Proceedings of the Korean Nuclear Society Autumn Meeting
Seoul, Korea, October 1999

Safety Evaluation for Communication Network Software Modifications of PCS in Ulchin NPP Unit 3

Seong Hyon Ji, Jung Soo Koh, Bok Ryul Kim, Soung Hun Oh

Korea Institute of Nuclear Safety
P.O. Box 114, Yusong-Gu, Taejeon, Republic of Korea, 305-600

Abstract

On February 2, 1999, an incident occurred at the Ulchin Nuclear Power Plant Unit 3 which resulted in the corruption of data on Perform Net of Plant Control System. This incident was caused by the ASIC (Application Specific Integrated Circuit) chip on the Rehostable Module which is a part of Network Interface Module. Regarding this incident, we required that the utility should propose new algorithms to detect the hardware failure of ASIC chip and evaluated the appropriateness of network software modifications. As a result of this evaluation process, we required that the safety related interlock signals using data communication path be hardwired to make up for the vulnerability of the system architecture. In this paper, we will discuss the system architecture of PCS and fault analysis and evaluation findings.

Ⅰ. Introduction

The data communication architecture of the Plat Control System for Ulchin Unit 3 has a single ring type topology logically. Because it has not sufficient operation experiences in nuclear field, an administrative measure which requires the utility to submit the performance verification report was taken to verify the reliability of PCS operation for the first fuel cycle. In this performance verification report submitted, it is reported that an incident caused by the failure of the Rehostable module resulted in the abnormal behaviors of non-safety

components, indicators and alarms. [1]

The problem of this failure was that the network control software couldn't detect the addressing error of network control software and consequently couldn't transfer to the unaffected network as designed. We think that this shows the network control software has insufficient ability to detect communication errors. So the utility and Eaton corporation have modified the network software algorithms to enhance the ability to detect communication errors. We performed the evaluation of the software modification and proposed supplementary measures.

Ⅱ. Overview of Plant Control System for UCN 3&4

1. Characteristics of Plant Control System

The Plant Control System consists of panel mounted devices, system cabinets (logic, termination, remote multiplexer, annunciator, data link, electronic), operator workstation, prefab cables, and fiber optic cables. 'PLμS 32' is an Integrated Control System designed by Eaton Corp. This system has various digital and analog I/O signal processing modules.(See Table 1) And control algorithms are implemented by Functional Interconnect Diagram which is compiled into source code by the schematic capture program "OrCad". This system has two redundant fiber optic networks. One is designed as Network '1', the other is Network '2'. Each cabinet contains two Network Interface Modules. Communications between PLμS 32 cabinets is provided through PERFORM Net(Performance Enhanced

Table 1. Types of Control and I/O Module

Module Number		Function
Digital	6N662-1	On-Off Loop Controller Module
Analog	6N664-1	Analog Loop Module
	6N665-1	4-20mA Output Module
	6N666-1	4-20mA Input Module
	6N667-1	T/C Input Module
	6N668-1	RTD Input Module

Redundant Fiber Optic Replicated Memory Network) which utilizes SCRAMNet network supplied by Systran Corp. This network is a 150 megabit per second fiber optic network configured in a ring topology.[2]

2. Configuration of Plant Control System

The PCS is a control system that allows for remote control of all Balance of Plant(BOP) process equipment (valves, circuit breakers, motors, etc) of plant. In addition to controlling the process equipment, the PCS provides indication of process equipment status, including indications of abnormal operations. Figure 1 shows the configuration of PCS. As shown in Figure 1, Operator Interface Subsystem within Control Workstation mainly performs the functions of monitoring data communication of each cabinet. Figure 2 shows the typical control cabinet which consists of power supply, control modules, I/O modules and Network Interface Modules(NIM). Each cabinet has two Network Interface Modules to manage Networks '1' and '2'. The NIM and Control and I/O modules communicate with each other over redundant RS-422 serial channels.

