*Transactions of the Korean Nuclear Society Spring Meeting*
*Pyeongchang, Korea, May 27-28, 2010*

# Spurious Activation of Digital Plant Protection System in Nuclear Power Plants

M. Khalaquzzaman[1*], Hyun Gook Kang[2], Man Cheol Kim[2], Poong Hyun Seong[1]

[1]*Nuclear and Quantum Engineering Department, Korea Advanced Institute of Science and Technology*
*373-1 Guseong-dong, Yuseong-gu, Daejeon 305-701*
[2]*Integrated Safety Assessment Team, Korea Atomic Energy Research Institute*
*P.O. Box 105, Yuseong, Daejeon, 305-600, Korea*
**email: swapan74@kaist.ac.kr*

## 1. Introduction

The Reactor Protection System (RPS) of a nuclear power plant (NPP) is employed to detect abnormal (hazardous) condition of the plant and perform automatic safe shutdown of a nuclear reactor. However, the reactor can shutdown within the normal range of plant process parameters, which is known as spurious trip of reactor. Spurious trip model for common process industries has been developed, which optimizes the maintenance frequency of a safety instrumented system (SIS) for process industries. Spurious activation of SIS due to constant random hardware failures has been addressed [1-5].

The spurious activation of SIS for oil and gas industries has been defined with developing a set of formulas for STR [3]. However, the maintenance human errors were not explicitly considered in those studies. Incidence of maintenance errors should be considered for spurious trip rate estimation since those are the major causes of unplanned shutdowns of process industries and nuclear power industries. Maintenance human error is an important factor for component failure and unplanned trip [3, 6, 7]. There appears to be no model available which can estimate spurious trip frequency of a reactor caused by random hardware failure and maintenance human error in a digital plant protection system for nuclear power plants. Our model is well defined and pragmatic for quantification of spurious trip rate and explicitly considers maintenance human errors. Fault-tree analysis has been done to estimate the spurious trip frequency of digital plant protection system. The model may be employed by the plant maintainer as well as designers to identify the influential components responsible for high spurious trip rate.

## 2. Concept and causes of spurious trip in DPPS

All RPSs are designed to be fail-safe. For instance, the loss of power supply to the DPPS would cause a reactor trip. An execution of spurious trip of a reactor depends on LCL logic configuration of DPPS. Failure of single or multiple components may not lead to spurious shutdown of reactor. Major causes of reactor spurious trip include [8] – (I) random hardware failure of DPPS components (e.g. transducer failure and processors failure); (II) component failure induced by human error in maintenance and periodic surveillance tests; and (III) loss of utilities (e.g. failure of electrical power supply system, failure of pneumatic or hydraulic system).

A channel trip condition can be generated when two or more components fail within a channel (for example, failure of two output modules of LCL processors (A1 AND A2) due to maintenance human errors or random hardware failures in a channel generate a spurious channel trip signal in the respective channel). Propagation of component failure signals for activation of channel trip is shown in Fig. 1 [8].

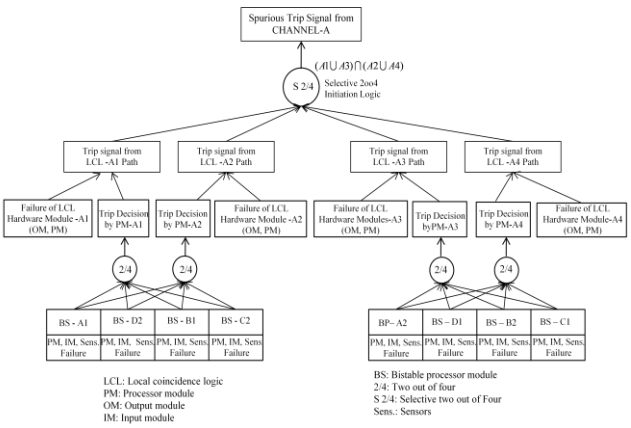


Fig.1. Conceptual structure for spurious activation of single channel of DPPS in NPP

