Virtual Modular Redundancy of Processor Module in the PLC

Kwang-Il Lee [a*], SungJae Hwang [a], DongHwa Yoon [a]
[a]*SOOSAN ENS Co. Korea Techno Complex Building, Korea University, Anam-dong, Soungbuk-Gu, Seoul, 02841*
[*]*Corresponding author: lee83t@soosan.co.kr*

1. Introduction

The Reliability of system is the most important from any other matter because the failures or accidents of nuclear power plant cause serious damages. Therefore, direct control system used in the nuclear power plant has to be shut down safely, even if a fatal error occurs. And it has to be guaranteed such as the no single point repair, fail isolation from failing component, and fault containment. For that reasons, safety control system for use in nuclear power plants is designed with as a combination of such fault tolerant system and a fail-safe system.

Dual Modular Redundancy (DMR) is mainly used to implement these safety control systems. DMR is conveyed when components of a system are duplicated, providing another component in case one should fault or fail. This feature has a high availability and large fault tolerant. It provides zero downtime that is required for nuclear power plants. However, the current industry or overseas nuclear power plant system reliability cannot be guaranteed only redundant control system. So nuclear power plant has been commercialized by multiple redundant systems.

The following paper, we propose a Virtual Modular Redundancy (VMR) rather than physical triple of the Programmable Logic Controller (PLC) processor module to ensure the reliability of the nuclear power plant control system. VMR implementation minimizes design changes to continue to use the commercially available redundant system. Also, the purpose of the VMR is to improve the efficiency and reliability in many ways, such as fault tolerant and fail-safe and cost.

2. Related Works

A control system used in the safety system for controlling a nuclear reactor in nuclear power plants is classified into the IEEE standard for qualifying class 1E. The safety control system can be used in high risk industries such as nuclear power plants only when the certain rating acquires. Accordingly, industry research institutions should design the system in a variety of techniques. Such as in a multiple redundant systems designed to acquire the class 1E [1].

This chapter lists the safety PLC redundant system while the system is researched or commercialized.

2.1 SOOSAN ENS 'POSAFE-Q'

POSAFE-Q is a system that consists of a duplicated CPU and power modules. The redundant processor module is shown in Fig. 1.

Fig. 1. Configuration of redundant processor module of POSAFE-Q [2].

CPU module of POSAFE-Q is a redundant processor module running as a master mode or slave mode. A CPU module that operates as a master module has a control for interfacing with another module. And CPU module operating in the slave mode can be only interfacing with the master module. The master module switchover occurs when there is a problem with the state of other CPU's diagnostic information. And slave module becomes a master.

2.2 SIEMENS 'SIMATIC S7-400'

SIEMENS S7-400 is configured by both hardware and software redundancy system [3]. Fig. 2 is shown when there is no error, if it does not have a problem with the system to work properly.

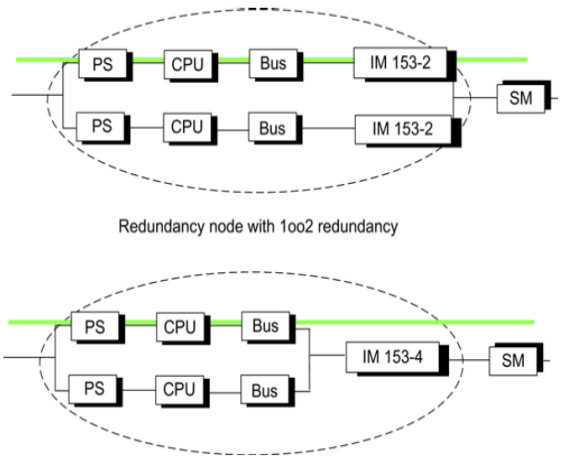

Fig. 2. Example of redundancy in a network without error [3].

Fig. 3 is a system if a failure or a disability exists. If a problem occurs as Fig 3 below, on one side is closed as the main system. Then a second system operates.

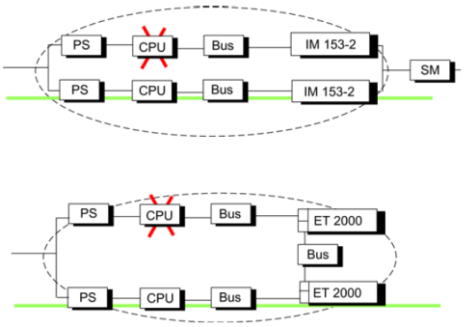

Fig. 3. Example of redundancy in a 1-out-of-2 system with error [3].

Fig.4 is when both failure in a redundant structure. It will operate in fail-safe in this state.

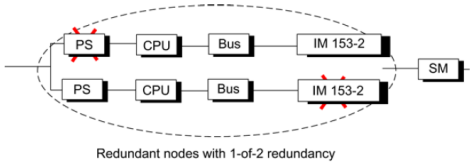

Fig. 4. Example of redundancy in a 1-out-of-2 system with total failure [3].

Such hardware, as well as software duplication, is implemented to keep the user programs.

