REACTOR PROTECTION AND CONTROL
PROCESS INSTRUMENTATION REPLACEMENT PROJECT AT
DONALD C. COOK NUCLEAR PLANTS UNITS 1 AND 2

QUALIFICATION COMPLIANCE

REPORT NO. 2985-HHH-01, REV. 1

Prepared by: Hal H Hoffman Date: 12/14/92

Concurred by: Neils Farr Date: 12/14/92

COOK NUCLEAR PLANT REACTOR PROTECTION SYSTEM QUALIFICATION WITH PROCESS INSTRUMENTATION REPLACEMENT PROJECT

TABLE OF CONTENTS

COOK NUCLEAR PLANT REACTOR PROTECTION SYSTEM PROCESS INSTRUMENTATION REPLACEMENT PROJECT

1.0 Purpose

The purpose of this report is to document the acceptability of the Cook Nuclear Plant safety system with the process instrumentation part of the safety system being replaced by SPEC 200 (analog) and SPEC 200 MICRO (digital) equipment. The modified safety system shall meet the requirements of IEEE-279 and IEEE-603-1991 and the standards referenced in the purchase order. The SPEC 200 MICRO portion of the modified safety system shall also meet the requirements of ANSI/IEEE-ANS-7-4.3.2-1982. A project overview is included in this report (See Reference 716).

2.0 Scope

The equipment and functions associated with the Cook Nuclear Plant Reactor Protection System include the sensing of plant parameters, processing that information to determine when protective action is required and initiating the required protective action. (See Figure 1).

The replacement project is limited in scope to replacing the equipment used to process plant information to determine when protective action is required. In an effort to minimize the impact of what amounts to a hardware upgrade for a portion of the reactor protection system, we have chosen a design approach that is limited to duplication of existing functions within the confines of the existing cabinets in a manner to minimize the impact of external cabling and power supply.

This approach was chosen to minimize the impact of the upgrade on continued compliance. Compliance in areas such as separation, independence, and single failure will not be affected by the change because the overall protection system architecture has been retained. Compliance in areas such as qualification, system integrity, and test and calibration have the potential to be affected and are discussed in detail.

2.1 Reactor Protection Equipment not being Replaced

The scope of the reactor protection upgrade impacts only a limited portion of the Reactor Protection System. The following equipment and functions belong to the Reactor Protection System but are not part of the Reactor Protection System upgrade (See Figures 1 and 2).

1. The process sensors that continually measure, produce and provide input signals representing the value of important plant parameters. These sensors are not being replaced, and will provide input to the new instrumentation.

FIGURE 1

COOK NUCLEAR PLANT REACTOR PROTECTION SYSTEM

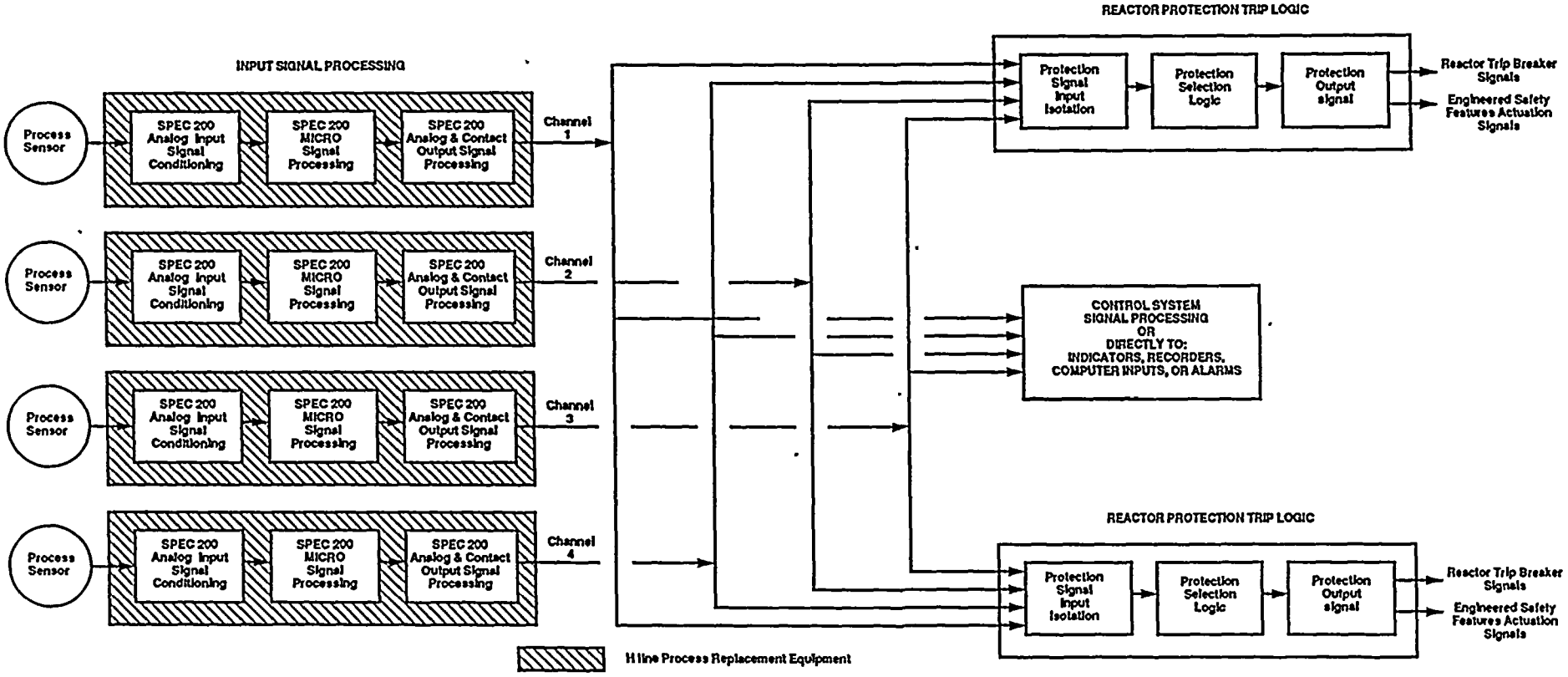
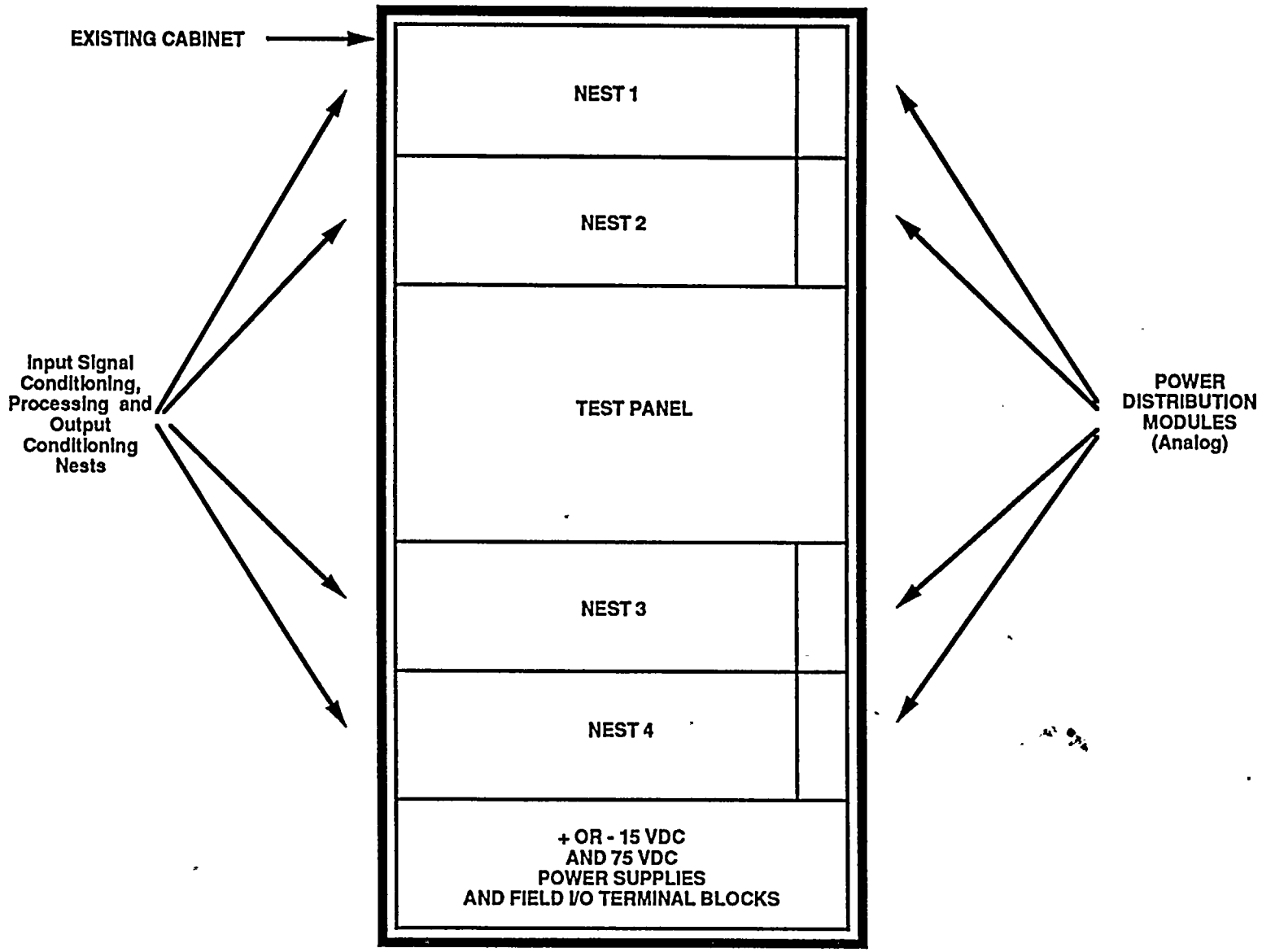


FIGURE 2
CABINET/RACK CONFIGURATION



2. The reactor protection logic equipment (SSPS) performing the following functions:

   a. Input and isolation of the trip signals from the protection group cabinets.
   b. Processing the trip signals through predetermined logic to establish the need for and the type of required protection function.
   c. Generation of signals to accomplish the required protection function.

3. The existing cabinets housing the Reactor Protection Process Instrumentation equipment. Cabinet internals will be replaced and internal structure and grounding modified to accommodate the new instrumentation.

4. The cables between the Reactor Protection and Control System equipment.

5. Cable, conduit and tray are not to be added or modified except within the Reactor Protection Process Instrumentation cabinets on a very limited basis.

2.2 Reactor Protection Equipment being Replaced

The following equipment and functions are part of Reactor Protection Upgrade (See Figures 1 and 2). This equipment will perform the same functions as the equipment it replaces.

1. Foxboro SPEC 200 type analog input signal conditioning equipment that changes the various types and values of input signals from the sensors into a common type of analog output signal that represents the input values at the channel level.

2. Foxboro SPEC 200 MICRO digital signal processing equipment that take the analog signal from the SPEC 200 analog input equipment at the channel level and:

   a. Changes the analog signals to digital signals.
   b. Process the digital signals including comparison against predetermined limits and when the limits are exceeded produces discrete trip signals to initiate the required protective action.
   c. Changes the processed digital signals back to analog output signals.

