The Interface Between Redundant Processor Modules Of Safety Grade PLC Using Mass Storage DPRAM

SungJae Hwang [a*], SeongHwan Song[a], YoungHun No[a], DongHwa Yun[a],
GangMin Park[a,] MinGyu Kim[a], KyungChul Choi[a], Uitaek Lee[a]
[a] *POSCO ICT Co. Korea Techno Complex Building Korea University, Anam-dong, Seongbuk-Gu, Seoul, 136-713*
[*]*Corresponding author: trustsky@poscoict.com*

1. Introduction

Processor module of safety grade PLC (hereinafter called as POSAFE-Q) developed by POSCO ICT provides high reliability and safety. However, POSAFE-Q would have suffered a malfunction when we think taking place of abnormal operation by exceptional environmental. POSAFE-Q would not able to conduct its function normally in such case. To prevent these situations, the necessity of redundant processor module has been raised. Therefore, redundant processor module, NCPU-2Q, has been developed which has not only functions of single processor module with high reliability and safety but also functions of redundant processor.

2. Methods and Results

Three modules are developed for redundant processor module of POSAFE-Q. They are NCPU-2Q processor module supporting redundant function, NBUS-5Q-A for controlling I/O and communication module and NBUS-5Q-B for sharing data between redundant processor modules.

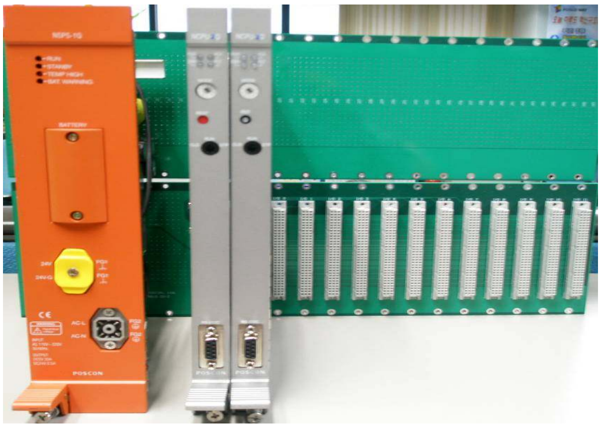

Fig 1. Configuration of redundant processor module of POSAFE-Q

2.1 The redundant method

One is operated as Master Mode(or Active Mode), the other is operated as Slave Mode(or Standby Mode) where 2 NCPU-2Q modules are equipped. It is designed so that the NCPU-2Q module being started first could be operated as master mode. The redundant method of POSAFE-Q is operated through bus module without additional memory or communication module. Each redundant processor module is equipped with 4Mbytes, mass storage DPRAM. The DPRAM is shared between master and slave module.

A master module writes all the necessary data when it conducts switch-over. The access authority of a slave processor module to the DPRAM is designed to read only. The communication, special and I/O module etc. being equipped in bus module is designed to be accessed from master module only.

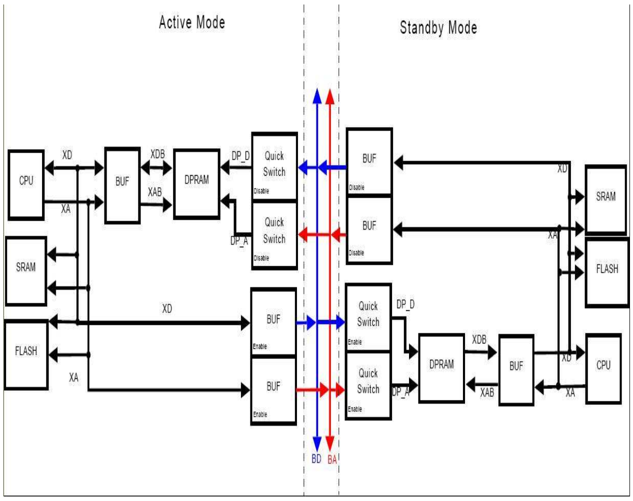

Fig 2. The operation mechanism of redundant duplex processor module

2.2 The operation method of redundant processor module

The operation method of redundant processor module. The master processor module send its data to the slave processor module so that it can have identical data. The slave processor module informs its abnormality when master/slave does not have the same data. The master processor module is designed to inform its abnormality when abnormal operation has occurred and switches its mode set as slave mode. At a time, the previous slave processor module becomes master mode.

This operation being called switch-over takes place for the reasons stated below.

- Watchdog timeout at master processor module.
- HW reset at master processor module.
- Bus timeout error at master processor module.
- Abnormal heartbeat between master/slave modules.
- Memory error at master processor module.
- The running state error of application has occurred at master processor module.

In the cases stated above, the processor module set as master mode transfer its control to the processor module set as slave mode and switches its mode as slave. The processor module that is newly works as master mode prevent the processor module which made a problem before from accessing communication module, special module and I/O module.

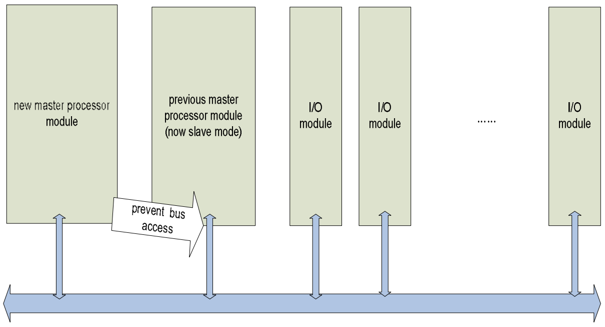
new master processor module
previous master processor module (now slave mode)
prevent bus access
I/O module
I/O module
......
I/O module

Fig 3. Blocking bus access after switch over

The equipped module is operated as master mode when only one process module is equipped in redundant processor system. If other module were equipped at this time, newly equipped module would be operated as slave mode. From this time, the processor module set as master mode transfers data which is needed when it conducts switch-over to the processor module set as slave mode. However, the redundant processor module system is designed not to be affected for the processor module set as master mode during transferring data to the processor module set as slave mode with respect to deterministic operation running application.

3. Conclusions

Interface between redundant processor modules which uses mass capacity DPRAM is designed to be able to access rapidly through bus module without any additional memory or communication module. This design guarantees that switch-over of master/slave mode does not affects to deterministic operation of POSAFE-Q by conducting switch-over within minimum time. The POSAFE-Q which has functions stated above would have better reliability and safety when it is used in nuclear power plant..

REFERENCES

[1] Criteria for Programmable Digital Computers System Software in Safety Related Systems of Nuclear Power Plants, USNRC Reg. Guide 1.152, Rev. 01, 1996

[2] Software Requirements Specifications for Digital Computer Software Used in Systems of Nuclear Power Plants, USNRC Reg. Guide 1.172, Rev. 00, 1997

[3] Standard Criteria for Digital Computers in Safety System of Nuclear Power Generating Stations, IEEE Std. 7-4.3.2-2003.

[4] POSAFE-Q System Requirements, POSAFE-Q-00000-D202-1, POSCO ICT.

[5] POSAFE-Q Design Specifications, POSAFE-Q-00000-D210-1, POSCO ICT

[6] POSAFE-Q NCPU-2Q Software Requirement Specifications, POSAFE-Q-00102-D210-1, POSCO ICT.