Transactions of the Korean Nuclear Society Spring Meeting
Gwangju, Korea, May 30-31, 2013

Vulnerability Identification and Design-Improvement-Feedback using Failure Analysis of Digital Control System Designs

Eun-Chan Lee*, Yeon-Kyoung Bae
Korea Hydro & Nuclear Power Co., Ltd., 1312 Yuseongdaero, Yuseong-Gu, Daejeon, Korea

**Corresponding author: eclee@khnp.co.kr*

1. Introduction

The failure analyses on the systems in the nuclear power plants (NPPs) are conducted by reviewing the effects that the failure of each component in the system has on the system, and on the plant, through failure-mode and effect analysis. Additionally, fault tree analyses let analysts establish the failure sequences of components as a logical model and confirm the result at the plant level. These two analyses provide insights regarding what improvements are needed to increase availability because it expresses the quantified design attribute of the system as minimal cutsets and availability value interfaced with component reliability data in the fault trees. This combined failure analysis method [1] helps system users understand system characteristics including its weakness and strength in relation to faults in the design stage before system operation.

2. Failure Analyses

This study compares the results of failure analyses between two digital control systems in the NPPs. One is the control system for OPR-1000 units with Design A [2], and the other is the control system for APR-1400 units with Design B [3]. That is, this study identifies differences, including single point vulnerabilities, and describes how to provide feedback to improve methods that increase availability from the perspective of system design.

2.1 System Design A

The system with Design A comprises loop controllers containing control logics to modulate components, I/O cards, and data communication devices to exchange data between control loops, and cabinets or systems. In this design, a communication master receives data from MUX cabinets in the field and transfers these data to the loop controllers. The communication master (CM) has a master-slave architecture and initiates fail-over during system faults. This redundancy of the CM prevents system failure.

The loop controllers for critical components such as reactor coolant pumps (RCPs), include the logics to control field components and have redundancy. However, the failure analysis of this system demonstrated that this redundancy could be lost if one of the redundant controllers fails due to the failure of specific subcomponents. This design may be vulnerable to calculation error or spurious actuation of one controller, because its redundancy does not cover a complete backup function. For I/O modules, a single failure can actuate a field component without a valid demand, in spite of their redundancy in the main loop.

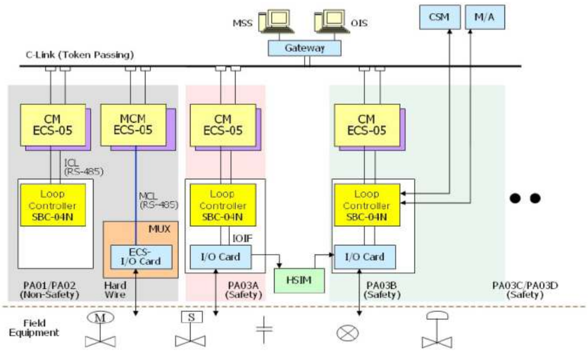

Figure 1 Block Diagram of System Design A

Regarding Design A, a number of optical signal processing modules are installed because all field data are transmitted using optical communication. This relatively increases system complexity and failure points when compared to Design B.

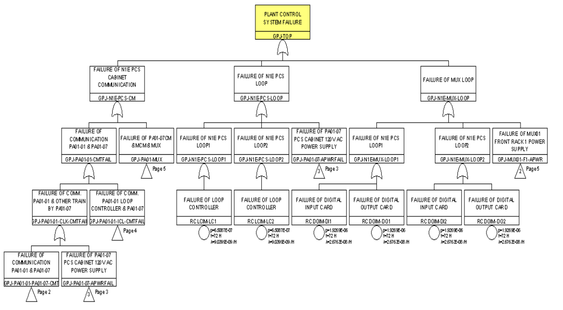
PLANT CONTROL SYSTEM FAILURE
GPJ-TOP
FAILURE OF N1E PCS CABINET COMMUNICATION
GPJ-N1E-PCS-CM
FAILURE OF N1E PCS LOOP
GPJ-N1E-PCS-LOOP
FAILURE OF MUX LOOP
GPJ-N1E-MUX-LOOP
FAILURE OF COMMUNICATION PA01-01 & PA01-07
GPJ-PA01-01-CMTFAIL
FAILURE OF PA01-07CM &MCM&MUX
GPJ-PA01-MUX
Page 5
FAILURE OF N1E PCS LOOP1
GPJ-N1E-PCS-LOOP1
FAILURE OF N1E PCS LOOP2
GPJ-N1E-PCS-LOOP2
FAILURE OF PA01-07 PCS CABINET 120V AC POWER SUPPLY
GPJ-PA01-07-APWRFAIL
Page 3
FAILURE OF N1E PCS LOOP1
GPJ-N1E-MUX-LOOP1
FAILURE OF N1E PCS LOOP2
GPJ-N1E-MUX-LOOP2
FAILURE OF MUX01 FRONT RACK1 POWER SUPPLY
GPJ-MUX01-F1-APWR
Page 5
FAILURE OF COMM. PA01-01 & OTHER TRAIN BY PA01-07
GPJ-PA01-01-CLK-CMTFAIL
FAILURE OF COMM. PA01-01 LOOP CONTROLLER & PA01-07
GPJ-PA01-01-ICL-CMTFAIL
Page 4
FAILURE OF LOOP CONTROLLER
RCLCIM-LC1
FAILURE OF LOOP CONTROLLER
RCLCIM-LC2
FAILURE OF DIGITAL INPUT CARD
RCDOIM-DI1
FAILURE OF DIGITAL OUTPUT CARD
RCDOIM-DO1
FAILURE OF DIGITAL INPUT CARD
RCDOIM-DI2
FAILURE OF DIGITAL OUTPUT CARD
RCDOIM-DO2
p=6.5087E-07 t=72 H λ=9.0399E-09 /H
p=6.5087E-07 t=72 H λ=9.0399E-09 /H
p=1.9269E-06 t=72 H λ=2.6763E-08 /H
p=1.9269E-06 t=72 H λ=2.6763E-08 /H
p=1.9269E-06 t=72 H λ=2.6763E-08 /H
p=1.9269E-06 t=72 H λ=2.6763E-08 /H
FAILURE OF COMMUNICATION PA01-01 & PA01-07
GPJ-PA01-01-PA01-07-CMT
Page 2
FAILURE OF PA01-07 PCS CABINET 120V AC POWER SUPPLY
GPJ-PA01-07-APWRFAIL
Page 3