3. Foxboro SPEC 200 type analog output signal conditioning equipment which take the analog output signals from the SPEC

200 MICRO and condition them for control system, indication and recording use.

4. Foxboro SPEC 200 type contact output equipment produces discrete trip signals from the SPEC 200 MICRO and provides trip signals for input to the reactor protection logic equipment (SSPS).

5. Foxboro SPEC 200 type power distribution equipment powering the signal conditioning and signal processing equipment as discussed above.

6. 75 VDC multi-loop power supply provides which provides power for the field transmsmitters.

2.3 Requirements

The Reactor Protection Upgrade is provided by Foxboro and is in compliance with the applicable standards and regulatory requirement as follows:

IEEE 603-1980, Standard Criteria for Safety Systems for Nuclear Power Generating Stations.

IEEE 279-1971, Criteria for Protection Systems for Nuclear Power Generating Stations.

Reg. Guide 1.153, Criteria for Power, Instrumentation, and Control Portions of Safety Systems.

IEEE 379-1988, Standard for the Application of Single Failure Criterion to Class IE Systems.

IEEE 384-1981, Standard Criteria for Independence of Class 1E Equipment and Circuits.

WCAP-7306 Reactor Protection System Diversity in Westinghouse Pressurized Water Reactors.

IEEE 323-1974, General Guide for Qualifying Class 1E Electrical Equipment for Nuclear Power Generating Stations.

UNSRC Reg. Guide 1.100, Seismic Qualification of Electrical Equipment for Nuclear Power Plant.

IEEE 420-1982, Standard for the Design and qualification of Class 1E Control Boards, Panels, and Racks used in Nuclear Power Generating Stations.

IEEE 344-1975, Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations.

ANSI/IEEE ANS-7-4.3.2-1982, Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations.

MIL-STD-461C August 1986, Electromagnetic Emission and Susceptibility Requirements for Control of Electromagnetic Interference.

IEEE 472-1974, Guide for Surge withstand Capability (SWC) Tests.

IEEE 336-1985, Installation, Testing Requirements for Instrumentation and Control Equipment at Nuclear Facilities.

IEEE 338-1987, Standard Criteria for the Periodic Testing of Nuclear Power Generating Station Safety Systems.

IEEE 381-1977, Standard Criteria for Type Tests of Class 1E Modules used in Nuclear Power Generating Stations.

IEEE 383-1974, Standard for Type Test of Class 1E Electric Cables, Field Splices, and Connections for Nuclear Power Generating Stations.

3.0 Analysis

The qualification of the Cook Nuclear Plant safety system with the Reactor Protection Upgrade equipment (SPEC 200 analog and SPEC 200 MICRO) will be established in three (3) parts as follows (See Figure 3):

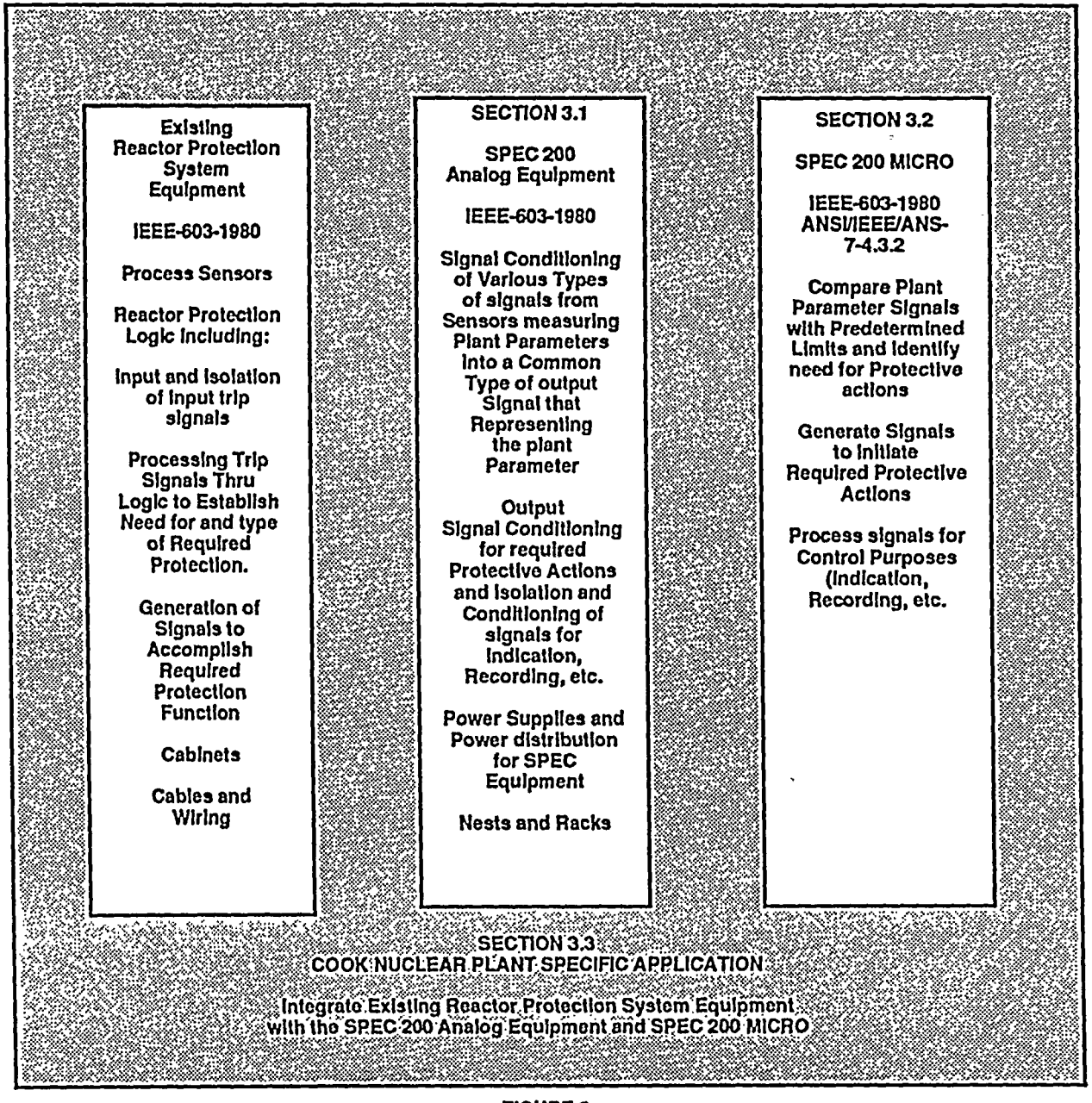


FIGURE 3
COOK NUCLEAR PLANT REACTOR PROTECTION AND CONTROL SYSYEM
QUALIFICATION
WITH PROCESS INSTRUMENTATION REPLACEMENT PROJECT

1. Qualification of the SPEC 200 analog equipment will be established by discussing its application to each section of IEEE-603-1980 in Section 3.1.

2. Qualification of the SPEC 200 MICRO equipment will be established by discussing its application to each section of IEEE-603-1980, ANSI/IEEE-ANS-7-4.3.2-1982 and IEEE-730.1-1989 in Section 3.2.

3. Qualification of our specific application will be accomplished thru verification and validation of the development process for our application in Section 3.3.

3.1 SPEC 200 Analog Equipment

3.1.1 Purpose

The purpose of this report is to document the acceptability of SPEC 200 analog equipment for use in safety systems of nuclear power generating stations by demonstration of SPEC 200 analog equipment level of conformance to the requirements of IEEE-603-1980. This standard establishes minimum functional design criteria for the power, instrumentation, and control portion of safety systems.

3.1.2 Conformance to Standards

SPEC 200 analog equipment is used as part of the Sense and Command Features portion of the Reactor Trip, Engineered Safety Features, and Auxiliary Supporting Features system. The application of the criteria in IEEE-603-1980 to the SPEC 200 analog equipment is discussed in Section 3.1.3 of this report.

3.1.3 SPEC 200 Analog Equipment Compliance with IEEE-603-1991

IEEE-603-1991 establishes the minimum functional design criteria for the power, instrumentation, and control portion of safety systems. As such, most criteria pertains to the overall safety system functions rather than individual pieces of equipment. The SPEC 200 analog equipment is limited to replacing existing signal processing equipment at the channel level with minimal effect on the overall protection system.

The requirements of IEEE 603-1980 apply to the SPEC 200 analog equipment as follows:

IEEE-603-1980, Section 5.1, Single Failure Criterion and IEEE-379-1988 Standard for the Application of Single Failure Criterion to Class 1E Systems.

Single failure criteria is applied at the overall safety system level. the compliance of the existing system is not being compromised because the qualified existing input signal processing equipment is being replaced by qualified SPEC 200 input signal processing equipment. The SPEC 200 analog equipment performs the same functions with the same overall safety system level of dependency, separation and isolation.

IEEE-603-1980, Section 5.2 Completion of Protective Action

Compliance is applied at the overall safety system level. The role of the SPEC 200 analog equipment in the completion of protective action is limited to processing the trip signals when protective action is required.

IEEE-603-1980, Section 5.3 Quality

The SPEC 200 analog equipment is designed, manufactured, inspected, and tested under the Foxboro Company Quality Assurance Program CQA-2 (See Reference #700). This quality assurance program is in compliance with 10 CFR 50 APP. B, ANSI N-45.2, and NQA-1. Detailed instruction manuals are provided to the user to provide assistance in installation, operation, and maintenance of the system. Validation of the application configuration is described in Q0AAE04 (See Reference #704).

IEEE-603-1980, Section 5.4 Equipment Qualification

The SPEC 200 equipment that is part of the process instrumentation replacement project is:

N-2AI-C2L	Contact Input Isolator
N-2AI-H2V	Current to Voltage Converter (10-50 ma)
N-2AI-12V	Converter, Current to Voltage (4-20 Isolated)
N-2AI-P2V(C)	Platinum Resistance to Voltage Converter (Custom)
N-2AI-P2V	Platinum Resistance to Voltage Converter
N-2AI-T2V	Series EMF to Voltage Converter
N-2AX+VE	Bypass Module
N-2AX+P(C)	Bypass Module (Custom)
N-2AX+P	Bypass Module
N-2CCA-S	Control Card
N-2CCA-D	Control Card
N-2AO-L2C-R(C)	Contact Output Isolator (Custom)
N-2AO-L2C-R	Contact Output Isolator
N-2AO-V2H(C)	Voltage to Current Converter (Custom)
N-2AO-V2H	Voltage to Current Converter
N-2AO-VAI	Converter, Voltage to Current (4-20 ma)
N-2AX+DP11	Power distribution Component
N-2ANU-DM	Analog Nests
P0300CQ	Multi-Loop Power Supply
N-2ARPS05-A6	Multi-Next Power Supply

The qualification of the SPEC 200 equipment is discussed in:

- Report 2985-HEI-07, Rev. 0, "Seismic Qualification Assessment of the Foxboro Spec 200 Equipment for the Cook Nuclear Plant".

- Report 2985-HEI-12, Rev. 0, "Donald C. Cook Nuclear Plant Units 1 & 2 Engineering Analysis of Temperature and Humidity Effects on Foxboro Spec 200 Instrumentation Reactor Protection and Control System Replacement Project".

