Not Completely Deterministic
- On-line Changeability
- Non-restrictive Data Communications (Process-CCS, DPS)
- Limited Restrictive Data Communications with Isolation (PCS)

Non-1E/Category II (DIAS-P, DIAS-N)

- Redundancy thru Systems
- Seismic Design
- Independent Verification
- Independent Validation
- Independent QA
- Complete Configuration Control
- Corrective Actions Program
- Multi-task CPUs
- Minimum Interrupts
- Deterministic Performance
- Off-line Changes Only
- Restricted Data Communications with Isolation

Class 1E/Safety (rPS, ESF-CCS)

- Channelized Redundancy
- Seismic
- Independent Verification

- Independent Validation
- Independent QA
- Complete Configuration Control
- Single Task CPUs
- No Interrupts
- Deterministic Design
- Off-line Changes Only
- Read-only Data Communications with Isolation

Number: 420.29 (Figure 7.7-6)

Question: Provide a description of the capabilities of the load dispatcher. Does this design include the capability of a remote load dispatcher to move control rods or otherwise directly affect plant operation?

Response: The load dispatcher does not have the capability to directly move control rods. The dispatcher can, however, effect plant operation using the Megawatt Demand Setter (MDS). When the MDS is in the Automatic Dispatch System (ADS) mode, the load dispatcher can demand turbine load changes which are limited by the MDS to within operating limits of the NSSS and BOP systems. The MDS continuously calculates available NSSS and BOP operating margin based on trip margins from the PPS and operating margins from the Core Operating Limit Supervisory System. If adequate margin exists, the dispatcher's loading request is sent by the MDS to the turbine control system. The NSSS will then respond by following turbine load. Failures of the MDS, such as erroneous demands, are bounded by worst case turbine control system failures which are accommodated in the plant safety analysis. The Nuplex 80+ MDS design is equivalent to the MDS designs for Arkansas Nuclear One - Unit 2 and Louisiana Power and Light Waterford Unit 3. The MDS is described in CESSAR-DC Section 7.7.1.1.3 and in the following document:

- o NPX80-1C-SD650*, System Description for Megawatt Demand Setter for Nuplex 80+

*This document is considered proprietary to Combustion Engineering, Inc. Access to this document will be provided to facilitate NRC staff review of CESSAR-DC. Information from this document determined to be necessary to support the staff's safety finding will be placed in CESSAR-DC in a future amendment.

Number: 420.30 (Appendix A, page A123d, I.D.4)

Question: This section of the Control Room Design Standards in the DC note that the control room should be designed only after a full analysis of the control tasks has been performed. This is similar to many of the EPRI requirements which require many designer tasks early in the design. Has this specific analysis been performed and is it available for review?

Response: A gross functional task analysis was performed prior to design of the main control room and panel arrangements for Nuplex 80+. A functional analysis was performed for the System 80+ design followed by a detailed task analysis to support the detailed design of the RCS panel controls, alarms and displays. The methodology and examples of the results are provided in Section 18.5 of CESSAR-DC. The full task analysis report is available in Volumes 7 and 8 of the Nuplex 80+ Reference Design Documentation (NPX80-IC-DP-790-02*). It is available for review and is based on previous task analysis methodology approved by NRC as part of the Detailed Control Room Design Review Process (see CEN-307). The same task analysis methodology, and control, alarm and display methods are extended to each panel in the control room.

*This document is considered proprietary to Combustion Engineering, Inc. Access to this document will be provided to facilitate NRC staff review of CESSAR-DC. Information from this document determined to be necessary to support the staff's safety finding will be placed in CESSAR-DC in a future amendment.

Number: 420.31 (7)

Question: Provide the verification and validation (V&V) plan that is being used for the development of the Nuplex 80+.

Response: Verification and validation of the Nuplex 80+ man-machine interface is described in CESSAR-DC Section 18.9. The Verification and Validation Plan for Nuplex 80+, NPX80-IC-VP-790-00*, Revision 00 provides additional information and is available (for review) in the Nuplex 80+ Reference Design Documentation*.

*This document is considered proprietary to Combustion Engineering, Inc. Access to this document will be provided to facilitate NRC staff review of CESSAR-DC. Information from this document determined to be necessary to support the staff's safety finding will be placed in CESSAR-DC in a future amendment.

Number: 420.32 (7)

Question: Provide the V&V plan that will be used for the ESF I&C systems. In particular address the verification and validation of commercially purchased components. Of specific interest to the staff is the method to be used by C-E to qualify the distributed microprocessors (PLCs). for example, if a PLC is provided by a company which in turn used chips and instruction sets from a subvendor, describe the method by which the end user would be notified of an error in the original instruction set.

Response: V&V for the ESF-CCS is in accordance with the generic Nuplex 80+ V&V plan provided in response to 420.31. Regarding the use of commercially purchased components, including software based products such as PLC's, C-E has established a commercial component dedication process that is controlled by our internal Quality Assurance Program (NRC approved).

With respect to hardware, the program includes testing and/or analysis of commercial components to demonstrate qualification for intended use and configuration controls to ensure conformance of nth-of-a-kind components. These configuration controls include incoming inspections and/or tests. In cases of complex products, C-E verifies the acceptability of configuration controls, failure analysis and corrective action reporting methods used by the original equipment manufacturer.

The commercial software dedication process is similar. Commercial software is procured only from suppliers that have an acceptable software development process which includes testing, configuration control and error/corrective action reporting. C-E then verifies the acceptability of the software through baseline (see response to 420.32) and module level application testing and then conducts validation testing at the system level. Throughout this dedication process the procured software is maintained under C-E's own configuration and error reporting control.

In response to the specific question addressed, "...describe the method by which the end user would be notified of an error in the original instruction set.", for both hardware and software, C-E reviews and accepts the original suppliers internal QA program. This program must include error and corrective action reporting to C-E. Upon notification of software errors (or hardware errors), C-E would then evaluate the impact of these errors on our specific application(s) of the product and notify our customers accordingly. If appropriate, a 10 CFR Part 21 report to the NRC would also be generated.

C-E's QA program is designed to minimize and detect defects. However, a more significant factor contributing to overall reliability is that Nuplex 80+ employs only proven products. A proven product is defined as equipment or commercial software which

has been in the field for at least 3000 operating years or has an equivalent installed base (e.g., 3000 units for 1 year). It is generally believed that this is sufficient time to detect errors in both software and hardware.

Number: 420.33 (7)

Question: Provide a description of the method used by C-E to assure that the compilers, assemblers, debuggers, and other tools used by C-E and software suppliers are reliable.

Response: In order to assure that compilers assemblers, debuggers and other tools used by C-E to develop and test software are reliable the following method is implemented. Procured products are logged into a record keeping (tracking) system on receipt. The product is then tested using existing proven software. On successful completion of these tests it is then released for custom software development use. Errors during use are logged and tracked along with any potentially damaging results and corrective actions. Software problem reports are then generated and submitted to the originating company. Problems are followed up for resolution and subsequent product revision. Each new revision goes through the same process as a new product before release for development use.

Regarding reliability assurance of software development tools used by suppliers, C-E does not impose specific reliability controls. However, it is noted that C-E uses the same baseline testing process described above for new revisions of procured executable software. Therefore, errors in the supplier's development tools can be detected before the software products are released for use within C-E.

Number: 420.34 (7)

Question: Identify any design standards, other than those required by the NRC, that are used for this design.

Response: The Nuplex 80+ design utilizes primarily commercial products. The product documentation references numerous industry design standards other than those required by the NRC. Those standards which are specifically required to ensure the safety of the design are referenced in CESSAR-DC, Section 7.1. Additional industry standards which relate to product durability, not safety, are only specified in the individual system documentation, based on their applicability to the system, the nuclear industry, and past experience. Typical families of standards which are referenced include the following:

AISI	American Institute of Steel Construction
ANS	American Nuclear Society
ANSI	American National Standards Institute
ASME	American Society of Mechanical Engineers
ASHRAE	American Society of Heating Refrigeration & Air Conditioning Engineers
AWS	American Welding Society
EIA	Electronic Industries Association
HFS	Human Factors Society
ICS	Industrial Controls & Systems
IEEE	Institute of Electrical & Electronic Engineers
ISA	Instrument Society of America
IPCEA	Insulated Power Cable Engineers Association
MIL-STD	Military Standards
NEC	National Electric Code
NEMA	National Electrical Manufacturers Association
NFPA	National Fire Protection Association
NRC	NUREGs
UL	Underwriters Laboratory

Number: 420.35 (7)

Question: Describe the method to be used to measure or estimate the reliability/availability of the safety system I&C components and subsystems. Of particular interest to the staff is the reliability of microprocessors, software, Cathode Ray Tubes (CRTs), plasma displays, fiber-optic links and any other relatively new technology used in this design.

Response: Reliability/availability of all Nuplex 80+ I&C components and subsystems is established in the following way. Each component vendor supplies mean-time between-failure (MTBF) and mean-time-to-repair (MTTR) information on their products. Due to the field proven requirement for any products used in Nuplex 80+ this information is readily available. This information is then used in an availability analysis of the particular system. Parallel or backup systems or components are provided to achieve high availability. In addition to designing for random failures, diversity between similar systems is also provided as in the case of the Data Processing System (DPS) and the Discrete Indication and Alarm System (DIAS) or the Control and Protection Systems, to provide defense against common mode failures.

Number: 420.36 (7)

Question: Describe the organizational relationship and the degree of independence between the people doing the verification and validation work and the software development team. At what point in the organization do they share a common manager?

Response: The independence requirements for V&V activities are provided in the NPX80+ plan, document NPX80-IC-VP790-00*, section 2.3. This document refers to the Requirements Team (RT), Design Team (DT) and Verification Team (VT). Per section 2.3, as a minimum, the RT and DT must have separate first line managers from the VT. AT C-E it is also common that the RT and DT have separate first line managers. In some cases the second line managers for all three teams are also unique.

*This document is considered proprietary to Combustion Engineering, Inc. Access to this document will be provided to facilitate NRC staff review of CESSAR-DC. Information from this document determined to be necessary to support the staff's safety finding will be placed in CESSAR-DC in a future amendment.

Number: 420.37 (7.2.1.1.8)

Question: Provide a defense-in-depth analysis. An acceptable methodology is described in NUREG-0493, "A Defense-in-Depth and Diversity Assessment of the Resar-414 Integrated Protection System," March 1979.

Response: Defense-in-depth analysis is addressed in the NPX80-IC-SD560*, "System Description for Plant Protection System". In the PPS there are two bistable processors in each of the four PPS channels, each performing multiple bistable functions. Each bistable processor is assigned process measurements for comparison based on a transient versus mitigating process analysis. Process measurements available for mitigating a transient are assigned to at least two different bistable processors. The CPC, which is diverse from the bistable processors, uses direct process measurements in their comparison logic and provides results directly to the coincidence processors. The CPCs are included in this analysis. A typical analysis matrix for reactor trip and ESF are shown on Attachments 1 and 2 which are taken from NPX80-IC-SD560*.

The Nuplex 80+ defense-in-depth approach for protection against common mode failure is further addressed in responses to Questions 420.23 and 420.25.

*This document is considered proprietary to Combustion Engineering, Inc. Access to this document will be provided to facilitate NRC staff review of CESSAR-DC. Information from this document determined to be necessary to support the staff's safety finding will be placed in CESSAR-DC in a future amendment.

SYS80+ RT FUNCTION vs TRIP PROCESSOR ASSIGNMENT

	TRIPS	SG1	SG2	CONT	SG1	SG2	SG1	SG2	SG1	SG2	PZR	PZR	LOG	DNBR	LPD	VORT	CONT	
		Lo	P	Lo	P	Lo	P	Lo	P	Lo	P	Lo	P	Lo	P	Lo	P	
TRANSIENTS																		
FW temp decrease		1*		2*												CPC*	CPC	1
FW flow increase										1	2					CPC	CPC	
Main steam flow increase		1		2												CPC	CPC	1
IOSGADV		1		2												CPC		
SLB i/o containment		1		2												CPC		
LOL													1,2					
TTRIP													1,2					
Loss of cond vacuum										1	2		1,2					
MSIV closure													1,2					
Loss of non-emerg AC to station aux																CPC		
Loss of norm FW flo						1	2						1,2					
Loss of RC flow																CPC		
1 RCP seizure																CPC		
RCP shaft break								1	2									
Uncont CEA withdraw at low pwr													1,2			CPC	CPC	1
at power																CPC		
1 f/! CEA drop																		
s/u of inactive RCP																		
Core flow rate incr																		
Inadvert deboration													1,2	2		CPC	CPC	1
CEA ejection																		1
CVCS malfunction													1,2					
SG tube rupture																CPC		
LOCA												2				CPC		

1* - BISTABLE PROCESSOR 1
2* - BISTABLE PROCESSOR 2
CPC* - CORE PROTECTION CALCULATOR

TABLE 1

System 80+ RT Function vs Trip Processor Assignment

SYS80+ ESF FUNCTIONS vs TRIP PROCESSOR ASSIGNMENTS

\	TRIPS	SG1	SG2	CONT	SG1	SG2	SG1	SG2	SG1	SG2	PZR	PZR	LOG	DNBR	LPD	VORT	CONT
		lo P	lo P	hi P	lo L	lo L	dp	dp	hi L	hi L	lo P	hi P	PWR	lo	hi		hi hi
TRANSIENTS \																	
FW temp decrease																	
FW flow increase																	
Main steam flow increase																	
IOSGADV																	
SLB i/o containment		1*	2*		1	2					2						
LOL																	
TTRIP																	
Loss of cond vacuum					1	2					2						
MSIV closure																	
Loss of non-emerg AC to station aux					1	2											
Loss of norm FW flo					1	2											
Loss of RC flow																	
1 RCP seizure																	
RCP shaft break																	
Uncont CEA withdraw at low pwr																	
at power																	
1 f/l CEA drop																	
s/u of inactive RCP																	
Core flow rate incr																	
Inadvert deboration																	
CEA ejection											2						1
CVCS malfunction											2						
SG tube rupture				1	1	2					2						
LOCA											2						

1* - BISTABLE PROCESSOR 1
2* - BISTABLE PROCESSOR 2

TABLE 2

System 80+ ESF Function vs Trip Processor Assignments

Number: 420.38 (7.2.2.3.2)

Question: Identify the specific sensors which will be shared between safety and non-safety systems and justify the design philosophy.

Response: Class 1E sensor analog signals (A, B, C, D) identified in Table 7.2-3 of CESSAR-DC are isolated (by qualified 1E isolators) and are then used in calculating a valid process representation value which is then used by the control systems.

This design approach is used for the following reasons:

1. The control system will take action based on a calculated signal that reflects the average of all good process signals, not a specific signal. Therefore, there will be fewer challenges to plant safety due to control system errors, since:
 - a. Higher reliability of 1E sensors.
 - b. Deviating sensors will be detected and eliminated before they adversely impact control system performance.
2. Fewer plant sensors result in:
 - a. Fewer penetrations into mechanical systems resulting in fewer potential leak sources.
 - b. Reduced calibration and maintenance requirements resulting in reduced radiation exposure.
3. Fiber optic isolation and signal validation allow the benefits described above without creating sources of single failures that can cause erroneous control system actions and concurrent degraded protection system performance. Therefore, the control/protection interaction requirements of IEEE-279 are met in this design.

Number: 420.39 (Table 7.2-5)

Question: Describe the analysis done to ensure that erroneous data cannot prevent a Departure from Nuclear Boiling Ratio (DNBR) or power density trip.

Response: The CPC data link design is the same as on previous C-E plants. The Core Protection Calculator Sub-system consists of four Trip Limit Calculators (TLCs) and two Control Element Assembly Calculators (CEACs). Each CEAC monitors all the CEA positions and calculates subgroup deviation penalty factors for different CEA configurations. The penalty factors are sent from each CEAC to all TLCs via serial data links. Any failure leading to all zeros (0) or ones (1) are invalid penalty factors and by design will be interpreted by the TLC as a CEAC failure. In addition, there is also parity check on each TLC/CEAC data link as part of the signal validation which is also used to detect a CEAC failure.

When the TLC determines that both CEACs are operable, the TLC applies the more conservative penalty factors from the two redundant CEACs in the local power density and DNBR calculation. If the TLC detects a failed CEAC, it alarms the condition and applies the penalty factors from the one remaining CEAC. If the TLC detects the remaining CEAC to also have failed, it applies the maximum possible penalty factor after a short time delay (discussed below). This penalty factor will result in a reactor trip under all operating conditions (with the exception of some extremely low power configurations). Each TLC will also alarm if the penalty factors from the two CEACs are different. Operators can remove deviating or failed CEACs from service. Restricted operation may continue under Technical Specification LCO with one or two CEACs failed or out of service. The time delay identified above is intended to allow the plant to reach the LCO prior to the trip occurring.

Number: 420.40 (7.2.1.1.7.2)

Question: The Control Element Assembly (CEA) positions are monitored by two diverse methods. Describe the diversity for the equipment from the reed switches/rod drive position to the position displays and associated calculators.

Response: CEA position monitoring is provided by diverse methods in the Power Control System (PCS) and by an additional diverse method in the Core Protection Calculators (CPC).

In the PCS the Automatic Timing Modules (ACTMS) monitor the load current through each of the CEDM Electro-magnetic coils, for each drive motor. Specific signatures in the load current wave forms are indicative of movements in the latching mechanisms inside the CEDM. The signatures are monitored by the ACTM to detect engaging, lifting and releasing of the upper and lower latch mechanisms. The ACTM detects these mechanical actions to ensure correct closed loop control of the CEDM for each step of CEA motion. From these mechanical actions, the ACTM can also determine when each insertion or withdrawal step has been completed. The ACTMS transmits the insertion/withdrawal step completion data for each CEDM to the Power Control Processors which calculate each CEA's position based on an accumulation of CEDM motion information.

In addition, the PCS monitors a direct rod position measurement from the Reed Switch Position Transmitter (RSPT) on each CEA. This contact information for Upper Electrical Limit (UEL), Lower Electrical Limit (LEL), and Dropped Rod Contact (DRC) is diverse from the previously discussed CEDM motion sensing. The RSPT information is transmitted to the Power Control Processors which use these limits to calibrate the previously described calculated CEA position. The resulting calculated CEA position is provided to the CEA Display Processor for CEA position display via the PCS Operators Module Located on the main control panels; and to the Data Processing System (DPS) for position display via CRT, and for use in the Core Operating Limit Supervisory System (COLSS) algorithms and the CEA position validation algorithms described below.

In a diverse monitoring method the CPCs utilize the resistance bridge portion of the RSPT provided for each CEA which is another direct method. Each of the redundant RSPT associated with a given CEA are wired to one of four channelized CEA multiplexers. Each CEA has an RSPT that is wired to two different channels of CEA multiplexers. The CEA multiplexers are fiber optic data linked to CEA Calculators (CEAC) located in CPC Channels B and C, and to the Trip Logic Calculator (TLC) of the same channel. The CEACs and the TLCs are fiber optic data linked to their respective channel's CPC Operator's Module located on the Main Control Panels, where the CEA position determined by either the TLC or CEAC can be displayed. The CEA position data from the CEACs is also transmitted to the

Plant Protection System (PPS) Interface and Test Processors (ITP). The ITPs are fiber optic data linked to the DPS which uses the redundant position data in the CEA position validation algorithms described below.