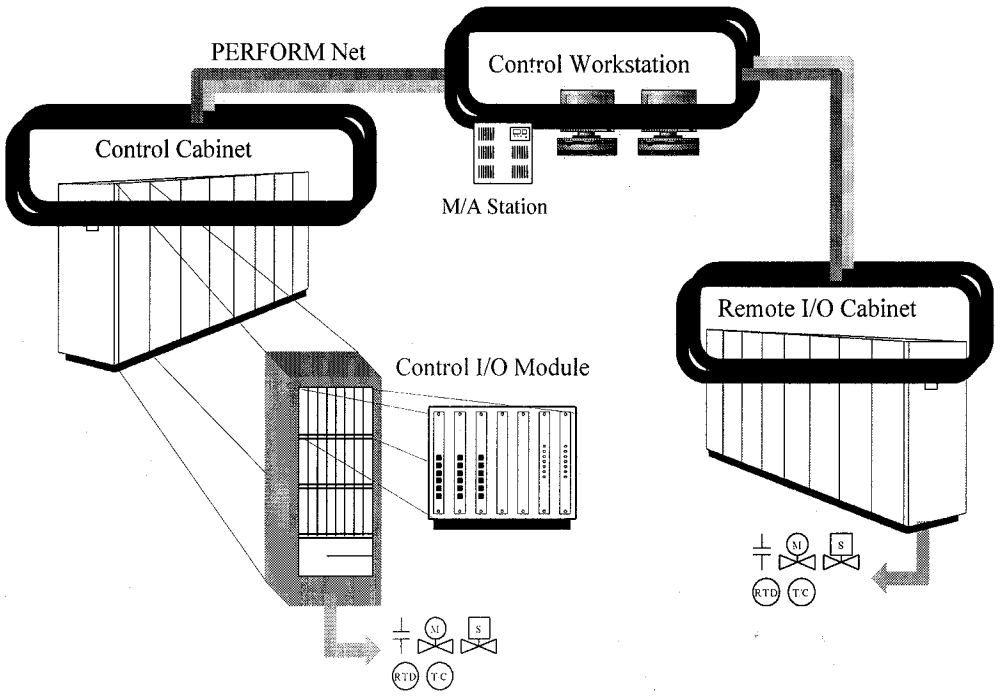

Figure 1. Configuration of PCS

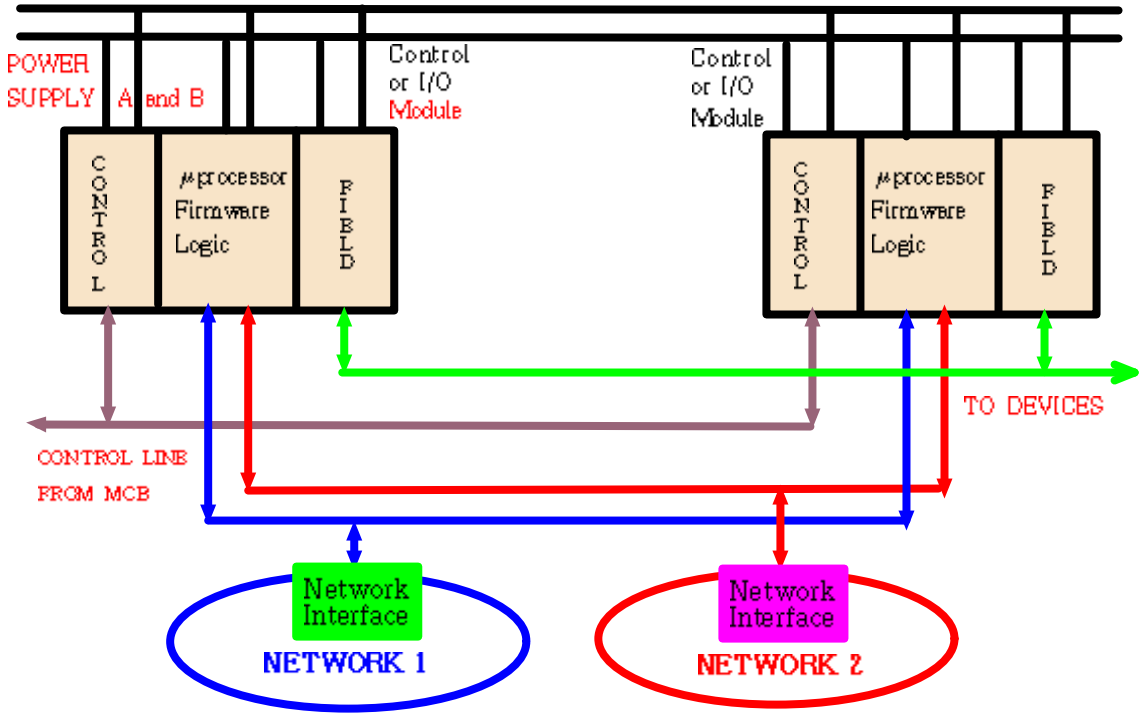

Figure 2. Typical Control Cabinet Configuration

3. PERFORM Network Communication

PERFORM Net on a NIM is configured to appear as general purpose RAM. In this way, network data is accessed by the NIM as if it were in local memory. So any data written into PERFORM Net memory is automatically sent to the same memory location in all nodes on the network. This is why it is also referred to as shared memory. Figure 3 is an illustration of replicated memory. The software of PLμS 32 is diveded up into 4 individual packages. 1) The control algorithm software is a library of small software modules containing the software algorithms to perform the analog and digital functions desired. 2) Control Operating System software(COS) is the core Operating System residing on each Control or I/O modules. It establishes communications with the NIM and serial peripherals and performs data validation and integrity testing. It also interfaces with the Control Algorithms and monitors module integrity through continuous on-board diagnostic testing. 3) Functional Interconnect Diagram compiler : A FID is a graphical representation of the logic to be performed by each control or I/O module in the system. These FIDs are compiled by "OrCad".