IEEE-603-1980, Section 5.5 System Integrity

Compliance is applied at the overall safety system level. Application of the SPEC 200 analog equipment qualified for a mild environment and performing the same function as the equipment being replaced will maintain system integrity.

IEEE-603-1980, Section 5.6 Independence

Adequate separation and isolation of control and protection functions are achieved by proper replication of the existing functions, observance of existing separation criteria for cables and cabinets including equipment inside, power dependence and due considerations for EMC issues with the addition of current design criteria. We are maintaining the current level of separation and independence of our plant design as stated in the FSAR (See Question 40.6 on Reg. Guide 1.75).

IEEE-603-1980, Section 5.7 Capability for Test and Calibration

There is no test and calibration associated with the SPEC 200 analog equipment.

IEEE-603-1980, Section 5.8 Information Displays

There are no information displays associated with the SPEC 200 analog equipment.

IEEE-603-1980, Section 5.9 Control of Access

There are no control of access requirements for the SPEC 200 analog equipment.

IEEE-603-1980, Section 5.10 Repair

The SPEC 200 analog equipment is modular in design and facilitates repair by replacement. Normal repair is accomplished by removing a protection channel from service, accomplishing repair and returning the channel to operation. The power supply provided with the SPEC 200 equipment, by design, do not require that the channel be placed out of service during repair, however, repair in service would be conditioned on personnel safety considerations.

IEEE-603-1980, Section 5.11 Identification

The channel identification used with the SPEC 200 analog equipment is consistent with the channel identification of our original design. The channel identification is used throughout the protection system and is in agreement with the requirements of the IEEE standards. Channel cabling is color coded and cabinets are appropriately labeled with the channel identification.

IEEE-603-1980, Section 5.12, Auxiliary Features

Auxiliary supporting features perform functions required for the safety systems to accomplish their safety functions. The SPEC 200 analog equipment is part of the safety system and not a supporting feature. The power supply provided with the SPEC 200 analog equipment is an auxiliary feature and meets the requirements of this section.

IEEE-603-1980, Section 6 Sense and Command Features

Sense and command signals features are defined at the overall safety system level and are not being changed by the SPEC 200 analog equipment.

IEEE-603-1980, Section 7 Executive Features-functional and Design Requirements

The SPEC 200 analog equipment is not part of the execute features.

IEEE-603-1980, Section 8 Power Source Requirements

The SPEC 200 analog equipment is not part of the power sources.

3.2 SPEC 200 MICRO Equipment

3.2.1 Purpose

The purpose of this section of the report is to document the acceptability of SPEC 200 MICRO for use in safety systems of nuclear power generating stations by demonstration of SPEC 200 MICRO conformance to the requirements of IEEE-603-1980, ANSI/IEEE-ANS-7-4.3.2-1982 and ANSI/IEEE-730.1-1984. These standards establish minimum functional design criteria for the power, instrumentation, and control portion of safety systems. Those criteria that do apply to SPEC 200 MICRO are addressed in this section of this report.

The reference Foxboro documents used are:

Q0AAE01 Acceptability of SPEC 200 MICRO for use in Safety Systems of Nuclear Power Generating Stations (See Reference #701).

Q0AAE02 Report on the Conformance of SPEC 200 MICRO to Application Criteria for Programmable Digital Computers (See Reference #702).

Q0AAE03 Report on SPEC 200 MICRO Software Validation and Verification (See Reference #703).

Q0AAE04 Report on Methodology used to Demonstrate Compliance of SPEC 200 MICRO Application Configuration for Specific Project (See Reference #704).

Q0AAE69 SPEC 200 MICRO 2CCA Series Style CB Control Cards, 2CDA Series Style B Display Modules and Associated Equipment (See Reference #717).

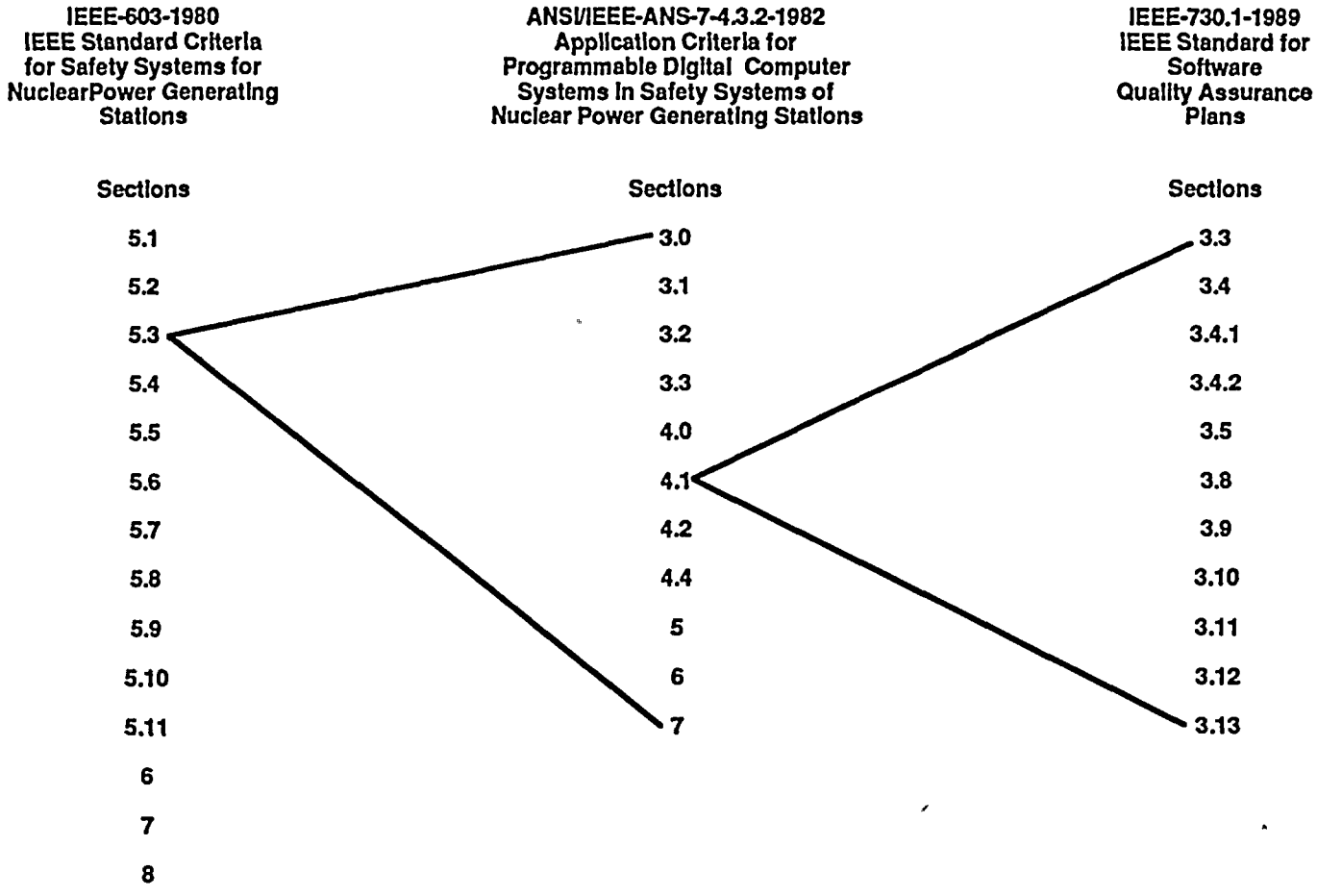
CQA 2 Corporate Quality Assurance Requirements (See Reference #700).

3.2.2 Conformance to Standards

The SPEC 200 MICRO equipment is used as part of the Sense and Command Features portion of the Reactor Trip, Engineered Safety Features, and Auxiliary Supporting Features System. The application of the criteria in IEEE Std. 603-1980 to the SPEC 200 Micro control modules is discussed in Section 3.2.3 of this report and Foxboro Q0AAE01 (See Reference #701). The application of the criteria in ANSI/IEEE-ANS-7-4.3.2-1982 to the SPEC 200 MICRO control modules is discussed in Section 3.2.4 of this report and Foxboro report Q0AAE02 (See Reference #702). The application of the criteria in ANSI/IEEE-730-1984 to the SPEC 200 MICRO control modules is discussed in Section 3.2.5 of this report and Foxboro report Q0AAE03 (See Reference #703). The relationship of these 3 standards are shown in Figure 4. Section 5.3 of IEEE-603-1980 references ANSI/IEEE-ANS-7-4.3.2-1982 and Section 4.1 of ANSI/IEEE-ANS-7-4.3.2-1982 references IEEE-730.1-1984.

FIGURE 4

FOXBORO SPEC 200 MICRO QUALIFICATION



3.2.3 SPEC 200 MICRO Compliance with IEEE-603-1980

IEEE-603-1980 establishes the minimum functional design criteria for the power, instrumentation, and control portion of safety systems. As such, most criteria pertains to the overall system functions rather than to individual pieces of equipment. The SPEC 200 MICRO control module is limited to replacing existing signal processing equipment replaced at the channel level with minimal effect on the overall protection system. The requirements of IEEE-603-1980 apply to the SPEC 200 MICRO control modules as follows:

IEEE-603-1980, Section 5.1 Single Failure Criterion

Single failure criteria is applied at the overall safety system level. The compliance of the existing system is not being compromised because the qualified existing input signal processing equipment is being replaced by qualified SPEC 200 input signal processing equipment. The SPEC 200 MICRO equipment performs the same functions with the same overall safety system level of dependency, separation and isolation.

IEEE-603-1980, Section 5.2 Completion of Protective Action

Compliance is applied at the overall safety system level. The SPEC 200 MICRO equipment function is limited to initiation of protective action when required at the channel level.

IEEE-603-1980, Section 5.3 Quality

The SPEC 200 MICRO equipment is designed, manufactured, inspected, and tested under the Foxboro Company Quality Assurance Program CQA2 (See Reference #700). This quality assurance program is in compliance with 10 CFR 50 APP B, ANSI N-45.2, and NQA-1. Detailed instruction manuals are provided to the user to provide assistance in installation, operation, and maintenance of the system.

See Section 3.2.4 for the quality of the SPEC 200 MICRO equipment to ANSI/IEEE-ANS-7-4.3.2-1982.

IEEE-603-1980, Section 5.4 Equipment Qualification

The SPEC 200 equipment that is part of the process instrumentation replacement project is:

N-2AI-C2L	Contact Input Isolator
N-2AI-H2V	Current to Voltage Converter (10-50 ma)
N-2AI-12V	Converter, Current to Voltage (4-20 Isolated)
N-2AI-P2V(C)	Platinum Resistance to Voltage Converter (Custom)
N-2AI-P2V	Platinum Resistance to Voltage Converter

N-2AI-T2V	Series EMF to Voltage Converter
N-2AX+VE	Bypass Module
N-2AX+P(C)	Bypass Module (Custom)
N-2AX+P	Bypass Module
N-2CCA-S	Control Card
N-2CCA-D	Control Card
N-2AO-L2C-R(C)	Contact Output Isolator (Custom)
N-2AO-L2C-R	Contact Output Isolator
N-2AO-V2H(C)	Voltage to Current Converter (Custom)
N-2AO-V2H	Voltage to Current Converter
N-2AO-VAI	Converter, Voltage to Current (4-20 ma)
N-2AX+DP11	Power distribution Component
N-2ANU-DM	Analog Nests
P0300CQ	Multi-Loop Power Supply
N-2ARPS05-A6	Multi-Next Power Supply

The qualification of the SPEC 200 equipment is discussed in:

- Report 2985-HEI-07, Rev. 0, "Seismic Qualification Assessment of the Foxboro Spec 200 Equipment for the Cook Nuclear Plant".

