Reliability Improved Design for a Safety System Channel

Eung-Se Oh *, Yun Goo Kim
Korea Hydro and Nuclear Power Co., Ltd, Central Research Institute, Daejeon, Korea
Corresponding author: eungse.oh@khnp.co.kr

1. Introduction

Nuclear power plant's safety systems are composed of plant protection system (PPS) and engineered safety features (ESF) component control system (ESF-CCS). Traditionally, these systems are designed as a separated and dedicated system with four channels redundancy. Nowadays, these systems are implemented with a same platform type, such as a qualified programmable logic controller (PLC) [1]. The platform intensively uses digital communication with fiber-optic links to reduce cabling costs and to achieve effective signal isolation. These communication interface and redundancies within a channel increase the complexness of an overall system design. This paper proposes a simpler channel architecture design to reduce the complexity and to enhance overall channel reliability.

2. Safety Channel Design Review and Improved Architecture

In this section, the APR1400 NPP safety system's channel configuration is reviewed and baseline channel reliability is calculated with some engineering assumptions. Then, simplified channel configuration is proposed and compared the reliability with baseline channel.

2.1 APR1400 Protection System Channel

Figure 1 shows simplified one channel block diagram of the APR1400 safety system as a baseline configuration. From sensor input modules (IN(X)) to communication links (LK2(XX)) are implemented in the plant protection system (PPS). Blocks from COM4(XX) to LK4 are implemented by the ESF-CCS.

In this figure, BP(X), LCL(X), GC(X), and LC(X) are same type processor module. Links denoted as LK1(XX) to LK3(XX) are consist of fiber-optic modems and optical cables.

COM1(XX) to COM6(XX) are communication modules that use serial communication signaling.

LK4 is a hard-wired link between loop controller's output module (OUT) and the component interface module (CIM).

Interfaces to/from other channels and monitoring and test devices are not considered for simple calculation.

2.2 Proposed Channel Design

The proposed channel configuration is shown in Figure 2. The configuration merges BP(X) to GC(X) logics in one logic processor module block (BLG). The other configuration is same as Figure 1.

This configuration reduces communication modules and link devices and cables (COM1(XX), COM2(XX), COM3(XX), LK1(XX), LK2(XX)).

In the proposed configuration, failures caused by these devices are eliminated and that simplification contributes to the reliability enhancement.

Furthermore, the simple configuration will reduce fabrication and maintenance costs.

2.3 Reliability Improvement

Using network reduction technic, channel reliabilities are calculated and compared with baseline channel and proposed channel.

Let denote the failure probability of BP1 to node N11 as "F(BP1)". We can assume the reliability of BP2 to N12 (F(BP2), LCL1 to N21 (FLCL1), LCL2 to N22 (FLCL2) has the same probability value of F(BP1).

Sample reliability calculation results are shown in Figure 3. Note that F(BP1) failure probability is assumed as 2.0E-5 for simple calculation.

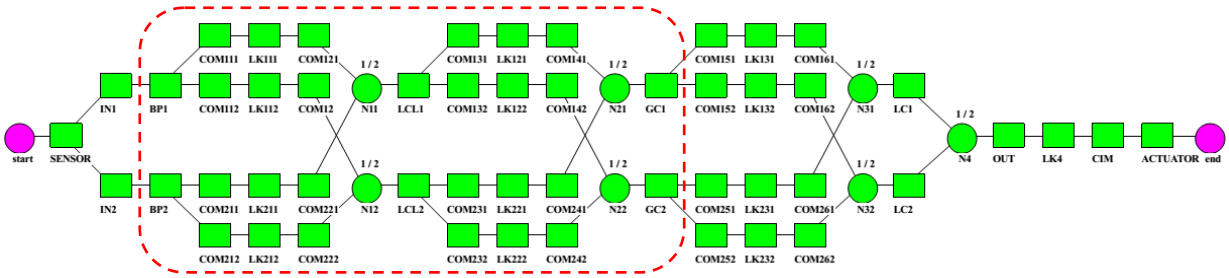

Figure 1. Baseline Safety System Channel Configuration

Upper part of Figure 3 shows baseline channel's failure probability and lower part shows simplified channel's failure probability.

About 40 percent ((5.0E-5-3.0E-5)/5.0E-5) failure reduction is achieved through proposed channel configuration

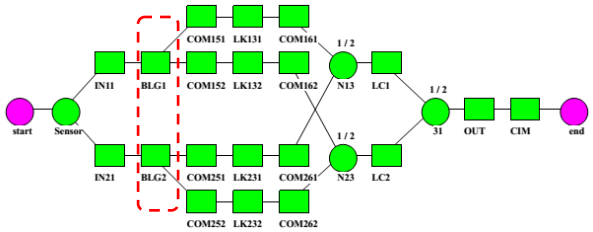

Figure 2. Simplified Safety System Channel Configuration

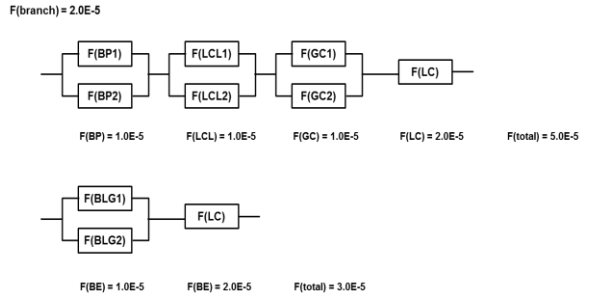

Figure 3. Channel Failure Probability Calculation

2.4 Assumptions

All software failures within the processor modules are not considered as a part of module component.

Interfaces to/from other channels and interfaces with monitoring and test devices are not considered for simple calculation.

The BLG (BP-LCL-GC) module is assumed to have enough processing and memory capacity to take all logic of BP, LCL, and GC.

Each branch, which includes communication module and data link devices with optic cable, has an assumed failure probability of 2.0E-5 to simplify the calculation. The number is considered as a feasible value for a safety systems modules.

3. Conclusions

Simplified safety channel configuration is proposed and the failure probabilities are compared with baseline safety channel configuration using an estimated generic value.

The simplified channel configuration achieves 40 percent failure reduction compare to baseline safety channel configuration.

If this configuration can be implemented within a processor module, overall safety channel reliability is increase and costs of fabrication and maintenance will be greatly reduced.

REFERENCES

[1] APR1400-K-X-FS-14002-NP, Rev. 0, APR1400 Design Control Document Tier 2 – Chapter 7 Instrumentation and Control. KEPCO/KHNP, 2014.

[2] IEEE Std 352, IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems, IEEE, 1987.