International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies
(NPIC&HMIT2000), Washington, DC, November, 2000

A Fault-Tolerant Design of the Digital Distributed Control Systems for Nuclear Power Plants

Hong-ju Moon †, Soo Young Shin ‡, Wook Hyun Kwon ‡,
Byung-Yoon Lee †, Myung-Hyun Yoon †, and Yong-Kwan Lee †
† Nuclear Instr. and Control Group,
Nuclear Power Generation Research Lab.
Korea Electric Power Research Institute,
Munji-dong, Yusong-ku Taejon 305-380, Korea
Email: contact@moonis.com
‡ Control Information Systems Lab.,School of Electrical Engr.
and ERC-ACI, Seoul National University,
Seoul, 151-742, Korea
Email: wdragon@cisl.snu.ac.kr

Key Words: digital distributed control system, nuclear power plant, fault-tolerance

Abstract

In this paper, a flexible and fault-tolerant architecture of the digital distributed control system(DDCS) is proposed and analyzed. Dual redundancy is adopted to achieve a fault-tolerance. General structure of dual redundant module is described and analyzed. The strategies and tactics to add the fault-tolerance in the DDCS are analyzed and compared in the module level. Pros and cons for each strategy are analyzed. This paper also proposes the guidelines on how they can be combined appropriately.

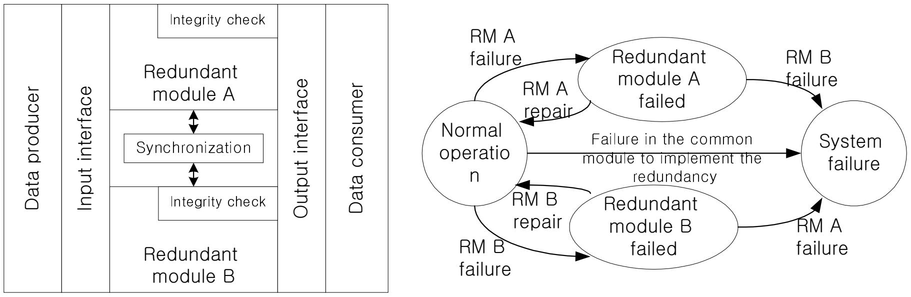
1 Introduction

The digital distributed control system(DDCS) consists of many components. A single fault in the system may have effects on the whole system. Unlike in an analog system, the faults in a digital system usually make discrete and abrupt changes in its output. To cope with these situations, the fault-tolerance is an inevitable property of the DDCS.

A DDCS consists of many modules and each module can be implemented by many different technologies. The fault-tolerance has to be implemented depending on the overall architecture and how each equipment is implemented. In the DDCS, the fault-tolerance is considered in many respects: I/O points, control modules, control functions, and communication networks. Different techniques are applied to each part of the DDCS and the relation between the parts and the overall operation have to be considered for the fault-tolerance of the DDCS.

Although there are many researches on fault-tolerant system[1, 2, 3, 4], there are few papers which provide an efficient way to combine the redundant modules of a DDCS in a systematic way.

In developing the DDCS for nuclear power plants, the strict verification and validation process for fault-tolerance has to be applied for the complex digital system, in which the hardware and the software are tightly coupled. Also, the instrumentation and control(I&C)



(a) General Structure of dual redundant module

(b) Changes of states of dual redundant module

Figure 1: General structure and changes of states of dual redundant module.

system requires high reliability and safety level maintaining enough performance and functionality.

This paper proposes a fault-tolerant computing architecture in the DDCS for nuclear power plants. The study analyzes the techniques for each part of the DDCS to get the fault-tolerance, and proposes a fault-tolerant architecture in the DDCS by combining them appropriately. The fault-tolerance is implemented by the redundancy for each component. In analyzing the fault-tolerant architecture, the qualitative approach is adopted.

This study starts from the evolving project KNX-5, which develops a DDCS for Korean nuclear power plants[6, 7].

In Section 2, the fault-tolerant module with dual redundancy is proposed and analyzed. An architecture of the DDCS for nuclear power plants is proposed in Section 3. In addition, modules consisting of the DDCS are analyzed. In Section 4, this paper is concluded.

2 Dual redandancy of a fault tolerant module

In this section, the general architecture of the dual redundant module is proposed and analyzed.