- Report 2985-HEI-12, Rev. 0, "Donald C. Cook Nuclear Plant Units 1 & 2 Engineering Analysis of Temperature and Humidity Effects on Foxboro Spec 200 Instrumentation Reactor Protection and Control System Replacement Project".

IEEE-603-1980, Section 5.5 System Integrity

Compliance is applied at the overall safety system level. Application of the SPEC 200 MICRO equipment qualified for a mild environment performing the same function as the equipment being replaced will maintain system integrity.

IEEE-603-1980, Section 5.6 Independence

Adequate separation and isolation of control and protection functions are achieved by proper replication of the existing functions, observance of existing separation criteria for cables and cabinets including equipment inside, power dependence and due consideration for EMC issues with the addition of current design criteria. We are maintaining the current level of separation and independence of our plant design as stated in the FSAR (See Question 40.6 on Reg. Guide 1.75).

IEEE-603-1980, Section 5.7 Capability for Test and Calibration

Capability for Test and Calibration is retained in the SPEC 200 MICRO design. The test panel supplied with the SPEC 200 replacement equipment will provide comparable Capability for Test and Calibration utilizing present manual methods and permanent installed test facilities very similar to what is now in use with the H-line equipment. This approach was chosen because

of the desire to take advantage of the present training and skills of plant I&C personnel.

IEEE-603-1980, Section 5.8 Information Displays

Information display requirements are met at the safety system level. There are no changes to the existing information displays.

IEEE-603-1980, Section 5.9 Control of Access

Administrative control of access for the SPEC 200 MICRO equipment is in two areas, the physical access to the installed equipment and access to configuration hardware, software and configuration data. Protection cabinets are kept locked under administrative control. Configuration hardware, software and configuration data will be administratively controlled via plant procedures and policy.

IEEE-603-1980, IEEE-603-1991, Section 5.10 Repair

The SPEC 200 MICRO equipment is a modular design that facilitates repair by replacement.

IEEE-603-1980, Section 5.11 Identification

The channel identification used with the SPEC 200 MICRO equipment is consistent with the channel identification of our original design. The channel identification is used throughout the protection system and is in agreement with requirements of the IEEE standards. Channel cabling is color coded and cabinets are appropriately labeled with the channel identification.

IEEE-603-1980, Section 5.12 Auxiliary Features

The SPEC 200 MICRO equipment is part of the safety system and not an auxiliary feature.

IEEE-603-1980, Section 6 Sense and Command Features

Sense and command features are defined at the overall safety system level and are not being changed. The SPEC 200 MICRO equipment function is limited to providing trip signals for automatic control. The SPEC 200 MICRO equipment provide the trip signals in essentially the same manner as the equipment being replaced. The SSPS which initiates reactor trip and engineered safeguards actuation is not part of the SPEC 200 replacement equipment.

IEEE-603-1980, Section 7 Executive Features-Functional and Design Requirements

The SPEC 200 MICRO equipment is not part of the execute features.

IEEE-603-1980, Section 8, Power Source Requirements

The SPEC 200 MICRO equipment is not part of the power source.

3.2.4 SPEC 200 MICRO Compliance with ANSI/IEEE-ANS-7-4.3.2-1982.

ANSI/IEEE-ANS-7-4.3.2-1982 establishes application criteria for programmable digital computer systems used in safety systems for nuclear power generating stations by expanding the quality and equipment qualification requirements of IEEE-603-1980 to encompass software design, software implementation, and computer system validation.

The SPEC 200 MICRO equipment is designed, manufactured, inspected and tested under The Foxboro Company Corporate Quality Assurance Program CQA-2. (See Reference #700) This quality assurance program is in compliance with 10 CFR 50 Appendix B, ANSI N-45.2, and NQA-1. Detailed instruction manuals are provided to the user to provide assistance in installation, operation, and maintenance of the system.

Conformance of the SPEC 200 MICRO equipment to ANSI/IEEE-ANS-7-4.3.2-1982 is described in Q0AAE02 (See Reference #702). Validation and verification of the software algorithms is described in Q0AAE03 (See Reference #703). Validation and verification of application configurations is described in Q0AAE04 (See Reference #704).

It has been noted that SPEC 200 MICRO equipment is not a programmable digital computer system. While SPEC 200 MICRO equipment does utilize digital technology to execute control functions, it is not programmable, but rather configurable. As such the application engineer can configure a system only within the bounds of the firmware. The control algorithms themselves are preprogrammed, and are identical on the SPEC 200 MICRO equipment. The control algorithms were developed under a software quality assurance program, subjected to extensive testing, and maintained under design control. The control algorithm programs are burned-in to an E-PROM which can be altered only by erasing and reburning at the factory. The software is maintained under design control. The actual application configuration varies for each SPEC 200 MICRO equipment.

The major difference between a programmable and a configurable system is that the software in the configurable system is not subject to change from application to application. Thus, one is able to accumulate a significant data base regarding the performance of the system. This data base is used to justify the acceptability for use of the algorithm software. It is felt that for configurable systems this data base provides an equivalent basis for acceptance to independent review of software design.

* These documents may be found in the Engineering Library at The Foxboro Company.

The SPEC 200 MICRO Equipment meets the requirements of ANSI/IEEE-ANS-7-4.3.2-1982 as follows:

ANSI/IEEE-ANS-7-4.3.2-1982, Section 3.0 - Computer System Requirements

The SPEC 200 MICRO equipment system requirements were developed and documented per Section 4.3.3.1 Concept Phase (Page 5), Section 4.3.3.2 Requirement Phase (Page 5) and Section 4.3.3.3 Design Phase of the SPEC 200 MICRO Equipment Software Validation and Verification Report Q0AAE03 (See Reference #703).

Appendix B (Page 13) Reference #703 lists the complete documentation structure of the system.

ANSI/IEEE-ANS-7.4.3.2-1982, Section 3.1 - Hardware Requirements

3.1.1 Input/output, including ranges, accuracies, and data rate capability:

Analog inputs and outputs (control card):

Normal range:	0 to 10 V dc
Full range:	-0.25 to 10.25 V dc
Accuracy:	±0.1% of span
Resolution:	2.5 mV per count (0 to 10 V dc range)
Scan rate:	Five times per second

Continuous display:

Analog bar graph:	2.0% (1 out of 50 bars)
Digital readout:	up to 0.1% dependent on configured scaling

2CCA-S Single width control card I/O
- 4 Analog Inputs
- 2 Analog Outputs
- 2 Contact Inputs
- 2 Contact Outputs

2CCA-D Dual width extended control card I/O
- 4 Analog Inputs
- 2 Analog Outputs
- 10 Contact Inputs
- 10 Contact Outputs

Reference Documents:

- PSS 2F-1A1 C (See Reference #707).
  "Product Specification - SPEC 200 MICRO Control Card".

* These documents may be found in the Engineering Library at The Foxboro Company.

- PSS 2F-1A1 D (See Reference #708).
  "Product Specification - SPEC 200 MICRO Display Stations".

* • CPS 1188 (1/4/85) SPEC 200 E Control Card Functional SPEC.

* • MI 280-300 (9/85) 2CCA Control Card.

* • MI 280-305 (10/85) 2CDA Series Continuous Display Station.

3.1.2 Design features (e.g. keylocks) that provide administrative control of all devices capable of changing the content of the stored programs or data images:

System configuration and any modifications to configuration must be done via a personal computer with configuration software. Removal of the personal computer prevents modification of the configuration on a module.

Tuning keylock - The continuous display station has a keylock to prevent unauthorized access to alarm adjustments or loop tuning.

Reference Documents:

- PSS 2F-1A1 D (See Reference #708) "Product Specification - SPEC 200 MICRO Display Stations" (See Reference #708).

* • MI 280-305 (10/85) 2CDA Series Continuous Display Station.

3.1.3 Initialization Requirements

Initialization is by:

- Day one start-up
- Return from power failure
- Following a watch dog timer timeout

Reference Documents:

* • CPS 1182 (Rev. C) PR1005 SPEC 200 MICRO Control Card Hardware Specification.

* These documents may be found in the Engineering Library at The Foxboro Company.

3.1.4 Design features for the detection of failures in the computer system:

SECURITY AND DIAGNOSTICS

Because it is important to accurately display information to process operators, the display stations perform several important security checks.

Power - up diagnostics

1. Checksum the entire ROM contents.
2. Check the entire RAM memory.

The display is considered FAILED until the power up diagnostics successfully complete.

ON-LINE DIAGNOSTICS

Run on a time available basis. The tests take multiple display cycles to be completed. All RAM memory is tested first, then all ROM memory is tested, then cycle repeats.

1. Test part of RAM in available time.
2. Test part of ROM in available time.

If a fault is detected during the on-line diagnostics, the watchdog timer expires, the processor gets a vectored reset, and the processor attempts to perform the power-up diagnostics. The display is considered FAILED until the power-up diagnostics is successfully complete.

Security and Maintenance philosophy is to:

1. Control - Provide diagnostics adequate to detect problems which could result in an invalid control action and prevent that control action from being taken.

2. Display - Provide diagnostics adequate to detect malfunctions and clear display data.

3. Communications - Provide diagnostics adequate to detect and retry failed communications and declare that portion of the system inoperative if retries are unsuccessful.

4. Generate System Alarms to the operator when any of the above happen.

* These documents may be found in the Engineering Library at The Foxboro Company.

5. Provide local indication of faults to allow the system to be readily repaired by board replacement.

Reference Documents:

* • CPS 1181 Rev. F PR1005A SPEC 200 MICRO Overview and Valid Hardware Configurations (Page 23).

* • MI 280-300 (4/87) 2CCA Control Card.

* • MI 280-305 (10/85) 2CDA Series Continuous Display Station.

3.1.5 In-Service Test Features and Diagnostics

These features are best described in *MI 280-300 (4/88) 2CCA Control Card.

3.1.6 Human-Factors Engineering

1. Operator interaction with SPEC 200 MICRO equipment is mainly through the Display Stations. Reference *MI 280-305 (10/85) 2CDA Series Continuous Display Station for a complete description.

2. Application engineering interaction with the SPEC 200 MICRO equipment is mainly through the Display Stations Reference *MI 280-200 (8/86) SPEC 200 MICRO equipment for configuration functions.

3. Maintenance functions and features for SPEC 200 MICRO equipment such as diagnostic LED's, display indications, etc. is described in *MI 280-300 (4/88) 2CCA Control Card.

