Defense-in-Depth and Diversity Evaluation to Cope with Non-LOCA with Concurrent Common Mode Failure in Digital Plant Protection System for KNGR

Cheol-Shin Lee, Gyu-Cheon Lee, Chul-Jin Choi and Jong-Tae Seo
Korea Power Engineering Co., Inc., Korea

ABSTRACT

A quantitative evaluation has been performed to determine the intrinsic capability of the Korean Next Generation Reactor (KNGR) design in coping with non-LOCA transients with concurrent Common Mode Failure (CMF) in the digital Plant Protection System (PPS). A best-estimate analysis methodology has been developed and utilized since design bases events with concurrent CMF in digital PPS are categorized as beyond design bases events. Due to diverse means not affected by CMF and a sufficient available over-power margin, the event consequences are well within the acceptance criteria. In addition, the KNGR design offers sufficient safety margin against non-LOCA events without operator actions up to 30 minutes after the initiation of an event even with CMF.

I. INTRODUCTION

The digital PPS to be designed into the KNGR could be vulnerable to CMF caused by software error, which could defeat the redundancy configured in the hardware architecture. The regulatory policy on CMF in the protection system software specifies that the licensee perform an evaluation which shows the Defense-in-Depth and Diversity (D-in-D&D) capability of the plant design to cope with the design bases events accompanied by CMF in digital PPS. The basis of this requirement is that the software design error is a credible source of CMF because software cannot be proven to be error-free. If a postulated CMF could disable any protection function that is required to respond to the design basis event, then a diverse means of effective protection would be necessary. Presented in this paper are the results of the detailed quantitative evaluations which has been performed to confirm the capability of KNGR to cope with non-LOCA events with a postulated CMF in digital PPS.
II. KNGR DESIGN APPROACH FOR DEFENSE-IN-DEPTH AND DIVERSITY

The KNGR digital Instrumentation and Control (I&C) system design related to D-in-D&D is to eliminate predictable CMFs and to obtain high reliability to reduce CMF potential for software in the digital PPS. Predictable CMFs are avoided through seismic and Electro-Magnetic Interference (EMI) qualification, aging analyses and geographic separation of equipment. High reliability is realized by deterministic design, simplicity, use of field proven products, a comprehensive verification and validation program, segmentation and diversity. The most severe common mode failure in the digital I&C systems has been found to be a complete malfunction of Plant Protection System (PPS), which disables reactor trip functions and the actuation of various Engineered Safety Features (ESF). The systems not affected by CMF in digital PPS are 1) Qualified Indication and Alarm System – P (QIAS-P), 2) Main Control Room (MCR) hardwired manual reactor trip, 3) MCR hardwired manual ESF actuation, 4) Information Processing System (IPS) which is a digital based monitoring system, and 5) Alternate Protection System (APS) which is a digital based system to meet Anticipated Transients Without Scram (ATWS) requirements [6]. The control echelon (line of defense) is the non-safety equipment that routinely prevents reactor excursions toward unsafe regimes of operation and is used for normal operation of the reactor. The Nuclear Steam Supply System (NSSS) control systems have D-in-D&D characteristics against CMF in digital PPS because these systems are diverse from PPS. In addition, manual operator action is allowed as a diverse means of responding to postulated CMFs if sufficient information and time is available for the operator to detect, analyze and act to mitigate the events with CMF in digital PPS.

III. ANALYSIS METHODOLOGY

Based on extensive qualitative study on all non-LOCA events, five events have been selected for quantitative analyses to demonstrate the D-in-D&D characteristics of the KNGR design to deal with the CMF in digital PPS. These events include 1) Increase in Main Feedwater Flow, 2) Main Steam Line Break, 3) Single Reactor Coolant Pump Shaft Seizure, 4) Letdown Line Break, and 5) Steam Generator Tube Rupture. The emphases of the evaluations have been placed on a required action time for plant operators to cope with the events in a manner which preserves core coolability, maintains Reactor Coolant System (RCS) integrity, and prevents excessive offsite doses.

The combinations of design bases events and CMF in digital PPS are categorized as beyond design bases events [1]. Therefore, a best-estimate analysis methodology has been applied according to the regulatory guidance [2]. Major characteristics of the best-estimate analysis methodology include utilizing nominal initial conditions and nominal design data,
crediting components and systems being independent and diverse from digital PPS, and crediting appropriate operator actions. In this analysis, the NSSS thermal hydraulic responses are simulated using the CESEC-III computer program [3] while the fuel performances are simulated using the CETOP-D [4] and STRIKIN-II [5] computer codes.

IV. ANALYSES RESULTS AND DISCUSSIONS

Increase in Main Feedwater Flow

The increase in main feedwater flow event is an Anticipated Operational Occurrence (AOO) which is caused by a further opening of the feedwater control valves or an increase in the feedwater pump speed. The increase in feedwater flow results in excessive cooldown of the RCS. This causes the core power to increase rapidly due to the moderator temperature feedback effect. A CMF in digital PPS prevents the reactor trip on high core power. Finally, the core power reaches a new elevated quasi-steady state at which a reactivity balance is regained by the fuel temperature feedback effect. The main concern of this event is how much the thermal margin would be reduced due to the increase in core power. Figures 1 and 2 show the core power and the Departure from Nucleate Boiling Ratio (DNBR) variations during the increase in feedwater flow event with CMF in digital PPS. Thermal margin reduction in the early stage results from the increase in the core power, followed by recovery of DNBR due to an appropriate actuation of Pressurizer Pressure Control System (PPCS). Considering the Specified Acceptable Fuel Design Limit (SAFDL) of 1.30 below which fuel cladding failure is assumed to occur, no fuel failure would occur throughout the transient. The best estimate overpower margin is approximately 150% for normal operating conditions assumed in this analysis.

