Transactions of the Korean Nuclear Society Spring Meeting
Jeju, Korea, May 22, 2009

A Study on the Inter-Channel Communication Independence for SMART I&C System

Kwang-Il Jeong, Jong-Yong Keum, Je-Yun Park
I&C HFE Department, Korea Atomic Energy Research Institute, 1045, Daedeokdaero, Yuseong, Daejeon 305-353, Republic of Korea.
*Corresponding author: hisunny@kaeri.re.kr

1. Introduction

In nuclear power plants (NPP) the greatest concern is to ensure the safety goal, so it is designed with a protection conception using diversity and redundancy methods. Usually the I&C (Instrumentation & Control) system of NPP is composed of four channels to enhance the performance of the safety functions and performs the monitoring and control functions. In these redundant structures, the most important thing is that a malfunction in one channel cannot affect the safety functions of the redundant channels. The communication network of the digital I&C system is playing a role in intra-channel communication and inter-channel communication in four-channel I&C structure. Recent licensee experience indicates that companies planning to use the inter-channel communication must perform a detailed analysis of all credible failure modes.

In this paper, we propose some evaluation criteria to evaluate the inter-channel communication independence of SMART I&C system and preliminary design for mitigating methodologies of each credible failure.

2. Inter-channel communication

The communication paths of inter-channel communication within SMART I&C system are as following:

- Channel trip decision for coincidence voting
- Chanel bypass interlock
- Reactor trip and ESFAS functions

In these communication environments, independence among redundant safety channels is the most important thing, so that a malfunction in one channel cannot affect the safety functions of the redundant channels. To satisfy communication independence, requirements and regulatory guide such as IEEE 603, IEEE 7-4.3.2, reg. guide 1.152, NUREG-0800 and so on, provided means for ensuring communication independence among redundant safety channels. But there are discrepancies between those requirements and regulatory guide. The NRC endorsed IEEE 7-4.3.2 in Reg. guide 1.1.52 revision 2, but did not endorse Annex E. But NUREG-0800 described Annex E of IEEE 7-4.3.2 acceptable means for ensuring communication independence. To resolve those discrepancies, ISG(Interim Staff Guidance) documents were issued to clarify or to address issue. The DI&C-ISG-04 (Digital Instrumentation and Controls) document provides acceptable methods for addressing communication issues in digital I&C system. In this document, various inter-channel communication guides and credible failures are provided and it requires that means for satisfying those should be demonstrated and verified.

3. Evaluation criteria

3.1 Evaluation Criteria

Based on current requirements, regulatory guide and ISG document, we propose some evaluation criteria to evaluate the inter-channel communication independence of SMART I&C system.

Table I. Evaluation Criteria

Criteria	Description
Point-to-Point communication	The sending node transmits the message to the receiving node directly by means of a dedicated medium.
One-way communication	The one-way communication path provides a point of software isolation.
Electrical isolation	The physical link between the sending node and receiving node use optic cable.
Physical separation	The communication equipments of redundant channels are physically separated to retain the capability of performing the safety function.
Handshaking and interrupt	No communication handshaking and interrupts are accepted.
Processor separation	The safety function processor should not be impacted by the communication processor
Data integrity	Use error-detection or error-correction code for ensuring the received messages correct
Power sharing	No power sharing between communication equipment in each redundant channel.
Fixed predefined location for message storing	Receiving message should be stored in fixed predefined location in the memory

3.2 Mitigating methodologies of credible failure

Communication failures in one channel should not affect the safety functions of redundant channels. There are some examples of credible communication failures in reference 5. We preliminarily design the mitigating methodologies of each credible failure as simple as possible.

Table II. Mitigating methodology

Credible failures	**Description**	**Mitigating methodology**
Corruption	Corrupted messages are received	Use error-detection code such as CRC-32
Unintended repetition	Messages are received repeatedly at an incorrect point in time	Use sequence number in message field and the discarding algorithm
Incorrect sequence	The predefined sequence of message is incorrect	Use sequence number in message field
Unacceptable delay	The receiving node receive messages beyond predefined arrival time	Discard received messages and indicate error
Insertion	An unexpected or unknown messages are received from unknown node	Use sequence number in message field and the discarding algorithm
Addressing	A message is sent to the wrong destination node	Use predefined MAC address based communication

4. Conclusions

We reviewed recent communication issues through analyzing various requirements and guidance documents such as IEEE Std. 603, IEEE Std. 7-4.3.2, Reg. guide 1.1.52, NUREG-0800 and DI&C-ISG-04 and produced some evaluation criteria to evaluate the inter-channel communication independence of SMART I&C system. To satisfy the inter-channel communication independence, we drew up a list of credible failures which are hazardous to the data integrity and designed the preliminary mitigating methodologies of each credible failure.

REFERENCES

[1] IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Systems, IEEE Std. 603, 1998.
[2] IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, IEEE Std. 7-4.3.2, 2003.
[3] Criteria for Use of computers in Safety systems of Nuclear Power Plants, Reg. Guide 1.152, Rev. 2, 2006
[4] Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, NUREG-0800, 2007
[5] Interim Staff Guidance on Highly-Integrated Control Rooms-Communications Issues (HICRc) U.S NRC, DI&C-ISG-04, 2007.