Using the direct redundant RSPT position information from the CEACs and the calculated position information from the PCS, the DPS calculates a validated position for each CEA. This position is displayed in a dynamic bar graph type graphic picture which is available on CRTs in the main control room.

Additional details on CEA position information in the PCS, CPC and DPS can be found in the following Nuplex 80+ documents:
 NPX-IC-SD630*, "System Description for Power Control System for Nuplex 80+;"
 NPX80-IC-SD570*, "System Description for Core Protection Calculators for Nuplex 80+;" and
 NPX80-IC-SD710*, "System Description for the Data Processing System for Nuplex 80+."

*This document is considered proprietary to Combustion Engineering, Inc. Access to this document will be provided to facilitate NRC staff review of CESSAR-DC. Information from this document determined to be necessary to support the staff's safety finding will be placed in CESSAR-DC in a future amendment.

Number: 420.41 (7.3.2.4)

Question: The Failure Modes and Effects Analysis (FMEA) provided in Table 7.2-5 does not adequately address failure modes other than total failure such as loss of power. Address system stall, lockup, runaway, degraded power supplies (voltage, frequency), power fluctuations, timing errors, etc. For example, data communication modules can send incorrect data as well as simply failing to send any data at all.

Response: The Failure Modes and Effects Analysis (FMEA) provided in CESSAR-DC Table 7.2-5 addresses all possible outputs from computers (e.g., communication failures); not all of the possible causes of the output conditions.

At the hardware interface level for all computers, the FMEA bounds all cases by considering the worst case effects at the computer outputs. For binary outputs, open and closed status is addressed. For digitized data, interfaces are analyzed for failure to transmit data, failure to receive data and communication of erroneous data.

In the case of the ESF-CCS, loss of data communications with multiplexor output modules results in fail safe output operation. Fail safe is defined as the state corresponding to the electrical failure mode of the controlled mechanical equipment (e.g., solenoid valves fail open or closed, motorized valves fail as-is, etc.). Loss of data communication with multiplexor input modules or loss of data link inputs generally results in continued control system operation with the last good input data. Specific exceptions to this are for equipment investment protection inputs and ESF actuation inputs from the PPS, which continue to control system operation with the input data set to its most conservative value. All data communication failures are alarmed.

Number: 420.42 (7.1.2.17)

Question: Describe the self-diagnostic features of the system. Describe which diagnostics are run on-line, in background or in maintenance (bypassed) mode. Describe the actions taken when an on-line diagnostic system detects an error.

Response: Reactor Trip System (RTS) and Engineered Safety Features Actuation System (ESFAS) functions are implemented in the Plant Protection System (PPS) and Engineered Safety Features - Component Control System (ESF-CCS). Two types of self-diagnostic testing are performed in the PPS and ESF-CCS.

The first level of testing functionally exercises the trip path logic for RTS and ESFAS to continuously verify operability of trip functions. This on-line testing is periodically initiated by the Interface and Test Processors (ITP) which are separate from the system trip path processors. Bypasses are not employed in the operation of this test feature. The ITP transmits test inputs to the trip processors. These test inputs correspond to the actual plant inputs. The trip logic always selects the most conservative of these signals (test or actual) and processes that signal in the remainder of the trip logic. Only one channel is tested at a time, such that trip signals are generated in only one channel. Since the test signal momentarily places the trip path logic in a trip condition, the occurrence of an actual trip cannot be blocked. Failure of the test criteria is annunciated via the DPS and DIAS. No additional automatic action is taken by the system.

The second level of self-diagnostic testing is the continuous automatic test of the PPS and ESF-CCS hardware. PLC equipment will be used for implementation of the PPS and ESF-CCS. This equipment does not utilize multi-tasking processors; therefore, testing is performed for a short millisecond duration at the end of each processor scan cycle. This testing is not run in background or in a bypass mode.

Typical examples of "self-health" test criteria are given as follows:

- AC Power On
- Processor Running
- Memory Parity Check
- Hot Standby Controller Active
- Program Checksum
- Memory Protect Status
- I/O Communications Active
- I/O Module Check

All self-diagnostic errors are annunciated via the DPS and DIAS.

Errors that have the potential to degrade system performance cause the system to assume a fail safe condition. Examples of this error type are:

- I/O Module Failure
- Memory Checksum Error
- Loss of I/O Communications (see response to 420.41)

Errors that only affect system robustness are annunciated but will not cause the system to assume a fail safe condition. Examples of this error type are:

- Loss of Redundant Processor
- Loss of Redundant Power Supply
- Memory Protect Battery Low

It is noted that trip processing does not occur during this self-health testing; however, the short delay imposed by these tests is accounted for in the overall system response time credited in the safety analysis.

Number: 420.43 (7)

Question: Describe the data bus used in the multiplexors. Provide enough detail to demonstrate that the multiplexors are not a single failure point. The previous question concerning common mode software errors will also be considered in the staff evaluation of the multiplexors.

Response: Multiplexors utilize an internal bus architecture to process several I/O points per multiplexor chassis. The I/O data that is serviced by the bus is then directed by a communications processor over a multi-drop serial network to a central processing unit (CPU) which serves several multiplexor chassis.

Multiplexors are totally independent between redundant safety channels and between safety and control channels. All IEEE-384 and Reg. Guide 1.75 criteria are met; therefore, multiplexors are not a source of single failure that could compromise channel independence.

Multiplexors are totally diverse in both hardware and software between safety and control systems, thereby eliminating the potential for common mode software errors.

Within an individual safety or control channel the design is such that a credible single failure will not degrade more than one multiplexor. To address this multiplexor failure susceptibility, I/O signals are assigned to separate multiplexor chassis to limit failure impact to a small set of functions. This I/O assignment methodology for the ESF-CCS and Process-CCS is presented in the following document:

- o NPX80-IC-DP640-01*, Design Procedure for Component Control System Component Functional Grouping for Nuplex 80+

Impact of single multiplexor failures on the PPS and ESF-CCS have been assessed and are defined in the failure Modes and Effects Analysis (FMEA) Table 7.2-5 of CESSAR-DC.

*This document is considered proprietary to Combustion Engineering, Inc. Access to this document will be provided to facilitate NRC staff review of CESSAR-DC. Information from this document determined to be necessary to support the staff's safety finding will be placed in CESSAR-DC in a future amendment.

Number: 420.44 (7)

Question: Are watchdog timers provided in the microprocessors: Describe the reset cycle and actions on timeout.

Response: Watchdog timer functions are built into all systems using three basic methods:

1. Processors that directly generate control or protection outputs as a binary or analog discrete interface (i.e., not digitized data communication) employ watchdog timers to force the outputs to a pre-determined state upon time-out. Examples of these are:

PPS - Bistable and coincidence processors
CCS - Segment processors

2. Processors that generate digitized data, interfaced to other control/protection processors rely on the data communication link to serve as the watchdog timer function. If the generating processor fails, the receiving processor will detect this via a communication link error. The receiving processor will then take the pre-programmed control action. In most cases, this would be to alarm the failure and continue the control algorithm with the last good communicated data. Examples of this are:

PPS - Interface and Test Processor trip channel bypass signals to the Coincidence Processors
CCS - Division Master Processor interface to the segment processor

There are also cases where a failure in the communication link will result in pre-defined data states, which may cause a deviation in the control actions. Examples of this are:

PPS - Interface and Test Processor auto test signals to coincidence processor

CCS - Inter-segment processor signals

3. Processors that generate operator displays are monitored via data communication links as described in item 2 above. In addition, the display itself provides an indication that the data is being continuously refreshed. This may be in the form of a dynamic ICON or simply a time of day field.

Number: 420.45 (7)

Question: Describe the provisions that have been put in place to assure that commercial equipment dedicated for Class 1E use is free of viruses.

Response: Responses to Questions 420.23 and 420.33 describe C-E's V&V activities, QA audit process, testing and log of all software problems, and software configuration management. These activities can be relied upon to maintain a virus-free environment.

Number: 420.46 (7.1.1.7)

Question: This section describes the description of the difference between the System 80+ and Palo Verde design. In addition to the few system level differences listed, this section (and ESF) should be expanded to note the very significant differences in design.

Response: In both the Palo Verde and System 80+ the functions are the same; however, the System 80+ implementation expands the use of technology utilized in the Core Protection Calculators (CPCs) to other systems. This technology transfer from the CPCs includes computer processing, fiber optics and multiplexing, will be expanded in a future revision to CESSAR-DC Section 7.1.1.7.

In the Palo Verde Reactor Protection System (RPS) design both the Plant Protection System (PPS) and the Engineered Safety Features Actuation System (ESFAS) are relay-based hardwired systems. In the System 80+ both the PPS and Engineered Safety Features Component Control System (ESF-CCS) are computer based systems, with the ESF-CCS utilizing the advantages of remote multiplexing. Use of computer based technology allows the System 80+ RPS system to remain functionally identical to the proven RPS design, while utilizing off-the-shelf commercially available equipment vs. equipment of custom design and manufacture. This computer based technology also provides the capability for enhanced features such as automatic continuous on-line testing, and utilization of fiber optic technology for isolation between protection system channels, and between equipment cabinets and operator's modules in the Main Control Room.

Number: 420.47 (7.3.1.1)

Question: Provide the protocol, configuration, and modes for the communication networks.

Response: Two network types are used in the Engineered Safety Features Actuation System (ESFAS) implemented in the PPS and the ESF-CCS. These are polled master/slave networks and token pass peer to peer networks. Both network types exhibit deterministic performance since all data is serviced (updated) on a continuous scan basis. Data update is not dependent on parameter change of state.

Using the ESF-CCS as an example, refer to Figure 7.3-3 of CESSAR-DC for the following discussion:

The polled master/slave type network is applied as the Multidrop I/O Network in each ESF-CCS segment. The Segment (or Master) Processor polls each node to elicit an update of its data base and to manipulate system outputs. The node then responds over the network and completes its transaction within a fixed time period. Each node on the network is successively serviced in this manner and the cycle is continuously repeated.

The token pass peer to peer network is applied as the Intradivision Network to interconnect all segments within an ESF-CCS Division. Upon receipt of the token, a Segment (or Master) Processor acquires use of the network to read and/or write data between other segments. The token is then passed to the next segment after a fixed time period and the cycle is continuously repeated.

The data protocols for these networks are contingent on the specific equipment selected for system implementation; however, error detection methods such as CRC or LRC are always employed.

Additionally, all networks have demonstrated field proven robustness to EMI. EMI tolerance will also be qualified by the methods defined in the following document:

- o NPX80-IC-QG790-00*, Qualification Guidelines for Instrumentation and Controls Equipment for Nuplex 80+.

Both the polled master/slave network and the token pass peer-to-peer network are redundant in the ESF-CCS to maximize availability.

*This document is considered proprietary to Combustion Engineering, Inc. Access to this document will be provided to facilitate NRC staff review of CESSAR-DC. Information from this document determined to be necessary to support the staff's safety finding will be placed in CESSAR-DC in a future amendment.

Number: 420.48 (7)

Question: Describe the fiber-optic and multiplexor arrangement in enough detail to show that the independence criteria are not violated.

Response: Fiber-optic and multiplexor arrangements for Nuplex 80+ are shown in the following drawings entitled "Nuplex 80+ Intersystem Communications:"

- o E-NPX80+-428-002*, Sheet 1 through 6

These drawings show the generic multiplexor fiber optic communications scheme. Actual quantities and in-plant locations of multiplexors are determined by various factors which include system requirements, appropriately channelized equipment areas, signal density, separation requirements and environmental requirements. Also considered in multiplexor location is equipment maintainability, that is multiplexor equipment is located outside of containment in equipment areas which are easily accessible to maintenance personnel.

These drawings are referenced by document NPX80-IC-DD790-03* Nuplex 80+ Architectural Design Data and are included in the Nuplex 80+ Advanced Control Complex Reference Design Documentation*, Volume 4, Section VIII.

Plant Protection System

The application of fiber optics and multiplexor arrangements between Plant Protection System (PPS) channels are detailed in the following document:

- o NPX80-IC-SD560*, System Description for Plant Protection System for Nuplex 80+

Electrical independence between PPS channels is maintained through the use of fiber optic data links. Fiber optic interface design considerations are addressed in the response to Questions 420.6 and 420.17.

Functional and software independence between Core Protection Calculator Channels is maintained as in previous C-E plant designs. No changes have been made for System 80+.

*This document is considered proprietary to Combustion Engineering, Inc. Access to this document will be provided to facilitate NRC staff review of CESSAR-DC. Information from this document determined to be necessary to support the staff's safety finding will be placed in CESSAR-DC in a future amendment.

Functional and software independence is maintained between Plant Protection Calculator (PPC) channels for Class 1E trip-related functions by using conventional hardwired I/O to interface the bistable trip signals of one channel to the coincidence processor inputs of a different channel. This is no data communication hand-shaking. Therefore, for example, failure of the bistable logic in Channel A cannot impact proper operation of the coincidence logic in Channel B.

In addition, functional and software independence is maintained between PPC channels for auxiliary test and channel bypass functions, by using data communication links only between the Interface and Test Processors (ITP) in each channel. The ITPs handle hand-shaking and data screening of inter-channel data link communications to ensure that the Class 1E trip processors remain segregated and, therefore, cannot be adversely effected by communication errors.

In addition, the trip processors include screening logic to ensure that only specific commands can be accepted from the ITPs. An example of this is in the trip channel bypass functions, where the coincidence processors contain first-in interlock logic that allows only one of four input channels to be bypassed, regardless of bypass requests for the ITP.

ESF-Component Control System

The application of fiber optics and multiplexor arrangements in the Engineered Safety Features Component Control System (ESF-CCS) is detailed in the following document:

- o NPX80-IC-SD640*, System Description for Component Control Systems (CCS) for Nuplex 80+

Electrical and functional independence is maintained between ESF-CCS divisions by similar methods as those described above for the PPS. Communications between ESF-CCS divisions is accomplished through dedicated point to point fiber-optic datalinks. Datalink processors in each ESF-CCS division function as the ITPs in the PPS to acquire data from their respective Intradivision Networks. Inter-channel data is transacted only between data link processors. Complete independence between ESF-CCS Intradivision Networks is maintained by this method. Intradivision Network Operation is discussed in the response to Question 420.47.

*This document is considered proprietary to Combustion Engineering, Inc. Access to this document will be provided to facilitate NRC staff review of CESSAR-DC. Information from this document determined to be necessary to support the staff's safety finding will be placed in CESSAR-DC in a future amendment.

Communication device failures and their consequences have been analyzed and are defined in the Failure Modes and Effects Analysis (FMEA) Table 7.2-5 of CESSAR-DC.

To ensure that erroneous interchannel ESF-CCS communications cannot disrupt multiple divisions, data communication is limited to the following:

1. Unrestricted data transmission is permitted only from safety channels to non-safety channels (i.e., unidirectional).
2. Data transmitted from non-safety channels to safety channels is disabled by reactor trip, ESFAS or manual signals from the operator. This disabling function occurs in the safety channels and is considered a Class 1E function. It is noted that, to date, no non-safety channel to safety channel data requirements have been identified for System 80+. Data communication of this type that existed in previous C-E plants, such as for the CVCS, have been eliminated in System 80+.
3. Between safety channels there is a data communication only between Channels A and C (Division I) and between channels B and D (Division II). To date, this has been limited to diesel load sequencing coordination within a division. There is no data communication between Division I and Division II (A or C to B or D).

Number: 420.49 (7)

Question: Does the DC for this design allow for, or intend to utilize, expert or artificial intelligence systems in the safety or non-safety systems?

Response: Nuplex 80+ safety systems require deterministic performance. C-E is not, therefore, utilizing artificial intelligence (AI) in safety system applications for Nuplex 80+, nor do we expect to use this technology in the future. For non-safety applications, although AI is not currently being utilized, its application is not precluded and would be considered if a benefit could be demonstrated.

Number: 420.50 (7)

Question: Do the safety systems require any rotating memory devices to perform their function?

Response: Safety systems do not utilize rotating memory devices for on-line operation. Only non-volatile solid state memory is used. Rotating memory devices are used however for system startup (e.g., initial memory load).

Number: 420.51 (7.3.1)

Question: Explain the "normal control" function of the ESF-Component Control System (CCS). Provide a more detailed explanation of the redundancy controller function. What happens if the redundancy controller malfunctions?

Response: The "normal control" function of the ESF-CCS refers to the use of the ESF-CCS to manipulate safety related plant components under non-ESF actuated conditions. Use of the system under normal control conditions can include component repositioning for test, maintenance, operational rotation, ... etc. In addition, safety related systems which are normally in use are controlled by the ESF-CCS. These include Component Cooling Water, Service Water and HVAC.

The redundancy controller coordinates the operation of the primary and standby ESF-CCS system processors. The standby system processors are employed to improve system availability only and are not credited for compliance to the single failure criteria. As such, it is assumed that primary/standby processor pairs can fail as a result of single failures in redundancy controllers. These failures and their consequences have been analyzed and are defined in the Failure Modes and Effects Analysis (FMEA) Table 7.2-5 of CESSAR-DC.

A description of typical redundancy controller operation is provided as follows:

Redundancy controllers reside in both the primary and standby processor chassis of each ESF-CCS segment controller. A high speed serial control datalink connects the redundancy controllers.

The primary ESF-CCS system processors execute the control software, read system inputs, and control system outputs. Timing and state memory information is provided to the standby processor from the primary processor via the redundancy controller to facilitate synchronization between the two processors and to keep the standby processor updated with current dynamic process values. This is necessary to facilitate bumpless transfer to the standby processor upon primary processor failure.

Primary processor failure is detected by self diagnostic tests described in the response to Question 420.42. The redundancy controller transfers system operation to the standby processor upon detection of primary processor failure. Standby processor status is continuously monitored to ensure that this transfer can occur. Transfer of system operation is inhibited if standby processor failure is detected. Similarly, transfer from the standby processor back to the primary processor is inhibited until the primary processor is restored to proper operation. Primary or standby processor failure is annunciated through the DPS and DIAS upon failure detection.

Failure of the redundancy controller will result in the inability to transfer system operation from the primary to the standby processor. This failure is also annunciated through the DPS and DIAS.