4) Network Interface Module(NIM) software controls all data transferring between the Control or I/O modules and network and monitors the status of various cabinet devices and provides interface to the Operator Interface Subsystem.

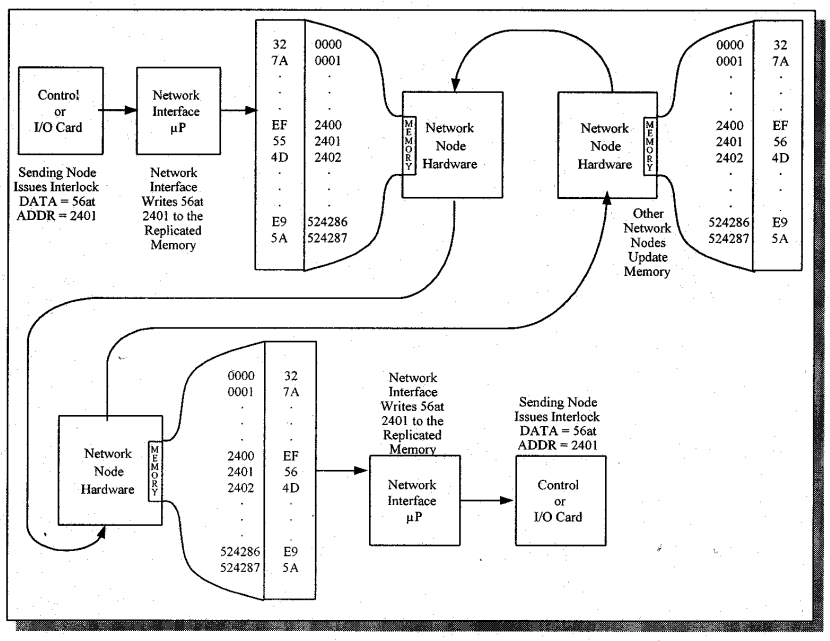

Figure 3. Replicated Memory Concepts

Ⅲ. Fault Analysis and Software Modifications

1. Summary of Network Failure

On Feb. 2. 1999, an incident occurred at the Ulchin Unit 3 which resulted in the corruption of data on PERFORM Net. 6 Non-Safety components functioned abnormally and 11 status lights showed 'inoperable' and values of 7 indicators oscillated and 51 alarms were generated erroneously during the incident. Despite of this incident, the plant could maintain its full power operation during the incident. This incident was caused by failures of ASIC chip on the Rehostable module. As shown in Figure 4, the Rehostable module contains various FIFO buffers used for temporarily storing information during normal send and receive operation of the node. Functions of each block are as follows : [6]

- Replicated Shared Memory : Any data written into Rehostable memory is

automatically sent to the same shared memory location in all nodes on the network.

