System Function Evaluation due to Hardware Failure of NSSS Control Systems in the APR1400

Juyoung Kim*, Myunghoon Ahn, Woogoon Kim, Hyeongsoon Yim
KEPCO E&C Company Inc., 989-111 Daedeokdaero, Yuseong-gu, Daejeon, 34057, Republic of Korea
**Corresponding author: jykim@kepco-enc.com*

1. Introduction

As the performance and failure modes of the control systems may affect the plant response to accidents or disturbances, an evaluation is done to identify potential control system failure modes resulting from single hardware failures. These failure modes are for use in the analytical evaluations that will be performed to assess the plant responses to various disturbances from the viewpoint of postulated system malfunctions.

2. Scope of Evaluation

The evaluation includes the following NSSS (Nuclear Steam Supply System) Control Systems depicted in Fig. 1:

- Pressurizer Pressure Control System (PPCS)
- Pressurizer Level Control System (PLCS)
- Feedwater Control System (FWCS)
- Steam Bypass Control System (SBCS)
- Reactor Regulating System (RRS)
- Reactor Power Cutback System (RPCS)
- Digital Rod Control System (DRCS)

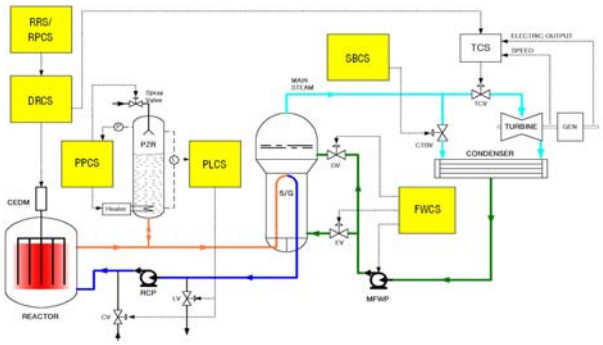

Fig. 1. Overview of NSSS Control Systems

This evaluation identifies the various failure modes of the NSSS Control Systems caused by component hardware faults including common sensing devices. As used in this evaluation, the components refer to signal processing devices within the various signal paths.

This evaluation also involves identifying mal-functions of control systems caused by the loss of a power supply. Only the 120 VAC buses that directly provide power to the NSSS Control Systems are considered.

If the failure of non-safety systems could produce results more severe than the failure of safety systems, the failures of both safety and non-safety systems will be included in the analytical evaluations [1]. But in this evaluation, only single failures of the non-safety NSSS Control Systems are assessed.

3. Assumptions

The single failure evaluation for the NSSS Control Systems identifies the most probable system failure modes and determines the effect of each mode on system performance. To provide consistency and standardization in the evaluation of each control system, general rules or assumptions are made. The following is a list of rules followed or assumptions made in this evaluation.

1. The control systems covered include NSSS Control Systems' components in the paths of the control signal: measurement devices, signal processors, and output modules to the Process Component Control System (P-CCS). The failure modes of P-CCS which interfaces with the actuated equipment are not addressed.
2. Signal sensing failures consider out-of-range high or low. Intermediate failures are not identified separately.
3. The control systems are in their automatic modes of operation. No operator intervention takes place.
4. The instrument air system, which provides support to certain control systems, is operating in its proper range.
5. Software common cause failure on the non-safety platform that results in multiple failures of one or more systems is not considered.
6. Control system failures resulting from abnormal environment, including earthquakes, fires and floods, are not considered.
7. High energy electrical faults that could propagate and cause multiple failures are not addressed. Only false signals, including credible short and open circuits, are considered.

4. Evaluation and Results

The control systems of concern in this evaluation are used to improve plant availability and prevent unnecessary reactor trips. As a result, certain of these systems share common signals and interchange signals with other control systems. Because of these

interactions, the failure modes identified can be categorized as follows:

1. Failure modes that affect the performance of only the control system that has failed.
2. Multiple failure modes that are caused by common sensing devices or common power supplies.

Failure modes that fall into any of the above categories will affect the performance of the control system and should be considered in the analytical evaluation of the NSSS responses to disturbances. The effects of the multiple failure modes in category 2 are considered more severe than those of the single failures. But it is evaluated that there are no failure modes in category 2 other than category 1 that affects the system performance.

The results of this evaluation identify the failure modes or malfunctions of the control systems in the APR1400. These results are presented in the Tables I, II, and the paragraphs followed.

Table I shows the failure modes of control systems for category 1. Each failure mode is caused by a single hardware fault, except failure of common sensing devices. The failure modes are listed as single events such that each item within a control system means one single failure. The combination of multiple items is excluded by considering single hardware failure. The failure modes may be not revealed until a failed system function is called upon during an event. But, due to the continuous operation of most control systems, the majority of failures triggered from the control systems are inherently self-detecting, because they will change the status of field components.