The general architecture can be shown in Figure 1 (a). The changes of states in the dual redundant module are shown in Figure 1 (b). A redundant module has a data producer and a data consumer. If the redundant module is a controller module, the data producer is the input module and the data consumer is the output module. The input interface exists between the redundant module and the data producer, and the output interface exists between the redundant module and the data consumer. Each redundant module has a sub-module to check the integrity, and a synchronization mechanism exists between the dual redundant modules.

An input interface to the dual redundant module could be one of the two types depending on the features of the interface and operation of the redundant module. The first one is the switching type. It operates in a selective manner. It has a selection mechanism and the data may be lost during switching delay period. The other one is the sharing type. It operates in a parallel manner. The data from the producer is passed to the dual redundant modules by broadcasting, duplicated transmission, or allowing common data access. The duplicated transmission or the common access operation requires twice bandwidth to the case of single mode.

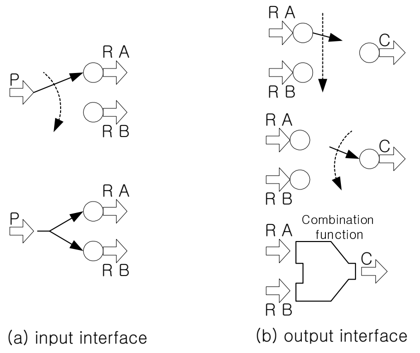


Figure 2: Input and output interfaces of the dual redundant module.

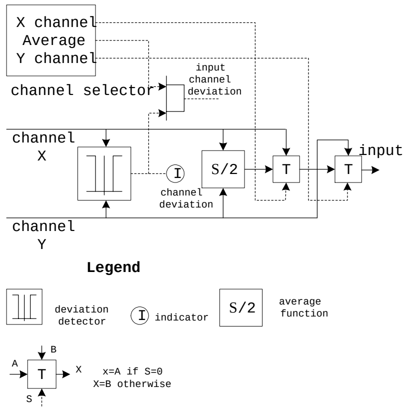


Figure 3: Example of using the average calculation.

The output interface may be one of the three types in Figure 2 (b). The first one is to switch the channel by the control of redundant modules. It requires selection mechanism and data can be lost during switching delay. The switching can be controlled by the consumer. In this case, the channel selection, the channel section, or the data selection can be controlled at each access to the data. With the data by data selection, no data is lost at the single failure situation, but additional data acquisition is required to determine the channel. The last one is to combine the two data by an appropriate function. It is not always possible. But, if it is implemented, it provides a graceful interface to the dual redundant modules and guarantees a continuous operation. But, there may be some deviation in the data to the consumer. These input and output interface are illustrated in Figure 2.

In interfacing the dual redundant modules, an appropriate method is chosen and implemented by considering following guidelines. The changes of state in operation should be minimized. An abrupt switching between the redundant module can cause an abrupt fault. The number of additional modules for redundancy must be minimized. To implement redundancy, not only redundant modules but also additional mechanisms or functional blocks are added. These additional modules may increase the possibility of failure and cause common mode failures.

3 Architecture of the DDCS for nuclear power plants

This section analyzes the fault-tolerant architecture for each components of the DDCS. This paper assumes the overall structure of the DDCS as shown in Figure 4.

3.1 Sensors and Actuators

The redundancy of sensors and actuators must precede the redundancy of controllers when high reliability is required.

The sensor input value can be determined from the duplicated inputs from multiple sensors by an appropriate calculation or exclusive selection. The calculation may take the average, the maximum, or the minimum (in case of analog inputs) depending on the system characteristics. The selection logic has to determine which is the valid input. It may be done

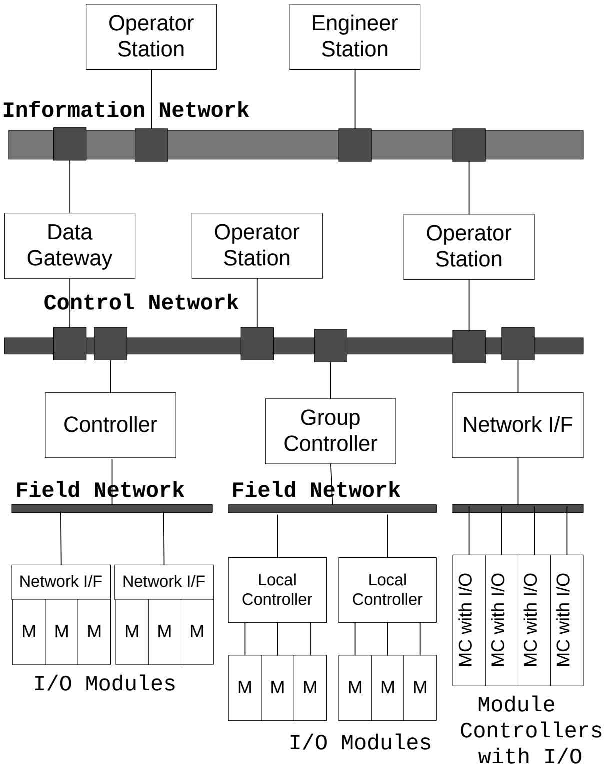


Figure 4: Architecture of a distributed digital control system.