- Receiver FIFO : This buffer is used to temporarily hold incoming foreign messages while shared memory is busy servicing a host request.
- Tranceiver FIFO : This buffer is used to receive foreign messages from the network and send them on or to hold received foreign messages.
- Transmitt FIFO : This buffer is used to hold native messages waiting to be transmitted.
- Dual Port Memory Controller : It allows the host to Read from or Write to shared memory with a simultaneous network write to shared memory.

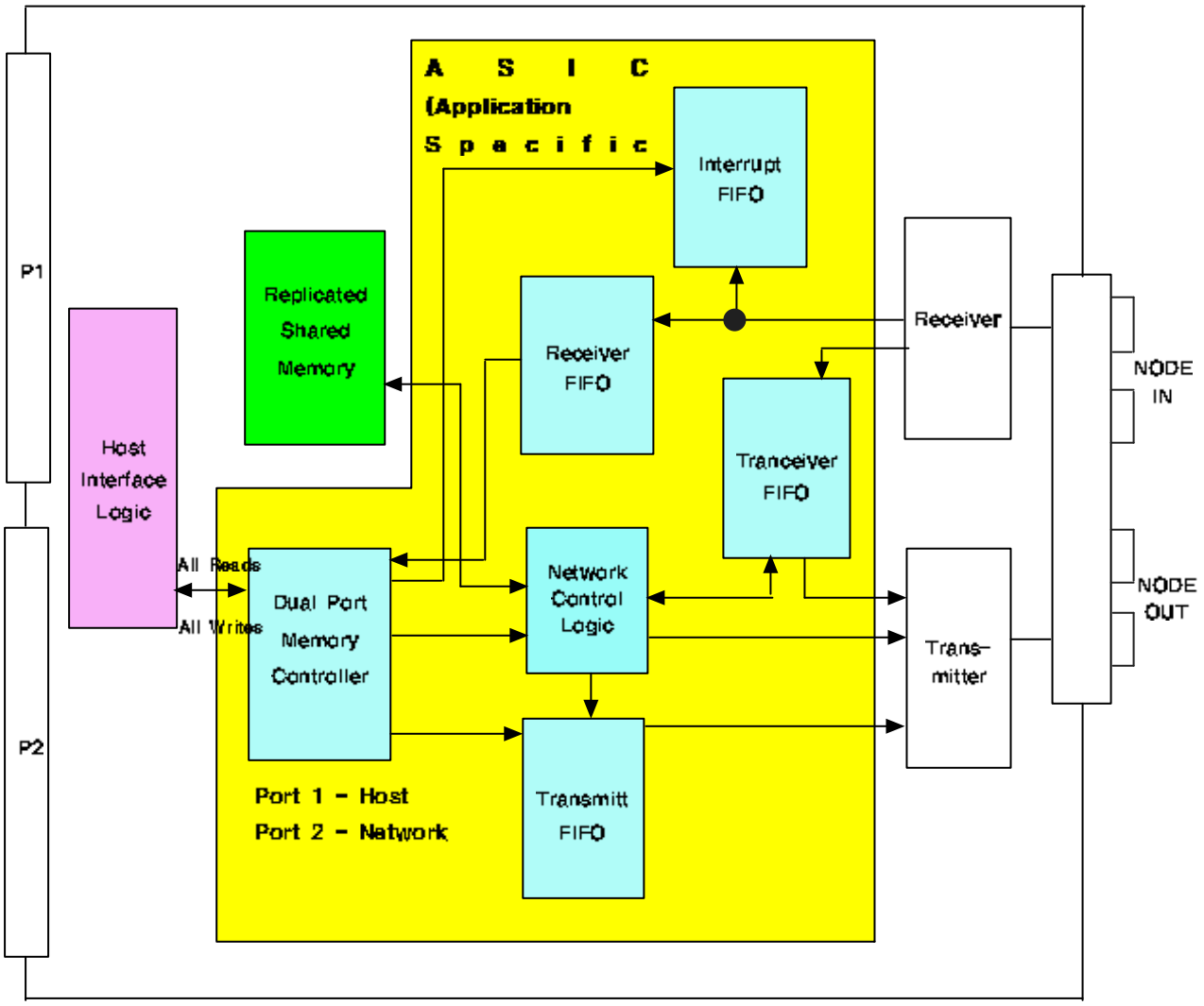

Figure 4. Functional Diagram of Rehostable Module

2. Fault Analysis Performed by Eaton Corp.

SCRAMNet Message consists of 82-bits, including 4 bytes of data. For every 8-bits of data in the message there is a parity bit attached, producing 9-bit bytes as shown in Table 2.

Table 2. Message contents of Rehostable module

START	ID	AGE	CONTROL	DATA ADDRESS	DATA VALUE
1	8+P	8+P	1 1 1 RES INT RTY	5+P 8+P 8+P	8+P 8+P 8+P 8+P

Eaton tested the EPROMs installed on the NIM. And they found no defects for EPROMs. But memory mapping error occurred for the testing of Rehostable Memory card removed from the NIM. After testing the suspected NIM within a small network, three failure types were observed. 1) The first failure type : A write to replicated memory was written to the wrong address from a valid node. It means that the replicated memory address was changed. 2) The second failure type : A write to the correct replicated memory address from a non-existent node. It means that ID portion of the message was changed. 3) The third failure type : A write to replicated memory was written to the wrong address from a non-existent node. It means that the node ID and replicated memory address were changed.[3]

3. Software Modifications Proposed by KEPCO

3.1 Data Format