Number: 420.52 (Figure 7.2-12)

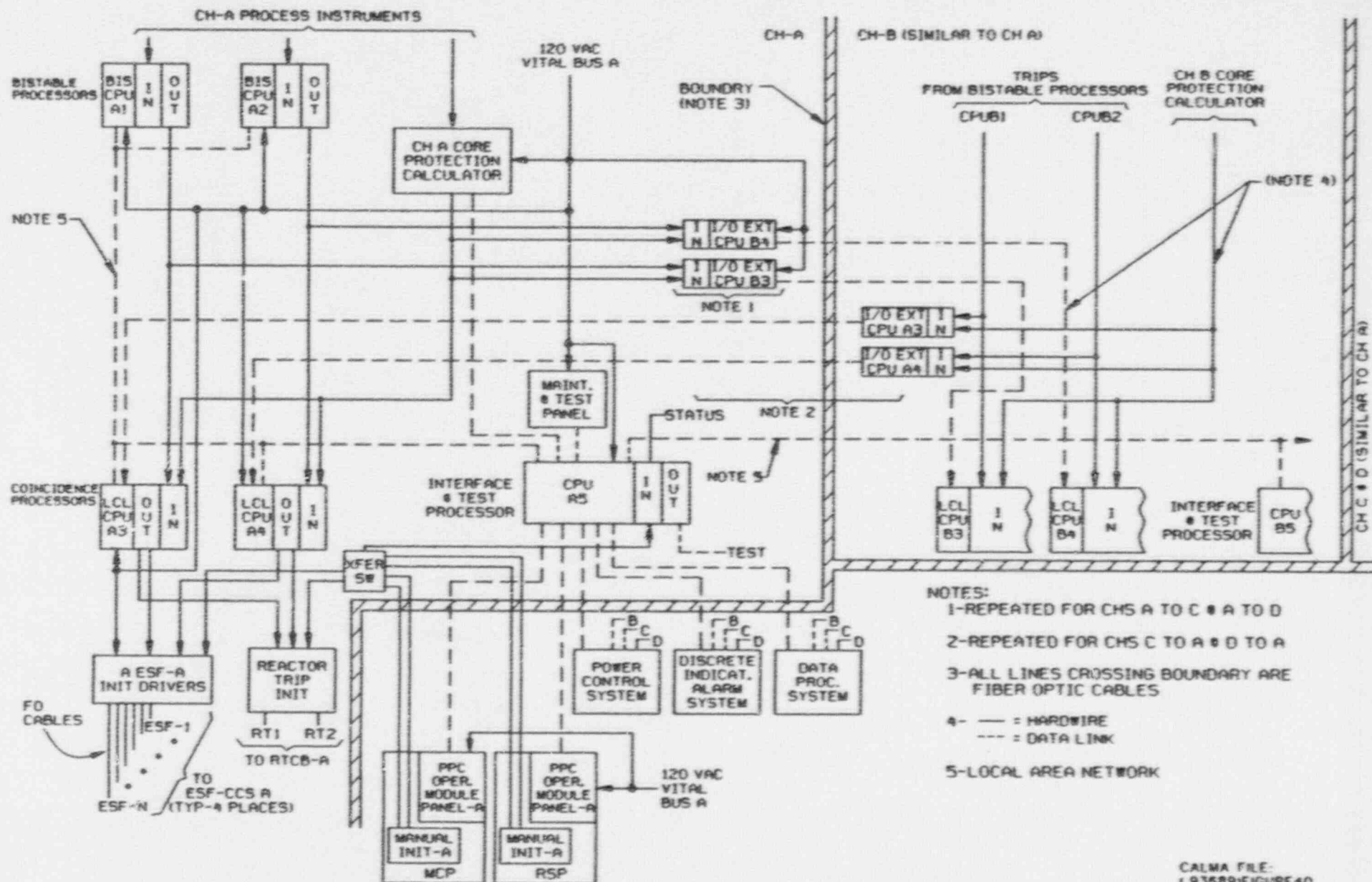
Question: Provide a detailed version of this diagram that shows individual power supplies, microprocessors, and connections. The staff understands that the details may change between this review and plant construction. As part of the "level of detail" discussions which are currently taking place, it would be helpful if C-E could provide their opinion, using the drawings as examples, of what should be "locked" into the design certification and what can be changed.

Response: Figure 7.2-12's primary purpose is to show (1) the two RTSG actuations, shunt trip and undervoltage, (2) that manual RT initiation is a hardwired interface to the RTSG, and (3) how the Alternate Protection System actuation devices are independent and diverse of the RSTG. This drawing depicts all of these features on a full system basis (i.e., four safety channels versus showing one safety channel and noting the other three are similar). The requested detail is more appropriately provided by Figure 2 of the System Description for Plant Protective System for Nuplex 80+ (NPX80-IC-SD560*). This figure is included here as Figure 420.52 with additions, as requested, to show application of the 120 VAC vital bus and power supplies for safety channel A. Discussion of connections, hardwire and data link, shown in the figure, can be found in NPX80-IC-SD560*.

The commission has issued its decision on the "level-of detail" question (see the Staff Requirements Memorandum on SECY-90-377, dated February 15, 1991). C-E has not reached a final determination on what portion of the design should be "locked" into the design certification.

*This document is considered proprietary to Combustion Engineering, Inc. Access to this document will be provided to facilitate NRC staff review of CESSAR-DC. Information from this document determined to be necessary to support the staff's safety finding will be placed in CESSAR-DC in a future amendment.

NPX80+ PPS CH-A SIMPLIFIED BLOCK DIAGRAM
FIGURE 420.52

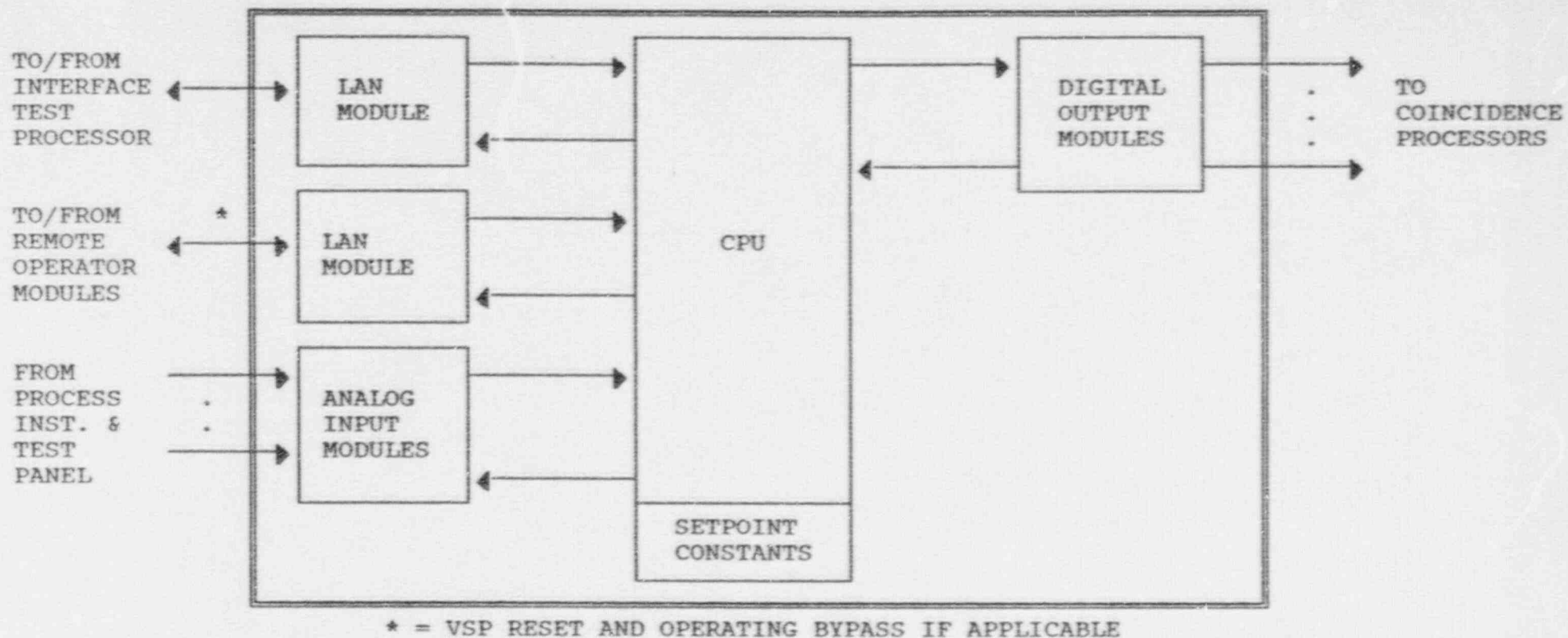


Number: 420.53 (Figure 7.2-11)

Question: It is unclear to the staff how the data flow through the functional blocks shown will actually be accomplished. Provide a more detailed figure.

Response: The attached Figure 420.53 is a block diagram of the bistable processor hardware. The analog input module converts the analog input signals (0-10 volt, 4-20 mA, etc.) to a binary number and stores them for use by the CPU. The CPU collects this data periodically as part of its execution cycle.

The bistable processor CPU uses the LAN modules to communicate with the Interface and Test Processor (ITP) within the PPS. The ITP transmits the variable setpoint reset and operating bypass enable states input by the operator at the remote operator modules. The bistable processor CPU executes logical functions in a fixed sequence as programmed in non-volatile memory. Included in the memory are setpoint constants (fixed setpoint values, variable setpoint reset offset values, rate limited variable setpoint rate and margin values, and allowable operating bypass range values. The CPU provides the calculated trip states (true or not true) to the digital output modules which are hardwired to the input multiplexors of the appropriate four redundant coincidence processors (one for each PPS safety channel). The bistable processor CPU also uses the LAN module to send its input data and calculated data to the ITP for display, alarm and test purposes. Another function of the LAN is to receive automatic test input signals from the ITP and to transmit test results status to the ITP.



PPS BISTABLE PROCESSOR FUNCTIONAL BLOCK DIAGRAM

FIG. 420.53

Number: 420.54 (7)

Question: Describe the trade-offs between analog and digital systems and describe the reasons why C-E considers the new microprocessor based design to be an improvement over previous designs.

Response: C-E has gone to microprocessor based digital system technology due to increasing obsolescence in the analog systems that were used in the past. Use of digital technology supports EPRI requirements for Advanced Light Water Reactors (ALWR) in numerous areas.

- Digital technology is drift-free. Setpoint values are not effected due to design (worst-case) temperature changes, voltage variations, etc., that can occur over time.
- Digital technology provides the capability to implement features which are difficult or impractical utilizing analog systems. For example, standby processing capability for critical applications, on-line DNBR and LPD calculations, bumpless control transfer between MCP and RSP, and signal validation to minimize control system errors which challenge plant safety.
- Digital technology based systems offer self-diagnostic features and aids to troubleshooting such as module health status, identifying circuit opens and shorts, and out of range indication. These features provide rapid failure and error detection, and, when combined with their modular construction, provides for rapid repair when failures do occur.
- Digital technology lends itself to utilizing signal multiplexing, including fiber optic cables for isolation. This results in reduction in cable quantities, and physical separation of redundant systems, which leads to major improvements in fire and sabotage protection.
- Although digital systems are sometimes considered more susceptible than analog systems to HVAC and EMI concerns, they are actually more robust. Digital systems can detect internal errors and then take corrective actions which can lead to an orderly, deterministic fail-safe condition. Analog systems response to these types of effects is much less predictable.
- Digital technology allows data management, reduction and display techniques which are keys to eliminating the historical industry problem of operator information overload.

C-E has had 15 years experience in the application of digital technology to nuclear power plants and knows of no negative aspects associated with the use of this technology.

Number: 420.55 (7)

Question: Describe the time frame for when preliminary experimentation ends and design under controlled formal and documented verification and validation begins for the design. Describe the time frame for the point in the design when simulators are available. The EPRI Requirements Document requires the use of dynamic simulators in the design process.

Response: The design of Nuplex 80+ follows the QA program described in CENPD-210-A (see Chapter 17). Results are presented in the application for design certification (CESSAR-DC). At the time of detailed equipment specification, the information in CESSAR-DC is input to the final design process (which will also be performed in compliance with the QA program), including independent design verification and validation. Formal documentation of V&V results will occur as plant specific engineering.

Figure 420.55-1 provides a design process time line for Nuplex 80+. Preliminary experimentation (not shown on this figure) occurred for Nuplex 80+ under the DOE Advanced I&C Program which ended in September 1989. Dynamic prototypes of both I&C equipment and man-machine interface devices have been used in the design process for over two years. I&C prototypes have been used for qualification and performance pre-testing. Dynamic man-machine interface devices with dynamic simulations have been used to do human factors suitability and availability verification analyses. The scope and fidelity of the dynamic prototypes and simulations have evolved continuously throughout the course of the design process as prescribed by the EPRI ALWR-URD. The design is now at the point where all MMI and I&C methods have been established and conformance to safety and operability criteria can be assessed.

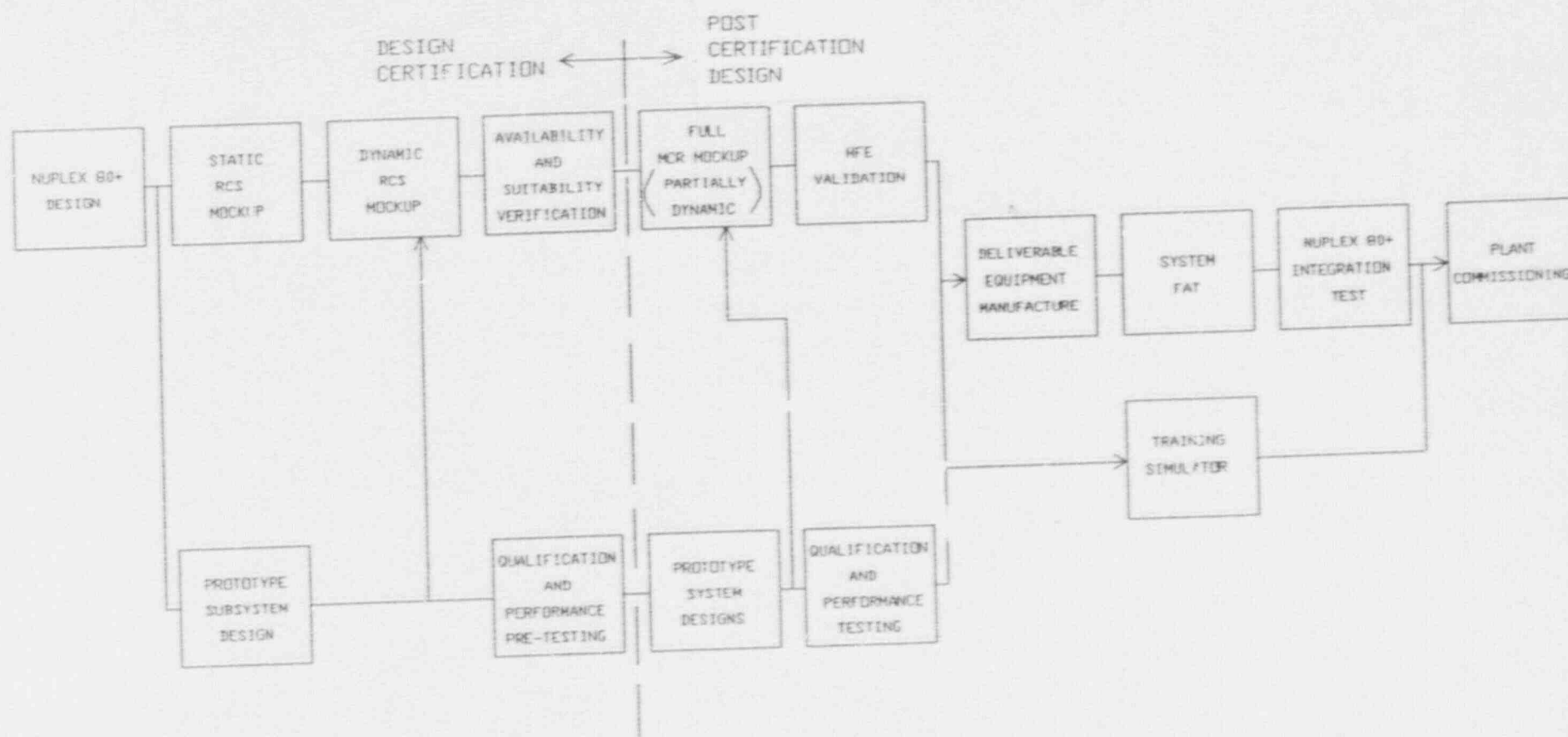
To minimize investment risk, it is expected that the owner/operator will require complete I&C prototype system designs and a full main control room mock-up will be completed before manufacture of deliverable equipment.

The simulator for a plant is required by current regulations for operator training. Its design typically comes after equipment manufacture has occurred and in parallel with factory acceptance tests and final integration tests. Procurement of a simulator is an owner/operator decision.

C-E has adopted a comprehensive development approach which is commensurate with the evolutionary nature of the Nuplex 80+ design. This is true of both the I&C system designs and the human factors design. Dynamic prototypes with dynamic simulations are used early in the design process. A full scope simulator is based on final as-procured equipment and is manufactured later for operator training.

Figure 420.55-1

NUPLEX 80+ DESIGN PROCESS



Number: 420.56 (7.7.1.1.11)

Question: Describe the diversity of the APS. Does this diversity include diverse sensors, processors, and power supplies? Address the detailed guidance provided with the ATWS Rule, 10CFR50.62 Statement of Considerations.

Response: The APS includes sensors, signal conditioning, control logic, electro-mechanical actuations and power supplies. The sensors are separate from those of the PPS and ESF-CCS, but not necessarily diverse from those of the PPS and ESF-CCS. The signal conditioning and control logic is implemented as part of the Process-CCS. The Process-CCS is diverse from the ESF-CCS and PPS. This diversity includes all hardware and software that specifically impacts computer operation, including power supplies, data links and multiplexors. Excluded are simple, well proven devices such as switches, terminations and wiring.

The APS final actuation devices for reactor trip are the Control Element Drive Mechanism Motor Generator Set output contactors. These devices provide diversity of design from PPS reactor trip switch gear circuit breakers.

The final actuation devices for the emergency feedwater system are the motor starters and solenoids for the EFW pumps and valves. These devices are shared with the Engineered Safety Feature Actuation System implemented in the PPS and ESF-CCS.

The plant power sources for the APS reactor trip logic and actuation devices are independent of the plant power sources for the PPS reactor trip system. The PPS and RTSG are powered from the Class 1E Vital Bus system. The APS reactor trip logic is powered from the non-Class 1E, Channel X and Y instrument busses; the APS reactor trip actuation device power is supplied from the MG Set Generator. These APS sources are independent of the Class 1E Vital Bus system.

The plant power sources for the APS emergency feedwater actuation logic power is independent of the plant power used by the PPS and RTSG. The PPS and RTSG are powered by the Class 1E vital bus system; the APS is powered by the non-Class 1E instrument busses. The emergency feedwater actuation device power is not independent between the APS and PPS, since the final actuation devices are shared by the PPS and the APS.

Turbine trip is initiated by CEDM bus undervoltage relays located in the CEDM power supply cabinets of the Power Control System (PCS). These relays will react to CEDM power interruption by either the PPS or APS. The PCS undervoltage relays are diverse from all PPS and RTSG equipment.

Number: 420.57 (7)

Question: It is not clear to the staff how the sensor transmitter outputs will be transferred to the Remote Shutdown Panel when required. Presumably the calibration data updates in the plant protection system would be disconnected during the transfer. Provide a more detailed description of the transfer from the main control room to the remote shutdown panel.

