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

Reliability Analysis Multiple Redundancy Controller for Nuclear Safety Systems

Gwang-Seop Son [a*], Dong-Hoon Kim. Blue [a], Choul-Woong Son [a]
[a]*I&C/Human Factor Research Division, Korea Atomic Energy Research Institute*
[*]*Corresponding author: ksson78@kaeri.re.kr*

1. Introduction

To enhance the reliability of the safety grade Programmable Logic Controller (PLC), a variety of fault tolerant method are utilized [1, 2]. In this paper, the Multiple Redundancy Controller (MRC) is introduced. This controller is configured for multiple modular redundancy (MMR) composed of dual modular redundancy (DMR) and triple modular redundancy (TMR). The architecture of MRC is briefly described, and the Markov model is developed. Based on the model, the reliability and Mean Time To Failure (MTTF) are analyzed.

2. Architecture

As four independent channels are typically configured in nuclear safety systems, component failures and consequential determination by the output logic are important requirements. Thus, as shown in Fig.1, the basic structure of SPLC for advanced nuclear safety systems is designed by applying TMR to a single rack, which satisfies the physical simplicity, high reliability, and availability, and also can cope with undetected failures. In this architecture, the input/output and processor modules are configured for TMR and the data communication, power, and bus modules are configured for DMR. The data communication module is designed to keep the control and status data being separated [3], and the bus is designed as a serial bus that has strengths in redundancy, high speed, and scalability.

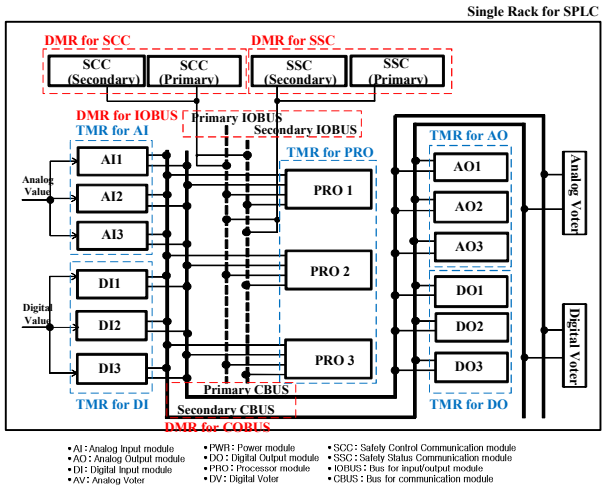

Fig. 1 Architecture of MRC

As shown in Fig.1, the process value that could be either a digital value or an analog value flows into TMR AI/DI. The output from each DI/AI flows into TMR PRO through DMR bus. Each PRO selects one out of two normal buses and performs a voting logic with the 3 results from TMR DI/AI. The result of voting logic of TMR PRO goes to TMR AO/DO. As the TMR PRO does, each AO/DO selects one out of two normal buses and performs a voting logic with the 3 results from TMR PRO. Then, the analog/digital voter selects a final value by using its voting logic.

3. Markov Model

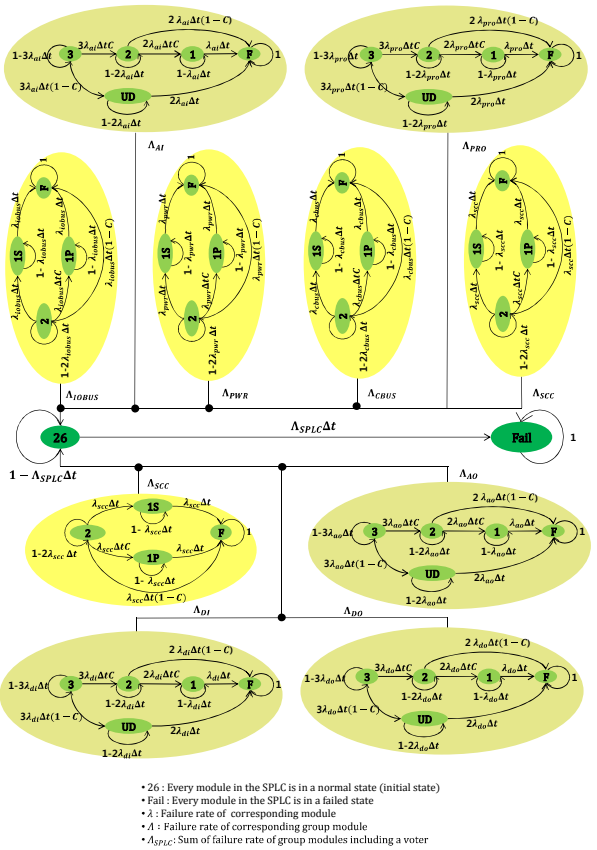

Fig. 2 Markov model of MRC

Fig. 2 represents the Markov model of the MRC. Based on Fig.1, AI, DI, PRO, AO, and DO are configured for TMR, and PWR, SCC, SSC, IOBUS, and CBUS are configured for DMR. Failures in each group (DMR or TMR) module or the voter cause the SPLC to fail. Therefore, the failure rate of SPLC is expressed as the sum of the failure rates of each group module and the voter.