2.3 Schneider Electric 'Tricon TMR System'

Tricon of Schneider Electric is a fault tolerant control system based on Triple Modular Redundancy (TMR) structures. The system is certified by a world recognized, independent safety agency (TÜ V) at International Electrotechnical Commission (IEC) Safety Integrity Level (SIL) 3 to be used for safety and critical control applications in process control and other industries. The Tricon is also certified by the Nuclear Regulatory Commission (NRC) to be used for safety (1E) and critical control applications in nuclear power plants [4].

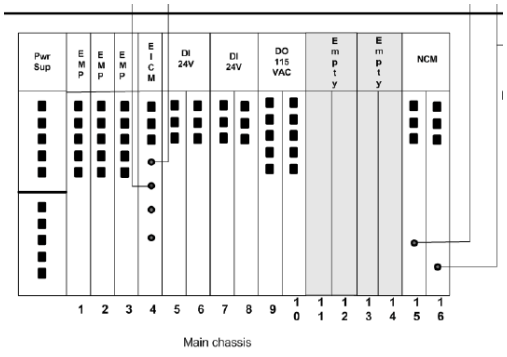

Fig. 5. Main chassis in Tricon TMR system [4].

The system is characterized by three isolated parallel control system, and a diagnosis function integrated into one system, the triple redundant system is using the time redundancy techniques. Tricon is implementing to basic functions of the voting TMR. Tricon are driven by triple, dual or single mode provides an availability of 99.99. Fig. 5 shows the main chassis installed TMR.

2.4 Westinghouse 'Advanced Logic System'

Advanced Logic System (ALS) is the logic controller of Westinghouse. The ALS platform incorporates two levels of diversity. The first level, core diversity, is implemented for each of the FPGAs on all of the ALS boards. Each of the FPGA images contains two sets of redundant hardware logic, called core [5].

ALS uses the concept of the module represented by the board. Each board is characterized in that the FPGA with the redundant core. The depth of the multiple redundancies is possible with n-level. Unlike other products, such as a switching operation or switching modules internally, that runs as a fail-safe system for recovery on the board itself. Fig. 6 is an ALS chassis.

Fig. 6. Example of ALS chassis [5].

2.5 Omron 'SYSMAC CS1 G/H'

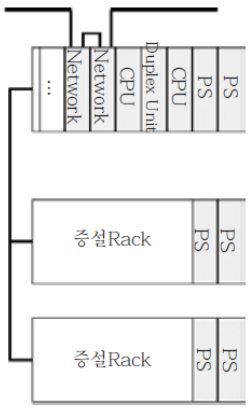

Fig. 7. Example of Omron SYSMAC CS1 system [6].

Omron redundant CPU is caused to switchover using standby mode. It does not affect system operation. Fig. 7 is a redundant system configuration diagram [6]. Omron's PLC redundancy system is using the hot standby mode. The switch CPU uses hot, warm, cold standby mode, and can depend on the switching operation in case of failure. The hot mode is the standby module that maintains a program execution state and the I/O, memory status, data, etc., as the active.

2.6 Yokogawa 'ProSafe-RS'

Features of the system highlighted in the Yokogawa ProSafe-RS are a Versatile Modular Redundancy (VMR^2) [7]. VMR^2 is the flow of the signal detected during a failure of the switching module to other modules. As shown in Fig. 8 refers to a structure which is flexibly changed.

The redundant configuration will change the flow of the signal in the event of a module failure part. Unlike systems which rely entirely on redundancy to achieve safety and availability, VMR^2 does not have a degradation mode, nor does it impose time limitations on such a mode.

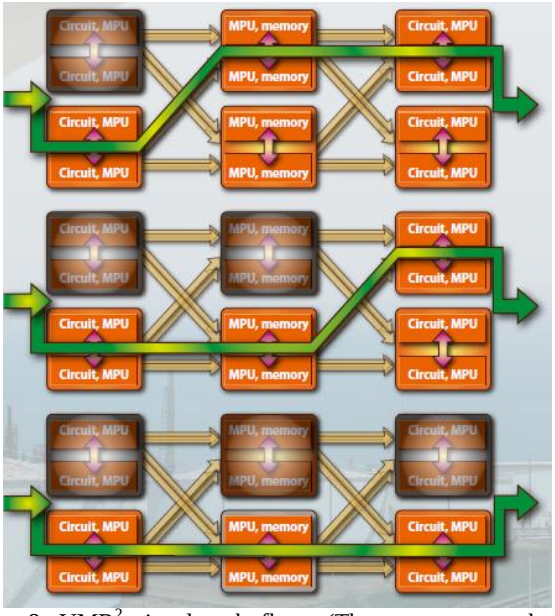

Fig. 8. VMR^2 signal path flows (The green arrow shows signal path when a failure occurs) [7].

In addition to those mentioned above, there is Quadruple Modular Redundancy (QMR) system from Honeywell.

3. Design Methods

3.1 Design Methods

Dual or triple redundancies of all the above mentioned previous studies PLC can be confirmed by all are configured in hardware. VMR proposed to this paper utilizes a shared control in the redundant system physically through the shared control and commands or receive data from other modules. The concept of the virtual module is controlling the peripheral circuits of B module by MPU of A module.