Main Steam Line Break

A large energy extraction caused by the steam line break reduces the steam pressure dramatically causing the turbine-generator shutdown terminating the condensate water supply to the feedwater system. The feedwater control system tends to increase the main feedwater flow to the steam generators in response to the decrease in the steam generator water level. All feedwater heating is assumed to be lost immediately due to steam line break. It is also assumed that the feedwater system and feedwater control system are able to maintain the mass of liquid in the steam generators essentially constant until the entire source of main feedwater supply is exhausted. Main concerns for this accident are the maintenance of core coolable geometry, radiological releases, and the primary system integrity.

Figures 3 and 4 show the core power and the RCS pressure variations for the main steam line break event with CMF in digital PPS. A rapid cooldown caused by the steam blowdown through the break causes a sharp increase in the reactor power as shown in Figure
3. Complete depletion of feedwater results in a steam generator dry out. The dry out of steam generators causes a rapid increase in the RCS pressure, which leads to a reactor trip on high pressurizer pressure by the APS. The RCS peak pressure is well below 3200 psia, which is adapted as acceptance criteria with respect to primary system integrity. The calculated peak core power and the minimum DNBR are approximately 189% of nominal power and 1.1, respectively. About 1% of fuel failure is predicted to occur as a consequence of the DNB SAFDL violation. The radiological dose release is found to meet the limits specified in 10 CFR 100 guideline. The maximum cladding and fuel centerline temperatures follow the same trend as the power, reaching peak values of less than 670°F and 4340°F, respectively. These ensure the maintenance of the core coolable geometry. Diverse systems such as the APS accompanied by intrinsic thermal margin are proven to be effective to mitigate the consequences of the main steam line break event with CMF in digital PPS.

Single Reactor Coolant Pump (RCP) Shaft Seizure

The single RCP shaft seizure event is an accident which is caused by a seizure of the upper or lower thrust-journal bearings of an RCP. This results in a rapid decrease in the reactor coolant flow. The flow reduction terminates within a few seconds and stabilizes at a flow of approximately 75% of the initial flow. The low reactor coolant flow reactor trip is not triggered due to the CMF in digital PPS. The core power decreases due to the fuel temperature feedback effect within several seconds and then restores to the initial core power due to moderator temperature feedback. When these two reactivity feedback effects lead to another balanced reactivity condition, a quasi-steady state is reached. Main concern for this event is how much the thermal margin would be degraded due to the decrease in the core flow rate. Figures 5 and 6 show the core flow rate and the DNBR variations for the single RCP shaft seizure event with CMF in digital PPS. The predicted minimum DNBR is 1.8156, which ensures no fuel failure.

Letdown Line Break and Steam Generator Tube Rupture

A direct release of the reactor coolant may result from a break or leak outside containment of the letdown line. The steam generator tube rupture accident is a penetration of the barrier between the RCS and the main steam system. Both events cause the RCS pressure to decrease due to the leakage of reactor coolant. The probable reactor trip signals for these events are generated by a low hot leg saturation margin or a low DNBR by the Core Protection Calculator (CPC), which is a part of PPS. The CMF in digital PPS prevents these reactor trips from being triggered. The main concern for these events is how much the thermal margin would be degraded due to the decrease in the RCS pressure within a specified time beyond which the operators are assumed to take manual actions to restore the degraded thermal margin. In addition, the radiological release to the atmosphere should be
limited within the regulatory guidelines. Figures 7 through 12 show the RCS pressures, DNBR, and leak flow rate variations for the letdown line break and the steam generator tube rupture event with CMF in digital PPS. For the letdown line break, the pressure excursion is controlled within the normal operating range by an appropriate response of the control systems such as PPCS and Pressurizer Level Control System (PLCS) while the RCS pressure for the steam generator tube rupture event decreases continuously. In the KNGR design, the letdown orifices are located inside containment, which increases the resistance to the break located outside containment and reduces the break flow rate through the letdown line. For both events, no fuel failure due to DNB is predicted until 30 minutes at which operators are assumed to take manual actions. The radiological release meets the regulatory limit with sufficient margin.

V. CONCLUSIONS

A new systematic best-estimate analysis methodology, which is partly conservative but licensable, for the analyses of non-LOCA events with CMF in digital PPS and applied to the KNGR D-in-D&D analysis. The analysis results demonstrated the capability of the KNGR design to accommodate the non-LOCA events with CMF in digital PPS, which are categorized as beyond design bases accidents. Due to the diverse means (APS and NSSS control systems) to cope with CMF in digital PPS and a sufficient available over-power margin, the consequences are well within the regulatory guidance limits. In addition, the KNGR design offers sufficient safety margin against non-LOCA events without operator actions up to 30 minutes after an event initiation even with CMF. Therefore, the intrinsic D-in-D&D capability of the KNGR design against CMF in digital PPS has been verified.
Fig. 1 Core Power Transient for Increase in Feedwater

Fig. 2 DNBR Transient for Increase in Feedwater

Fig. 3 Core Power Transient for Steam Line Break

Fig. 4 RCS Pressure Transient for Steam Line Break

Fig. 5 Core Flow Rate Transient for Single RCP Shaft Seizure

Fig. 6 DNBR Transient for Single RCP Shaft Seizure

XI-288
Fig. 7 RCS Pressure Transient for Letdown Line Break

Fig. 8 DNBR Transient for Letdown Line Break

Fig. 9 RCS Pressure Transient for Steam Generator Tube Rupture

Fig. 10 DNBR Transient for Steam Generator Tube Rupture

Fig. 11 Break Flow Rate Transient for Letdown Line Break

Fig. 12 Leak Flow Rate Transient for Steam Generator Tube Rupture
REFERENCES