Figure 2 Fault Tree of System Design A

A fault tree was built to compare the system availability of selected designs for this study. The mean time between failures (MTBF) from the system vendor was used to quantify the overall system unavailability that would be expected with Design A. In addition, the importance of the modeled components was calculated. Their importance values were evaluated as large with an order of digital output cards, loop controller cards, power supplies, and communication masters.

2.2 System Design B

System Design B consists of the information display and processing layers such as an engineering workstation system, operator interface system, and communication network layer for controls and data gathering, as well as the field layer for receiving and processing field signals.

To compare this design to Design A, a system configuration as in Figure 3 was built using a field control unit (FCU) in the main control room and mux base unit (MBU) and mux extension unit (MEU) in the field. Because Design B should have the same structure for data flow as that of Design A to compare the two designs, the configuration of Figure 3 uses I/O modules in the MEU instead of in the FCU.

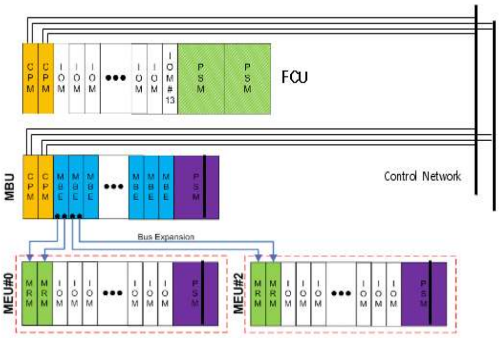

Figure 3 Block Diagram of System Design B

For Design B, failure analyses indicated that the central processing module (CPM) was not determined to be a single point vulnerability (SPV) because this CPM, which has a similar function to the loop controller, could initiate an automatic fail-over. In other words, the secondary module in standby is in charge of controls for I/O modules, when one of the CPMs fails. However, digital I/O modules were categorized as SPVs due to their possibility to the subcomponent failure.

Failure analysis confirmed that it was different from Design A, in that a CPM, which is responsible for communication between cabinets, had control logics. That is, a controller module implements communication functions as well as controls.

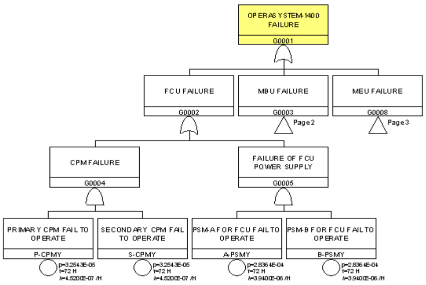

Figure 4 Fault Tree of System Design B

The fault tree of this digital system used the same MTBFs for components as those of Design A. The component importance was calculated as large with an order of IO modules (IOMs), power supplies (PSM) and communication modules (MBE/MRM).

2.3 Feedbacks to Design Improvements

The quantified result presented that the unavailability of Design A was 3.59E-2 and that of Design B was 2.99E-7 for the specific configurations used for this study. There are two major reasons that the unavailability of Design A is relatively larger than that of Design B. First, this greater unavailability resulted from inadequate design of the redundant loop controllers. In addition, Design A contains more vulnerable points due to use of optical devices and the power supplies for their controls.

A design change of the modules is needed because a single failure in the loop controller, or I/O modules, can cause spurious actuation of field components even if they have redundancy. The current ‘OR’ configuration connecting the two redundant modules should be changed into an ‘AND’ using hardware or software improvements, based on the cost and benefit of the change, if it is permitted. Otherwise, we can upgrade the CPUs to compare output demand to the real output signal to prohibit spurious output initiations due to internal faults. This countermeasure can prevent system failures and resultant plant trips or transients.

3. Conclusions

This study explained why a digital system could have weaknesses in methods to transfer control signals or data and how those vulnerabilities could cause unexpected outputs. In particular, the result of the analysis confirmed that complex optical communication was not recommended for digital data transmission in the critical systems of nuclear power plants. Regarding loop controllers in Design A, a logic configuration should be changed to prevent spurious actuation due to a single failure, using hardware or software improvements such as cross checking between redundant modules, or diagnosis of the output signal integrity. Unavailability calculations support these insights from the failure analyses of the systems.

In the near future, KHNP will perform failure mode and effect analyses in the design stage before purchasing non-safety-related digital system packages. In addition, the design requirements of the system will be confirmed based on evaluation of overall system availability or unavailability.

REFERENCES

[1] TR-1022985, Failure Analysis of Digital I&C Equipment and Systems, Appendix D, EPRI, Palo Alto, 2011

[2] I&C Training Manual Vol. II, pp. 108-189, KHNP, 2004

[3] S11D01-AMT-002, System Manual, pp. 9-22, W. Tec., 2012