First of all, a shared control of the processor module prior to the design. In the paper, a shared control is that is the authority to control the peripheral circuits of the other module. There is a variety of ways to share control mainly using the CAN and BUS. Share control is never invading the control of another module during normal operations. Second, it needs to detect errors. The shared control system is the detected error module system itself so other errors or memory can be found. It is sufficient to use the existing technology.

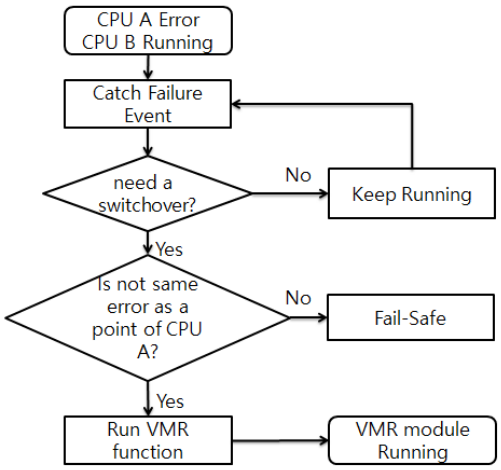

Fig. 9. Flowchart of the VMR running.

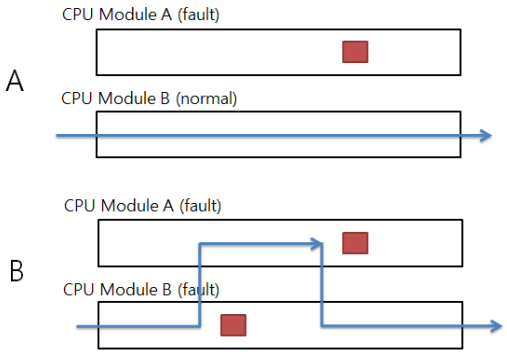

Fig. 10. VMR signal path flows (Red boxes shows error parts, the blue arrow shows signal path when a fault occurs).

If an error occurs to a typical redundant system, all modules generate such fail-safe and the system is stopped. VMR can implement the function of slowing down defense in this failover. Fig. 9 is a flowchart for the operating condition of the VMR.

If a problem occurs to a CPU A module, then CPU B becomes the master module. It looks like A of Fig. 10. In this situation, CPU B goes through the process of Fig. 9. If you pass the procedure of Fig. 9, it operates as the VMR like B of Fig. 10.

3.2 Example of Design Methods

Example of the design method uses POSAFE-Q. It does not support CAN communication or control sharing. However, there is a control signal BUS that is implemented to communicate. Also, it has the error detection function. And it adds the communication function of the control signal to the MCU and to the FPGA. Finally, it adds the pseudo code in Fig. 11 to implement the VMR.

```
Print “CPU_A  error”;
Set CPU_A_fault_Type to faultType;
While(fault checked(CPU_B)){
If  CPU_B  is fault
      Print “CPU_B  error”;
      Set CPU_B_fault_Type to faultType;
   If CPU_A_fault_Type != CPU_B_fault_Type
      Run VMR_function;
   Else
      Run Fail-Safe;
Else
   Skip;
}
```

Fig. 11. Pseudo code of VMR function.

If VMR is designed and implemented in the same way as the POSAFE-Q, it is possible to guarantee the reliability without changing the hardware design.

4. Conclusions

VMR guarantees a wide range of reliable fault recovery, fault tolerance, etc. It is prevented before it causes great damages due to the continuous failure of the two modules. The reliable communication speed is slow and also it has a small bandwidth. It is a great loss in the safety control system. However, VMR aims to avoid nuclear power plants that were suspended due to fail-safe. It is not for the purpose of commonly used. Application of VMR is actually expected to require a lot of research and trial and error until they adapt to the nuclear regulatory and standards.

REFERENCES

[1] Jinpyo Noh, Jaehyun Park, Kwang-Seop Son, and Dong-Hoon Kim, Reliability Analysis of Redundant Architecture of Dependable Control System, Journal of Institute of Control, Robotics and Systems, Vol.19, p.328-333, 2013.
[2] SungJae Hwang, SeongHwan Song, YoungHun No, DongHwa Yun, The Interface Between Redundant Processor Modules Of Safety Grade PLC Using Mass Storage DPRAM, Transactions of the Korean Nuclear Society Autumn, Vol.2, p1209-1210, 2010
[3] SIMATIC Fault-tolerant systems S7-400H, SIEMENS System Manual, 2014.
[4] Tricon Triple Modular Redundant (TMR) Digital System for Feedwater Control and Safety Application in Nuclear Power Plants, Invensys, 2011.
[5] Warren Odess-Gillett, Advanced Logic System Topical Repott, WestingHouse, 2013.
[6] KyungHwa Kang, The corresponding redundant PLC Base Controller, Omron Korea, 2002.
[7] Safety Instrumented System ProSafe-RS, Yokogawa, 2005.