SAFETY EVALUATION REPORT OF THE
COMBUSTION ENGINEERING EVALUATION
FOR RPS/ESFAS
EXTENDED TEST INTERVAL (CEN-327)

1.0 INTRODUCTION

The Combustion Engineering Owners Group (CEOG) submitted a topical report prepared by Combustion Engineering (CE), "RPS/ESFAS Extended Test Interval Evaluation", CEN-327. This report provides a basis for requesting changes to the Technical Specification surveillance testing requirement for selected components in the Reactor Protection System (RPS) and Engineered Safety Features Actuation System (ESFAS). The CE report presented analysis to justify the extension of the channel functional and logic unit surveillance test intervals from 30 days to 60 days and 90 days for selected RPS parameters and from 30 days to 90 days for ESFAS actuation logic. Subsequently, Supplement 1 to CEN-327 was submitted and presents a re-evaluation of the RPS to justify a ninety (90) day test interval (for all RPS parameters) with sequential testing. These analyses evaluated the impact of the proposed extended test intervals on core melt frequency and system unavailability to demonstrate that the proposed changes did not increase the plant risk when compared with the current technical specifications requirements. The Idaho National Engineering Laboratory (INEL) reviewed the CEOG report. The result of that review is reported in detail in EGG-REQ-7768, "A Review of the Combustion Engineering Evaluation For Extending The RPS and ESFAS Test Intervals" dated September, 1988, and summarized in this report. The following is the results of our audit review of the CEOG report and its supplement, and our review of EGG-REQ-7768.

Reactor Protection System Test Interval Evaluation (CE-NPSD-277) presents a fault tree model for each of the four basic Reactor Trip System (RTS) designs supplied by CE. For each design, the fault tree modeled the RTS from the reactor trip switchgear (or contactors) to the sensors for the high pressurizer pressure trip parameter. Each model specifically addressed common mode failures, operator error, reduced redundancy, and random component failures.

These models were used to evaluate the RTS availability given the current test intervals specified in the Technical Specifications. The CE report (CEN-327) expanded each of the four RPS fault tree models presented in CE-NPSD-277 to cover all RPS trip parameters. These expanded models were then quantified to determine the RPS reliability for the current and the extended test interval for each trip parameter.

Fault tree models were also constructed for each ESFAS for the different plant classes used for the RPS analysis in CE-NPSD-277. Similar to the RPS fault tree models, each ESFAS fault tree model specifically addressed common mode failures, operator errors, reduced redundancy, and random component failures. These models were then evaluated to determine the reliability of the ESFAS for both the current and extended test intervals. The core melt frequency impact of extending the RPS and ESFAS test intervals was evaluated for a core melt event tree presented in the Calvert Cliffs Interim Reliability Evaluation Program study.

There are four basic RPS designs and three ESFAS designs and both system types are functionally applicable to all CE 2-loop plants. Maine Yankee, a 3-loop design, was not included in the CE analysis and, as a result, is not covered by this report. CE stated in CEN-327 (report) that the models were developed only for comparison purposes and were not detailed plant specific models.

2.0 RPS AND ESFAS MODELS AND ASSUMPTIONS

Following the Salem ATWS event in 1983, the NRC issued Generic Letter 83-28 specifying a number of actions to be taken by licensees and applicants. One of these required actions was to review the Reactor Trip System (RTS) test intervals to determine if they are consistent with achieving high RTS availability. CE conducted an analysis, documented in Reactor Protection System Test Interval Evaluation, CE-NPSD-277, to address this required action for nuclear plants with a CE supplied NSSS. This activity included development of generic fault tree models for the RTS and numerical analysis of these models with the component test intervals fixed at the value currently required by the Technical Specifications. Using these models as the basis, fault trees were

developed by CE to evaluate the impact of extended testing intervals on the unavailability of the RPS and ESFAS. The CE RPS and ESFAS models reviewed herein represent the entire population of CE supplied 2-loop Nuclear Steam Supply Systems (NSSS). The only plant with a CE supplied NSSS not included in the CE evaluation is Maine Yankee, which is a 3-loop NSSS design.

