Docket F16

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

March 16, 1992

Docket No. 52-002

APPLICANT: Combustion Engineering, Inc. (CE)

PROJECT: CE System 80+

SUBJECT: SUMMARY OF MEETING WITH CE REGARDING CE SYSTEM 80+ DESIGN CERTIFICATION FOR INSTRUMENTATION AND CONTROL (CHAPTER 7, CESSAR-DC)

A meeting was held between members of the Nuclear Regulatory Commission (NRC) staff and representatives of CE at the CE office in Windsor, Connecticut, on March 2, 1992, regarding the design of System 80+. An agenda of the meeting is provided as Enclosure 1. A list of the meeting participants is Enclosure 2.

CE provided an overview of the NUPLEX 80+ instrumentation & control (I&C) systems used to control the CE System 80+ plant. The NUPLEX 80+ uses commercial hardware and software products that have at least 3000 hours field experience, with a minimum of one-year service (i.e., 6000 units in the field for 1/2 year would not qualify as field proven equipment).

The NUPLEX 80+ is a totally digital system that provides control and protection system functions and system monitoring functions through digital displays. The safety systems are diverse from the non-safety systems in software design and hardware components. The safety related digital system architecture is based on the Intel 80x86 microprocessor, the DOS operating system, and the ArcNet data highway. Included in this digital network are the Plant Protection System, the Engineered Safety Features Component Control System (ESF-CCS), and the Discrete Indication and Alarm System (DIAS).

The non-safety related system architecture uses the Motorola 68000 family of microprocessors, the Unix operating system, and an Ethernet data highway. Included in this digital network are the Process Component Control System (P-CCS), the Power Control System (PCS), and the Data Processing System (DPS).

The DIAS and the DPS provide information to the operators via the display panels in the control room and the remote shutdown panel (RSP). The displays are the same in both operator control areas to facilitate transfers of control from the control room to the RSP. Sharing of instrumentation is done upstream of the diverse network remote multiplexors.

The capacity of the data highways was designed to significantly exceed the anticipated data requirements of the NUPLEX 80+ to ensure reliability of the networks. Additionally, the data system was designed to process by exception many of the system variables, instead of processing every variable for each time step. This reduces the data processing workload while maintaining system process status information on the operator displays.

DF03

NRC FILE CENTER COPY

A tour of the static and dynamic mockups of the control room was conducted, and testing being performed on two different programmable logic controllers (PLCs), Modicon PLCs and Allen-Bradley PLCS, was observed. Diverse PLCs will be used in the control systems to prevent CMF events caused by defects in design or manufacturing process.

CE provided an overview of the Reactor Protection System (RPS), the Engineered Safety Features Actuation System (ESFAS), and the Alternate Protection System (APS). The purpose of this presentation was to familiarize the NRC staff with the basic concepts of the CE System 80+ protection and control systems.

CE stated that their testing process will provide the basis for acceptability of the software product. A discussion on the use of software reliability measures as a means to quantify the quality of the software modules was held. The NRC staff suggested using some of the metrics described in IEEE 982.2-1988, Guide for the Use of Standard Dictionary of Measures to Produce Reliable Software. NRC did not intend to review the values of any software metric outputs as a criteria for acceptance. Rather, NRC would view the use of reliability metrics as an indication of software quality. NRC recommended that CE review IEEE 982.2-1988 for possible use as a means to internally control their software development process. CE does not appear to be receptive to the use of software reliability metrics as an internal control of software development methodologies and philosophy. NRC staff will use this observation as an audit point during the inspections, tests, analyses, and acceptance criteria (ITAAC) phase.

NRC staff expressed concerns regarding incorporation of indefinite bypass in the technical specifications. As currently stated, one RPS channel could be placed in bypass until the plant achieves Mode 2 operations following the next Mode 5 (refueling) operation. CE stated that they had not intended that the technical specifications limit the bypass interval to the next Mode 5, and that they will be submitting a more lenient bypass criteria. The use of indefinite bypass is based upon CE's probabilistic risk assessment (PRA). CE initially stated that the PRAs had been performed using 2/4 channels, but that the difference between 2/3 and 2/4 was minimal. Subsequent conversations revealed that CE may have used 2/3 channels in their analyses. Confirmation of this will be provided. The indefinite bypass issue was not resolved at this meeting.

Defense-In-Depth was not considered for software common mode failures. Nevertheless, some credit will be given for the diversity of the non-safety related protection systems (i.e., diverse architectures, operating systems, and data highways).