Response: In the Nuplex 80+ systems, sensor transmitter outputs are not transferred. Upon transfer of control from the Main Control Room (MCR) to the Remote Shutdown Panel (RSP) the only transfer that occurs is the enable/disable of the man-machine interface (MMI) at each location. The sensor transmitter outputs are wired to multiplexers or equipment, which are located in field areas or equipment rooms as applicable. These areas are totally independent of the MCP and RSP areas, including electrical, HVAC and fire protection. Both the RSP and Main Control Panels (MCPs) interface with the system's equipment via fiber optic cabling and multiplexing, providing electrical isolation and fault protection to system's equipment.

Transfer of control from the MCR to the RSP is accomplished on a per channel basis via control transfer switches located in channelized equipment areas outside of the MCR fire zone. Transfer of control of any or all channels of equipment from the MCR to the RSP is alarmed in the MCR to alert the operator the transfer action is taking place.

In the event of transfer of control from one location to the other, the transfer action enables the operator's manually entered control signals from the location being transferred to, and blocks the operator control signals from the other. Therefore, upon transfer of control no actual disconnecting takes place, only enabling or blocking of MMI signals from the MCP/RSP as applicable. This transfer is completely bumpless, meaning no setpoints are disturbed and, therefore, there is no disturbance to the output of any control or protection system. Bumpless transfer is accomplished by retaining the memory of all operator entered setpoint and control commands, within the system electronics located in the channelized equipment areas, not in the MMI devices of the MCP or RSP. All MMI devices are totally passive, meaning they can be disconnected at any time (for control transfer or more routinely for maintenance) with no disturbance to the plant.

Number: 420.58 (Non-docketed backup material review)

Question: As part of the staff's review to date there have been meetings with the licensee and material presented and discussed which has not been placed on the docket. These questions are labeled as "review" questions. In Volume 1 of the backup documentation that was available for the staff to review there was a description of the priority 1 and 2 alarms which are processed and displayed independently by the DIAS and DPS systems which also cross check each other. How is independence and isolation maintained.

Response: Independence and isolation between DIAS and the DPS is maintained in the following manner:

1. Input data to DIAS and DPS is transmitted separately from other NPX80+ systems (e.g., PPS, CCS, PCS) via data links. All data links to DIAS are fiber-optic to maintain electrical independence from DPS.
2. DIAS and DPS are powered from independent battery-backed instrument busses as follows:

 DPS - Channels X, Y
 DIAS-N - Channels C, D
 DIAS-P - Channels A, B
3. DIAS and DPS each process their input data independently to generate their respective alarms and displays. However, fiber optic data links are used between DIAS-N and DPS for the following functions:
 - a. Alarm and display outputs generated by DIAS-N are transmitted to DPS periodically for comparison to the corresponding DPS generated data. Unacceptable discrepancies are alarmed by the DPS. The DPS uses DIAS data only for comparison to its own data. It does not use the DIAS-N data as input to any of its own calculations. Errors in the data would not impact DPS generated data.
 - b. Data that is calculated only by the DPS (such as COLSS) is transmitted to DIAS-N for input directly into DIAS-N alarms and displays. This data is not used in any DIAS-N calculations. Therefore errors in this data would not impact DIAS-N generated data.
 - c. If an alarm is acknowledged by the operator on DIAS-N, that acknowledgement signal is transmitted to DPS to also acknowledge the corresponding DPS alarm. Similarly, DPS acknowledgements are transmitted to DIAS-N to acknowledge the corresponding DIAS-N alarms. Errors in this data could prematurely acknowledge alarms but could not block the generation of alarms.

- d. DIAS-N health status including a memory checksum is transmitted to DPS for alarming. This data is not used in any DPS calculations, therefore errors would not impact DPS performance.

C-E has minimized the potential for data corruption between DIAS-N and DPS by carefully restricting the manner in which inter-system data may be used in the respective systems, and by employing communication error detection. In addition, as an added precaution DIAS-N includes a separate micro-processor that is dedicated to DPS communications. This processor handles all DPS communications handshaking to avoid any disturbance to the deterministic performance of the DIAS-N internal communication network or other DIAS-N processors performing calculation or display functions. The communication processor checks DPS data for reasonability before it can be passed on to the rest of the DIAS-N system.

The discussion in item 3 above pertains only to DIAS-N/DPS interfaces. It is noted that for DIAS-P the only communication with DPS is unidirectional to transmit signal validation calculation results. DPS compares this data to its own calculations to alarm differences (as it does with DIAS-N data). There is no data transmission from DPS to DIAS-P. As in DIAS-N, DIAS-P contains a separate microprocessor to handle communication hand shaking with DPS.

Number: 420.59 (Review)

Question: A description of the touch screen discrete indicators was presented. Does the operator need to select different screens to see the RG 1.97 Cat 1 variable.

Response: The operator does not need to select different screens to see the RG 1.97 Cat 1 variables. The displays provided on DIAS-P are dedicated to the RG 1.97 Cat 1 variables. RG 1.97 Cat 1 variables are also displayed on DIAS-N and DPS but in these systems they do not necessarily have dedicated displays, selection by the operator is often required. It is noted however, that in DIAS-N some RG 1.97 Cat 1 variables do have dedicated displays if these variables are also considered key indicators of critical function status or success path performance. Selection criteria for all DIAS displays is defined in CESSAR Chapter 18.

Number: 420.60 (Review)

Question: The DPS is described in the manuals available to the staff as having an RS-232 datalink available and that bi-directional communication is supported. Describe any area in which non-safety systems provide information to safety systems.

Response: Section 6.3 of NPX80-IC-SD710-00*, Revision 00, "System Description for the Data Processing System for Nuplex 80+," describes in detail the communications between the DPS and the other Nuplex 80+ systems. Each subsection under 6.3 describes the unique communications requirements to each Nuplex 80+ system. There is bi-directional data communications between DPS and DIAS where DIAS is defined as important to safety. The design will ensure that the DPS cannot compromise the integrity of the DIAS (see response to Question 420.58). There is no bi-directional data communications with any protection system. If bi-directional communications is required with any protection system, the design will ensure that erroneous data on these links cannot compromise the single failure integrity of the protection systems. Appendix G, "Summary of Data Communication Interfaces," summarizes all the DPS communications interfaces.

*This document is considered proprietary to Combustion Engineering, Inc. Access to this document will be provided to facilitate NRC staff review of CESSAR-DC. Information from this document determined to be necessary to support the staff's safety finding will be placed in CESSAR-DC in a future amendment.

Number: 100.1

Question: What plans does C-E have for addressing the National Environmental Policy Act, including potential severe accident mitigation design alternatives?

Response: C-E is participating in NUMARC's Standardization Oversight Committee. This committee is developing a proposed approach to NEPA and will be discussing this approach with NRC staff prior to finalization by the Committee. At the conclusion of these discussions, C-E will inform the staff of the approach to NEPA. A similar question was asked in a letter dated February 21, 1991 from D. M. Crutchfield to A. E. Scherer.

Number: 620.1

Question: Provide a detailed human factors program plan which includes (1) a scope of work, (2) the organization of the human factors group and their reporting structure, (3) a description of the human engineering and system analysis studies to be performed, (4) the standards and guidelines that will be generated as a result of human factors efforts, (5) a schedule of major human engineering milestones and technical reviews with anticipated levels of human engineering support, and an outline of the human factors test and evaluation plan.

Response: (1) & (5)

Human factors planning for the Nuplex 80+ design process was incorporated as part of the overall advanced control complex design process planning. A high level human factors plan indicating the organization of the Nuplex 80+ design team, its reporting structure, the scope of work and the principal human factors activities of the process was provided in CESSAR-DC Sections 18.1-18.4. These sections were submitted in Amendment D and developed prior to the major part of the work being performed.

Further details related to the human factors planning are provided in the program plans for FY87-FY89 for the DOE Advanced I&C Program. Work plans for these fiscal years were sent to DOE in letters ALWR-87-109, ALWR-88-014 and ALWR-89-028. This program was used to perform most of the human factors activities during the design process as part of the Alarm and Display Methodology and Control Systems Performance tasks. The Advanced I&C Program plans indicate the scope of work performed and a detailed schedule, including milestones and reviews. The plans are available for staff review at C-E.

- (2) The reporting structure for the design team is shown on Figures 620.1-1 (a and b) and 620.1-2. Most of the design team were members of the I&CE department in Nuclear Power Systems and reported to the supervisor of the Advanced Instrumentation Design group. The organization is shown in Figure 620.1-1a. The human factors specialists were members of the Nuclear Power Services division reporting to both the Advanced Instrumentation Design supervisor and Human Factors and Cognitive Services supervisor (Figure 620.1-2). A recent I&CE organizational change (Figure 620.1-1b) has the ALWR human factors specialists reporting to the supervisor of Control Complex Engineering.
- (3) Table 620.1-1 lists the major human factors analyses and studies performed during the Nuplex 80+ design process.

- (4) The Nuplex 80+ human factors effort generated an implementation methods document early in the design process. This document is the "System Description for Control Complex Information System for Nuplex 80+" (NPX80-IC-SD791-01*). As the design proceeded, additional methodologies were added and documented temporarily in other documents for efficiency. The control complex system description is now under revision to consolidate all methodologies again. The Nuplex 80+ process did not establish "guidelines" as guidelines would lead to different implementations by different designers. Human factors criteria were obtained from the references provided in the response to Question 620.31 for all man-machine interfaces used in Nuplex 80+.
- (5) The test and evaluation plan is discussed in the response to Question 620.30. This includes activities that have been performed for certification and activities that are planned for the future. The level of human engineering support varies according to the tasks being performed. The level of effort of human factors specialists is discussed in the response to Question 620.4.

*This document is considered proprietary to Combustion Engineering, Inc. Access to this document will be provided to facilitate NRC staff review of CESSAR-DC. Information from this document determined to be necessary to support the staff's safety finding will be placed in CESSAR-DC in a future amendment.

11/15/89

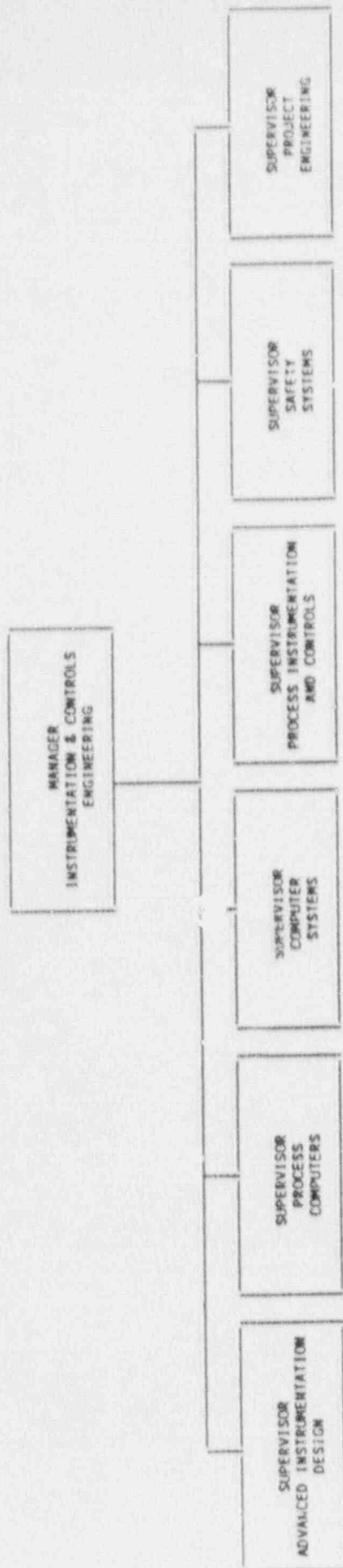
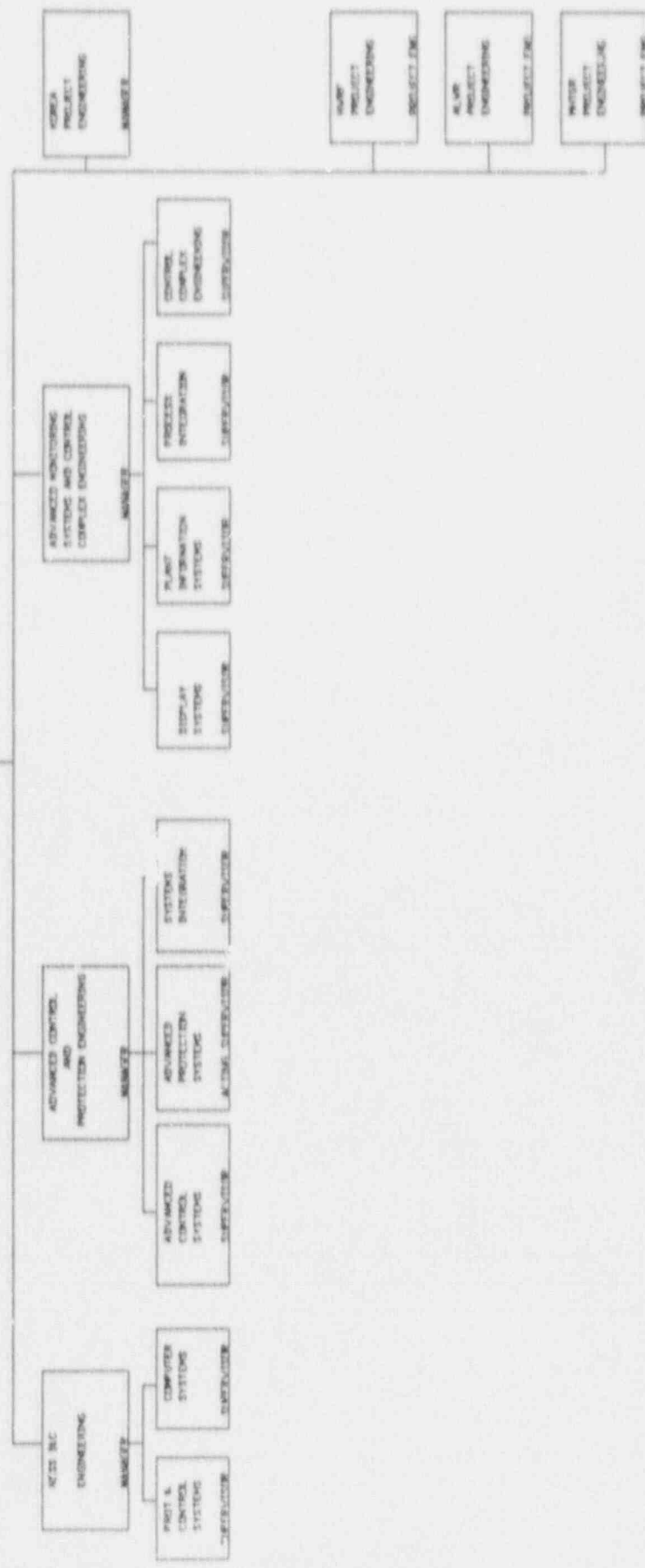


Figure 620.1-1a
Organization and Reporting Structure for
the Nuplex 80+ Design Team
Pre-1991

INSTRUMENTATION & CONTROLS
ENGINEERING
MANAGER



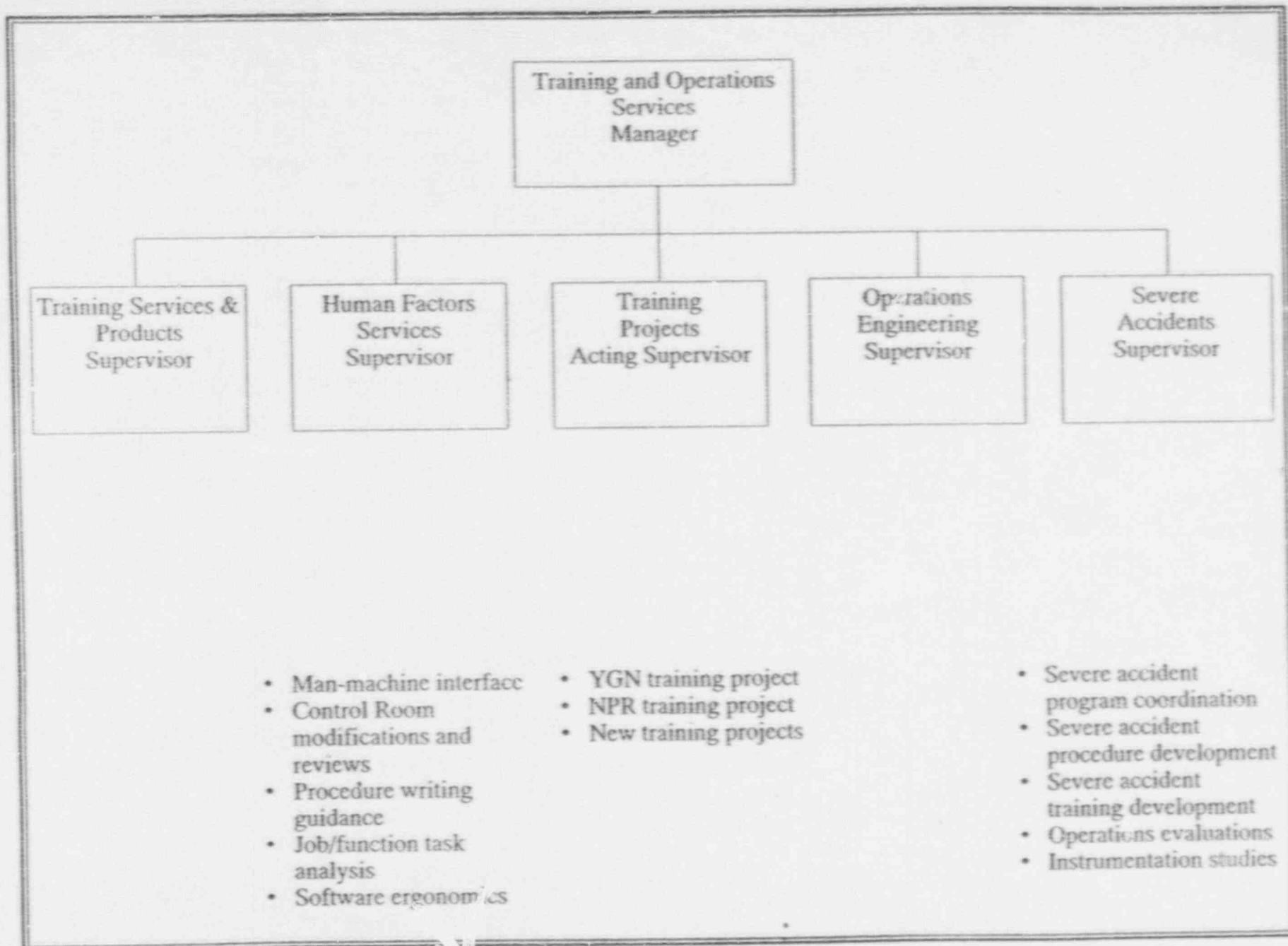


Figure 620.1-2

Human Factors Services
Organization and Reporting Structure

January 18, 1991

Table 620.1-1

Nuplex 80+ Studies and Analyses

Completed:

- o Nuplex 80 Studies
- o Halden Reactor Project Validations
 - Critical Function Monitoring System (CFMS)
 - Success Path Monitoring System (SPMS)
 - Integrated Process Status Overview (IPSO)
- o Advanced I&C Human Factors Studies

Alarm Problems

Alarm Handling

Operator Aids

Control Room Configuration Evaluation

Task Analysis/Function Allocation

Indication Reduction Study

Visibility, Mobility and Access Study

Human Factors Verification - Availability and Suitability

Planned:

Continued Verification Analysis

Human Factors Validation

Number: 620.2

Question: Describe the human engineering studies that led to the selection of the flat panel programmable displays used on the control boards. Describe how they meet the operator and instrumentation requirements identified in the task analysis, as well as the maintainability, and reliability requirement established for control room instrumentation. Also address how they contribute to the goal of redundancy and diversity. Include relevant findings from task analyses and product evaluations.