3.1.7 Margins for Timing and Memory Size

1. Display processor chip 80C31 runs at 7.83 MHz, the 80C31 is specified to run 35% faster, up to 12 MHz.

2. Control card processor chip 80C86 runs a 4.914 MHz, the 80C86 is specified to run 1.7% faster, up to 5 MHz.

3. Memory margins are initially planned for less than 80% usage.

4. The controller card contains 64K bytes of ROM and 4K bytes of RAM.

* These documents may be found in the Engineering Library at The Foxboro Company.

5. The display contains 4K bytes of ROM and 128 bytes of RAM (internal to the 80C31 processor).

6. For timing requirements including response times, refer to Section 3.2.10.

3.1.8 Interrupt Features

External interrupts via display keyboards, configurator PC, tuning controls, keylocks, internal diagnostics, etc., are handled by the control card or display hardware interrupt controller and associated display and controller interrupt handler routines.

Interrupt Levels

The INTEL 8086 has two interrupt input request lines: Maskable Interrupt Request (INTR) and Non-Maskable Interrupt Request (NMI). The NMI interrupt request input to the 8086 CPU is of a higher priority than the INTR input. All of the interrupt requests is handled by the 8259A Programmable Interrupt Controller (PIC) are passed to the CPU via the INTR line. The use of the 8259A allows software control of interrupt priority and enable/disable states. There are 8 levels of Priority within the maskable interrupt with 0 being the highest, 1 the next highest, etc. Below is a list of the CCC interrupts and their vector addresses. It should be noted that Power Fail/Watchdog Timer is not an interrupt level but is included in the table because it is implemented using hardware vectoring.

VECTOR ADDRESS	PRIORITY	FUNCTION
FFFOH	N/A	Power Fail/Watchdog Timer/Fail Timer
0080H	0	Memory Priority Low Low Byte Error
0084H	1	Memory Priority High Byte Error
0088H	2	A/D conversion Complete (used as interval time)
008CH	3	DCM HPIL Interface
0090H	4	Display Station HPIC Interface

The A/D conversion complete interrupt is given high priority because it is used as an interval timer for determination of the 200 ms control cycle.

* These documents may be found in the Engineering Library at The Foxboro Company.

Reference Documents:

* • CPS 1182 (Rev. C) PR 1005 SPEC 200 MICRO Control Card Hardware Specification.

* • CPS 1183 (Rev. D) PR 1005A Spec 200 MICRO Display Station Hardware Style B.

* • ED 00750 SPEC 200 MICRO CCC Software Design Specification.

* • ED 00841 S200E Display Station Software Design Specification.

A partial hardware and software audit of Foxboro was conducted on March 23-26, 1992. A follow up audit was conducted on the hardware in October 1-2, 1992. These audits reports are included in this report (See References #709 and #710).

ANSI/IEEE-ANS-7.4.3.2-1982, Section 3.2 - Software Requirements

3.2.1 Process inputs, including ranges, accuracies, and sampling intervals and the conversion of process input signals into engineering unit values:

Refer to Section A.1 for ranges, accuracies, and sampling intervals.

Conversion of process input signals into engineering unit values (display scaling) is required for the display station only. Blocks require input signal conditioning. Configurator software is used to build display data base files to include this display scaling into engineering units.

Analog input/output signal conditioning translates the input or output into nominalized values.

1. Input Signal Conditioning

CCC analog input signal conditioning is performed for the four analog inputs. For all Signal Conditioning Index (SCIX) types, the calibrated 13-bit signed value in linearized counts (LC) is first normalized such that 0 to 4000 counts represents 0 to 100% of the desired signal span. The normalized value (NC') then undergoes out-of-range alarming and limiting which restricts the normalized value within the range, -80 to 4080 counts (-2% to 102% of span).

After out-of-range processing, the normalized value (NC') undergoes final conditioning, depending on the actual SCIX function (e.g., square root) to produce the desired value (NC).

Conditioning is performed according to each input's configured SCIX type as follows:

SCIX 1: Linear (0 to 4000 LC)

NC' = LC; -80 ≤ NC' ≤ 4080
NC = NC'; No further processing performed.

SCIX 2: Linear with Elevated Span (800 to 4000 LC)

NC' = (LC - 800) *5/4
NC = NC'; -80 ≤ NC' ≤ 4080

SCIX 3: Linear with Square Root (0 to 400 LC)

NC' = LC; -80 ≤ NC' ≤ 4080
IF NC' is negative (< 0 counts)
THEN NC = 0
ELSE NC = SQRT(4000 * NC')
ENDIF

SCIX 4: Linear with Square Root and Low Cutoff (0 to 4000 LC)

NC' = LC; -80 ≤ NC' ≤ 4080
IF NC' < 30 counts (0.75%)
THEN NC = 0
ELSE NC =SQRT(400 * NC')
ENDIF

2. Output Signal Conditioning

CCC analog output signal conditioning translates the span of an normalized data value such that 0 to 4000 counts represents 0 to 100% of the desired analog output signal span. Table 2-1 shows the relationship between output SCIX types, signal conditioned linearized count values (LC), and output signal span for the normalized range, 0 to 4000 counts.

Table 2-1. Output SCIX Types

SCIX	CONDITIONED VALUE (LC)	OUTPUT SIGNAL SPAN (V dc)
1	0 to 4000	0.0 to 10.0
2	800 to 4000	2.0 to 10.0

Conditioning is performed by converting the 13-bit sign value in normalized counts (NC) by a linear equation to produce a conditioned value in linearized counts LC. The conversion equations for all output SCIX types are as follows:

SCIX 1: Linear (0 to 4000 LC)

LC = NC; No further processing performed.

SCIX 2: Linear with Elevated Span (800 to 4000 LC)

LC = NC*4/5+800

3.2.2 Operating systems, utility routines, or other auxiliary programs required for operation of the application software:

1. Software for the SPEC 200 MICRO equipment displays is coded in 8051 Assembly language.

2. Software for the SPEC 200 MICRO equipment controller is programmed in PLM/86 except for functions that are time critical, memory critical, or require 32 bit integer math results. These functions are coded in 8086 Assembly language.

3. Software for the SPEC 200 MICRO equipment configurator runs under the MS-DOS operating system on most IBM PC compatible computers. The configurator is implemented using the Turbo Pascal compiler.

4. The application is not programmed in software but consists in the configuration of the standard algorithms within the bounds allowed by the firmware.

Reference Documents:

* • ED 00750 SPEC 200 MICRO CCC Software Design Specification.

* • ED 00841 S200E Display Section Software Design Specification.

* • ED 00843 S200E Configuration Software Design Specification.

3.2.3 Algorithms to be programmed with consideration given to and handling of postulated abnormal inputs:

The SPEC 200 MICRO equipment includes 21 control algorithms that are based upon previously implemented block design. Each control block tests for a multiple of appropriate input and output levels, etc. The project specific application consists in configuration of these standard control algorithms to the project functional requirements.

* These documents may be found in the Engineering Library at The Foxboro Company.

CONTROL BLOCK TYPES

• Control:

PID	-	Proportional/integral/derivative controller
TUNE	-	Self-tuning extender
NONL	-	Non-linear extender
INT	-	Integral - only controller
AMB	-	Automatic/manual station with bias
RTIO	-	Ratio

• Input & Conversion:

MIB	-	Multiple input block
CHAR	-	Piecewise linear characterize

• Digital Logic:

DIN	-	Digital input
DOUT	-	Digital output
GATE	-	Multiple gate
SEQ	-	Sequence

• Dynamic Compensation:

LLAG	-	Lead/log dynamic compensator
DTIM	-	Read Time

• Miscellaneous:

SWCH	-	Switch
SSEL	-	Signal Selector
ALRM	-	Alarm and Limiter
RAMP	-	Universal ramp generator
TIMR	-	Timer
ACUM	-	Accumulator
CALC	-	Calculator

BLOCK DESCRIPTIONS

PID - Enhanced version of proportional (P), integral (I), and derivative (D) controller with manual or automatic operation. Features include: process alarming; self-tuning and non-linear operation (using extender blocks); and many logic operation.

TUNE - Automatic "Expert System" adjustment of PID control

* These documents may be found in the Engineering Library at The Foxboro Company.

tuning Parameters. This sis based on continuous monitoring of the process management.

NONL - PID block error term processing extender.

DGAP - Deleted.

INT - Produces time integration of the error with integral feedback action.

AMB - Controllable auto/manual with bias station.

RTIO - Adjustable ratio multiplier with input/output scaling, bias, and alarm.

MIB - Four-Channel signal gathering and conditioning block. The UCMII block is single channel.

CHAR - Linear segment X-Y function calculator. Eleven X-Y specifiable coordinates allow piecewise - linear, ten - segment curve approximation for specialized signal characterization. Permits you to build "custom fit" functions for non-linear signals.

DIN - Digital signal contact or logic input and comparator block, with pattern recognition for up to sixteen user - specifiable patterns.

DOUT - Digital auto/manual station. Logic signal collector/output block.

GATE - Eight element logic block.

SEQ - Eight-step pattern generator

LLAG - Computational dynamic compensator (contains on load-log element).

DTIM - Adjustable length, tapped delay line with selectable top-off points.

SWCH - Two independent, single-pole, double throw switches. The UCMII switch toggles are not independent.

SSEL - Multi-signal discriminator/selector.

ALRM - Signal out-of-range detector/indicator/rate limiter.

* These documents may be found in the Engineering Library at The Foxboro Company.

RAMP - Dual linear ramp generator with single output.

TIMR - Two-Stage, variable-length, timed-pulse generator with repeat capability.

ACUM - Integrator/totalizer.

CALC - Multiple input, 35-step, floating-point, programmable calculator; Separate store and access operations interfacing to three independent memories; Has seven arithmetic and logical functions; Uses normalized inputs from either stored constants, I/O points, or block outputs; provides three outputs.

Reference Documents:

* • CPS 1188 (Rev. D) PR 1005A SPEC 200 MICRO 2CCA Control Card Functional SPEC.

* • MI 280-205 (12/85) SPEC 200 MICRO Control Block Description.

3.2.4 Data files and data required by the algorithms including engineering units, symbolic names, and requirements for flexibility:

For SPEC 200 MICRO equipment this includes the following controller data bases:

Control Data Base
Alarm Data Base
DCM Data Base (for NCM)
Security Data Base
Display Data Base
System Data Base

Reference Documentation:

* • ED 00750 SPEC 200 MICRO CCC Software Design Specification.

3.2.5 All outputs, including ranges, accuracies, and update intervals:

Reference Section 3.1.1 for ranges, accuracies, and update intervals.

Reference Section 3.1.6 for Operator interface requirements.

* These documents may be found in the Engineering Library at The Foxboro Company.

3.2.6 Initialization requirements for example initial value of variables, start up sequence:

The controller card initialization module is executed during power up and watchdog timeouts and performs the following functions:

1. Initialize 8086 processor by setting all global flags, the stack pointer, base, and segment registers, etc.

2. Initialize CCM/NCM HPIL Interface.

3. Initialize CCC/Display HPIL Interface.

4. Initialize 82C59 Programmable Interrupt Controller and clears parity error-interrupt.

5. Initialize the executive and requests the security task level.

6. Initialize system mode.

7. Enables interrupt levels.

8. Starts control cycle by requesting A/D conversions.

9. Transfers control to the Executive Task Scheduler. This causes the execution of the security tasks to be initiated at the base level. As each A/D conversion completes interrupt, the 200 ms control cycle is initiated.