by detecting the invalid range or by using the voting logic. They are summarized in Table 1. Figure 3 shows an example of using the average calculation.

The redundant actuators can be used in parallel or selective manner. The parallel actuators can be implemented in an additive way or prohibitive way depending on their usage.

3.2 Input/Output modules

The redundancy of the I/O modules usually goes with the redundancy of the sensors and the actuators. In most cases, the input module alone is not duplicated. Instead, it is duplicated according to the duplication of input signals or sensors. The input modules are also duplicated when the control systems are duplicated. If the input sources are from the same sensor, a splitter circuit is required. The output modules may be duplicated to drive duplicated actuators separately. The output modules are also duplicated when the control systems are duplicated. If the actuators are not duplicated in this case, the single output generation logic is required.

3.3 Control modules

The redundancy of control modules is implemented depending on the controller types and the communication network architecture. Redundant control modules can be implemented to operate in a selective manner or in parallel. The selection logic has to be operate to activate a control module selectively. To operate in parallel, either the selection logic is implemented for the output of the control modules or the component module to use the output from the

Table 1: Sensor/Actuator redundancy.

	sensor		actuator	
usage	calculation	selection	parallel	selection
Appropriate type	analog(digital)	analog/digital	control of continuous value	action
Advantage	simple implementation	accurate value	simple implementation	accurate
Disadvantage	deviation	dependable selection logic	deviation	selection logic

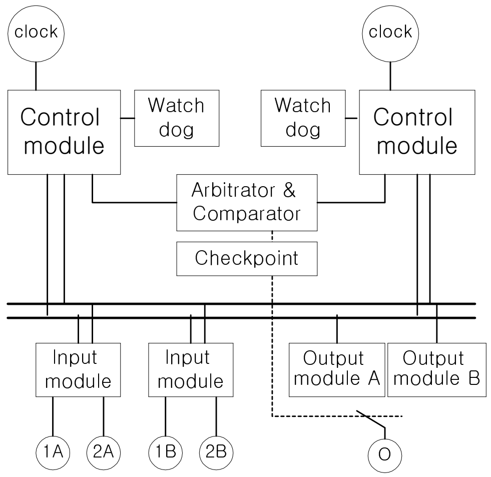


Figure 5: A dual redundant control module.

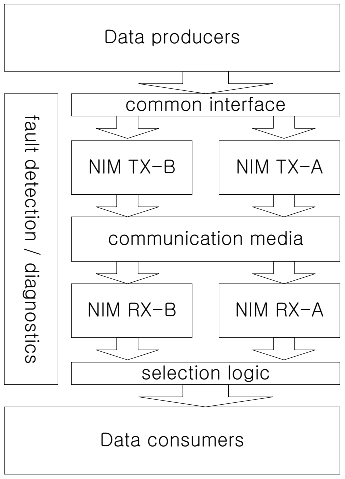


Figure 6: A redundancy architecture of a communication network.

control modules must have a selection function. These redundancy modes are summarized in Table 2.

Whether they operate in parallel or in a selective manner, a synchronization mechanism is required to narrow the difference in the operation phase between the redundant control modules. The synchronization can be achieved in two ways. One is the communication among the redundant modules to keep track of others' operation phase while they are running. The other is to restore the status information by memory dump when a module takes over the control function. When the redundant modules operate in parallel mode, the synchronization can be minimized. If the output phase is mainly determined by the input phase, the synchronization mechanism can be eliminated given the phase difference is within a bound small enough.

The example of dual redundant control module is illustrated in Fig 5 [8]. The dual redundant control module can be combined in the synchronous or asynchronous architecture. In the synchronous architecture, the results are compared in a comparator or arbitrator and each control module performs diagnostic tests. In the asynchronous architecture, the control modules periodically transmits data to the standby control module. To analyze fault tolerance for this example, fault tree method can be applied. The result of fault tree analysis

Table 2: Control module redundancy.