Response: Many factors contributed to the selection of flat panel displays for use on the MCR control panels. This included both human engineering and instrumentation performance factors. Flat panel display technology was selected for discrete indicators and alarms based on the following required characteristics:

Diversity from CRTs to provide common mode failure protection of the MMI,

Seismic Qualification to meet requirements for Regulatory Guide 1.97 Category 1 parameter display,

Selectability of displayed information to support continued plant operation at power upon the failure of the DPS resulting in loss of all CRT information, sensor deviation diagnostics, alarm details and control selections.

Reliability and Maintainability including short MTTRs and long MTBFs.

Dynamic Graphic Displays for trends, automatic scaling, bar charts, etc.

Interface useability that is satisfactory to meet Nuplex 80+ human factors methodology and acceptance criteria.

Standardization because one programmable device serves needs of Nuplex 80+ applications for indicators/recorders, alarms and controllers.

Other positive characteristics include low sensitivity to electric and magnetic fields and low voltage.

The human engineering focus of the flat panel evaluation was on the acceptability of the interface in the proposed Nuplex 80+ applications. A preliminary evaluation initially determined if flat panel devices could acceptably provide the features required (i.e., touch selection, flash, bar charts and digital display). Later the devices were evaluated in specific Nuplex 80+ applications during the suitability verification analysis.

The function task analysis results indicated that for many tasks a single value of a parameter is required not multiple channels of data that may be provided by plant instrumentation. Discrete indicators using flat panel displays meet this need specifically by providing a single validated parameter value instead of multiple channels. The selectability of individual channels meets needs for other tasks and equipment failure situations. Similarly, spatially dedicated displays of high priority alarms required dynamic tiles (i.e., could be either Priority 1 or 2) with the ability to display multiple messages for alarm conditions grouped in a tile. The flat panel devices met these operational needs. Controllers were designed similar to conventional plant controllers using flat panel displays. Task analysis results indicated that selection of inputs, selection of setpoints, output control and mode selection were required to meet operational needs.

Flat panel electroluminescent displays are easily removable from Nuplex 80+ panels by disconnection of quick disconnect cables and removal of four bolts. Replacement of a device takes less than one-half hour. The published expected MTBF of these devices is 30,000+ hours resulting in an availability of 99.998%. Actual in-service experience is exceeding this number and revised published numbers exceeding 40,000 hours can be expected.

Flat panel displays provide indications and alarms on diverse technology that are redundant to information provided on Data Processing System CRTs. This directly supports the Nuplex 80+ approach to address potential common mode failures with diversity. Additionally, flat panel displays for DIAS N and P provide redundant display of Category 1 PAMI parameters required by Regulatory Guide 1.97, with all of the required characteristics of Category 1 variables.

A flat panel product evaluation was conducted comparing Liquid Crystal Displays (LCD), Electro-Luminescent Displays (ELDs) and Plasma Displays. The conclusion of the product evaluation was to select ELDs for Nuplex 80+ applications based on ruggedness and display quality.

Number: 620.3

- Question: (1) Describe the technical and administrative methods used by C-E's human factors specialists to track the evolution of the design and to influence the design process.
- (2) Describe the documentation control system that is in place to ensure that the evolution of the man-machine interface elements of the design have been documented and provide an auditable documentation trail. How are the results of studies, design decisions and trade-offs documented?

- Response: (1) The I&CE department has a comment-resolution tracking system that is used to assure future implementation of open items identified during the design process. This is available to human factors specialists as well as engineers involved in the design. For short term tracking, HF specialists comments and recommendations have been documented in reports and then integrated into the subsequent revision to design documents. A CESSAR-DC open items list also provided tracking for specific items to be resolved and incorporated into CESSAR-DC if appropriate (e.g., Amendment I closed out I&C open items).
- (2) The design was tracked as it evolved through internal memoranda and Nuplex 80+ documentation. The internal memoranda were the primary means for documenting design decisions and trade-offs. C-E is developing a design document that consolidates the design evolution memoranda with emphasis placed on the bases for design decisions (this document will be included in the set of Nuplex 80+ Reference Design Documents*). Results of studies are documented in either Nuplex 80+ documents or milestone reports for the DOE Advanced I&C Program.

*This document is considered proprietary to Combustion Engineering, Inc. Access to this document will be provided to facilitate NRC staff review of CESSAR-DC. Information from this document determined to be necessary to support the staff's safety finding will be placed in CESSAR-DC in a future amendment.

Number: 620.4

Question: How many human factors specialists are currently dedicated, on a full-time basis, to the System 80+ design? Into how many hours of face-to-face contact time does this translate with the NSSS and BOP engineering and design staffs per weeks?

Response: Currently there are four human factors specialists dedicated to the Nuplex 80+ design. The number has ranged from one to four, depending on the work being performed at any given time in the design process.

Depending on the activities being performed, the direct contact with engineering staffs ranged from 0% to 100% of the human factors specialist's time with an average of approximately 25%. Activities such as the functional task analysis required a relatively small amount of face-to-face contact, since the functions for System 80+ are similar to those for previous System 80 plants. Other activities such as design review meetings and the suitability analysis required a relatively high level of face-to-face contact.

Number: 620.5

Question: Chapter 18 Section 17.7.1.1.2 describes the use of 11 colors; TE 790-01* Paragraph 3.1.2, Point 1, identifies another two colors; and SD640* Paragraph 6.1.4.1 identifies two or more colors. There is no clear and concise presentation of the information coding scheme used in the System 80+ control room.

Provide a matrix of all the information coding methods and their meanings used in the control room. This would include, at a minimum, the colors, the symbols, changes to alphanumeric and symbols such as case or size, any patterns, position/location/denotation of data that would convey information, flash, flash rate, figure-background changes, reverse video, color changes (include contrast ratios), changes in intensity, etc., or any combinations thereof that are used on software driven and hardwired displays that provide some kind of quantitative or qualitative information to operators or maintenance personnel.

Response: The Nuplex 80+ coding methods were documented in the System Description for Control Complex Information System, NPX80-IC-SD790-01*, Revision 00. As the design evolved and was reviewed, additional coding conventions were established and revisions to coding methods were required. Changes have been documented in the verification analysis report and the Component Control System (CCS) System Description as noted in the questions.

The recent submittal of Amendment I of CESSAR-DC clarifies the current coding methods. In addition, as previously indicated to NRC staff, the System Description for Control Complex Information System for Nuplex 80+ (NPX80-IC-SD791-01*) is being revised to incorporate all Nuplex 80+ coding methods. This document revision includes the requested matrix which is provided in Figure 620.5-1.

*This document is considered proprietary to Combustion Engineering, Inc. Access to this document will be provided to facilitate NRC staff review of CESSAR-DC. Information from this document determined to be necessary to support the staff's safety finding will be placed in CESSAR-DC in a future amendment.

Figure 620.5-1 Nuplex 80+ Coding Matrix

PROPERTY/CODING	ASTERISK	UNDERLINE	TRIANGLE	CROSS	HATCHED	HOLLOW	FILL	REV	VIDEO	BOX	BRACKETS	RED	GREEN	BLUE	YELLOW	GREY	FLASH	CYAN	WHITE	ORANGE	PURPLE
ACTIVE/ON/OPEN						X						X*				X**					
INACTIVE/CLOSED/OFF							X					X*				X**					
AUTO														X							
UNACK. PRI 1 ALRM								X							X		X(F)				
UNACK. PRI 2 ALRM									X						X		X(F)				
UNACK. PRI 3 ALRM										X					X		X(F)				
UNACK. OP AID		X															X(F)			X	
ACK. PRI 1 ALRM								X							X						
ACK. PRI 2 ALRM									X						X						
ACK. PRI 3 ALRM											X				X						
ACK. OP AID		X																		X	
CLEARED PRI 1 ALRM								X									X(A)	X(crt)	X(S)		
CLEARED PRI 2 ALRM										X							X(A)	X(crt)	X(S)		
CLEARED PRI 3 ALRM											X						X(A)	X(crt)	X(S)		
CLEARED OP AID		X															X(crt)	X(S)			
RESET ALARM (1)																			X		
DYNAMIC DATA																					
STATIC DATA																					
STATIC DATA LABEL'S																					
DYNAMIC DATA LABELS																		X			
SYSTEM			X																		
ABNORMAL MAN CNTL																				X	
LINES/BORDERS/PIPES																					
NR BAR CHART										X											
WR BAR CHART						X															
SUSPECT DATA	X																				
REG GD 1.97 PARM LBL																					X
SLCTD TOUCH TARGETS									X										X(crt)		

(F)=Fast rate (A)= Alarm Tiles only (I)= Indicators (C)= Controllers * Indicates operability from the control room ** Indicates inoperability from the control room
(1)= Reset alarms shown in pre-alarm condition coding

Number: 620.6

Question: Describe the standardized training materials (e.g., content, format, and development process) being provided to the purchasers of the C-E System 80+ for those aspects within the CESSAR design scope.

Number: 620.7

Question: Describe the guidance that will be provided to purchasers of the C-E System 80+ to ensure consistent adaptation of the standardized training materials to site-specific training materials.

Number: 620.8

Question: Given the advanced technology of the C-E System 80+ what are the specific skills, knowledge, abilities, and aptitudes, based on the task analysis, that will be provided to purchasers to assist in the development of site-specific personnel selection criteria?

The information provided in Section 13.5 indicates that information concerning the site-specific operator plant procedures is within the referencing applicant's scope and shall be provided in the site-specific SAR. Since this is not consistent with the staff's position on standardization, the following should be addressed.

Number: 620.9

Question: Describe the standardized normal, abnormal, and emergency operating procedures C-E will provide to the purchasers of the C-E System 80+.

Number: 620.10

Question: Describe the standardized procedural development guidelines to be provided to referencing applicants for those normal, abnormal, and emergency operating procedures (e.g., writer's guide, verification, and validation guide, procedural maintenance guide). Describe the interface information that will be provided to ensure that site-specific procedures will be consistent with the standardized procedures.

Response: Response to Questions 620.6-620.10

As stated in CESSAR-DC, Sections 13.2 and 13.5, the procedures and training for a particular plant are within the scope of the site-specific SAR. C-E intends to comply with the staff's "training and procedures" position by providing standardized training and operating procedures guidance. This guidance would then be input to the site-specific training program and operating procedures. This approach is necessary as a result of site-specific component selection (meeting standard functional requirements) and utility-owner responsibility for plant operation.

Number: 620.11

Question: Does System 80+ use advanced and intelligent operator aids based on expert systems or other artificial intelligence (AI) technologies? If so, describe the following:

- a. The extent and dependence on intelligent operator aids necessary to achieve the single operator design goal.
- b. The specific operator aids that are planned and technology on which they are based.
- c. The methods of knowledge engineering that will be used.
- d. The approach to be taken to develop operator confidence in the systems to assure that they will be appropriately utilized.
- e. The methods to be used for the verification and validation of the performance of intelligent operator aids.

Response: The Nuplex 80+ ACC uses no expert systems or AI technology in any of its system designs, including the advanced operator aid designs.

Number: 620.12

Question: How will C-E demonstrate that the System 80+ design objectives of improving operator performance, reducing maintenance time, and improving reliability are met?

Response: C-E is taking a phased approach during the design process to demonstrate acceptable operator performance with the Nuplex 80+ interface. Some features had been demonstrated to improve operator performance prior to incorporation into Nuplex 80+. This includes critical function monitoring, success path monitoring and IPSO, all of which were validated at the OECD Halden Reactor Project. These validations are discussed in the response to Question 620.30. As design features were selected qualitative evaluations were performed to determine if the feature(s) solved existing operational problems without introducing new performance problems. These evaluations included multi-disciplinary reviews with participation by both C-E and Duke Power Company operators to assess the impact on operations.

After design of the feature(s) and development of a prototype, a suitability verification analysis was performed to verify that the indication and control capabilities adequately and appropriately supported performance of operator tasks. This analysis focused on performance of individual MMI prototypes and the ensemble of the interfaces provided on a Nuplex 80+ panel. The suitability analysis also considered the big board overview of plant status on IPSO. In addition to the verification analysis, more than 100 dynamic demonstrations have been given to power plant engineers, operators and maintenance people with positive feedback on Nuplex 80+ improvements to operator performance and maintenance. Finally, acceptable operator performance is demonstrated through validation of the complete interface on a dynamic mockup of the entire controlling workspace. This includes operator walk through and talk through of procedures with an approximation of the real time response. The validation effort will be completed after certification.

Nuplex 80+ equipment is designed to provide easy failure detection and maintenance. This is demonstrated by determining a mean time to repair for Nuplex 30+ display and processing devices. Nuplex 80+ is designed to meet the EPRI ALWR-URD requirements of a mean time to detect and repair equipment of less than 4 hours with a maximum time to detect and repair failures of 8 hours. Design features such as modularity, easy access, self-diagnostics and automatic testing are incorporated into the design. MTBF data for all equipment is readily available from manufacturers since Nuplex 80+ is composed almost entirely of commercial products. Custom parts of Nuplex 80+ are already in use in other C-E plants. Times to detect and repair failures are determined based on required repair activities plus reasonable allowances for personnel

access, paperwork and security. Availability analyses are performed for all Nuplex 80+ systems. A representative availability analysis document has been included in the Nuplex 80+ Reference Design Documentation*.

*This document is considered proprietary to Combustion Engineering, Inc. Access to this document will be provided to facilitate NRC staff review of CESSAR-DC. Information from this document determined to be necessary to support the staff's safety finding will be placed in CESSAR-DC in a future amendment.

Number: 620.13

Question: How does C-E plan to demonstrate that "improved plant comprehension" has been achieved over the reference design for:

- a. improved alarm presentation and handling
- b. continued plant operation with loss of 1 or 2 diverse information display systems
- c. integration of normal and accident monitoring displays
- d. improved usability of the information presentation methods used to reduce required operator information processing requirements.

Response: The Nuplex 80+ man-machine interface has been designed with specific features to improve comprehension of plant conditions compared to conventional control room technology. Specific features are provided for each of the question items. These are discussed on an item-by-item basis.

- a. The Nuplex 80+ design improves alarm presentation and handling through the following features:

Alarm Presentation

- i) using both spatially dedicated alarm tiles and serial access to alarms via CRT at any MCR panel takes advantage of pattern recognition for high priority alarms and allows operators to bring alarms to him via CRT for acknowledgement, if desired,
- ii) consistent display coding for alarm priority (based on time required for operator action) is used in both CRT and DIAS alarm presentation,
- iii) using grouped alarms with dynamic messages, IPSO indication of high priority alarm locations, and critical function alarm algorithms to allow the operator to quickly correlate alarm conditions to plant safety or performance impact,
- iv) redundant and diverse presentation of high priority alarms in an integrated manner on DIAS and CRTs for reliability; i.e., even with expected equipment failures alarms will be available to operators,
- v) addressing potential alarm overload conditions by providing a "stop flash" and "resume flash" feature to temporarily allow viewing only existing Priority 1 alarms and all subsequent alarms while deferring the acknowledgement of all other alarms.

Alarm Handling

- i) basing process alarms on validated process representation parameters and indicating channel failures by lower priority alarms,
- ii) basing alarms on current plant operational modes, including post-trip, to reduce nuisance alarms,
- iii) using an acknowledgement method that requires operators to acknowledge all alarms individually without excessive non-critical task loading,
- iv) using equipment dependent alarms to minimize nuisance alarms,
- v) providing capability for operator established alarms to allow operators some flexibility in setting operationally beneficial alarm points,
- vi) correlating critical function monitoring directly to the emergency operating procedure being used, to avoid confusion between procedure setpoints and critical function monitoring setpoints.

A quantitative assessment has determined a 60% reduction in alarm tiles for Nuplex 80+ compared to a conventional plant.

- b. The Nuplex 80+ man-machine interface is designed for continued operation with failure of either the entire DPS or DIAS channel.

A complete description of the Nuplex 80+ approach to degraded conditions is provided in the response to Question 620.35. DIAS has been designed to provide all information required for continued operation for 24 hours, including high priority alarms, key validated parameters with multiple parameter channel availability. The basis for selection of DIAS parameters is those required for technical specification surveillance, accident monitoring of critical functions and success paths and Regulatory Guide 1.97 parameters, and investment protection of major components (e.g., RCPs). The advantage of Nuplex 80+ upon DPS failure is that improved comprehension is still supported by alarm processing and signal validation which are performed by DIAS. In a conventional plant, loss of the plant computer means that all information processing for the primary operator interface is lost. Continued operation without DPS CRT displays is evaluated as part of the Nuplex 80+ verification and validation program. The Nuplex 80+ approach is also an improvement over other advanced control room designs which require plant shutdown when the plant computer fails. This

approach puts the plant and operators through a transient with a degraded interface instead of staying at a stable known condition as with Nuplex 80+.

DIAS failures are discussed fully in the response to Question 620.35. Complete loss of DIAS is not a credible event because of the segmentation of the design. Either DIAS N or P would remain with any credible failure to provide Regulatory Guide 1.97 Category 1 parameter monitoring. If either part of DIAS were inoperable, the DPS CRTs at every panel in the control room would be available for continued operation. All plant information and alarms provided by DIAS are available through the DPS, including all information processing to support improved comprehension. DIAS failure would impact operations because of the loss of spatially dedicated information. This condition is also evaluated in the Verification and Validation Program.

Loss of both the entire DIAS or other DIAS channel and DPS simultaneously is not a design basis event for Nuplex 80+.

- c. Nuplex 80+ is designed to integrate normal and accident monitoring displays. Integration of normal and accident monitoring displays is accomplished through four Nuplex 80+ design features.
 - (1) The SPDS function is integrated into the normal DPS interface using the same coding and navigation conventions instead of being a stand-alone system. This simplifies the transition to post trip monitoring, since the same interface is used.
 - (2) Critical function monitoring is used for power production (making megawatts) during normal operation in the same manner as it is used for safety post trip. Thus, operators are familiar with operation by function normally which is easily extended to safety during off-normal events.
 - (3) Another integration feature pertains to monitoring of Regulatory Guide 1.97 Category 1 parameters. DIAS channel N flat panel displays are part of the normal interface at appropriate functional locations on control room panels. These displays use a validation algorithm to compare the process representation signal to the PAMI channels for consistency. Successful validation is indicated to the operator on the display to allow use of the validated parameter display during accidents. A redundant display of all Category 1 parameters is provided on the safety monitoring panels. The Regulatory Guide 1.97 approach is explained in Section 7.4 of CESSAR-DC.

