Analysis of the redundant architecture for the fault-tolerance of a distributed control system

Hong-ju Moon *

Abstract

The distributed digital control system has many shared common components, and a single fault in the system may have effects on not a single function. Not as in an analog system, the faults in a digital system usually make discrete and abrupt changes in its output, which are hard to be expected. To cope with these situations, the fault-tolerance is an inevitable property of a distributed control system. A distributed digital control system consists of many equipments, and each equipment 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. The paper analyzes and compares the strategies and tactics to add the fault-tolerances in a distributed digital control system, and studies how they can be combined appropriately.

Key Words: redundant architecture, fault-tolerance, distributed control system

1 Introduction

Many traditional process control systems and manufacturing systems have been replaced by a distributed digital control system. The role of the distributed digital control system has been increased constantly and most of the plant operation relies on it.

Many traditional control systems consist of module type analog controllers. In such a system, the control loops are separated and many functions are replicated throughout the system. As they evolve to a modern digital integrated control systems, the control loops are concentrated and functions are distributed efficiently. This evolution makes the fault-tolerance of a control system more important than before.

The distributed digital control system has many shared common components and a single fault in the system may have effects on not a single function. Not as in an analog system, the faults in a digital system usually make discrete and abrupt changes in its

*Nuclear Instr. and Control Group, Korea Electric Power Research Institute 103-16 Munji-dong, Yusong-ku, Taejon 305-380, Korea, hjmoon@kepri.re.kr

output, which are hard to be expected. To cope with these situations, the fault-tolerance is an inevitable property of a distributed control system.

A distributed digital control system consists of many equipments, and each equipment 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 a distributed control system, 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 a distributed control system, and the relation between the parts and the overall operation have be considered to obtain the fault-tolerance of the distributed control system.

This study proposes a fault-tolerant computing architecture in a distributed control system. This study analyzes the techniques for each part of a distributed control system to get the fault-tolerance, and propose a fault-tolerant computing architecture in a distributed control system by combining them appropriately.

2 Architecture of a distributed digital control system

In this section, an architecture of a distributed digital control system is presented and each component of the system is discussed on its characteristics.

2.1 Overall architecture

The paper assumes the overall structure of a distributed digital control system as shown in Figure 1.

The architecture consists of several major components which will be discussed as follows. In the figure, three types of controllers are connected to the control network, and the middle one among the three will be presented in this subsection. Others will be discussed in the next subsection.

Input/Output modules An input/ouput module converts a signal from a sensor or a transmitter to the digital data which the digital controller can handle, or converts the data generated by the controller to the signal for the actuators.

Local controllers A local controller executes the major control functions which usually require fast operations. The functions provided by the local controller are simple but play key roles in controlling the processes. A single or not many control loops are treated in a local controller.

Group controllers A group controller supervises and coordinates the local controllers. It can also execute the major control functions.

Communication networks The communication network has the hierarchy which consists of three types of networks. The field network connects local controllers and a group controller. The control network connects group controllers and the data gateways. The operator interface stations can be connected to the control network. The information network connects the data gateway, the operator interface station, and the engineer interface station.

Data gateways The data gateway is defined in the considered architecture of the distributed digital control system to exchange data between the control network and the information. In the paper, a data gateway for two different networks is defined with the following properties. 1) A data gateway exchange the data between the two communication networks. 2) A data gateway does not allow a direct connection between the two nodes in different networks. 3) A data can be controlled to be passed in bi-direction or uni-direction, and not to be passed.

Operator interface stations An operator interface station provides various operator functions. They include alarm management, process management, data logging, historical data store, and system management.

Engineer interface stations An engineer interface station provides various engineering function. They include graphic builder, control loop and logic builder, data point configuration, logging and historical data configuration, and system configuration.

2.2 Classification of controller types

This paper defines three types of controllers architecture, which are depicted in Figure 1.

The first one consists of one powerful controller and many input/output modules. The second one consists of a group controller and multiple local controllers, which has been presented above. And, the third one consists of many modular controllers which have embedded input/output functions.

Module based control systems make it possible to isolate each control loop, and usually have a simple structure. They enhance the independency to achieve safety features at the expense of costs. Many modern digital control systems consist of powerful control units which may handle many control loops in a single unit. They provide various functionalities and save costs.