The display initialization module is executed during day-one startup of the processor, after a watchdog timer timeout and after a return from power fail. The module performs the following functions:

1. Initialize the 80C31 processor by clearing internal RAM and setting the stack pointer.

2. Clears external RAM.

3. Makes a call to the initialize section of each of the following:

   Exec
   Message Processor
   Display Builder
   HPI Handler
   RS-232 Handler
   Keyboard Handler
   Security

* These documents may be found in the Engineering Library at The Foxboro Company.

Thereby initializing global data base, interrupt priorities, timer/counter modes of operation, serial port operation, and the HPIL chip - and executing power up diagnostics.

4. Requests the base level/security task.

5. Enables and sets the watchdog timer.

6. The module loops until the first real time clock interrupt is generated (approximately 1 ms).

   At this point the hardware is refreshed and the Executive's Task Scheduler is entered.

3.2.7 Program logic for response to all detected failures in the computer system:

Refer to Section 3.1.4.

3.2.8 Operator Interface

Refer to Section 3.1.6.

3.2.9 In-service Test Features, or Diagnostics or Both

Refer to Section 3.1.4. These features are best described in *MI 280-300.

3.2.10 Timing requirements, including overall computer systems response time:

Input scan rate = 5 times a second
Display update rate = at least once per second
Time frame for processing = 200 ms

SPEC 200 MICRO equipment stand-alone system timing is as follows:

	CPU Time	CPU%
Display processing	35 ms	18.5
Control blocks and I/O	97 ms	48.5
Overhead	3 ms	1.5
	135 ms	68.5%

Based upon a typical two loop cascade with two CALC blocks, two PID blocks, 1 CHAR, 1 GATE block.

* These documents may be found in the Engineering Library at The Foxboro Company.

Reference Documents:

* • ED 00750 S200E CCC Software Design Specification.

3.2.11 Processing idle time and excess memory consistent with hardware capability:

Refer to Section 3.2.10 for processing idle time.
Refer to Section 3.1.7 for memory requirements.

3.2.12 Security Requirements (e.g. passwords)

Refer to Section 3.1.2.

SECURITY MODULE

ELEMENT NAME	ON-LINE	FUNCTIONS
ADCAL-CHK		Checksum on A/D calibration co-efficient ROM.
BASE-SEC		Base Level Security Task (level 5) that invokes on-line security elements.
CCCSTAT-UPDATE		Update CCC status in Block 7.
DCMLNK-MONITOR		Monitor link status for CCC/NCM interface.
DSPLNK-MONITOR		Monitor link status for CCC/NCM interface.
IO-RECOVER		I/O recovery sequence test.
PARITY-CHK parity		Read of RAM memory to flush errors.
PARITY-INT		Memory parity interrupt service routine.
READBACK		Readback check on I/O.
ROM-CHK		Checksum of ROM SAMPLE-PID Sample. PID algorithm check.
SET-SBYFAIL		Set mode to Standby Fail.

SET-STANDBY	Set mode to Standby.
SET-CONTROL	Set mode to control or Control Inst.

IEEE-Std. 379-1988 - IEEE Standard Application of the Single - Failure Criterion to Nuclear Power Generating Station Safety Systems

3.2.13 Configurator

3.2.13.1 The configurator runs on an IBM Compatible Personal Computer with the Following specifications:

- IBM Compatible
- MS-DOS version 1 or 2
- Monochromatic Display of 25 lines, 80 characters/line
- 256 kilobytes of RAM
- Dual 5 1/4, double-sided double-density diskette drives, or single 5 1/4 in diskette drive and Winchester disk
- RS-232 interface with programmable band rates of 2400 to 9600.

3.2.13.2 The main menu of the configurator has 6 items as follows:

- Configure to Controller
- Configure to Disk
- Controller Operations
- Disk Utilities
- Set up Configurator
- Exit to MS-DOS

Reference Documents:

* • ED 00843 S200E Configurator Software Design Spec.

* • CPS 1187 Rev. B. PR1005 Spec 200 Micro Configurator.

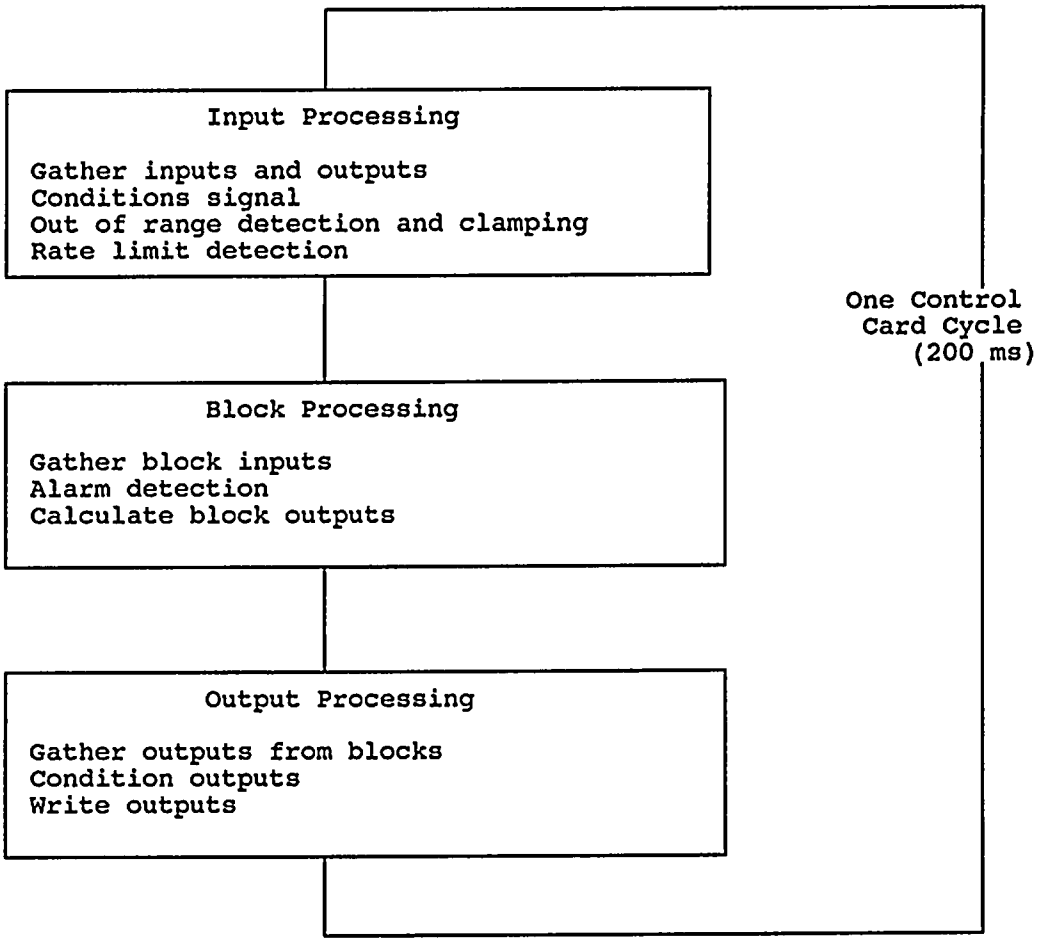
ANSI/IEEE-ANS-7-4.3.2-1982, Section 3.3 - Hardware - Software Integration Requirements

3.3.1 At the time of SPEC 200 MICRO equipment development a specific comprehensive software verification and validation plan was not documented for the project. The SPEC 200 MICRO equipment development team did follow an organized methodology to verify and

* These document may be found in the Engineering Library at the Foxboro Company.

validate software developed for the SPEC 200 MICRO equipment system that is for the most part consistent with the requirements of the standard for software verification and validation plans, ANSI/IEEE Std. 730.

3.3.2 Control Package Processing



3.3.3 The factory acceptance test (FAT) draft plan (See Reference #717) is considered to be the hardware and software integration test procedure for acceptance of the software and hardware.

* These document may be found in the Engineering Library at The Foxboro Company.

ANSI/IEEE-ANS-7-4.3.2-1982, Section 4.0 - Software Development

The life cycle phases for development are described in Q0AAE03 Rev. B (See Reference #703).

4.1 Development Plan

See Section 3.2.5 Compliance of the SPEC 200 MICRO control modules to IEEE-730.1-1989.

4.2 Design

System design was conducted in accordance with developmental plan procedures described above. Corporate Product Specifications (CPS) and Detail Functional Specifications (DFS) were written to document product concepts and requirements. Each CPS was reviewed by Product Planning, Sales, and D&E Management to insure requirements were properly documented.

4.3 Implementation

*ED00750, *ED00841, and *ED00843 specify the computer programming techniques for the Controller Display and Configurator.

Documentation standard used are referenced in SPEC 200 MICRO Software Compliance Report, Q0AAE03, Section 4 (See Reference #703).

*ED00750, *ED00841, and ED00843 specify the coding conventions and development test tool requirements.

*ED02134 documents the SPEC 200 MICRO Panel System Test requirements.

Section 9 of the SPEC 200 MICRO Equipment Software Compliance Report, Q0AAE03 (See Reference #703), describes the tools, techniques, and the methodologies used.

ANSI/IEEE-ANS-7-4.3.2-1982, Section 5 - Hardware/Software Integration

The development team followed Corporate Engineering Standard CES 281:13 practices and procedures for reporting, tracking, and resolving software problems.

Results of system testing is documented in the Corporate Problem Log.

ANSI/IEEE-ANS-7-4.3.2-1982, Section 6 - Computer System Validation

SPEC 200 MICRO equipment system validation is performed for each application on a project basis. Testing is performed to validate the proper performance of the system to meet safety system requirements. A formal test plan is prepared and independently reviewed in addition to customer review. The plan includes the required input signals and their values, anticipated output signals, and acceptance criteria. The results of the validation testing is documented in a formal test report that demonstrates compliance with safety system requirements. The reports are included in the project documentation package.

Refer to Report Q0AAE04 (See Reference #704) for further details.

ANSI/IEEE-ANS-7-4.3.2-1982, Section 7 - Verification

The requirement for software verification of computer systems stems from attributes of these systems that make them different from traditional analog controls. Since software is not flexible each application tends to become a unique approach. Thus, there is little experience with the specific software application to justify the design. Because the digital system is a series of software bits the optional paths in the software proliferate to the point that exhaustive testing to prove the software is impossible. In order to demonstrate that the system will perform as desired an approach requiring an independent review of each and every software step has evolved. This often proves inadequate however since a logical error by one programmer or designer is likely to be repeated by another.

The Foxboro Company approach to verification of the SPEC 200 MICRO software design is in two parts. The hardware and software system underwent a series of reviews and tests throughout the design phase. These various reviews are documented in many volumes of procedures and report. A summary of the process is documented in Foxboro Report No Q0AAE03 (See Reference #703).