- (4) The IPSO display also integrates normal and accident monitoring. IPSO provides both power production and safety information through major systems and components status, existence of high priority alarms, deviations from setpoints and parameter trends and key representative parameters. IPSO uses the same display and methodology to provide both sets of information, thus improving operator's comprehension of accident monitoring during the infrequent times when it is required.
- d. The Nuplex 80+ design uses information processing in monitoring and control systems to reduce the information processing requirements of the operator. The reduction in the number of displays required is based primarily on the application of signal validation which provides process representation parameter values by processing multiple channels of data for the operator. Failed sensor inputs are eliminated from the calculation and alarmed, and a process representation value is calculated using the good inputs. The reduction in the number of alarm tiles results from prioritization, signal validation and alarm grouping. Alarm actuations during events are reduced by post-trip mode dependency and alarm grouping. Both tile and alarm actuation reduction contribute to providing useful alarm information instead of data.

The benefit of display and alarm reductions has been quantified to demonstrate that the operator will have less data which requires processing. Typical numbers for a panel section are an 80% reduction in displays and a 60% reduction in alarm tiles compared to conventional plants. Acceptable information content of both interfaces was verified by the availability verification process as described in the Verification Analysis Report.

Each of the aforementioned features has been built into the Nuplex 80+ prototypes of the RCS panel man-machine interface and IPSO. Dynamic simulation of complex plant events, such as SGTR with loss of off-site power, have been used to evaluate the effectiveness of these features and to verify that new problems have not been introduced. Experience with the mock-ups has shown a qualitative improvement in alarm presentation and comprehension.

As discussed in the response to Question 620.12, further evidence of comprehensive improvement has been provided through Halden validations of CFM, SPM and IPSO, design reviews and demonstrations to power plant personnel.

Number: 620.14

Question: What is the projected reliability of the controls and displays in the control room?

Response: The reliability of all Nuplex 80+ control and display systems is documented based on representative hardware (final hardware selections are not made for design certification). Typical of Nuplex 80+ system reliability is the availability of control room information from the DPS which has been calculated to be 99.98% with an MTTR of 4 hours. The DPS availability analysis report documenting this calculation has been made available to the NRC in the C-E Rockville, MD office. It is important to note that in the Nuplex 80+ design, information is presented through two separate system interfaces (DIAS and DPS) so the availability of information and reliability of the ensemble in providing it is higher than individual system availabilities.

Control systems (Process-CCS, ESF-CCS and PCS) have redundant controls available in the MCR via dedicated controls and system operators' modules, thus the availability of a given control function is significantly greater than in present control rooms

Number: 620.15

Question: Describe the human engineering analyses and the findings of the analyses that supported the decision to use CRTs and flat panel displays as the primary sources of operator information and hardwired instrumentation as the back-up instrumentation.

Response: There are no backups used in the Nuplex 80+ design and no hardwired instrumentation is provided. The entire ensemble of computer based man-machine interfaces, including flat panel displays (DIAS), CRTs (DPS), process controllers, component controls and operators modules (control and protection systems), is treated as an integrated package. Although information and control may be accessible via two media devices, each device is designed such that its attributes encourage its use during all modes of operation. Therefore, all media are familiar to the operator and less likely to induce error under stressful conditions, such as accidents and/or operation with equipment failures. All indicators and controls are qualified to the degree required for their intended function.

The basis for selection of flat panel displays was provided in the response to Question 620.2. The use of CRTs were chosen because of their superior multi-color graphics capabilities for display. In addition, their flexibility and ability to present serial data with little limitation on space and their ease of design changes for software based interfaces contributed to the decision. No specific studies were performed during the Nuplex 80+ design process related to use of color graphic CRT displays. Presentation of data in the context of color graphic mimic displays has been long accepted as a significant improvement over large quantities of non-context related analog indicators. The deficiencies with CRT media (also long recognized) of paging to access frequently needed key information and the keyhole effect during transients and upsets are overcome in Nuplex 80+ by supplementing the CRTs with a limited number of spatially dedicated indicators and alarm tiles. As stated previously, all devices are used in compliment without unused backups.

Number: 620.16

Question: How was the task analysis used by those responsible for the individual panel designs? On what basis was the allocation of tasks made to specific places of equipment?

Response: The task analysis data was used by designers, as one of several inputs into the design process, to determine what information and controls would be placed on a panel and its corresponding displays. Other input included panel designs and instrument lists of other C-E plants and previous Nuplex 80 panel designs. Another key to this process was that the designers were experienced reactor operators and design reviews were held with other operators as well as a multi-disciplined engineering team. C-E has also factored in feedback from more than 10³ demonstrations of the design to multi-disciplined industry personnel. The panel design process is fully described with an example in CESSAR-DC Sections 18.7.2 and 18.7.3 and in more detail in NPX80-IC-RR-791-01*.

The function allocation between man and machine was initially assumed to be the same as for System 80 control rooms. This assumption was made because no function allocation problems had been identified in the System 80 designs. With the evolutionary approach to the Nuplex 80+ design, no significant changes in function allocation were sought. This assumption was checked through a task loading analysis as part of the task analysis process. No instances of unacceptable task loading were identified so no changes to the allocation between man and machine were required. For allocation of information to specific equipment, essentially all information was allocated to be presented on the CRTs. This was further allocated to general monitoring (Level 1), control (Level 2), or diagnostic (Level 3) displays per criteria found in NPX80-IC-SD710-01*, Section 6.0. The information selected for spatially dedicated display on DIAS devices was determined using criteria in Section 7.0 of that document. The final selection decisions were made by the designer of individual panel sections and reviewed by the design team, design review team and verification analysis.

*This document is considered proprietary to Combustion Engineering, Inc. Access to this document will be provided to facilitate NRC staff review of CESSAR-DC. Information from this document determined to be necessary to support the staff's safety finding will be placed in CESSAR-DC in a future amendment.

Number: 620.17

Question: How was the adequacy of the information supplied to the operator to perform the tasks determined for the following:

- a. Type of data
- b. Amount of data
- c. Usability of data
- d. Compatibility with other forms of information/data supplied in the plant at local control stations, on specific pieces of equipment, etc.

Response: a)b) The adequacy of information required was determined using the data generated in the task analysis. The characteristics of that data are identified in CESSAR-DC Section 18.5 and in more detail in CEN-307. Specific characteristics for the information and controls of the System 80+ design were identified in the System 80+ task analysis. The Nuplex 80+ design was developed using this data and the other sources of input identified in the response to Question 620.16. The design was independently verified to have sufficient data with proper characteristics in the Availability Verification. This analysis is described in the response to Question 620.30.

- c) Determination of the useability of data provided on MMI devices was the key result of the suitability verification as described in the response to Question 620.30.
- d) Compatibility of the various forms of information throughout the plant is assured by commitment to use the same Nuplex 80+ conventions plant-wide. This is possible since System 80+ is a complete plant design. The C-E document review system assures that all disciplines including human factors are aware of potential interfaces. Therefore, the design of interfaces at local control stations or specific pieces of equipment will use Nuplex 80+ conventions and be reviewed and approved by Nuplex 80+ design team members.

Number: 620.18

Question: Who is on the initial design team and who is on the review team? Are they the same people or are the teams composed of different people?

Response: The initial design team was composed of human factors specialists, nuclear systems engineers, senior reactor operators, I&C engineers, computer specialists and project managers. Table 18.2-1 of CESSAR-DC indicates the number of full-time and part-time members of the design team that were in each discipline. It is noted that the team included members from Duke Power Company (now Duke Engineering Services, Inc.) who provided both a constructor's and plant operator's perspective on advanced control complex design.

The design review team was composed of representatives from reactor engineering, fluid systems and component engineering, startup services, nuclear licensing, instrumentation and control engineering, human factors services and plant operation and construction. This composition is provided in Table 18.2-3 of CESSAR-DC. The review team was composed of individuals independent from the design team, except for two individuals who were included to respond to questions on the design and design process. This overlap also provided communication between the teams and to facilitate resolution of comments.

The review team for Nuplex 80+ verification and validation activities consists of people that are independent of the design team, including administratively reporting to separate management. In addition to the formal design review team the design has been reviewed by many individuals and organizations during more than 100 mockup demonstrations during the last two years. This has included utilities, regulatory agencies, national labs and many foreign organizations. Though their comments are not part of the formal review, comments are considered for changes to the design.

Number: 620.19

Question: Human engineering is not included under Design Process Activities. Under Primary Responsibilities a human factors specialist is also not included. Please explain the scope, responsibility, and reporting structure of the human engineering function in the System 80+ program.

Response: The intent of Table 18.2-2 was to show a high level list of activities performed during the design of the Nuplex 80+ Advanced Control Complex and to indicate in which activities each discipline, including human factors, had a primary role. Thus, human factors is shown not as a design process activity itself but rather an integral part of many of the activities performed.

The scope of the human engineering function includes all those activities listed in Table 18.2-2 with primary responsibility being with a human factors specialist. Human factors specialists also had lesser involvement in other areas such as development of the design bases. The human factors responsibilities included performing the task analysis, defining MMI conventions and methodologies and reviewing resulting interface designs, developing control room environmental criteria, assessing the MCR configuration and performing verification (availability and suitability) and validation activities.

Human factors members of the design team report technically to the supervisor of Advanced Instrument Design of the Instrumentation and Controls Department. Human Factors members of the review team reported to the supervisor of Human Factors and Cognitive Engineering in the Operational Services Department. This was discussed with illustrations in the response to Question 620.1.

Number: 620.20

Question: Identify the human engineering principles established for Nuplex 80. What analyses were used to identify the areas requiring improvement. What "specific improvements" were added?

Response: The human engineering principles that Nuplex 80 was based on are very similar to those of Nuplex 80+. The design was based on a functional task analysis, human factors specialists and operators were heavily involved in all phases of the design, availability and suitability verification analyses were performed and a dynamic mock-up was used to evaluate and refine the design.

A significant source used to identify areas requiring improvement in Nuplex 80 was customer feedback. Nuplex 80 was sold to Jersey Central P&L, TVA, and New York State Gas and Electric for System 80 plants. As is indicated in CESSAR-DC, a significant amount of design work was done for TVA. The design was also bid to Tai Power in the early 1980's. A number of the areas addressed in the Nuplex 80+ were identified by customers during the design and bid processes.

During the Nuplex 80+ design process areas in the Nuplex 80 design requiring improvement were identified and considered through design review meetings. These meetings included operators, human factors specialists, instrumentation and controls engineers and project management. Each improvement area was considered for regulatory requirements, customer desires and technical considerations, such as advances in technology. Specific areas requiring improvement were identified and addressed as indicated in Section 18.6.1 of CESSAR-DC. These include removing hardwired backups for indications and alarms and integrating spatially dedicated indications and alarms into the primary interface with no backups. This allows the operator to use his normal interface during stressful situations such as losing CRT display capability. A dedicated console for a control room supervisor was added since utilities desired a supervisor to perform a monitoring and direction role and no workstation to support this role was available in Nuplex 80. To meet plant availability goals, Nuplex 80+ is designed for continued operation upon complete failure of the DPS instead of requiring shutdown as with Nuplex 80. Nuplex 80+ incorporates alarm handling improvements, such as mode dependency, to address industry concerns with alarm systems. Incorporation of the big board IPSO into the design provides a plant functional and system overview not available in Nuplex 80. Integration of the SPDS function into the normal man-machine interface through critical functions monitoring makes it part of the everyday interface and, thus, familiar during accident situations. Application of advanced control system improvements which were developed for conventional plants (e.g. automatic low power feedwater control) and were not available for Nuplex 80 also improve plant availability. Integration of divisional equipment

into common panels rather than separation by panel sections as in Nuplex 80, allows multiple success path coordination by one operator and improved task performance.

Number: 620.21

Question: How was the potential for human error identified, reduced, and documented in "Reduce the potential for human error that could affect safety or availability?"

Response: Specific problem areas where there was a relatively high potential for human error were identified during the early phases of the DOE Advanced I&C program. This was accomplished by reviewing LERs, Regulatory Guides, I&E bulletins, NUREGs, EPRI reports and other industry reports (e.g., Halden reports). For example, Regulatory Guide 1.97 recommends that the same instruments should be used for accident monitoring as are used for normal operations to enable operators to use familiar instruments during accidents. This led in part to the no backup approach of Nuplex 80+. Other specific areas for improvement were identified in Chapter 10 of the EPRI ALWR-URD. Documentation of the areas requiring improvement was provided through milestone reports in the Control System Performance and Reliability task and the Alarm and Display Methodology task of the Advanced I&C program.

Solutions were formed for the problems identified and incorporated into the design. For example, one area identified as resulting in a high potential for operator error at conventional plants was low power feedwater control. Numerous reactor trips have resulted from manual control during this condition. Digital feedwater systems providing automatic control at low power have been installed at existing plants and have reduced the potential for error in this condition significantly. The same digital control system design is incorporated into the Nuplex 80+ ACC.

C-E has no plans to attempt to quantify the reduction in human error potential. C-E will only verify that new problems have not been introduced by the solutions to existing problems. The Nuplex 80+ verification and validation analyses are the final tests that those features incorporated to solve problem areas do perform without introduction of new errors. The suitability of the interface was evaluated in the verification analysis. Validation of the features in relation to plant operation using the complete control room design will occur later in the design process using the dynamic mockup. The software based designs used in Nuplex 80+ are more suited to incorporating changes identified during V&V because of the relative ease in making changes in software rather than hardware.

Number: 620.22

Question: How was the reduction of operator information processing identified, reduced, and documented in "Reduce the operator's information processing while meeting all of his information needs."

Response: Stimulus overload has been identified as a concern with conventional nuclear plant control rooms. The quantity of data generated from the plant is enormous and little data processing is performed in conventional plants before presenting it to the operator. This led to presentation of more information than a person can reasonably comprehend, particularly during plant upset conditions when many parameters may be changing. The 1979 TMI-2 accident provides a good example of key information being lost in the sea of data provided. This fact has been documented in numerous industry reports (e.g., EPRI NP-3448 for alarm overload). The reality of information overload was confirmed by operators on the Nuplex 80+ design team.

Based on the stimulus overload problem identified above, the Nuplex 80+ goal to reduce the amount of data operators must process, while still meeting their information needs, was formulated through design review meetings and discussions with operators. It was identified that additional information resulting from I&C design and licensing requirements (e.g., 16 instrument channels of the same parameter) was partly responsible for data that added to the operators task loading. Alarm systems presenting more alarms than can be comprehended during upsets, including non-applicable alarms, were also a contributor. The Nuplex 80+ approach is to integrate information to meet the operators needs (as identified in the functional task analyses) while reducing the amount of data to be sifted through to obtain that information.

The amount of processing required of the operator was reduced by validating process signals to provide one correct "process representation value," instead of indicating all parameter channels. That value is used on all spatially dedicated displays and all video displays, including IPSO. Individual sensor values are available on specific Level 3 diagnostic CRT displays. The "process representation value" is also used in all application programs, including control system algorithms and alarm algorithms. The result is that all systems, and the operator, make their decisions based on the most accurate information available. Other processing which was provided to reduce that required by operators includes alarm grouping and mode dependency, critical function and success path monitoring, and the IPSO display which provides a continuous plant overview.

Number: 620.23

Question: How will C-E demonstrate that improvements in the reliability of the man-machine interface have been achieved, as noted in the statement, "Improve the reliability of the man-machine interface through redundancy, segmentation, and diversity"? Does the term man-machine interface refer to the reliability of the hardware or a reduction in human error?

Response: The statement in CESSAR-DC does not refer to human error. The reliability referred to in this statement is the functional reliability of the entire man-machine interface as a whole; i.e., the probability that a given piece of information or a control is available if needed. A goal of the Nuplex 80+ design is to provide a high functional reliability through redundancy and segmentation within systems and diversity between systems. This approach provides highly reliable hardware systems (redundancy), limits the effect of failures in a system (segmentation) and protects against common mode hardware or software failures. For example, redundant processors and data communication exist within DIAS and CCS segments and redundant computers are used for the DPS design. This results in single failures having no effect on the performance of the system related to the availability of information or a control. In addition, both the DIAS and DPS present high priority alarms and indications to assure information access even with multiple failures.

The DIAS and CCS are based on segments related to panel sections and plant functions, respectively. Segmentation limits the impact of multiple failures (e.g., failure of both segment processors) to relatively small, manageable areas. Nuplex 80+ uses diversity to improve reliability by protecting against common mode failures. For example, the DIAS and DPS monitoring systems employ diverse types of processors (super mini-computers vs. micro-computers) and different interface devices (CRTs vs. electroluminescent displays). The result is a reliable system that can continue to operate with failures.

The hardware reliability of individual systems has been or is being calculated, but no quantitative evaluation of the functional reliability is planned.

Number: 620.24

Question: Describe the workload analysis for one and three person operation of the controlling workspace. Describe how the task loading and work loads change.

Response: One-person operation is the minimum staffing level for Nuplex 80+. Note that one-person operation refers to one person in the controlling workspace. Other operators are available in the control room. However, the ACC is designed to accommodate other staffing levels that utilities may desire during normal operation or are required by emergency operation. A workload analysis was performed for one-man operation as part of the task analysis. The workload analysis evaluated operator workload during events expected to tax the operator, such as the first minutes after a reactor trip. The analysis was performed to determine if the existing function allocation was acceptable for one-person operation. A description of the analysis is provided in Section 18.5.1.8 of CESSAR-DC. The workload analysis found no conflicts with the Nuplex 80+ function allocation for one-person operation. Further details of the analysis are available in the Function Task Analysis report, NPX80-IC-DP-790-02*.

The expected division of work for other staffing levels has also been evaluated. The maximum staffing level designed for in the controlling workspace is six people, as specified in the EPRI ALWR-URD. For this situation it is expected that two operators (either RO or SRO) would be located at the MCC, one each at the auxiliary console and safety console and two individuals (either the control room supervisor or shift supervisor and an STA) at the CRS console. Analysis has shown adequate workspace and information access for all individuals for this situation. There is an infinite range of task loading possible for operator staffs between one and six people, dependent on different plant events and conditions. These were not all analyzed but bounded by the extremes previously discussed.

Further information on allocation of tasks during different staffing levels is provided in the response to Question 620.25. That response addresses the minimum staffing during accidents (i.e., three operators) with expected work allocations.

*This document is considered proprietary to Combustion Engineering, Inc. Access to this document will be provided to facilitate NRC staff review of CESSAR-DC. Information from this document determined to be necessary to support the staff's safety finding will be placed in CESSAR-DC in a future amendment.

Number: 620.25

Question: Describe the basis for the design goal of one person control of operations between hot standby and full power. Were separate task analyses performed for one and three person operations? How does the allocation of tasks among the staff change in the control room for one person, three person and a full six person shift?

Response: The basis for the design goal of one person operation between hot standby and full power is the EPRI ALWR-URD. This is specified by Chapter 10 Requirement 4.2.4 which also provides a basis indicating that this is a design capability desired by utilities. Only one task analysis was performed for different staffing conditions as the tasks do not change but allocation to different staff members does.