Redundancy mode	parallel	selection
Advantage	simple structure, minimized backup latency	stable operation in normal condition
Disadvantage	selection logic in output modules, possibility of continual jitters in output	complexity in the selection and synchronization logic, backup latency

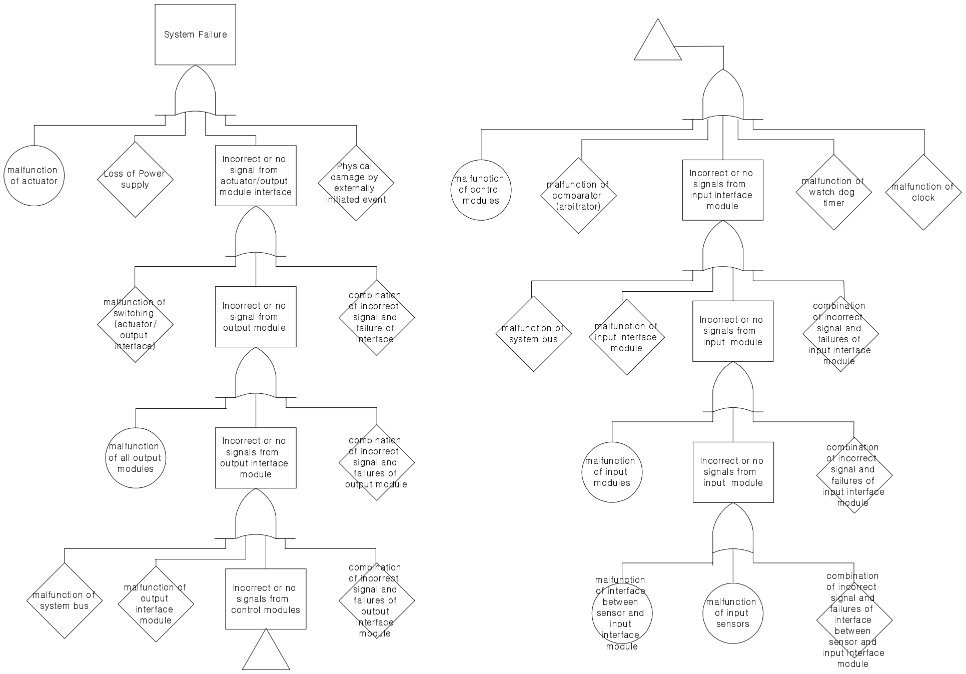

System Failure
malfunction of actuator
Loss of Power supply
Incorrect or no signal from actuator/output module interface
Physical damage by externally initiated event
malfunction of switching (actuator/ output interface)
Incorrect or no signal from output module
combination of incorrect signal and failure of interface
malfunction of all output modules
Incorrect or no signals from output interface module
combination of incorrect signal and failures of output module
malfunction of system bus
malfunction of output interface module
Incorrect or no signals from control modules
combination of incorrect signal and failures of output interface module
malfunction of control modules
malfunction of comparator (arbitrator)
Incorrect or no signals from input interface module
malfunction of watch dog timer
malfunction of clock
malfunction of system bus
malfunction of input interface module
Incorrect or no signals from input module
combination of incorrect signal and failures of input interface module
malfunction of input modules
Incorrect or no signals from input module
combination of incorrect signal and failures of input interface module
malfunction of interface between sensor and input interface module
malfunction of input sensors
combination of incorrect signal and failures of interface between sensor and input interface module

Figure 7: Fault tree of a dual redundant control module.

are illustrated in Figure 7. It shows qualitative properties of faults in the dual redundant module.

3.4 Communication networks

For the redundancy, the communication network is considered respectively on the cable with connecting devices and the network interface module. The network cable and connecting devices are prone to noise and fault. They have to be implemented, installed, and maintained with special attention[5]. For the most of all the DDCSs, the network cables are duplicated.

For the fault-tolerance of the whole DDCS, the isolation of a fault has to be considered in designing the system with more importance than the other parts of the system. The fault may have not only a passive effect but also an active effect on the system. An active fault propagates the fault state throughout the system. The communication network connects the distributed controllers and the possibility of the fault propagation is greater than other parts.

Table 3: Communication network redundancy.