## 3. Spurious trip for a system with redundant components

The failure of a DPPS component is revealed to the operators in the main control room. If bypass of the faulty component is allowed through changing the LCL configurations, the plant operator bypasses the faulty component soon after the detection of the failure, and

the maintenance crews are informed to fix the fault. If another failure takes place in another channel before restoration or bypassing of the first component (the duration between failure and bypass/restoration of the component called mean *down-period*) then reactor trip signal will be generated. For instance, if component-1 fails first at time $t_1$, and the corresponding channel is bypassed at time $t_2$. The interval $t_2$-$t_1$ is the mean *down period*. If another component from other channels fails at any time in the interval $t_1$-$t_2$, DPPS will generate a trip signal based on 2oo4 logic configuration employed in LCL processors.

The failure probability of component-2 in the mean *down-period* ($t_2$-$t_1$) before restoration of component-1 is $P_2$, which can be estimated for a combined constant failure rate ($\Lambda_2$) of component-2 by eq. (1) [3, 8]:

$$P_2 = \int_{t_1}^{t_2} \Lambda_2 e^{-\Lambda_2 t} dt \approx \Lambda_2 (t_2 - t_1) \text{.....(1)}$$

Similarly, $P_1$, the failure probability of component-1 in the mean *down-period* before restoration of component-2 is estimated for a constant failure rate of $\Lambda_1$.

The spurious trip rate for selective 2oo4 (selective two-out-of-four) coincidence logic configuration (C1 OR C3) AND (C2 OR C4) can be derived by eq. (2) [8]:

$$STR_{S2oo4} = P_2\Lambda_1 + P_1\Lambda_2 + P_3\Lambda_4 + P_4\Lambda_3 + P_1\Lambda_4 + P_4\Lambda_1 + P_2\Lambda_3 + P_3\Lambda_2 \text{.....(2)}$$

### 3. Conclusions

The study found that the reactor STR changes significantly with the variation of maintenance human error probability, frequency of periodic surveillance tests, and time delay to restore a component. Human error is unavoidable. However, efficient maintenance policy and support for the maintenance team reduces the mean restoration time of a component after a failure and the chances of human errors in plant maintenance activities. Spurious trip rate of nuclear reactors for operator's errors in plant main control has not been included in the study.

### REFERENCES

[1] Torres-Echeverria A. C., Martorell S, Thompson HA.,. Modeling and optimization of proof testing policies for safety instrumented system". Reliability Engineering and System Safety; 2009, 94 , 838–854.

[2] Torres-Echeverria A. C., Martorell S, Thompson HA,. Design optimization of a safety-instrumented system based on RAMS+C addressing IEC 61508 requirements and diverse redundancy. Reliability Engineering and System Safety; 2009, 94, 162–179.

[3] Lundteigen M. A, Rausand M.,. Spurious activation of safety instrumented systems in the oil and gas industry: Basic concepts and formulas. Reliability Engineering and System Safety; 2008, 93, 1208–1217.

[4] Summers AE,. Viewpoint on ISA TR84.0.02—simplified methods and fault tree analysis. ISA Trans; 2000, 39(2):125–131.

[5] Lu L, Jiang J. Analysis of on-line maintenance strategies for *k-out of-n* standby safety systems. Reliability Engineering and System Safety; 2007, 92, 144 – 55.

[6] INSC Database,. International Nuclear Safety Center, Nuclear News Country Review: South Korea, 1995.

[7] Kim, J, Park, J., Jung, W, Kim, J.T. Characteristics of test and maintenance human errors leading to unplanned reactor trips in nuclear power plants. Nuclear Engineering and Design; 2009, 239, 2530-2536.

[8] Khalaquzzaman, M., Kang, H.G., Kim, M.C., Seong, P.H. A Model for Estimation of Reactor Spurious Shutdown Rate Considering Maintenance Human Errors in Reactor Protection System of Nuclear Power Plants; submitted to Nuclear Engineering and Design, February, 2010.