Theoretically, an infinite number of task allocations exist in this control room, as in any control room, with utility and crew preferences being a significant factor in the actual allocations. For normal operation between hot standby and full power one, two or more operators can be used to operate the plant. A function allocation analysis for one-person operation was discussed in the response to Question 620.24. A typical allocation of tasks for two operators would be one RO at the MCC performing actual hands on monitoring and control of the plant. The second operator, likely an SRO, would be at the CRS console overseeing operation, coordinating with maintenance and other plant personnel, performing administrative tasks and performing or directing surveillance. The CRS console has two CRTs for monitoring, but no controls. During startup and shutdown conditions an additional operating staff member would be at the Auxiliary Console interacting with equipment that must be started or stopped during these modes. The SRO would again be primarily at the CRS console coordinating the startup or shutdown activities in the control room and with other plant personnel.

During emergency operations the minimum staffing in Nuplex 80+ is three operators. An SRO would man the CRS console to monitor plant conditions and safety functions, direct recovery approaches and select appropriate procedures, and communicate with the rest of the plant. One RO would monitor and control normal success paths using non-safety systems at the MCC while another RO would control and monitor emergency success paths at the safety console. The three-person minimum staff for emergencies is based on emergency success paths that meet the single failure criterion, i.e., even with a failure they will perform their function. Upon system failures an additional RO would be required to restore success paths at either the safety console or auxiliary console (e.g., electrical power). Typical tasks for others who may be in the controlling workspace include an STA, who monitors safety functions and assures that the recovery approach is appropriate and the shift supervisor who coordinates overall plant station response to the emergency.

Number: 620.26

Question: How does the Nuplex 80+ configuration minimize required access to the controlling space? A desk/barrier does not appear to reduce the requirement for maintenance personnel access to control room equipment and face-to-face communications with the operating staff.

Response: The Nuplex 80+ Advanced Control Complex includes a number of features designed to minimize required access to the controlling workspace and lessen traffic in both normal and emergency operations.

To access information NEO's can use CRTs in the ARO/NEO support office or the TSC without entering the controlling workspace. For maintenance, testing and other routine interfaces between operators and NEO's (or other plant staff) the design allows the interface to occur at the CRS desk, outside the controlling workspace or in control room offices. Both locations minimize traffic in the controlling workspace. Having local maintenance and test panels on the CCS and the fact that all calibration is performed outside the main control room further reduces traffic. NEO's primarily need to enter the main control room for discussion.

Nuplex 80+ panel design features further reduce interference which could be caused by maintenance activities. Panels are designed for quick equipment removal. Typically, removal of four screws and detachment of quick disconnect connectors will allow removal of ELD devices. Thus, all discrete indicators, alarm tiles and controllers are easily and quickly removable. Switches are modular and easily replaced. Only items which require rare maintenance and have low failure rates (e.g., power supplies) are in the less accessible portions of the panel.

For both normal and emergency operations the availability of all CRT monitoring displays in the SS and CRS offices will reduce control room access requirements. Access to plant status information to support management and operations discussions is available without entry into the controlling workspace. The direct viewing window from the TSC will minimize control room access needs of emergency response personnel during emergencies by enhancing communication between TSC personnel and the operating staff. It also allows visitors or plant staff to view the main control room without entry during normal conditions. DPS CRTs, with all the same displays as in the control room, are located in the TSC to meet the information needs of response personnel.

Number: 620.27

Question: Describe the duties and responsibilities of the control room supervisor and describe the tasks expected to be performed at the CRS console in the control room. Which tasks will be performed in the supervisor's office? Who will be the primary operators of the CRTs on the control room supervisor's console and what displays are they expected to use or access?

Response: The control room supervisor (CRS) performs a wide range of duties related to administration of the operations crew and plant evolutions, monitoring of plant status, and interfacing with maintenance and technical personnel. The responsibility of the CRS in the Nuplex 80+ ACC is primarily to oversee and direct and does not differ notably from his duties at current LWRs. The exact nature of his duties and responsibilities will be determined by the individual utility and its operating philosophy. The CRS may be in his office having meetings, conducting administrative tasks, or communicating with other groups when his presence is not required in the controlling workspace. All of the CRS's activities can be performed in his offices, except where face-to-face communication with operators at the panel is required. Further details on the CRS console and control room offices are provided in CESSAR-DC Sections 18.6.5.3 and 18.6.5.4, respectively.

The CRS, shift supervisor and shift technical advisor will all use the CRS console in the control room. All DPS CRT display page selections are available to these individuals on two CRTs at the CRS console. Their use of them depends greatly on plant condition and the operations in progress. Control room operators will not use this console, as it is primarily a monitoring station with no controls. However, any and all Nuplex 80+ CRT displays can be accessed from the CRS console.

Number: 620.28

Question: Explain how the control room design addresses the issues of habitability and the storage requirements for working documentation, procedures, supplies and personal effects. Describe the process used to establish the requirements for areas that support the control room such as the Technical Support Center, shift supervisor's office, etc.

Response: The habitability and storage requirements for the Nuplex 80+ control room have been defined and documented in detail in CESSAR-DC, Section 18.6.6. For habitability of the control room the Nuplex 80+ design adheres to the guidance of 10CFR50, Appendix A, NUREG-0737, Supplement 1, and other pertinent regulatory documents applicable to fire, smoke and radiation conditions. Toxic gas limits are defined as in Regulatory Guides 1.78 and 1.95.

In addition to the aforementioned regulatory documents, habitability and storage requirements were based on EPRI ALWR-URD/Chapter 10, utility experience and discussions with experienced reactor operators. Significant input to this aspect of the design was provided by Duke Power Company as both a utility and plant constructor with extensive experience. Storage for reference documents such as frequently used procedures and manuals is provided on rolling bookcases. Dedicated rolling bookcases are provided for the MCC, AC and SC with frequently used procedures and manuals for each console. Control room furnishings, laydown space, and miscellaneous storage, are described in CESSAR-DC, Section 18.6.5.5. The provisions for the control room office are described in Section 18.6.5.4. Adequate storage for all necessary documents and personal effects is provided in the MCR, CRS offices and TSC.

Number: 620.29

Question: How was "sufficient instrumentation" identified for the Remote Shutdown Panel? Describe the human engineering efforts or studies which contributed to the design of the Remote Shutdown Panel and the "convenience controls" distributed at equipment locations.

Response: Sufficient instrumentation for the RSP was identified based on a function task analysis, as with the main control panels. The description of the human factors engineering task analysis for safe shutdown is described in Section 18.8.1 of CESSAR-DC. In addition, C-E's extensive experience in designing remote shutdown panels for Palo Verde 1, 2 and 3 and other plants was considered. Sections 7.4 and 7.5 of CESSAR-DC give full listings of what was determined to be sufficient instrumentation for the RSP. This list was reviewed by all engineering disciplines within C-E to assure all system designer requirements, as well as operational requirements, were met.

Essentially the same design process was followed for the RSP as for the main control room panel designs. The RSP design is based on the standard Nuplex 80+ indication and control methodologies (CESSAR-DC, Section 18.7.1) and HF design criteria (Section 18.7.2). Special needs which differentiate the RSP from MCR panels are described in Section 18.8.1.2-4.

As indicated in Section 18.8 of CESSAR-DC, cold shutdown is achievable from the RSP without the need for local equipment controls. However, local convenience controls are maintained to the same degree as in existing plants. Appropriate human factors criteria are applied to the design of local controls.

Number: 620.30

Question: Describe the human engineering test and evaluation methodologies that have been, or will be, used. How does the human engineering test and evaluation program fold into the System 80+ verification and validation program?

Response: The human factors test and evaluation methodologies can be divided into three phases; those occurring before the start of the Nuplex 80+ design, those occurring during the design certification process and those that will occur after certification.

Prior to the initiation of the Nuplex 80+ design effort much of the advanced technology used in the Nuplex 80+ man-machine interface had been tested. Critical Function Monitoring System (CFMS) designs are operating in numerous plants as an SPDS and have been evaluated as part of the DCRDR process. In addition to CFMS plant operating experience, a human factors validation program was performed by the OECD Halden Reactor Project on the CFMS design. The extension of the critical function approach to success path monitoring (SPM) was also validated at Halden. This validation demonstrated improved performance for operators using SPM compared to control operators without it. Similarly, after development of IPSO, but before installation at the Borselle plant, the design was evaluated by Halden with favorable results. Halden reports exist for all of these evaluations and the most significant ones are included as part of the Nuplex 80+ reference design documents.

Another significant group of evaluations conducted prior to the Nuplex 80+ program occurred as part of the Nuplex 80 ACC development program. This included configuration studies for which the Nuplex 80+ master control console is based and many studies related to CRT display of information and the benefits of hardwired annunciators. The Nuplex 80 studies included a significant amount of interaction with plant operators and use of a complete control room dynamic mock-up. The pre-Nuplex 80+ evaluations, tests and experience are shown on Figure 18.4-5 of CESSAR-DC.

During the Nuplex 80+ design process for certification, test and evaluations have included the functional task analysis and corresponding workload analysis, and the verification analysis. The functional task analysis and workload analysis are documented fully in the Functional Task Analysis Report, NPX80-IC-DP-790-02*, of the Nuplex 80+ reference design documents (also see Question

*This document is considered proprietary to Combustion Engineering, Inc. Access to this document will be provided to facilitate NRC staff review of CESSAR-DC. Information from this document determined to be necessary to support the staff's safety finding will be placed in CESSAR-DC in a future amendment.

620.24). The availability analysis of the verification process assured availability of required instrumentation and controls with appropriate characteristics. The methodology and results of the analysis are described in the verification analysis report NPX80-IC-TE-790-01* in the reference design documentation. The suitability analysis evaluated the usability of each of the MMI devices and, on a panel basis, the ensemble as a whole using the RCS panel and IPSO prototypes. This is also documented in the verification analysis report. Other tests and evaluations were related to product evaluations (e.g., flat panel displays) and specific man-machine interface conventions. The analyses and evaluations performed during certification are shown in Figure 18.4.1 of CESSAR-DC.

Subsequent to design certification a main control room mockup will be completed with dynamic MMI components at selected panel sections. This complete, partially dynamic mockup facility will be used to conduct a HFE validation program using operators and representative operating procedures. This is described in Section 18.9 of CESSAR-DC. Before Nuplex 80+ is delivered to a plant, a factory integration test of all systems, including a complete set of hardware, will be performed. This will include additional human factors validation activities. The Nuplex 80+ design process, including evaluations and tests, is shown in Figure 620.30-1.

This approach to Nuplex 80+ verification and validation activities was selected because of the evolutionary nature of the Nuplex 80+ design. For conventional power plants, a static mock-up of the main control panels, combined with detailed factory testing of equipment has been used for validation of nuclear plant instrumentation and controls.

For an advanced control complex design, more detailed integration of the static mock-up and dynamic factory acceptance testing is desired. The dynamic mock-up approach is acceptable for the support of Nuplex 80+ verification and validation activities because the design of key man-machine interfaces have not changed radically from conventional designs. All time critical parameters and alarms are provided on discrete indicators and alarm tiles which closely resemble conventional meters and alarms. Primarily a different computer-based hardware implementation is used. Important component controls are essentially identical to those

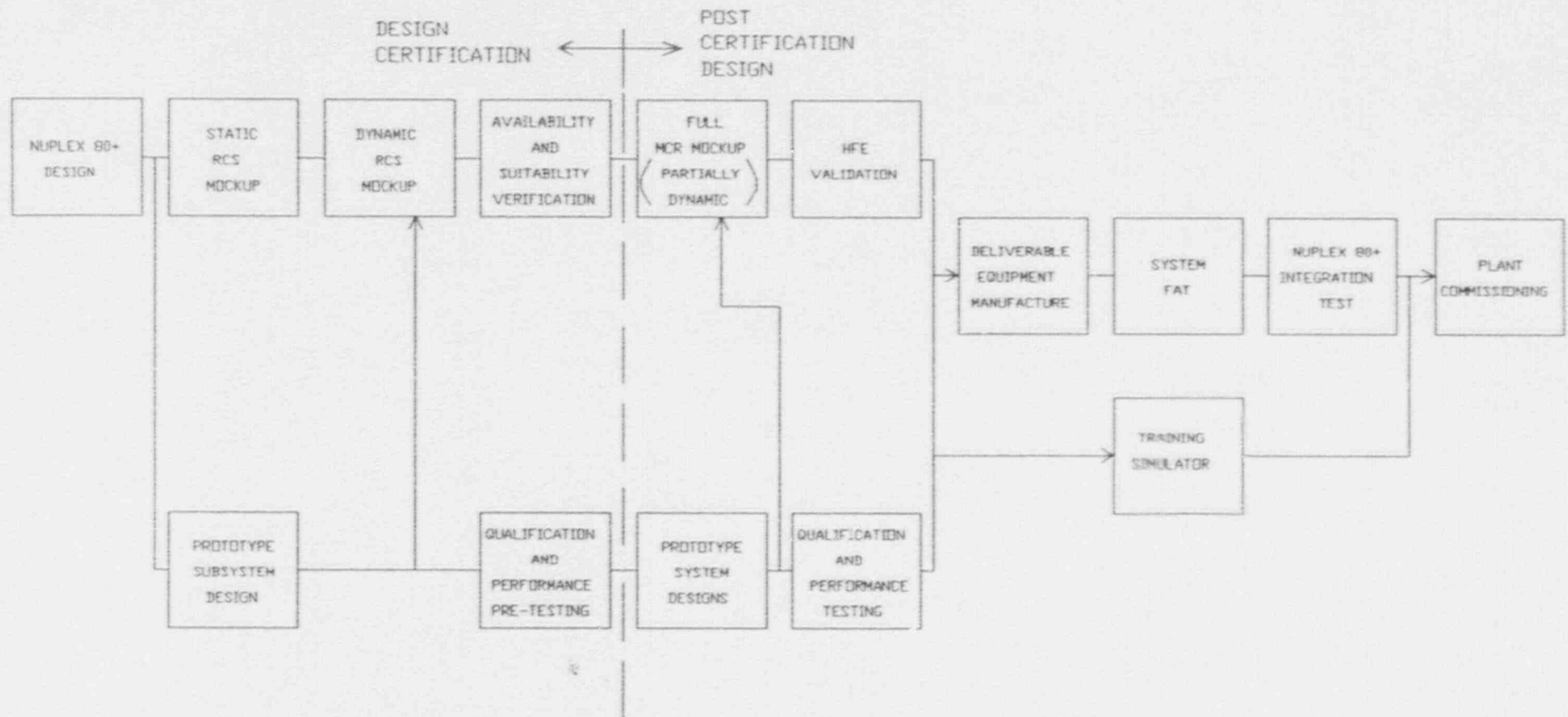
*This document is considered proprietary to Combustion Engineering, Inc. Access to this document will be provided to facilitate NRC staff review of CESSAR-DC. Information from this document determined to be necessary to support the staff's safety finding will be placed in CESSAR-DC in a future amendment.

used on System 80 designs. Based on C-E evaluations and review by independent engineers and operators, these small changes to indications and controls are not expected to induce any new potential for operator error.

The integration of CRTs and soft controllers into the interface can effectively be evaluated on selected dynamic panel sections with little benefit obtained by implementing them dynamically in the entire control room. All Nuplex 80+ MMI devices, including touch screens, are used in existing nuclear power plants. Nuplex 80+ panel layouts follow conventional designs (i.e., by system from heat source to heat sink, with auxiliary panels also arranged by system). The design is based on existing procedures and crew operating methods with no intent to change. Thus, a full scope simulator is not used for verification and validation of the Nuplex 80+ main control room, as it might be if the design was radically different from conventional designs.

The human factors verification and validation activities are part of the overall Nuplex 80+ verification and validation program plan. The remainder of the test and evaluation program as described above is not part of the Nuplex 80+ V&V program.

FIGURE 620.30-1
NUPLEX 80+ DESIGN PROCESS



Number: 620.31

Question: The System 80+ control room design currently includes several types of control and display instrumentation. Some of it is new to control room applications, some is not. This paragraph states, "The man-machine interface is based on accepted human engineering methods, principles and criteria such as those presented in NUREG-0700." Identify the principal human engineering source documents used in the development of the man-machine interfaces, such as:

- a. Identify which elements of the man-machine interface were developed based on existing human engineering documentation. Identify the documentation.
- b. Identify which elements of the man-machine interface required the development of additional human engineering guidance. Identify the guidance.
- c. Describe the means C-E will use to ensure (1) that the man-machine interface aspects of the new technology will be compatible with that of the established technologies, (2) that the new man-machine interfaces will meet the requirements of the tasks, as defined by the human engineering studies, and (3) that the differences as well as the similarities among the man-machine interface devices enhance operator and maintainer performance.

Response: a. Most of the Nuplex 80+ man-machine interface elements were developed based on existing principles and criteria. This was possible because elements were either similar to conventional control room technology or an evolution from conventional technology. Man-machine elements for which criteria exist include IPSO, flat panel displays used for alarm tiles, discrete indicators and controls, CRTs and switches. The source documents used for criteria for these interfaces are provided in Table C20.31-1.

- b. The only element of the man-machine interface which required additional human engineering guidance was the use of touch screen interfaces for the CRTs, flat panel displays and controls. The existing guidance used to design touch access were for target size, target separation, response time, input duration, input sequence, and feedback. Two other criteria were developed for implementation of Nuplex 80+ touch screen interfaces:
 1. Actuation occurs upon removal of touch from the screen not engagement. This allows the operator the ability to correct any incorrect selections that may have occurred before actuation.

2. Touch targets are identifiable from other display elements. Systematic target conventions and spatial dedication of the targets allow the operator to clearly identify which targets are selectable and which are not.
- c. 1. The Nuplex 80+ design uses consistent and compatible interfaces and conventions throughout the interface. Technologies for implementing the interface were selected to support compatibility. A good example of Nuplex 80+ interface compatibility is provided by CRT displays and other MMI devices in the MCR. Red and green color conventions are used identically on conventional switches and dynamic CRT displays. Similarly, a standard set of graphic symbology is used between CRTs, switches and controller displays. The yellow alarm color is used on CRTs to ensure compatible with the monochromatic ELDs used for spatially dedicated alarms.

The suitability analysis of the Nuplex 80+ verification process evaluated the compatibility of the different technologies used in the man-machine interface. As identified in Part b, there was only one application of new technology in the Nuplex 80+ MMI with the other devices being used previously in control room applications. Compatibility will be validated during the Nuplex 80+ validation activities, as described in the response to Question 620.30.

2. The availability analysis of the Nuplex 80+ verification analysis specifically evaluated whether task performance requirements were met by the interface devices. Documentation is provided in the reference design documentation in NPX80-IC-TE790-01*.
3. Nuplex 80+ is designed to provide an acceptable interface for operators and maintainers. To facilitate this the design uses to its advantage the similarities and differences in the MMI technologies employed. For example, similarities in technologies allow consistent coding conventions to be employed across all interface devices. Specifically, alarms presented on DIAS alarm tiles and through the CRTs use the same flash rates and shape codes for priority. However, the differences in

*This document is considered proprietary to Combustion Engineering, Inc. Access to this document will be provided to facilitate NRC staff review of CESSAR-DC. Information from this document determined to be necessary to support the staff's safety finding will be placed in CESSAR-DC in a future amendment.

these technologies is also used. For example, spatially dedicated displays use the monochromatic ELDs to present key information simply without color codes. Color graphics CRTs are used to present very detailed information with more extensive coding allowed by color. The technologies used in the interface are all employed in existing nuclear plant control rooms, though Nuplex 80+ extends the use of these technologies. Similar combinations of different technologies have been made in other industries, including fossil power plants.