Table I: Control System Failures Caused by a Single Hardware Fault

Control System	Failure Mode
PPCS	▫ Insufficient pressurizer (PZR) spray flow ▫ Excessive pressurizer spray flow ▫ Insufficient heater capacity ▫ Excessive heater capacity ✓ Effect: PZR High Pressure or PZR Low Pressure
PLCS	▫ Insufficient charging flow ▫ Excessive charging flow ▫ Insufficient letdown flow ▫ Excessive letdown flow ✓ Effect: PZR High Level / Pressure or PZR Low Level / Pressure
FWCS	▫ Insufficient feedwater flow ▫ Excessive feedwater flow ✓ Effect: Steam Generator (SG) High Level / PZR Low Pressure
	or SG Low Level / PZR High Pressure
SBCS	▫ Insufficient open of one or more Turbine Bypass Valves (TBVs) ▫ Excessive open of one or more TBVs ▫ Failure to quick open four or more TBVs ▫ Failure to generate reactor power cutback signal ▫ Failure to generate turbine runback signal ▫ Failure to generate auto motion inhibit signal ▫ Failure to generate auto withdrawal prohibit signal ✓ Effect: PZR/SG High Pressure / Excessive Reactor Power or PZR/SG Low Pressure
RRS/ RPCS	▫ Failure of Control Element Rod Assembly (CEA) insertion demand signal ▫ Failure of CEA withdrawal demand signal ▫ Failure to generate auto motion inhibit signal ▫ Failure to generate auto withdrawal prohibit signal ▫ Failure to generate arm and drop signals ▫ Failure to generate turbine runback, setback, or load increase inhibit signal ✓ Effect: Excessive Reactor Power / PZR/SG High Pressure / RCS High Temperature or PZR/SG Low Pressure / SG Low Level / RCS Low Temperature
DRCS	▫ Failure to insert CEAs ▫ Excessive insertion of CEAs ▫ Failure to withdraw CEAs ▫ Excessive withdrawal of CEAs ✓ Effect: Excessive Reactor Power / PZR/SG High Pressure / RCS High Temperature or PZR/SG Low Pressure / RCS Low Temperature

Table II evaluates the failures of multiple control systems caused by failure of a common sensing device, which is of category 2. However, for each of the common sensing devices, the NSSS Control Systems are less prone to the failures by applying the input selection algorithms with redundant transmitters in addition to redundant input/output modules.

Table II: Control System Failures Caused by a Common Signal Failure

Common Signal	Control Systems Affected	Failure Mode
PZR Pressure fails	PPCS SBCS	No Malfunctions -PPCS: Input Selection

		Algorithms (ISA) -SBCS: 2 out of 2 from Main and Permissive (2OO2)
Steam Flow fails	SBCS FWCS	No Malfunctions -SBCS: ISA, 2OO2 -FWCS: Selected Signal from SBCS
Reactor Power fails	RRS FWCS SBCS	No Malfunctions -RRS: ISA -FWCS, SBCS: Selected Signal from RRS
RCS Temperature fails	RRS FWCS SBCS PLCS	No Malfunctions -RRS: ISA -FWCS, SBCS, PLCS: Selected Signal from RRS
Turbine Load Index fails	RRS SBCS FWCS	No Malfunctions -RRS: ISA -FWCS, SBCS: Selected Signal from RRS

The malfunctions caused by loss of power sources are based on the current assignment of power sources for the control systems. The failure modes of multiple control systems caused by the failure of a common power supply buses, either N1 or N2 are evaluated as the category 2. However, for each of the power buses, the NSSS Control Systems are not affected from the failures by applying the redundant power sources to each system [2]. A single failure results in loss of no more than one control system power source unless both of the buses (N1 and N2) are lost.

5. Conclusions

An evaluation was performed to identify the failure modes of the NSSS Control Systems, caused by a hardware component, a common sensing device, and a common power supply. The multiple failure modes across the NSSS control Systems are limited by the improved design features, redundancy within each systems, and segmentation between systems. Also, the effects from the failure modes are expected to be acceptably terminated by the Plant Protection System. The failure modes derived through this evaluation will be further considered in the analytical evaluation of the NSSS responses to disturbances in order to identify the single failures which could create the most adverse conditions during a given transient.

REFERENCES

[1] IEEE 379, Application of the Single-Failure Criterion to Nuclear power Generating Station Safety Systems, IEEE Power Engineering Society, 1994

[2] Failure Mode and Effect Analysis of the Ovation Control and I/O System, Westinghouse, 2014