The MSB of the current digital data is used to denote data quality. A logic zero is denoted as '0x00' and a logic one is denoted as '0x01'. In the new digital data format, the source Control-I/O Module encodes a logic zero as its corresponding node ID. It also encodes a logic one as the complement of its corresponding node ID. We think that new digital data format can detect the corruption of data field because each node has a unique encoded data format which includes the information of source node ID.

For example: Source Node ID: 0x43

Logic Zero: 0x43

Logic One: 0xBC

In the current analog data format, a word (2 bytes) is used to represent data. But in the new analog data format, this will be changed to allow for the use of a third byte of data that is used to contain a checksum of the analog data and the source node ID. The receiving module will then decode the data to ensure that it came from the proper node. We believe that new analog data format will improve the reliability of analog data since new analog data format can detect the corruption of data by checksum byte. The calculation of the checksum to be used for analog data will be as follows :

(Not((Node ID)+(Hi byte of Analog data)+(Lo byte of Analog data)))+1

For example : Source Node ID : 0x9C
Current data : 0x1234
New Format : 0x12341E

3.2 PERFORM Net Mirror Test

When data is received from a Control-I/O Module by the NIM, it is immediately placed in LOCAL RAM. If this data is required outside of the cabinet, it is then written to PERFORM Net. The test will periodically check the LOCAL copy of the data against the PERFORM Net copy of the data. This test checks one 64 bytes block of data per operating cycle resulting in all data tested at least once every second ((48 Modules + NIM) * 20ms). Although it takes almost 1 second to check all data, PERFORM Net mirror test will help to detect the mismatch between Local RAM and PERFORM Net memory.

3.3 PERFORM Net Status Testing

During Power-up, the NIM initializes the PERFORM Net node control registers to predetermined values. A test is being added to normal operation that will periodically check the integrity of these control registers to ensure that they have not changed.