2.1 RPS MODELS

The basic design for the RPS is functionally applicable to all CE plants, however there are differences in implementation from plant to plant involving signal processing methods and trip devices. Based on these differences, the CE RPS designs were divided into four general classes. The Class 1 design, representing Palisades and Fort Calhoun, includes a thermal margin/low pressure setpoint calculator and uses four (4) contactors as the trip devices. The class 2 design, representing Millstone 2, Calvert Cliffs 1 & 2, and St. Lucie 1 & 2, includes a thermal margin/low pressure setpoint calculator and uses eight (8) reactor trip circuit breakers as the trip devices. The Class 3 design, representing Arkansas 2, San Onofre 2 & 3 and Waterford 3 includes Core Protection Calculators (CPCs) and uses eight (8) reactor trip circuit breakers as the trip devices. The Class 4 design, representing Palo Verde 1, 2, & 3 includes CPCs and uses four (4) reactor trip circuit breakers as the trip devices. The RPS for each plant within a class are functionally equivalent.

Reactor Protection System Test Interval Evaluation (CE-NPSD-277) presents a fault tree model for each of these four basic RTS designs. For each design, the fault tree modeled the RTS from the reactor trip switchgear (contractors) to the sensors for the high pressurizer pressure trip parameter. Each model specifically addressed common mode failures, operator errors, reduced redundancy, and random component failures. These models were used to evaluate the RTS availability given the current test intervals (30 days) specified in the Technical Specifications. In the CE report, each of the four RPS fault tree models presented in CE-NPSD-277 were expanded to cover all RPS trip parameters. These expanded models were then quantified to determine the RPS

reliability for the current and the extended test interval for each trip parameter.

Four measurement channels with electrical and physical separation are provided for each parameter used in the direct generation of trip signals, with the exception of control element assembly (CEA) position. A two-out-of-four coincidence of like trip signals is required to generate a reactor trip signal.

The basic fault tree developed by CE for each of the four RPS plant classes models only the major active components from the sensor channels to the trip devices. These components include bistables, relays, under voltage and shunt trip devices and circuit breakers. The models were compared to RPS functional diagrams supplied by CE for plants in each of the four plant classes. The intent of the CE fault trees was to provide sufficient detail in the model to examine the impact of extended test intervals on the overall system unavailability. No attempt was made by CE to model the system such that the absolute unavailability could be determined.

The RPS modeling assumptions are given in Section 3.4.1 of CEN-327 and are consistent with the design of the system and the intended use of the models. Both the level of resolution in the RPS fault trees and the modeling assumptions are considered to be adequate for the intended use. Based on the comparison with the RPS functional diagrams, the basic fault trees for the four classes were judged to be adequate models of the system for the purposes of the comparison.

2.2 ESFAS MODELS

Fault tree models were constructed for each of the engineered safety feature actuation signals for each of the different plant classes used for the RPS analysis in CE-NPSD-277. Similar to the RPS fault tree models, each ESFAS fault tree model specifically addressed common mode failures, operator errors,

reduced redundancy, and random component failures. Once the models were constructed, they were evaluated to determine the reliability of the ESFAS for the current and extended test intervals.

The ESFAS at plants with CE supplied NSSS were divided into three classes in CEN-327: (1) Plants that utilize an ESFAS designed by CE, (2) Plants that utilize a non-CE ESFAS design with relay logic, and (3) Plants that utilize a non-CE ESFAS design with solid state logic.

Although the three ESFAS plant class designs are functionally equivalent, there are differences in signal processing devices and types of components used. For each ESFAS class, generic fault tree models were constructed by CE for each applicable ESFAS signal. Where there were significant system design differences between plants within the general classes, the generic fault trees were modified to be more representative of the individual plants.

The ESFAS consists of sensors, logic and actuation circuits which monitor selected plant parameters and provide actuating signals to each actuated component in the Engineered Safety Features System which is required to be actuated. There is one actuation signal for each of the ESF System functions. Each actuation signal is functionally identical except that specific inputs and logic vary from system to system and the actuated devices are different. The following actuation signals are generated by the ESFAS when the monitored variable reaches the levels that are indicative of conditions which require protective actions:

(1) Containment Isolation Actuation Signal (CIAS)
(2) Containment Spray Actuation Signal (CSAS)
(3) Main Steam Isolation Signal (MSIS)/Steam Generator Isolation Signal (SGIS)
(4) Safety Injection Actuation Signal (SIAS)
(5) Recirculation Actuation Signal (RAS)
(6) Emergency (Auxiliary) Feedwater Actuation Signal (EFAS/AFAS)

Four redundant measurement channels with electrical and physical separation are provided for each signal used in the direct actuation of an ESF System. A 2-out-of-4 coincidence of like parameter signals is required to actuate any of the ESFAS signals which in turn actuates an ESF System.

