

Donald C. Cook Nuclear Plant Units 1 & 2  
Failure Modes and Effect Analysis (FMEA)  
Protection Set 1 Foxboro Spec 200  
Reactor Protection and Control System Replacement Project  
Report Number 2985-HEI-14, Rev. 0

Subject:

This report shall document the results of a Failure Modes and Effects Analysis (FMEA) comparison study performed for the Donald C. Cook Reactor Protection And Control System Upgrade. This analysis reflects the installation of Foxboro Spec 200 / Spec 200 Micro equipment utilized to replace the original Foxboro H Line equipment.

References:

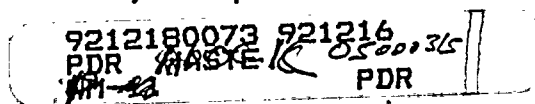
1. Foxboro Document 92-FM-02F; FMEA: D.C. Cook Nuclear, Spec 200 Configuration; October 30, 1992 (Appendix A).
2. Foxboro Document FM-502; Failure Modes and Effects Analysis, Spec 200 / Spec 200 Micro For The Upgrade Of The Reactor Protection Process Instrumentation; November 16, 1992 (Appendix B).
3. Foxboro Document 92-SA-50F; Study: A.E.P. D.C. Cook Nuclear Reliability Spec 200 Configuration; August 31, 1992.
4. Foxboro Document 92-SA-66F; Study: A.E. P. D.C. Cook Nuclear Reliability "H" Line Configuration; November 17, 1992.
5. IEEE Std. 352-1987; IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Protection Systems.
6. IEEE Std. 577-1976; IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Power Generating Stations.
7. IEEE Std. 279-1971; IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations.

---

D.C. Cook Units 1 & 2

Reactor Protection System Replacement

AEPfmea



Failure Modes and Effects Analysis (FMEA)  
Protection Set 1 Spec 200 Equipment  
Report Number 2985-HEI-14 Rev. 0  
Page 1 of 10

8. Specification No. DCC-IC-500-QCN; Reactor Protection and Control Instrumentation; Revision 0.
9. Hurst Engineering Report No. 2985-HEI-06; Power Quality Evaluation; Revision 0.
10. Hurst Engineering Report No. 2985-HEI-12; Temperature and Humidity Effects; Revision 0.
11. Hurst Engineering Report No. 2985-HEI-02; Grounding Issues; Revision 0.
12. Hurst Engineering Report No. 2985-HEI-09; Supplemental Cabinet Heat Rise Testing; Revision 0.
13. Hurst Engineering Report No. 2985-HEI-01; Response Time Evaluation; Revision 0.
14. Hurst Engineering Report No. 2985-HEI-10; Lithium Battery Analysis; Revision 0.
15. Hurst Engineering Report No. 2985-HEI-13; Isolation Evaluation; Revision 0.
16. Hurst Engineering Report No. 2985-HEI-14; EMI / RFI Evaluation; Revision 0.
17. Foxboro Document FM-503; Failure Modes and Effects Analysis, H Line For The Upgrade Of The Reactor Protection Process Instrumentation; November 23, 1992 (Appendix C).

Issue:

The Donald C. Cook Nuclear Plant, Reactor Protection and Control System is being upgraded to Foxboro Spec 200 / Spec 200 Micro equipment. General Design Criteria and the Donald C. Cook Nuclear Plant licensing basis require that the quality and types of instrumentation provided are adequate for safe and orderly operation of all systems and processes over the full operating range of the plant. Protection systems must be designed for high functional reliability. Redundancy and independence must be sufficient to assure that no single failure or removal from service of any component or channel of such a system will result in loss of the protection function. The system shall be designed to fail into a safe state or into a state established as tolerable on a defined basis, for all credible failure modes.

IEEE 279, "Criteria For Protection Systems For Nuclear Power Generating Stations" requires that protection systems shall, with precision and reliability, automatically initiate appropriate protective action whenever a condition monitored by the system reaches a preset level. Components and modules which comprise the protection system shall be of a quality that is consistent with minimum maintenance requirements and shall have low failure rates.

