Donald C. Cook Nuclear Plant Units 1 & 2
Reliability and MTBF Analysis
Reactor Protection and Control System Replacement Project
Report Number 2985-HEI-15, Rev. 0

Subject:

This report shall document the results of a Reliability and Mean Time Between Failure (MTBF) 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 equipment Foxboro H Line system.

References:

1. Foxboro Document 92-FM-02F; FMEA: D.C. Cook Nuclear, Spec 200 Configuration; October 30, 1992.

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.

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.

9. Foxboro Document FM-503; Failure Modes and Effects Analysis, H Line For The Upgrade Of The Reactor Protection Process Instrumentation; November 23, 1992.

Issue:

The Donald C. Cook Nuclear Plant, Reactor Protection and Control System is being replaced and upgraded with 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.

IEEE Standard 279-1971, "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 low failure rates.

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 Reliability and Mean Time Before Failure (MTBF) analysis. This analysis performed for the Protection Set 1 instrumentation 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 system is equivalent to the original equipment H Line instrumentation with respect 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 reliability analysis is limited to the Donald C. Cook Nuclear Plant, Protection Set 1, Reactor Protection and Control System. The analysis presented within this report has been configured to provide a systematic approach to evaluate system design. This evaluation is confined to the bounds of the Spec 200 equipment and is not intended to be a comprehensive protection system analysis.

This analysis 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.

Discussion:

The Donald C. Cook Nuclear Plant, Reactor Protection and Control System project will replace and upgrade the original equipment Foxboro H Line instrumentation with Foxboro Spec 200 / Spec 200 Micro equipment. This task represents a significant design change effort and requires analysis to ensure that the protection system has been configured to meet regulatory guidance and that the plant licensing basis is maintained. A reliability analysis which includes Mean Time Between Failure (MTBF) data shall be utilized to document that the Foxboro system will perform its intended function with a high degree of functional reliability. This analysis shall also include a comparison evaluation which documents that the new Spec 200 system provides a higher degree of availability and reliability than the original equipment.

Description of Change:

The original equipment, Reactor Protection and Control Instrumentation will be replaced and 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 is 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 action. 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 a buffer to protect the system against malfunctions and 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.

Reliability and MTBF Analysis

As stated previously, the scope of this reliability analysis 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 evaluation 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.

Foxboro Spec 200 System

Foxboro has provided Report No. 92-SA-50F; "A.E.P. D.C. Cook Nuclear, Reliability Spec 200 Configuration", which documents the reliability analysis performed on the Spec 200 system proposed for the Donald C. Cook Nuclear Plant. This report provides an availability numeric and a MTBF value for each system function.

A "function" is defined as a discrete output function (i.e. bistable trip, alarm, analog output, etc.) which is represented by the referenced functional drawing (see Table I). Each Spec 200 function, identified on the drawing, has been evaluated utilizing the Fault Event Tree method of reliability system analysis. This technique graphically depicts the contributions of the individual modules to the system total and calculates system availability. The Fault Event Tree method calculates overall availability of the system by manipulating the availability values for each module, according to the mathematical rules of probability and the system configuration. The equivalent function MTBF is calculated from the availability numeric for the applicable function.

The results of Report No. 92-SA-50F indicate that the Spec 200 system, with its added redundancy features and high degree of availability provides an availability numeric of better than 0.9997. This availability numeric, a dimensionless, decimal value between 0.00 and 1.000, represents overall system function availability. Unity (1.000) would represent 100% availability.

Calculated Mean Time Between Failure (MTBF) data indicates that the limiting loop has an MTBF of greater than four years.

Foxboro "H" Line System

Foxboro has provided Report No. 92-SA-66F; "A.E.P. D.C. Cook Nuclear, Reliability "H" Line Configuration", which documents the reliability analysis performed for the original equipment "H" Line system. This document provides an availability numeric and a MTBF value for equivalent system functions.

Each "H" Line function is identified as being equivalent to the similar Spec 200 system function as shown on the drawings identified in Table 1 of this report. Each function has been evaluated utilizing the Fault Event Tree method of reliability analysis identified above.

Due to the vintage of the Foxboro "H" Line hardware, availability and MTBF prediction data is not documented. Therefore, a standard single value of 7.1 failures/million hours of MTBF is used for each "H" Line module. This value was derived from material presented in the November 1987 issue of "The Operational Performance of Reactor Protection Systems in U.S. Pressurized Water Reactors, 1981 - 1985", from the Institute of Nuclear Power Operations. The use of this "average" INPO MTBF value for all "H" Line modules results in the lower, worst case boundary for the function's availability and MTBF.

The standard value was assigned to each "H" Line module and utilized in all calculations. A conservative assumption that the failure of any one module causes failure of the entire loop was utilized in the Fault Event Tree analysis of complex loops.

The results of Report 92-SA-66F indicate that the original "H" Line equipment produced an equivalent system availability numeric of 0.9990 or better. Calculated Mean Time Between Failure (MTBF) results were calculated to be as low as one year.

Conclusion:

The reliability analysis 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.

The Spec 200 system design is consistent with that of the original Foxboro "H" Line equipment. Operation, functionality, and interfaces as described in Section 7 of the Donald C. Cook FSAR are unchanged. A comparison of availability and MTBF data indicates that the Spec 200 system will provide a higher degree of availability with lower failure rates than that realized from the original "H" Line system.

In summary, the new Reactor Protection and Control System utilizing Foxboro Spec 200 / Spec 200 Micro instrumentation has been designed with components and modules which will provide a high level of system reliability. The quality of system components is such that failure rates are low and a minimum of maintenance is required to ensure operability. The system has incorporated all appropriate facets of protection system design as specified in IEEE 279-1971.

Approvals:

David W. Clark — Prepared By — 11/28/92 — Date

Peter A. deSanza — Reviewed By — 11/28/92 — Date

[signature] — Approved By — 11/30/92 — Date

Table 1

DRAWING LIST - FOXBORO SPEC 200 EQUIPMENT

FUNCTIONAL DRAWING NO.	DESCRIPTION
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 CONTAINMENT 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

DRAWING NO.	DESCRIPTION
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