CE implements commercial grade dedication (CGD) procedures and configuration management procedures for commercial software. CE will use a graded approach for CGD. More details will be obtained at a later date.

A discussion was held concerning the environmental qualification of the digital systems. The control room maximum temperature qualification limit is 85°F. CE intends to qualify the digital equipment to meet that environment.

NRC staff is concerned that this will relax the quality envelope for the digital equipment to such an extent that inferior quality equipment could be substituted for digital components that have higher environmental qualification envelopes. NRC staff believes that the digital systems should be qualified for the normal 120° to 140°F envelope.

NRC staff presented the schedule for completing the design certification (DC) review of the CE System 80+ design. CE is aware that they will be required to provide ITAAC prior to completion of our DC review. The ITAAC should be submitted in May to facilitate our schedule.

CE wants to know, as soon as possible, what NRC considers to be the significant design acceptance criteria (DAC) issues that they will need to address. There is a preliminary commitment to meet with CE at the end of March, April, and May, to facilitate resolution of 1) upcoming issues, 2) potential DAC, and 3) open items.

Original Signed By:

Thomas V. Wambach, Project Manager
Standardization Project Directorate
Division of Advanced Reactors
and Special Projects
Office of Nuclear Reactor Regulation

Enclosures:
1. Meeting Agenda
2. Meeting Attendees

cc w/enclosures:
See next page

DISTRIBUTION:

Docket File	PDST R/F	DCrutchfield	WTravers
NRC PDR	CPoslusny	VMcCree	TMurley/FMiraglia
RNease	JNWilson	RPierson	TBoyce
KBorchardt	FHasselberg	THiltz	TKenyon
MMalloy	GGrant, EDO	PShea	ACRS (10)
TWambach	JHWilson	JMoore, 15B18	EJordan, MNBB3701
RNg	MWaterman, 8H7	HHeimburger, RES	SNewberry, 8H7
MCniramal, 8H3			

OFC:	LA:PDST:DAR	PM:PDST:DAR	SC:PDST:DAR
NAME:	PShea:tz	Tom Wambach	JNWilson
DATE:	03/16/92	03/16/92	03/16/92

OFFICIAL DOCUMENT COPY: CEMTG3-2.TW

cc: Mr. E. H. Kennedy, Manager
Nuclear Systems Licensing
Combustion Engineering
1000 Prospect Hill Road
Windsor, Connecticut 06095

Mr. C. B. Brinkman, Manager
Washington Nuclear Operations
Combustion Engineering, Inc.
12300 Twinbrook Parkway
Suite 330
Rockville, Maryland 20852

Mr. Stan Ritterbusch
Nuclear Licensing
Combustion Engineering
1000 Prospect Hill Road
Post Office Box 500
Windsor, Connecticut 06095

Mr. Daniel F. Giessing
U. S. Department of Energy
NE-42
Washington, D.C. 20585

Mr. Steve Goldberg
Budget Examiner
725 17th Street, N.W.
Washington, D.C. 20503

Enclosure 1

NRC MEETING AGENDA
SYSTEM 80+ I&C TOPICS
MARCH 2, 1992

I. NUPLEX 80+ OVERVIEW

II. A. STATIC MOCK-UP
B. DYNAMIC MOCK-UP
C. PLC HARDWARE

III. C-E PRESENTATION

A. OVERVIEW OF RPS/ESFAS/APS

1. PPS
2. ESF-CCS
3. PROCESS-CCS

IV. DISCUSSION TOPICS

A. INDEFINITE BYPASS ISSUES
B. DEFENSE-IN-DEPTH ANALYSES
C. RPS/AMSAC DIVERSITY VIA APS DIGITAL SYSTEM
D. ENVIRONMENTAL SPECIFICATIONS FOR CLASS 1E DIGITAL SAFETY SYSTEMS
E. CONFIGURATION MANAGEMENT OF THIRD-PARTY DIGITAL SYSTEMS
F. DCR SCHEDULE FOR I&C

DLH233.WP

Enclosure 2

NRC/ABB MEETING ON SYSTEM 80+ INSTRUMENTATION AND CONTROL

MARCH 2, 1992

MEETING ATTENDEES

NAME	ORGANIZATION
Mike Waterman	NRC/NRR
Harn Heimburger	NRC/RES
Scott Newberry	NRC/NRR
Matt Chiramal	NRC/NRR
Stan Ritterbusch	ABB/CE
Daryl Harmon	ABB/CE
Michael Novak	ABB/CE
Ken Scarola	ABB/CE
Dave Van Olinda	ABB/CE
Alfred Hyde	ABB/CENP