The second part of the verification process is the use of field experience to provide the performance of the SPEC 200 MICRO equipment hardware and software. The use of SPEC 200 MICRO equipment in nuclear applications was purposely withheld for over two years following introduction of the product. During this time Foxboro accumulated thousands of unit years of operation of the equipment as the generic algorithm set has been implemented in identical fashion in over 3200 field applications operating in excess of 300 plants. The accumulated field experience provides a statistically significant demonstration of the capability of the SPEC 200 MICRO equipment algorithms to perform as designed. If field data demonstrates the need the modify selected algorithms, nuclear customers are notified under 10CFR21.

The validation of the specific application as described in Section 6 is verified by the functional testing performed on an individual project basis and by

independent review of the design, test procedure, and test report. This process is documented in Foxboro Report No. Q0AAE04 (See Reference #704).

3.2.5 SPEC 200 MICRO Compliance with IEEE-730.1-1989

IEEE-730.1-1989 provides uniform, acceptable requirements for the preparation and content of Software Quality Assurance Plans. This standard applies to the development and maintenance of software. The SPEC 200 MICRO equipment meets the requirements of IEEE-730.1-1989 as follows:

IEEE-730.1-1987, Section 3.3 - Management

This section describes the organizations, tasks, and responsibilities of those involved in the software development of SPEC 200 MICRO.

Project Team Responsibilities

The SPEC 200 MICRO project team was established to develop the product and achieve the goals of reliability and maintainability for the product. The team members had the following responsibilities:

- PROJECT MANAGER - G. McLachlan: Responsible for the development project.
- PROJECT LEADER - D. Fellows: Responsible for the execution of the development plan.
- PROJECT ADMINISTRATOR - Bob Harpin, Stan Wengal, Bov Darling: Assisted the Project Manager in scheduling and communicating the status of development task.
- PRODUCT PLANNER - T. Myron: Defined the product requirements (program objectives and product features).
- SYSTEM ENGINEER - C. Piper, Steve Ciavarini: Responsible for the technical coordination of the project.
- SOFTWARE ENGINEERS:

  Greg Diomandes: Responsible for the overall control (CCC card) software design, implementation, and design verification effort.

  Arthur Romanelli: Responsible for the overall display software design, implementation, and design verification effort.

G. Zajac: Responsible for the overall configurator software design, implementation, and design verification effort.

John Kulesza: Consultant, for overall product/system software design, quality, and verification.

- SYSTEM TEST ENGINEER - D. Fellows: Provided the Development Test Plan and test cases for specification reviews and to perform independent incremental testing during development.

- TEST ENGINEERS - T. Tuttle, H. Fritschi, R. Healer, S. Ciavarini, C. Piper: Developed and documented the Test Plan *(ED02134). Executed the Test and Evaluation (T&E) Plan and test cases.

Software Quality Assurance Responsibilities

The Software Quality Assurance Organization:

Software Quality Assurance Manager:	Kevin Diggins
Software Quality Assurance Analysts:	Mohan Prasad David Noon John Gavin

1. Provided STANDARDS for software development and maintenance.

2. Provided TRAINING in software engineering.

3. Provided COACHING for technical review and walk-throughs.

4. Provided CHECKLISTS of QUESTIONS to be used in technical reviews.

5. Ensures Software Quality RECORDS are maintained.

6. Provide techniques to analyze defects found in T&E testing.

IEEE-730.1-1989, Section 3.4 - Documentation

This section:

Identifies the documentation governing the development, verification

* These documents may be found in the Engineering Library at The Foxboro Company.

and validation, use and maintenance of the software.

States how the documents were checked for adequacy.

IEEE-730.1-1989, Section 3.4.1 - Governing Documentation

3.4.1.1 Corporate Product Specification

Corporate Product Specifications (CPS) specify the external features, characteristics, and performance of a product. The CPS is the master technical document and identifies the other technical documents that relate to the product. Contents of a CPS are as follows:

1. General Description
2. Product Configurations and Options
3. Functional Specification
4. Product Safety Specifications
5. Physical Influences
6. External Influences
7. Performance Specifications
8. Space Parts and Maintenance Policy

For details of the contents of a CPS refer to *CES 280:23a.

Detailed Functional Specification

Detailed Functional Specification (DFS) specify the internal, functional operations to be performed. The format and content for a DFS are stated in *CES 281:21. The SPEC 200 MICRO functional specifications are integrated into the Corporate Product Specifications (CPS).

1. Objective
2. Reference Documents
3. Decisions
4. Configurations
5. External Interface
6. Principles of Operations
7. Data Structures
8. Functions
9. How to install and initialize
10. How to operate the product
11. Security
12. Maintenance

* These documents may be found in the Engineering Library at The Foxboro Company.

For details and content of a detailed functional specification refer to *CES 281:21 Rev A.

Hardware Design Specification

Hardware Design Specification (HDS) are written for hardware modules and/or any commonly shared hardware subassemblies. The format and content for a HDS are stated in *CES 280:51.

Software Design Specification

Software Design Specifications (SDS) specify the high level software design by specifying the software components, shared data bases, control relationships, and data interfaces of the components. The format and content for an SDS are stated in *CES 281:20.

Program Technical Description

Program Technical Descriptions (PTD) specify the detailed software design by specifying the design of the data base, the logical decisions that are made, and the calculations performed by modules. The format and content for a PTD are stated in *CES 281:6.

Test and Evaluation Plan

The Test and Evaluation (T&E) Plan specifies comprehensive testing that will verify that the code, when executed, meets the requirements expressed in the CPS. The requirements for a T&E Plan are stated in *CES 281:11.

Software Generation and Maintenance Document

The Software Generation and Maintenance Document (SGMD) describes how the software will be manufactured and how long term product support (e.g. procedures to correct defects and install enhancements) will be provided. The requirements for a SGMD are stated in *CES 281:12.

User Documentation

Product Specification Sheets (PSS)

Pre-sales documents that can serve as contractual specifications. PSS's describe features and benefits as well as specifications.

* These documents may be found in the Engineering Library at The Foxboro Company.

Reference Documents:

- PSS 9-7C1 A SPEC 200 Display Stations for Nuclear Services (See Reference #712).
- PSS 9-7A1 A SPEC 200 Seismic Racks and Rack-mounted Equipment (See Reference #713).

Technical Information Sheets (TI)

These pre- and post-sales documents fall into three major categories:

- System Overview TI - Presents a comprehensive description of a complete system - its functions, components, capabilities, and features - without stressing benefits or specifications.
- System Functional TI - Presents information on one or more system, subsystem, or component functions, describing both concept and performance.
- Component/Subsystem TI - Presents a technique for using a product or describes how it works.

General information in the form of tables and/or graphs that are of value in using or calibrating Foxboro instruments may also be printed in Technical Information sheets.

Confidential TI's provided for use by Sales Personnel, compare benefits and features of Foxboro products with comparable products of competitors.

Reference Documents:

- TI 280-110 SPEC 200 MICRO Control Blocks (See Reference #714).
- TI 280-100 SPEC 200 MICRO Control System Overview (See Reference #715).

Instructions (Master Instructions) (MI)

These post-sales reference documents are supplied for all Foxboro products, from individual instruments to complete systems. - hardware and software. They contain detailed information on site planning, installation, configuration, operation, maintenance,

* These documents may be found in the Engineering Library at The Foxboro Company.

diagnostics, engineering drawings, and concepts.

A detailed listing of the above documentation for SPEC 200 MICRO by document number and description is found in Appendix B Page 13 *Q0AAE03 (See Reference #703).

Documentation Evaluation

Each document was checked for adequacy by project team walk-throughs. Refer to Appendix C QA0AAE03 (See Reference #703) for a listing of document, walk-through date, reader and recorder. Walk-throughs were conducted in accordance with requirements stated on Page 46.

IEEE-730.1-1989, Section 3.4.2 - Minimum Documentation Requirements

Software Requirements Specification (SRS)

The Corporate Product Specifications (CPS) defined on Page 43 is the SRS.

Software Design Description (SDD)

The Software Design Specification (SDS) (See Page 44) and Program Technical Description (PTD) (See Page 44) are the SDD.

Software Verification and Validation Plan (SVVP)

At the time of SPEC 200 MICRO development a specific comprehensive SVVP was not documented for the project. The SPEC 200 MICRO development team did follow an organized methodology to verify and validate software developed for the SPEC 200 MICRO system that is for the most part consistent with the requirements of the DRAFT Standard for Software Verification and Validation Plans, ANSI/IEEE STDP1012/D6.0, 6 June 1986. Life Cycle phases defined in the above standard are used here to describe the SPEC 200 MICRO development.

Concept Phase

Development schedules and concept documentation were focused by the Project Manager and reviewed by Product Planning, Sales, and D&E Management.

* These documents may be found in the Engineering Library at The Foxboro Company.

Requirements Phase

- Corporate Product Specifications (CPS) were written to document product concepts and requirements. Each CPS was reviewed by Product Planning, Sales, and D&E Management with the project team to insure requirements were properly documented. Refer to Page 49 for review and audit definitions.

- Test plan requirements were defined and associated staffing and equipment planning were initiated.

Design Phase

Hardware Design Specifications (HDS), Software Design Specifications (SDS), and Program Technical Description (PTD) were developed to be consistent with the product requirements specified in the Corporate Product Specification (CPS).

Implementation Phase

- System Walk-throughs and PTD walk-throughs were conducted to insure designs met CPS requirements. Refer to Page 49 for review and audit definitions.

- Documented Source Code Walk-throughs were held as well for control card algorithms to insure compliance with design documentation.

- Code compliance with design documentation were evaluated as well by component test execution (White Box Testing) performed by each software engineer.

- Test Plans were generated and component and integration test requirements were defined. Reference *ED02134, SPEC 200 MICRO PANEL SYSTEM TEST.

Test Phase

- Initial System Integration Tests were conducted beginning at the lowest levels of stand-alone display station test execution and stand-alone control card test execution.

- System Integration Tests were then conducted to verify system level functionality of a fully integrated system consisting of display stations, control cards, and configurators.

- Problems found in Integration testing were corrected and

* These documents may be found in the Engineering Library at The Foxboro Company.

controlled software release "T" (Test) releases were issued to undergo formal T&E per *ED02134 and *CES 281:11.

- Problem Reporting and Corrective action during the formal T&E was conducted per *CES 281:16 (refer to Section 8).

- Formal System Release were issued to document that system configuration Model Codes and Styles, Manufacturing Specifications (M.S.), and user documentation.

Installation and Checkout Phase

For the purposes of this report, which is written post project completion, this phase of Software Verification and Validation has been satisfied by over 3200 successful field applications of SPEC 200 MICRO systems in over 300 different plants.

Problems found in initial installations relative to user documentation and system design have been reported and resolved.

Software Verification and Validation Report (SVVR)

A specific Software Verification and Validation Report was not documented for the SPEC 200 MICRO Development Project at the time of project completion. This document serves as the Foxboro Company's Software Verification and Validation Report for the SPEC 200 MICRO Development project.

IEEE-730.1-1989, Section 3.5 - Standards, Practices, and Conventions

CES 281:18 Standards for Software Design

This CES specifies the standards for software design. These standards apply to the preparation and technical evaluation of software Design Specifications and Technical Descriptions of software. The standards for software Design include sections on NAMES, PARTITIONING THE PROGRAM, MODULE DESIGN, DATA, AND ERRORS.