The FMEA is an effective tool in identifying significant failures and their consequences. It provides a qualitative reliability analysis used to locate possible failures and identify proper precautions that will reduce the frequency or consequences of such failures.

As part of the design process, a comparison evaluation between the original Foxboro H Line equipment and the new Foxboro Spec 200 equipment is being undertaken. This evaluation will take the form of a limited FMEA which documents the Protection Set 1 design. This analysis represents the "Typical" protection set and is intended to be bounding for all four protection set channels. The goal of this evaluation is to document that the new Spec 200 equipment is equivalent to the original H Line instrumentation with regard to failure modes, and that the original licensing basis as defined in the Donald C. Cook FSAR is valid, applicable and bounding.

### Scope:

The scope of this Failure Modes and Effects Analysis (FMEA) is limited to the Donald C. Cook Nuclear Plant, Protection Set 1, Reactor Protection and Control System. The detailed analysis presented within this report has been configured to provide a systematic approach to evaluate system design. This limited FMEA is confined to the bounds of the Spec 200 equipment and is not intended to be a comprehensive protection system analysis.

This FMEA is representative of all four protection sets in design philosophy and overall intent. The analysis presented is intended to document that the new Spec 200 system design is consistent with the original equipment design basis. Protection Sets 2, 3, and 4 will be reviewed to validate that this FMEA is bounding. This will be documented by separate report at a later date.

### Discussion:

The Donald C. Cook Nuclear Plant Reactor Protection and Control System replacement project will replace and upgrade the original Foxboro H Line instrumentation with Foxboro Spec 200 / Spec 200 Micro equipment. This task represents a significant design change effort and requires extensive analysis to ensure that the protection system has been configured to meet regulatory guidance, and that the plant licensing basis is maintained. The Failure Modes and Effects Analysis (FMEA) is a tool utilized to identify credible failure modes and their consequences. By utilizing a systematic approach in evaluating the design, the protection system reliability can be quantified.

### Description of Change:

The original equipment, Reactor Protection and Control Instrumentation will be upgraded due to spare parts unavailability, obsolescence, and increasing failure rates. Specification No. DCC-IC-500-QCN was developed to provide the technical, commercial and quality assurance requirements necessary to implement the replacement project.

The upgrade will involve complete replacement of the protection system signal processing electronics, internal power supplies, test panels, and associated hardware, located in 27 racks/cabinets. The new Foxboro Spec 200 / Spec 200 Micro instrumentation will be installed in the existing racks/cabinets.

The Spec 200 equipment has been configured to be functionally identical to the original system. As such, the design basis, protective actions, bypass and testing functions, and operation are essentially unchanged from that described in Chapter 7 of the Donald C. Cook FSAR.

The Spec 200 system utilizes a "modular" design approach. Power Supplies, Input, Output, Signal Processing Modules and associated hardware are installed in dedicated "nest" locations. The appropriate number of nest assemblies and power supplies are arranged in the rack / cabinet and interconnected to produce the desired loop configuration. The Spec 200 Micro is a microprocessor based control card which can be configured to perform a wide variety of operations. Loop specific "control blocks" are developed utilizing flexible algorithms which perform the desired control actions. All output signals are routed through qualified isolation devices. A +/- 15 Volt DC multi-nest power supply is installed in each rack to provide system power requirements.

Field interface at the input to the Spec 200 system is provided by input modules which convert the field signal, and function as buffers to protect the system against malfunctions, as well as provide some measure of noise rejection. Each interface module is individually fused such that accidental short circuit, or the connection of an incorrect voltage potential, will not propagate to other system components. A 75 Volt DC power supply is provided in each rack to power multiple transmitter loops.

The protection system has been provided with redundant multi-nest and transmitter loop power supplies. As described above, each rack / cabinet contains a +/- 15 Volt DC and 75 Volt DC power supply. Should the primary power supply fail, the redundant sources have been sized to provide adequate system power requirements. The 118 Volt AC regulated feed which energizes the protection set is paralleled to each rack / cabinet.