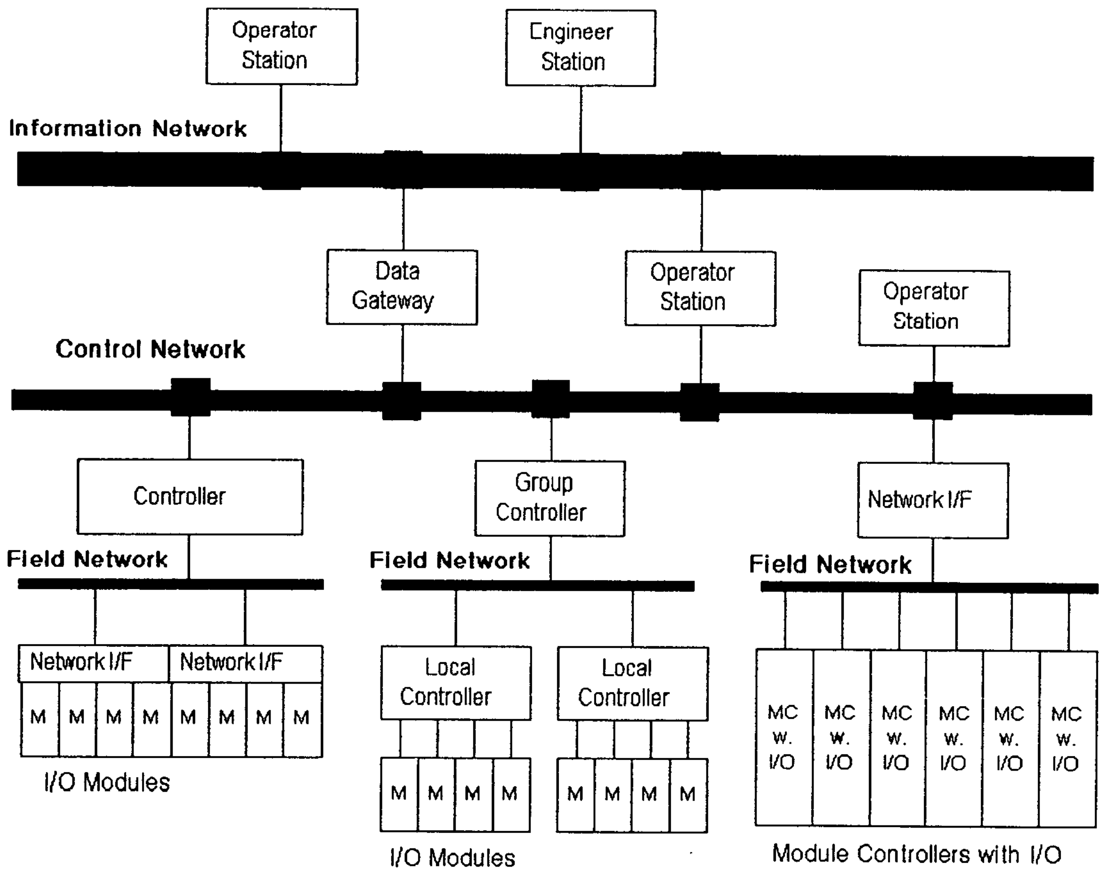

Figure 1: Architecture of a distributed digital control system

3 Analysis of fault-tolerant architectures

This section analyzes the fault-tolerant architecture for each components of the distributed digital control system. The fault-tolerance is implemented by redundancy for each component.

3.1 Sensors and Actuators

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

The duplicated inputs from multiple sensors can be used by their average or selected one with an appropriate mechanism. The selection logic can be by detecting the invalid range or the voting logic.

Table 1: Input redundancy.

Input usage	Appropriate signal type	Advantage	Disadvantage
average	analog	simple implementation	deviation
selection	analog/digital	accurate value	selection logic

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.

Table 2: Actuator redundancy.

Actuator usage	Appropriate type	Advantage	Disadvantage
parallel	control of continuous value	simple implementation	deviation
selection	action	accurate	selection logic

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 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 architecures.

Redundant control modules can be implemented to operate in parallel and in a selective manner. 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 control modules must have a selection function. 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.

3.4 Communication networks

For the redundancy, the communication network is considered separately 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. For the most of all the distributed digital control systems, the network cables are duplicated.

3.5 Operator interface stations

Most distributed control systems 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.

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 a redundant distributed digital control system.

The procedure shown in Figure 2 may be possible way to design the overall architecture.

4 Conclusion

The paper analyzed and compared the redundancy strategies for the components of a distributed digital control system, and studied how they can be combined appropriately.

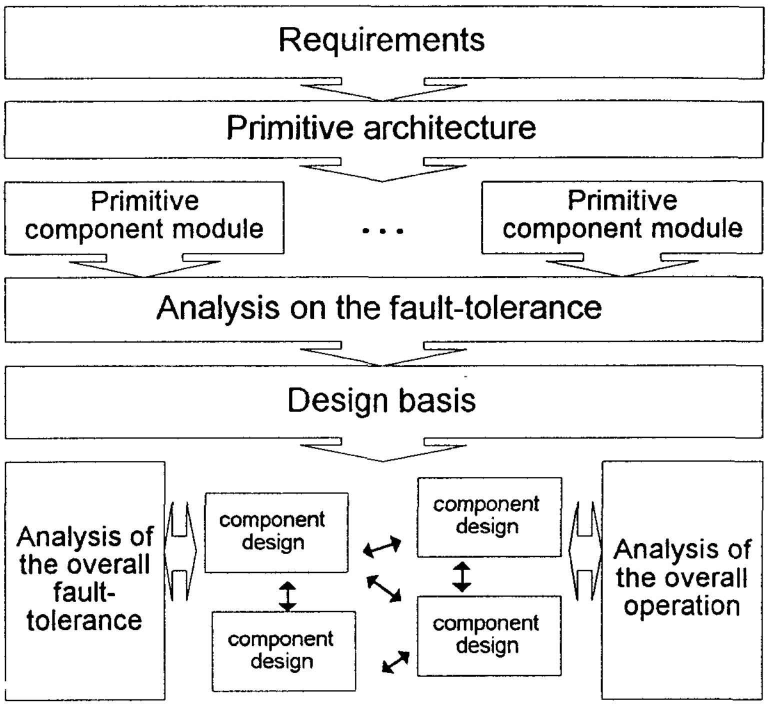

Figure 2: Procedure to design the redundant architecture

The fault-tolerance has to be implemented depending on the overall architecture and how each equipment is implemented.

The fault-tolerance of a distributed digital control system have to be considered at two phases. When the distributed digital control system is designed and implemented, it has to be considered first. Then, when the system is applied to a plant, the fault-tolerance has to be considered again. At this phase, the requirements and the characteristics of the plants have to be considered.

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] Barry W. Johnson, Design and Analysis of Fault-Tolerant Digital Systems, Addison-Wesley, 1989.

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

[5] 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.

[6] ong-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.

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

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