3.4 PERFORM Net Hardware Foreign Write Protection

During Power-up, the NIM will initialize the PERFORM Net node control

registers to provide indication if a foreign node writes within the 4Kbyte block reserved for itself. A test will then be added to normal operation that check the PERFORM Net status registers to see if a foreign write has occurred. If a foreign write has occurred, the NIM will set a new bit in the NIM Status Byte indicating a Foreign Write has occurred. The NIM Status Byte is transmitted to the Alternate NIM every operating cycle. Currently, the quad switches located within the Datalink Cabinets are controlled from a 6N662-1 Module such that on a Loss of Carrier, the ring will isolate. A similar function will be implemented such that the quad switch isolate on the detection of a Foreign Write. We have confirmed that this foreign write protection is a fault detection algorithm to detect a Foreign Write to one node from other nodes. It will ensure the independence between channels.[5]

V. Evaluation Findings

The evaluation findings that include the evaluation of follow-up measures we have required after reviewing the performance verification report such as software modifications, supplementation of the vulnerability of the system architecture, installing new alarm window for network failures, development of an emergency operation procedure, a test using the failed NIM and fault analysis are as follows :

1. Appropriateness of the Software Modifications

We believe that the software modifications which include the change of data format, the mirror test, status testing, hardware foreign write protection can detect similar types of failure occurred at UCN unit 3. So these modifications could help to enhance the integrity of data communication system. During the first overhaul of Ulchin unit 3, we have verified that the test using failed NIM installed on PCS did successfully detect the data corruption and isolate from the corrupted network.

2. Supplementation of the Vulnerability of the System Architecture

Because the safety critical interlock signals had been hardwired by KINS' request during the SAR review phase, the safety related components were

operated normally despite of the communication failure. During the phase of SAR review, we had also required that a hardwired backup panel be installed to prepare for software common mode failures.[4] We evaluated that the system architecture still has the vulnerability to a Foreign Write in the Rehostable module despite of the Foreign Write Protection. So we required that all possible safety related signals be hardwired to supplement the vulnerability of the system architecture. And we verified that 40 of 110 signals were hardwired during the first overhaul. And we also required that the rest of interlock signals be separated from data communication path gradually using hardwire.

3. Alarm for the Network Failure

We verified that the alarm window we required as one of the follow-up measures was added in MCR to alert operators to prepare for the network failures which include foreign write error and bad data and so on.

4. Emergency Operation Procedure for the Network Failure.

We required the utility to develop an emergency operation procedure to prepare for the failure of PCS caused by data communication errors. And we verified that the emergency operation procedure for network failures was being developed appropriately.

5. Appropriateness of the Fault Analysis

The root cause of the network failure does not come out yet. It is required that a thorough analysis of the ASIC chip on the Rehostable module should be done. Although it depends on the result of analysis, we think that the plan such as changing the manufacturing process using consensus standard should be considered to improve the reliability of ASIC chip.

VI. Conclusion

The incident occurred at Ulchin unit 3 was one of the hardware failures caused by an ASIC chip. It was not the one caused by software program itself. After reviewing the fault analysis and software modifications, we have required that all possible safety related signals be hardwired to supplement the

vulnerability of the system architecture. And we have confirmed that the counter actions which include the installation of a new alarm window and development of an emergency operation procedure for the failure of PCS and hardwiring safety related interlock signals were appropriate. We verified that the integrity of Plant Control System was improved by the software modifications. However, to prevent the network malfunctions due to ASIC chip failures repeatedly, the root cause of this network failure shall be investigated in the near future and the quality assurance activities, including manufacturing process, on the microchips used to safety-related systems shall be strengthened further. And as more communication network systems are being implemented in nuclear power plants, the software verification and validation activities about communication protocol shall be strengthened to improve the safety of nuclear power plant.

References

[1] Performance Verification Report of Plant Control System for Ulchin Unit 3, June 1999.

[2] PLμS 32 Plant Control System Operating & Maintenance Manual, 1996.

[3] Engineering Report 7344/01 : Detailed Description of Modifications for Network Memory Fault Detection, July 1999.

[4] KINS/DR-175, "Safety Evaluation of Plant Control System for Ulchin 3&4", 1995.

[5] IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

[6] SCRAMNet+ Network VME6U Hardware Reference, 1996