*CES 281:19 Standards for Software Code

This CES specifies the standards for software code. These standards apply to the development and technical evaluation of the actual code. The Standards for software code contain a section on COMMENTING PROGRAMS and a section on EXECUTABLE SOURCE STATEMENTS.

* These documents may be found in the Engineering Library at The Foxboro Company.

*CES 281:22 Program Design Language (PDL)

This CES describes a "Structured English" Program Design Language (PDL). It includes sections on what a PDL is, the purpose of using a PDL, "Structured English" PDL conventions, and an example of this PDL.

Review and Audits

This section:

Defines the technical and managerial reviews conducted.

States how the reviews and audits were accomplished.

The SPEC 200 MICRO Development Project Team conducted reviews and audits according to the following criteria:

Technical Reviews

Reference Procedure 5.4.3 - RD&E Manual and *CES 281:24 (a draft of *CES 281:24 dated 4 Sept 1984 was used by the project team.)

The following types of technical reviews were conducted:

- Documented walk-throughs in which a small group of peer engineers carefully examined each specification line by line (refer to Appendix C).
- Documented monthly Project Reviews in which project team members were able to review each specification that may effect their area.
- External Reviews in which representatives of other departments and functions were able to review the product and the specifications that describe the product. (Minutes of these reviews were not formally documented).

Status Reviews

The project manager conducted status reviews at regular intervals during the project. The following subjects were addressed:

- Personnel changes.
- The number of successful reviews that were completed.

* These documents may be found in the Engineering Library at The Foxboro Company.

- Status of planned program materials.
- Project schedule milestones.
- Major difficulties encountered, tasks that are currently behind schedule (or have anticipated schedule changes), their effects on completion, and steps being taken to remedy schedule delays.
- Problems which will potentially cause deviation from approved specifications.
- Change Request status.
- Problem Reporting status - progress on previous problems.

Relative to the requirements specified in ANSI/IEEE STD 730-1984 Section 3.6.2 the following applies:

Software Requirements Reviews (CPS Reviews) were conducted.

Preliminary Design Reviews (CPS Reviews) were conducted.

Critical Design Reviews (SDS Reviews) were conducted.

Software Verification and Validation reviews were conducted as described in IEEE-730.1-1989, Section 3.4.2 on Page 46.

Functional Audits were conducted by the System Engineers and Test engineers to verify CPS and DFS Functional Specifications had been met via a comprehensive test and evaluation.

Physical Audits were conducted by the system engineers an test engineers to verify product software and product documentation technical Information sheets (TI), and Master Instructions (MI), were internally consistent and ready for delivery.

In process audits were held by the project team to verify consistency of the design. These audits took the form of technical reviews described on Page 49.

Managerial reviews to assess and insure the execution of the development plan including the proper use of quality standards and practices were held weekly by C. Cooper, the Manager of Development and Engineering with the following people: (Minutes of these reviews were not formally documented).

C. Cooper - Manager D&E
D. Cornall - Manager of Area 1 Systems Engineering
J. Taliano - Manager of Corporate Program Management
L. Adams - Manager of Corporate Product Engineering
G. McLachlan - Project Manager

Software Configuration Management

Reference *CES 280:1 (Engineering Documentation Release System).

IEEE-730.1-1989, Section 3.8 - Problem Reporting and Corrective Action

The SPEC 200 MICRO Development team followed Corporate Engineering Standard *CES 281:13 practices and procedures for reporting, tracking, and resolving software problems.

The Corporate Product Engineering responsibilities listed in section 3.2 were provided by the individual team members assigned to the respective product areas Display and Control Card.

Ongoing problem reporting and corrective action is the responsibility of CPE. *CES 281:13 practices and procedures are followed by Corporate Product Engineering.

IEEE-730.1-1989, Section 3.9 - Tools, Techniques, and Methodologies

- The Intel Microcomputer Development system Model MDS 720 was used throughout the "white box" testing phase to verify the software. Specific examples include:

  - Tracing decision paths through blocks of code
  - Proper addressing
  - Set-up of message control blocks
  - Content of message buffers
  - Validation of proper HPIL command processing

- The following software reliability analysis techniques were used to evaluate the SPEC 200 MICRO software development:

  - Duane Growth - Error Rate of Change
  - Software Error Discovery Rate

* These documents may be found in the Engineering Library at The Foxboro Company.

- Software Error Pareto Profile

- McCabe Cyclomatic Complexity Analysis

Reference Reports:

Report No	Software Reliability Report
*87-SRR-001F	Control Card Software
*87-SRR-003F	Display Software
*87-SRR-008F	Software Complexity Analysis

IEEE-730.1-1989, Section 3.10 - Code Control

The SPEC 200 MICRO Development team followed the Code Control Guideline within *CES 281:15 to maintain and store controlled versions of identical software.

The same Code Control Guideline is used in the ongoing product maintenance phase under the responsibility of Corporate Product Engineering.

IEEE-730.1-1989, Section 3.11 - Media Control

The SPEC 200 MICRO Development Team followed Media Control Guidelines, not documented within *CES 281:14, to protect computer program physical media from unauthorized access or inadvertent damage or degradation.

The same Media Control Guideline is used in the ongoing product maintenance phase under the responsibility of Corporate Product Engineering.

IEEE-730.1-1989, Section 3.12 - Supplier Control

This section is not applicable to this plan as vendor-provided software and subcontractor supplied software are not a part of the SPEC 200 MICRO product under consideration for Nuclear Qualification.

* These documents may be found in the Engineering Library at The Foxboro Company.

IEEE-730.1-1989, Section 3.13 - Records Collection, Maintenance, and Retention

The following SQA documentation will be retained according to *CES 280:20.

Q0AAE01 (See Reference #701).

Acceptability of SPEC 200 MICRO to Application Criteria for Programmable Digital Computers in Nuclear Power Generating Stations

Q0AAE02 (See Reference #702).

Conformance of SPEC 200 MICRO to Application Criteria for Programmable Digital Computers in Nuclear Power Generating Stations

Q0AAE03 (See Reference #703).

SPEC 200 MICRO Software Validation and Verification.

Q0AAE04 (See Reference #704).

Report on Methodology Used to Demonstrate Compliance of the SPEC 200 MICRO Application Configuration.

Q0AAE05 (See Reference #705).

SPEC 200 MICRO Panel System Test Report.

3.3 Cook Nuclear Plant Specific Application

3.3.1 Purpose

The purpose of this part of the report is to document the methodology used to demonstrate compliance of the project specific SPEC 200 analog equipment and SPEC 200 MICRO equipment application configuration, with the guidelines Sections 6 and 7 of ANSI/IEEE-ANS-7-4.3.2-1982. It must be emphasized however, that while this report addressed the SPEC 200 analog equipment and the SPEC 200 MICRO product, the testing methodology is the same as has been used by Foxboro for many years of Control System testing.

3.3.2 Conformance to Standards

The specific application of the SPEC 200 analog equipment and the

* These documents may be found in the Engineering Library at The Foxboro Company.

SPEC 200 MICRO is part of the Sense and Command Features portion of the Reactor Trip, Engineered Safety Features, and Auxiliary Supporting Features system. The criteria in Sections 6 and 7 of ANSI/IEEE-ANS-7-4.3.2-1982 apply to the equipment. These criteria and the conformance of SPEC 200 analog equipment and SPEC 200 MICRO to the criteria are discussed in Section 3.3.3 of this report and Foxboro Q0AAE04 (See Reference #704).

3.3.3 Cook Nuclear Plant Specific Application Compliance with ANSI/IEEE-ANS-7-4.3.2-1982.

3.3.3.1 ANSI/IEEE-ANS-7-4.3.2-1982, Section 6 Validation and 7 Verification

Customer Specification Review

Customer specification review and development of an order package by a project team consisting of:

- Sales order folder with billing and shipping instructions
- Quotation
- customer purchase order
- Customer specifications (commercial, administrative, technical, quality, etc.)

A detailed review of the customer specification by the project team to determine:

- Technical compatibility with Foxboro product specifications
- Customer Quality requirements
- Special requirements

Design Drawings

Project team prepares a design procurement package which includes the following:

- Customer purchase order
- Customer specifications
- Customer block diagrams
- Quality assurance requirements

Project team implements the design according to the above and generate Rack Loading, factional, wiring, termination, and power drawings and configuration database.

Project leader reviews and approves design, customer reviews and returns comments, project team resolves and implements customer comments.

Application Configuration

Project team member makes the connections between function blocks of the SPEC 200 MICRO equipment to meet the customers requirements. This is accomplished by use of the SPEC 200 MICRO configurator.

The configurator is an off line interactive tool with which the project team member configures the control parameters that are used to load the SPEC 200 MICRO equipment blocks. The configurator is then disconnected from the system and not used during normal operation. Further, the team member creates a back up copy of the configuration parameters on a personal computer floppy diskette. A hard copy data base printout is part of the design package used during checkouts and is submitted to the customer as part of the final documentation package.

Test Procedure

The project team prepares a system test procedure showing the test method used for the testing of the analog/digital SPEC 200 MICRO instrumentation. The procedure includes a description of the test equipment and documentation used, a System Description, and a detailed procedure for testing the system based on the drawings and documentation supplied. The test procedure specifies as a minimum, several input values for the input converters, calculates the output values for input and output converters, defines the alarm set points and alarm and control action for bistables, relays and controllers, derives formulas for transfer functions of various process devices and projects output values based on the customer approved function and the originally assigned input values.

These calculated values are compared, point by point, to the hand-written actual values empirically found by the checkouts technician. Any deviation between these values is acceptable when within the limits of Foxboro defined procedures.

The test procedure is submitted to the customer for approval before final test and a signed data-filled copy is submitted to the customer as part of the final documentation package.

A post installation test procedure will be prepared by Cook Nuclear Plant personnel. Testing will be done following installation at the plant.

* These documents may be found in the Engineering Library at The Foxboro Company.

Checkouts

The system, designed and implemented per the customer specifications and Foxboro drawings, is checked per standard checkouts reference procedure, *EOP-201, and is tested per the System Test Procedure to insure that all instruments will function together as a control system. Using the specified test equipment and customer approved drawing, the checkouts technician first checks the calibration of the SPEC 200 MICRO equipment as independent units, then checks the system following the guidelines detailed in the test procedure. Any discrepancies and/or problems are brought to the attention of the project leader and are resolved.

When the requirements of the test procedure are met, demonstrating the validity of the design package, the checkouts test is repeated in the presence of the customer who approves the results before shipment.

Verification

The verification requirements are satisfied by the assignment of a qualified Foxboro Independent Reviewer to review the comment of Foxboro design drawings for adequacy of translation. The review includes the following:

- Adherence to customer specifications
- Adherence to quality requirements
- Inclusion of special requirements
- Inclusion of applicable codes
- Revision level

At the start of the project the Independent Reviewer receives a design package consisting of the customer specification and preliminary drawings of Foxboro functional diagrams. He reviews this design package, comments, and initials the completed design drawings at Rev. 0, before submittal to the customer. The submitted drawings are subsequently reviewed by the customer. Revisions are handled in a similar manner. This same review method is followed as the following documents become available:

- Application configuration
- Test Procedure
- Checkouts Test Results

\cld\SPEC\HLINEPIP.WP

* These documents may be found in the Engineering Library at The Foxboro Company.