The Foxboro system has been evaluated for various operational and qualification issues which are not the subject of this report. These are:

Power Quality Evaluation (Reference #9)  
Temperature and Humidity Effects (Reference #10)  
Grounding Issues (Reference #11)  
Cabinet Heat Rise Effects (Reference #12)  
Response Time Evaluation (Reference #13)  
Lithium Battery Evaluation (Reference #14)  
Voltage to Current Card Isolation Evaluation (Reference #15)  
EMI / RFI Evaluation (Reference #16)

### System Interfaces:

The primary Protection Set interface is with the Reactor Trip Logic channels and the Engineered Safeguards System. The protection channels also interface with or provide input to various control systems, Regulatory Guide 1.97 readout devices, plant computers and annunciator systems. These interfaces are identified on the applicable functional drawings identified in Table 1 of this document.

### Failure Modes and Effects Analysis

As stated in Section IV of this document, the scope of this FMEA is confined to the bounds of the Protection Set 1, Spec 200 equipment and is not intended to be a comprehensive protection system analysis. The FMEA which follows has been limited to the major modules in the Spec 200 configuration. In general, the techniques of Appendix A of ANSI/IEEE Std. 352-1987, "IEEE Guide for General Principles of Reliability Analyses of Nuclear Power Generating Station Safety Systems" have been utilized.

The FMEA has been assembled to provide a systematic approach to evaluating the overall design and reliability of the Spec 200 protection set instrumentation. The applicable reference drawings are identified in Tables 1 & 2 of this document. The format of the FMEA is as follows;

Appendix A: Foxboro Document No. 92-FM-02F; FMEA: A.E.P. D.C. Cook Nuclear Spec 200 Configuration.

This Appendix identifies the major Spec 200 modules utilized for trip functions in the Reactor Protection and Control System replacement project and their credible failure modes which will be considered in this FMEA.

Appendix B: Foxboro Document No. FM-502; Failure Modes and Effects Analysis, Spec 200 / Spec 200 Micro.

This Appendix provides the detailed FMEA for the Protection Set 1 instrumentation. This analysis includes all trip functions, analog output functions, Spec 200 power supplies, and power distribution modules.

Appendix C: Foxboro Document No. FM-503; Failure Modes and Effects Analysis, H Line.

This Appendix provides the detailed FMEA for the original equipment Foxboro H Line instrumentation. This analysis includes all trip functions and analog output functions.

### Conclusion:

The FMEA which has been performed on the Spec 200 / Spec 200 Micro instrumentation adequately documents that the system has been designed to provide a high level of reliability. The Spec 200 instrumentation has been configured to initiate protective actions with precision and reliability over the full range of operation.

All protective functions have been designed to fail in the safe state or into a state which has been defined and determined to be tolerable. The FMEA has identified those credible failure modes with the highest probability of occurrence with regard to individual module effects and overall loop impacts. Review of the analysis has not identified any different significant failure modes than those identified for the original equipment.

The Spec 200 system design is consistent with that of the original equipment Foxboro H Line. Operation, functionality, and interfaces as described in Section 7 of the Donald C. Cook FSAR are unchanged.

While the FMEA does not specifically address "Method of Detection" for the failure modes identified, the design has incorporated the detection techniques which existed for the original equipment system. Additionally, the Spec 200 system provides increased failure detection capabilities with alarms that are initiated upon rack / cabinet power supply failure and Spec 200 Micro control card failure.

In summary, the new Protection Set 1 Reactor Protection and Control System utilizing Foxboro Spec 200 / Spec 200 Micro instrumentation has been designed to meet regulatory requirements and the Donald C. Cook Nuclear Plant specific licensing basis. The system has incorporated all facets of protection system design as specified in IEEE 279-1971.

A similar analysis shall be performed for Protection Sets 2, 3 and 4 to ensure that this is a bounding FMEA. These evaluations will be documented by separate report at a future date.