The suitability analysis has evaluated the acceptability of the interface, including the similarities and differences between technologies. Because of the standardized interface approach across panels and the use of only two display technologies (CRTs and ELDs), in place of many display technologies in conventional control rooms, maintainer and operator performance will be significantly improved. In order to minimize the detrimental effects of standardized designs such as making interpretation of control and display relationships difficult, Nuplex 80+ uses a hierarchical labeling scheme, lines of demarcation, functional or system mimic groupings and system-related panel orientation. This supports familiarity with a component's operation (e.g., a switch or ELD device) while putting it on the context of system operation.

Table 620.31-1

Sources of Human Factors Criteria Used for Nuplex 80+

1. MIL-STD-1472D, "Department of Defense Human Engineering Design Criteria," 1989
2. DOD-HDBK-761A, "DOD Management Information Systems Guidelines," 1987
3. ESD-TR86-278, "User-System Interface Software Guidelines," Smith and Mosier, 1986
4. ANSI/HFS-100, "ANSI VDT Workstation Standard," 1988
5. "User-Computer Interface in Process Control: A Human Factors Engineering Handbook," Gilmore, et al, 1989
6. NASA-STD-3000, "NASA Man-Systems Integration Standards," 1989
7. NASA-USE-100, Ver. 2.1, "NASA Space Station Freedom Program Human Computer Interface," 1989
8. EPRI NP-3659, "Human Factors Guide for Nuclear Power Plant Control Room Development, 1984
9. EPRI NP-4350, "Human Factors Engineering Design Guidelines for Maintainability," 1985
10. NUREG/CR-3517, "Recommendations to NRC on Human Engineering Guidelines for Nuclear Power Plant Maintainability," 1986
11. NUREG-0700, "Guidelines for Control Room Design Reviews," 1981

Number: 620.32

Question: In the context of being presented as a design basis for Nuplex 80+ this paragraph states, "The number of physical display devices and the quantity of data presented to the operator is reduced compared to control rooms for existing plants."

Provide the human engineering studies C-E has done to determine the benefits and drawbacks of reducing the number of display devices and quantity of data presented to the operator. Include specifically the studies which determined the optimal levels of reduction of display devices and data. Include the results of human engineering studies which were used to support the quantity of data presented to the operator, any consolidation of instrumentation, and any changes in the modes of displaying data to the operator in the Nuplex 80+ control room.

Response: The intent of this design basis statement was to partially address the stimulus overload concern. This issue was discussed in the response to Question 620.22 as it relates to increasing the operator's information processing burden. By reducing the number of physical displays in an appropriate manner, the information required for task performance is presented to the operator without all the clutter added by presenting all available data. The need to reduce stimulus overload and, hence, the number physical devices and amount of data provided to operators, has been documented in various industry sources. This includes the EPRI ALWR-URD, industry reports (e.g., NUREG-3448 for alarms), and papers (many identifying this concern as a result of TMI).

Qualitative analyses were performed to evaluate the benefits and drawbacks of reducing the number of physical display devices. An assessment was made based on using the combination of serially presented information (via CRTs) and spatially dedicated information (on flat panel discrete indicators and alarm tiles) to determine an acceptable combination. All data is accessible at any panel through the CRT's serial presentation of information. Thus, the focus of the assessment was on how much spatially dedicated data should be presented in a parallel manner. The result of the assessment led to spatial dedication of Priority 1 and 2 alarms and key parameters on discrete indicators and IPSO. Key parameters for discrete indicators were defined as frequently monitored parameters, parameters most indicative of critical safety function and success path status, Regulatory Guide 1.97 Category 1 parameters and parameters required for investment protection or continued operation without the DPS. The design was then evaluated through the availability and suitability analyses of the verification to assure that an acceptable amount of spatially dedicated data was presented. No quantitative studies were performed to determine optimal levels of reduction, since optimal can only be determined if all possible transients and events are known.

The modes of displaying data in the Nuplex 80+ control room do not change. The interface has been designed to function the same for normal power operations, startup/shutdown or emergencies. This approach specifically includes the use of critical functions for both power and safety and the integration of PAMI displays into a functional panel location via the qualified discrete indicators and CRTs.

Number: 620.34

Question: What studies did C-E perform to determine the amount and type of "operator information overload?" Provide the quantitative and qualitative results of the investigations.

Describe the baseline control room in which the studies were performed and the parameters that were measured or assessed. Were the studies replicated on the C-E System 80+ control room design? What thresholds were established for acceptable and unacceptable levels of operator cognitive loading? How does the System 80+ control room design specifically address each of the parameters assessed by the studies?

Response: The "operator information overload" issue is the same basic concern as addressed in Question 620.22 related to information processing and Question 620.32 related to the number of physical displays. As discussed in those responses, the identified concern is to reduce stimulus overload in a control room. As explained in other responses, the need for reducing operator information overload was identified through industry sources as well as qualitative studies performed for Nuplex 80+.

Qualitative analyses identified the amounts and types of information overload in conventional nuclear plant control rooms. Primary areas identified were information overload from the alarm system after a reactor trip and overload of information from multi-channel indicators of the same process parameter.

The System 80+ control room addresses operator cognitive overload by validating process signals prior to display or alarm, grouping alarms into a relatively small number of alarm tiles, and eliminating Priority 3 alarms and operator aids (e.g., permissives which were previously alarms in many existing control rooms) from spatially dedicated displays. Additional reduction in information overload is provided by reducing the number of alarm actuations during transient events. This is provided in Nuplex 80+ by validating signals before generating alarms and mode and equipment status dependent logic. The design also provides operator aids such as critical function monitoring (to support normal operation and emergency procedure response), success path monitoring (to aid in identifying and restoring success path problems) and IPSO (which provides a plant overview for operators). Each of these advanced features performs a function automatically and continuously that otherwise would have to be performed by operators. For example, IPSO takes several thousand plant parameters and reduces them to a few easily understood process representation symbols.

Quantitative studies were performed comparing the numbers of alarm tiles and indicators for conventional control rooms and Nuplex 80+. Results from the studies have shown a 60% reduction in alarm tiles and an 80% reduction in the number of spatially dedicated displays

for Nuplex 80+ compared to conventional units. Cognitive loading levels were analyzed as part of the task analysis for specific events, as discussed in the response to Question 620.24. This analysis is documented in Section 18.5 and the task analysis report in the reference design documents. Acceptable levels of loading were based on determining cumulative processing times for tasks performed during an event and identifying situations of operator overload based on cognitive loading.

Number: 620.35

Question: This paragraph states, "The effectiveness of modern man-machine interface devices will be demonstrated through the use of prototypes and HFE evaluations." Does this refer to demonstrating the software and hardware attributes of the instrumentation? Or does it refer to human factors and human performance evaluations of (1) the device (as a stand-alone instrument) and (2) in the context of the System 80+ control room environment. When in the design process are the HFE evaluations scheduled to occur? Describe in detail the HFE evaluations that will be performed. Provide a basis for the criteria that will be used to determine a device's effectiveness (as a stand-alone instrument) from the human performance perspective. Also provide the assessment methodology that will be used to determine the suitability of a device for incorporation into the System 80+ control room design.

Response: This statement refers to both demonstrating hardware and software attributes and the suitability of the interface from a human factors perspective. The Nuplex 80+ design process has already and will continue to do hardware attribute evaluations using prototypes. This has included seismic evaluations of equipment to demonstrate the ability to qualify equipment for safety-related applications and hardware configuration studies on prototypes to assure adequate throughput. Software studies have prototyped software implementations using ladder logic programming in programmable logic controllers and software required for data processing features such as success path monitoring, alarm processing and signal validation.

The man-machine interface devices have also been evaluated from a human performance perspective as part of the verification analysis documented in the reference design documentation and discussed in the response to Question 620.30. The suitability analysis evaluated both the man-machine interface devices as stand-alone devices and in the context of the ensemble of Nuplex 80+ interface devices.

HFE evaluations are scheduled throughout the Nuplex 80+ design process. The design process and scheduling of HFE evaluations were discussed in the response to Question 620.30, as was the type of HFE evaluations performed. The criteria used to evaluate the man-machine interfaces were developed from the list of references provided in the verification analysis and in the response to Question 620.31. Individual bases for specific criteria can be found in these references. Similarly, the assessment methodology for the suitability analysis is provided in the verification

analysis report in the reference design documents (NPX80-IC-TE-790-01*). The eventual determination of a device's suitability was determined not only from the human factors acceptability, determined in the suitability analysis, but also by other tests and prototype evaluations such as the seismic analysis. A good example of this process is provided in the response to Question 620.2 for determining the acceptability of flat panel displays.

*This document is considered proprietary to Combustion Engineering, Inc. Access to this document will be provided to facilitate NRC staff review of CESSAR-DC. Information from this document determined to be necessary to support the staff's safety finding will be placed in CESSAR-DC in a future amendment.

Number: 620.35

Question: This paragraph states, "Under degraded conditions, operators will continue to have access to all required information. Equipment failures impacting automated data process and presentation features are accommodated by increased operator surveillance."

What constitutes a degraded condition? Is it the loss of one computer driven display, one electrical bus (potentially affecting many instruments) or all digitally driven equipment?

How does increased surveillance on the part of the operator compensate for the loss of technical data? Are the data and the synthesized information normally available through the computer database available from other sources? Where will the alternate sources of information be located?

From the human performance perspective, how will "increased surveillance" compensate for loss of the computer? Will operators be required to perform calculations, adjustments, or operations (manual, cognitive, decision-making, etc.) that would normally be done by the computer? Describe the impact on operator and crew performance in the control room, at the Technical Support Center and at the Emergency Operations Facility.

Response: A degraded condition referred to in this paragraph is constituted by credible equipment failures, including failure of processors, data communications or a display device itself. The worst case degradations assumed are total loss of DIAS-N or DIAS-P or DPS failure. These worst case conditions encompass loss of an electrical bus. Loss of all digitally driven equipment is not a credible failure and is therefore not considered in the design. This position is acceptable because digital electrical equipment is protected against EMI and the diverse designs used in man-machine interface systems preclude other undefined common mode failures, including software failures, from rendering both diverse designs simultaneously inoperable.

Figure 7.5-1 of CESSAR-DC illustrates the architecture of the Nuplex 80+ monitoring systems. The following credible failures were considered as degraded conditions: failure of the entire DPS system and, thus, all CRT displays, failure of DIAS-P channel or failure of DIAS-N. Each of these cases will be discussed individually.

The worst case degraded condition from an information access perspective is complete failure of the DPS. This is a highly unlikely event, since the DPS is a redundant system with a calculated and demonstrated availability of greater than 99.98% with an MTTR of less than 4 hours. To address this failure, the DIAS has been designed to provide operators with all information required to continue operation for 24 hours. Increased

surveillance is not required to compensate for loss of technical data but rather to accomplish technical specification monitoring and to support information access that is normally enhanced by the DPS and panel CRTs. All functions of the DPS can be performed manually, with additional staff, without the DPS. For example, the Core Operating Limit Supervisory System (COLSS) DPS function which provides core surveillance will have to be performed by an operator. This increased operator surveillance will compensate for not having computer processing to accomplish the function. All required data for this function is available to the operator on DIAS or other displays from the control and protection systems.

Synthesized information from critical function monitoring (CFM) and success path monitoring will also not be available upon complete DPS failure. Since these functions have been designed to support procedures, not replace them in Nuplex 80+, these functions can be performed manually by additional operating staff. For example, the CFM function of performing safety function status checks, normally done by the DPS automatically, can be performed by an STA. This is currently the practice at conventional plants. The alternate source of data will be the DIAS displays, which are located on each panel as part of the primary man-machine interface. Additional information will be provided by operator's modules (CCS and PPS) and switch indicators for component status which are also part of the primary integrated interface.

The impact of DPS failure on the TSC and EOF will be the same as for existing plants. No CRT data would be available in either location and, hence, plant status would not be available via CRT. This situation would be partially compensated for in the Nuplex 80+ TSC design by visibility into the MCR. The viewing window includes a view of IPSO which will continue to be driven by DIAS to provide an overview of plant status. The viewing window also enhances communication with control room operators.

The other credible failures relate to loss of DIAS Channels P or N (see Figure 7.5-1). DIAS P is an independent channel segment of the system which provides one redundant method of monitoring all Regulatory Guide 1.97 Category 1 parameters, including ICCM parameters. Its primary MMI is two flat panel displays of these parameters on the safety monitoring panel. If this channel is lost (though it too has redundant communication and processing), Regulatory Guide 1.97 parameters are still available to operators. Parameter indications are on DIAS N displays dispersed at appropriate functional panel locations throughout the MCR and through any CRT at any panel. This degraded condition will have no functional impact on operations in either the MCR or TSC; however, a technical specification LCO is anticipated to limit the time DIAS-P can be unavailable, since both DIAS-N and P are required to meet the required level of redundancy for qualified systems.

Failure of the DIAS N channel is the other credible degraded condition, though all DIAS N segments have redundant processors and communication. DIAS N failure would render inoperable all spatially dedicated indicators and alarms on the panels. No information would be lost, because all information processing, including signal validation, would still be available through the DPS. Operators would use the DPS for alarm acknowledgement and plant status monitoring as is normally the case, but without the support of spatially dedicated information. IPSO would be unaffected. Little additional surveillance would be required and impact on the operating crew would be significantly less than in the failure of DPS case. This degraded condition has no impact on operations in the TSC.

Operability of accident monitoring instrumentation is covered by a technical specification limiting condition for operation in System 80+. This failure of either DIAS-N or DIAS-P will result in a technical specification action statement to restore the segment within seven days because both DIAS-N and DIAS-P are required to meet the level of redundancy required for qualified systems. Because of the length of the time for action this will not significantly impact daily operations.

Other degraded conditions, such as loss of individual display devices (e.g., CRT or ELDs), loss of any electrical buss, loss of a control device or failure of individual processors (DIAS segments or DPS) are all bounded in terms of impact on the operating crew by the above cases.

In summary, for the worst-case degraded condition, failure of the DPS, increased surveillance will be required to monitor continued compliance with technical specifications. All required data is available on other MCR devices. Some additional calculations and decision-making operations will be required by operators which is expected to be handled by additional crew members in the controlling workspace. No impact on controls, e.g., additional adjustments or manual operations, is expected. The primary impact on crew performance will be additional coordination requirements because of the additional surveillance and potential for manual information processing such as critical function monitoring. Coordination will be the responsibility of the CRS.

Number: 620.36

Question: This paragraph states that, "A standard set of display and access conventions is applied consistently for all information presentation methods." Provide the human engineering document that identifies and discusses the standardized display and access conventions for all the information presentation methods. Do the standards apply to vendor supplied equipment and "off the shelf" hardware and/or software?

Response: The display and access conventions for Nuplex 80+ are provided in the NPX80-IC-SD710-01*, Rev. 0, document in the Nuplex 80+ reference design documents which are available in the C-E Rockville, MD office. This document is currently being updated to incorporate all design changes that have been made as part of the design process (e.g., resulting from the verification analysis).

Off the shelf hardware and software used in Nuplex 80+ is configured to meet the conventions of this document. Vendor supplied equipment in the MCR will be limited to the turbine/generator control system. It is the intent that this equipment conform to the Nuplex 80+ conventions. If this is not possible, C-E will ensure that no conflicts exist between that design and standard conventions which could potentially lead to significant human errors. It is also the intent that vendor-supplied equipment outside the MCR conform to the Nuplex 80+ conventions. Again, if this is not possible, C-E will ensure that no conflicts exist which could potentially lead to significant human errors.

*This document is considered proprietary to Combustion Engineering, Inc. Access to this document will be provided to facilitate NRC staff review of CESSAR-DC. Information from this document determined to be necessary to support the staff's safety finding will be placed in CESSAR-DC in a future amendment.

Number: 620.37

Question: This paragraph states that, "Critical functions established for both safety and power production serve as a primary basis for information and alarm presentation." What is the definition of the term "critical function?" How were "critical functions" identified? Was a critical task analysis performed on critical operator and maintainer tasks in the control room and to what level of detail were the critical task analyses performed? If a critical task analysis was not performed, explain why. How were the contributions of the human engineering task analysis and the critical task analysis integrated into the development of information and alarm presentations?

Response: A critical function is one of a minimum set of functions required to be controlled to keep the plant either in a safe, stable condition (critical safety functions) or producing power (critical power production functions). The critical functions approach to monitoring the safety of a plant is required by NUREG-0696 and NUREG-0737, Supplement 1. These documents identified a minimum set of critical safety functions. C-E, in development of the critical function monitoring system as an SPDS, has identified additional critical functions for safety. Power production functions were identified as part of the Nuplex 80+ design process. Some of the initial concepts relating to power production functions were developed in the EPRI Disturbance Analysis and Surveillance System Program (EPRI NP-1684 and EPRI NP-3595). The critical function approach for Nuplex 80+ is described in NPX80-IC-SD790-02* which is found in the Nuplex 80+ Reference Design Documentation*.

No critical task analysis was performed as part of the Nuplex 80+ design process. This was not necessary because all tasks required of operators could be performed by the assumed staffing levels in the times required using the Nuplex 80+ MMI design. This was confirmed in the event time sequences developed as part of the functional task analysis. Historically in the nuclear industry, responses of operators even during emergencies are not time critical because of the slow response time of a nuclear plant's process system. It has long been a nuclear industry design philosophy to automate time critical responses related to safety. The basis of the plant's safety analysis is that no operator actions are required for 30 minutes to maintain safety during any design basis event.

*This document is considered proprietary to Combustion Engineering, Inc. Access to this document will be provided to facilitate NRC staff review of CESSAR-DC. Information from this document determined to be necessary to support the staff's safety finding will be placed in CESSAR-DC in a future amendment.

A description of how the functional task analysis data was incorporated into the design is provided in the response to Question 620.16.

Number: 620.38

Question: This paragraph says, "Operating staff targets for Nuplex 80+ were established to accommodate a variety of staffing assignments during both normal and emergency operations." How many extra people are expected to be in the control room and the Technical Support Center during an emergency? Provide the analysis that identifies and describes the duties, responsibilities, and capabilities of the additional personnel and the space, equipment, and information they will require. Describe how the current configurations of the control room and Technical Support center meet the requirements and support the duties to be performed.

Response: A discussion of the number of operating staff members expected to be in the control room during emergencies was provided in the response to Question 620.25. The duties, responsibilities and information required for additional control room staff and the Nuplex 80+ design which accommodates them is again addressed in the response to Question 620.25. Duties expected to be performed in the TSC are documented in NUREG-0737 and the EPRI ALWR-URD.

The number of people expected in the TSC is highly variable, but NRC regulations require that it be designed for 25 people (NUREG-0737). The Nuplex 80+ TSC is designed with adequate space, information through the DPS CRTs, personnel access and communication to meet the regulatory requirements. The Nuplex 80+ TSC is described in CESSAF-DC, Section 13.3.3.1. No additional design requirements beyond the ALWR-URD have been imposed on the TSC.