Transmit	Receive	Feature
selection	receive all	data loss during switching with detection latency, complex transmit control, sequence in order, no global synchronization in selection logic
parallel	channel selection	data loss only during switching process, complex receive control, possible violation of sequence order, no global synchronization in selection logic
parallel	consumer's choice	simple, selection mechanism for the consumer
selection	selection	complex selection logics, possible inconsistency of selections

Figure 6 shows a redundancy architecture of the communication network in the DDCS. The data producer passes the data to the two network interface modules at once or to one of the two selectively. The data selection can be done in the way that the logic selects one of the two network interface module for the receiving channel or that the data consumer selects a dependable data actively from the duplicated data. The methods for transmit control and receive control can be combined in various ways and these combinations are explained in Table 3. The choice of the methods may depend on the communication protocol, the implemented architecture, and the characteristics of the data traffic.

3.5 Operator interface stations

Most of DDCSs allow multiple operator interface stations, and they can define their function separately. Therefore, the redundancy of the operator interface station can be implemented rather freely. The operation interface station may manage a database, and a backup mechanism is required.

3.6 Overall architecture

The whole structure and redundancy mechanism of each component have to be analyzed and determined by considering the whole architecture and implementation of all the components in the redundant DDCS. The procedure shown in Figure 8 may be a possible way to design the overall architecture.

4 Conclusion

In this paper, an general dual redundant module for the DDCS is analyzed and compared in the viewpoint of fault-tolerance. This fault-tolerant method with dual redundancy is applied to each module of the DDCS. The appropriate combination of these modules are studied and analyzed. The whole procedure is proposed to implement a fault-tolerant DDCS.

This paper can provide a reference to implement a fault-tolerant DDCS and combine modules in the systematic and appropriate way. The quantitative analysis about fault tree analysis and reliability analysis using Petri net can be the future works.

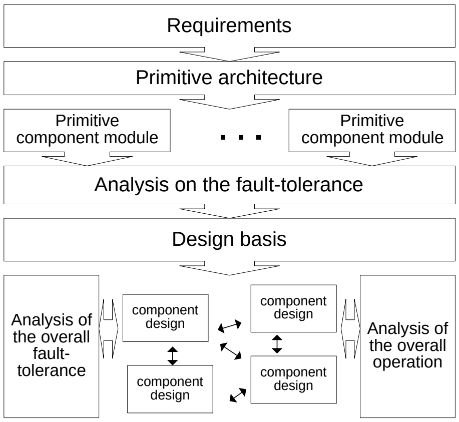

Requirements
Primitive architecture
Primitive component module
. . .
Primitive component module
Analysis on the fault-tolerance
Design basis
Analysis of the overall fault-tolerance
component design
component design
component design
component design
Analysis of the overall operation

Figure 8: Procedure to design the redundant architecture

References

[1] U. Minoni, G. Sansoni, and N. Scarabottolo, "A Fault Tolerant Microcomputer Ring for Data Acquisition in Industrial Environments," *IEEE Trans. on Instrumentation and Measurement*, Vol. 38, No. 1, pp. 32-36, Feb. 1989.

[2] M. R. Basila Jr., G. Stefanek, and A. Cinar, "A Model-Object Based Supervisory Expert System for Fault Tolerant Chemical Reactor Control," *Computers and Chemical Engineering*, Vol. 14, Iss. 4-5, pp. 551-560, 1990.

[3] David A. Rennels, "Fault-Tolerant Computing - Concepts and Examples," *IEEE trans. on Computers*, Vol. C-33, No. 12, pp. 1116-1129, Dec. 1984.

[4] Jean-Michel Ayache, Jean-Pierre Courtiat, and Michel Diaz, "REBUS, A Fault-Tolerant Distributed System for Industrial Real-Time Control," *IEEE Trans. on Computers*, Vol C-31, No. 7, pp. 637-647, July 1982.

[5] Hong-ju Moon and Wook Hyun Kwon, "A Fault Detection and Recovery Mechanism for the Fault-Tolerance of a Mini-MAP System," *Journal of Control, Automation and Systems Engineering*, Vol. 4, No. 2, April, 1998, pp. 264-272.

[6] Project report, *The Development and Application of Digital Distributed Cotnrol System for Boiler in the Power Plant*, Korean Electric Power Research Institute, 1993.

[7] Project report, *Development of an Integrated Digital Control System for Nuclear Power Plants (III)*, Korean Electric Power Research Institute, 1999.

[8] Project report *Fault Tolerance Architecture: Evaluation Methodology*, Electric Power Research Institute, 1992