Approvals:

Daryl W. Clark  
Prepared By

11/28/92  
Date

Peter A. deSanya  
Reviewed By

11/28/92  
Date

A. J. [Signature]  
Approved By

11/30/92  
Date



Table 1

DRAWING LIST - FOXBORO SPEC 200 EQUIPMENT

<u>FUNCTIONAL DRAWING NO.</u>	<u>DESCRIPTION</u>
FD-2101 sh. 1	PRESSURIZER PRESSURE
FD-2101 sh. 2	PRESSURIZER LEVEL
FD-2101 sh. 3	REACTOR COOLANT FLOW LOOP 1 & 2
FD-2101 sh. 4	REACTOR COOLANT FLOW LOOP 3 & 4
FD-2101 sh. 5	STEAM GENERATOR 2 & 3 LEVEL
FD-2101 sh. 6	AUXILIARY FEEDWATER FLOW S/G #3
FD-2102 sh. 1	Tave / DELTA T LOOP 1
FD-2102 sh. 2	OVERTEMP / OVERPOWER DELTA T
FD-2102 sh. 3	STATIC GAIN UNIT
FD-2102 sh. 4	WIDE RANGE HOT LEG TEMP LOOP 2 & 4
FD-2103 sh. 1	STEAM FLOW / FEED FLOW S/G #1
FD-2103 sh. 2	PRESSURE S/G #1 & 2
FD-2103 sh. 3	STEAM FLOW / FEED FLOW S/G #2
FD-2103 sh. 4	LOWER CTMT PRESSURE MAIN FEEDWATER START UP FLOW
FD-2104 sh. 1	TURBINE IMPULSE PRESSURE S/G #1
FD-2104 sh. 2	STEAM FLOW / FEED FLOW S/G #3
FD-2104 sh. 3	PRESSURE S/G #3 & 4
FD-2104 sh. 4	STEAM FLOW / FEED FLOW S/G #4

Table 1 cont.

DRAWING LIST FOXBORO SPEC 200 EQUIPMENT

<u>DRAWING NO.</u>	<u>DESCRIPTION</u>
RL-2101	RACK LOADING, PROTECTION SET 1 RACK 1
RL-2102	RACK LOADING, PROTECTION SET 1 RACK 2
RL-2103	RACK LOADING, PROTECTION SET 1 RACK 3
RL-2104	RACK LOADING, PROTECTION SET 1 RACK 4
PWR-2101	POWER DISTRIBUTION DRAWING PROTECTION SET 1 RACK 1
PWR-2102	POWER DISTRIBUTION DRAWING PROTECTION SET 1 RACK 2
PWR-2103	POWER DISTRIBUTION DRAWING PROTECTION SET 1 RACK 3
PWR-2104	POWER DISTRIBUTION DRAWING PROTECTION SET 1 RACK 4

Table 2

DRAWING LIST - FOXBORO H LINE EQUIPMENT

<u>FUNCTIONAL DRAWING</u>	<u>DESCRIPTION</u>
CD-1 Sh.1	PRESSURIZER FLOW, LEVEL AND PRESSURE
CD-1 Sh.2	PRIMARY COOLANT FLOW SYSTEM
CD-1 Sh.3	STEAM GENERATOR 2 & 3 LEVEL
CD-1 Sh.x	S/G #3 AUXILIARY FEEDWATER FLOW
CD-2 Sh. 1 & 2	REACTOR COOLANT LOOP #1 Tave & Delta T
CD-2 Sh.3	REACTOR COOLANT WIDE RANGE HOT LEG TEMPERATURE LOOPS 2 & 4
CD-3 Sh.1	S/G #1 STEAM FLOW, FEED FLOW, PRESSURE
CD-3 Sh.2	S/G #2 STEAM FLOW, FEED FLOW, PRESSURE
CD-3 Sh.3	CONTAINMENT PRESSURE
CD-3 Sh.x	S/G #1 MAIN FEEDWATER START UP FLOW
CD-4 Sh.1	S/G #3 STEAM FLOW, FEED FLOW, PRESSURE
CD-4 Sh.2	S/G #4 STEAM FLOW, FEED FLOW, PRESSURE
CD-4 Sh.3	TURBINE IMPULSE PRESSURE