No attempt was made by CE to model the ESFAS signal paths such that the absolute ESFAS unavailability could be determined. To meet the intended purpose, CE included in the models the major components of the ESFAS from the sensors to the input of the actuation devices. The modeling assumptions used for the ESFAS fault trees are given in Section 3.4.2 of the CE Report and reflect the differences of the three ESFAS design classes. Based on the INEL review of the fault tree models and our understanding of the ESFAS system differences, the models and the modeling assumptions used for the ESFAS signal fault trees are considered adequate for their intended purpose.

2.3 RESULTS

2.3.1 REACTOR PROTECTION SYSTEM (RPS)

The results of the CE analysis in CEN-327 and the audit calculations performed by INEL both estimate a slight increase in RPS unavailability as a result of extending the test interval from monthly to 60 or 90 days, depending on the parameter. CE also estimated the reduction in scram frequency from the expected reduction in test-induced scrams and the corresponding reduction in core melt frequency. INEL reviewed and found these estimates to be acceptable. Supplement 1 provides additional analysis to show that extending the test interval to 90 days still results in very small increases in RPS unavailability. The change to 90 days for all parameters will simplify the testing schemes and reduce the possibility of error as discussed in the INEL report. The overall impact of the reduced testing on safety is judged to be negligible.

2.3.2 ENGINEERED SAFETY FEATURES ACTUATION SYSTEM (ESFAS)

The results of the CE analysis and the INEL audit calculations regarding the impact of reduced ESFAS testing on core melt frequency are similar to those for the RPS. The increase in certain ESF actuation system unavailabilities for some plants is somewhat more significant, since these systems do not have the level of redundancy of the RPS. For example, the Ft. Calhoun auxiliary feedwater actuation unavailability is estimated in CEN-327 to increase from 1.8×10^{-4} to 2.4×10^{-4} per demand by extending the test interval to 90 days. This increase is judged to be small considering the uncertainty in these analyses and the effect on overall core melt frequency.

3.0 CONCLUSION

The major conclusions of the technical review of the analysis performed to establish a basis for extending the testing intervals from 30 days to 90 days for RPS and ESFAS components at CE plants are as follows:

1. The fault tree models of the RPS and the ESFAS are developed in sufficient detail and logic to allow evaluations of the effects of extended test intervals on RPS and ESFAS unavailability.

2. The data used by CE to quantify the fault trees and establish the effects of extended test intervals have been developed in sufficient detail to conduct the evaluation.

3. The methodology used by CE to estimate changes in RPS and ESFAS unavailability and core melt frequency due to test interval changes is deemed adequate by this review and applicable to all CE plants with the exception of Maine Yankee.

4. The analysis provided by CE and reviewed by INEL provides sufficient basis for extending the RPS channel functional and logic test interval for all CE plants with the exception of Maine Yankee. The extension should cause fewer inadvertent scrams and the risk models estimate a corresponding reduction in core melt frequency from this type of transient. Extending the time between tests does increase the estimated reactor protection system unavailability a very small amount. This extension has little effect on safety and is judged to be acceptable.

5. The analysis provided by CE and reviewed by INEL provides sufficient basis for extending the ESFAS channel functional and logic test interval from monthly to quarterly. While a standard does not presently exist for judging instrumentation reliability, this methodology suggests that the extension will increase the ESFAS unavailabilities at the plants a very small amount. Another consideration is that the estimated impact on core melt frequency is quite small. We conclude that the expected safety impact from extending the channel functional test to quarterly for these plants is very small and is acceptable.

6. We find that the effects of drift in both the sensors and the instrument strings were not considered in this analysis, it is individual to each specific plant, and therefore should be addressed and factored into the analysis on a plant specific basis. Each licensee should, therefore, confirm that they have reviewed drift information including as found and as left values for each instrument channel involved and have determined that drift occurring in that channel over the period of the extended test intervals will not cause the setpoint value (the setpoint value is defined as the uppermost (least conservative) value of the leave-alone zone) to exceed the allowable values as calculated for that channel by their setpoint methodology. Each licensee should maintain onsite records (2-3 years of monthly drift information) showing the actual setpoint calculations and supporting data that are available for planned future staff audits.