Any failures of in the 10 group modules or the voter in Fig. 11 cause the SPLC to be in a failed state. By using Fig. 10, the reliability function is obtained as follows:

$$R_{MRC} = e^{-\int \Lambda_{MRC} dt} = e^{-\left(\int \sum_{i=1}^{10} \Lambda_i + \lambda_{voter}\, dt\right)} =$$

$$= \prod_{i=1}^{5}\left(\frac{3e^{\lambda_i t}+3C^2-6C^2e^{\lambda_i t}+3C^2e^{2\lambda_i t}-2}{e^{3\lambda_i t}}\right)\prod_{i=6}^{10}\left(\frac{e^{\lambda_i t}-C+Ce^{\lambda_i t}}{e^{2\lambda_i t}}\right)e^{-\lambda_{voter}\, t} \quad (1)$$

where $\Lambda_{M\,RC} = \Lambda_{AI} + \Lambda_{AO} + \Lambda_{DI} + \Lambda_{DO} + \Lambda_{PRO} + \Lambda_{DBUS} + \Lambda_{CBUS} + \Lambda_{SSC} + \Lambda_{SCC} + \Lambda_{PW\,R} + \lambda_{voter}$,

$[\Lambda_1 \;\; \Lambda_2 \;\; \Lambda_3 \;\; \Lambda_4 \;\; \Lambda_5 \;\; \Lambda_6 \;\; \Lambda_7 \;\; \Lambda_8 \;\; \Lambda_9 \;\; \Lambda_{10}] =$
$[\Lambda_{AI} \;\; \Lambda_{DI} \;\; \Lambda_{PRO} \;\; \Lambda_{AO} \;\; \Lambda_{DO} \;\; \Lambda_{DBUS} \;\; \Lambda_{CBUS} \;\; \Lambda_{SCC} \;\; \Lambda_{SSC} \;\; \Lambda_{PW\,R}]$
$,[\lambda_1 \;\; \lambda_2 \;\; \lambda_3 \;\; \lambda_4 \;\; \lambda_5 \;\; \lambda_6 \;\; \lambda_7 \;\; \lambda_8 \;\; \lambda_9 \;\; \lambda_{10}] =$
$[\lambda_{ai} \;\; \lambda_{di} \;\; \lambda_{pro} \;\; \lambda_{ao} \;\; \lambda_{do} \;\; \lambda_{dbus} \;\; \lambda_{cbus} \;\; \lambda_{scc} \;\; \lambda_{ssc} \;\; \lambda_{pwr}]$

$\Lambda_i = \frac{3\lambda_i(e^{\lambda_i t}-1)(C^2e^{\lambda_i t}-3C^2+2)}{3e^{\lambda_i t}+3C^2-6C^2e^{\lambda_i t}+3C^2e^{2\lambda_i t}-2}$ *for* $i = 1\sim5$,

$\Lambda_i = \lambda_i - \frac{C\lambda_i}{e^{\lambda_i t}-C+Ce^{\lambda_i t}}$ *for* $i = 6\sim10$

MTTF is defined as follow [4]:

$$\mathrm{MTTF_{M\,RC}} = \int_0^\infty \mathrm{R_{M\,RC}}(t)\,dt \quad (2)$$

where $\mathrm{R_{M\,RC}}(t)$ = The reliability function of the MRC

3. Analysis

Fig. 3 shows the reliability function of MRC with various failure rates. It is assumed here that failure rates of all modules in MRC are the same as λ, and Fault Coverage Factor (FCF) is 0.9. As shown in Fig. 3, the reliability decreases drastically as time increases in case that the failure rate λ is higher than 10^{-4}/hour. Thus the failure rate of each module in the SPLC should be less than 10^{-5}/hour.

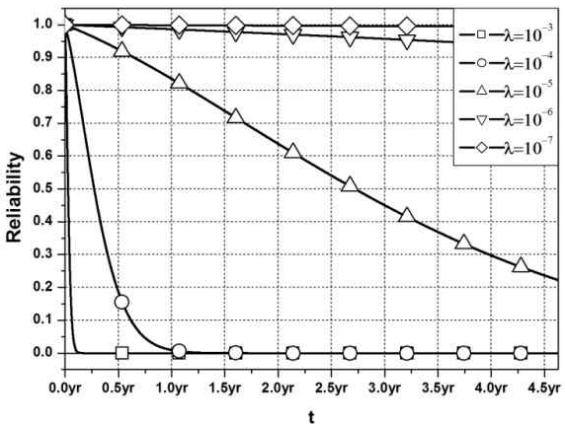

Fig. 3 MRC reliability vs. time with various failure rates

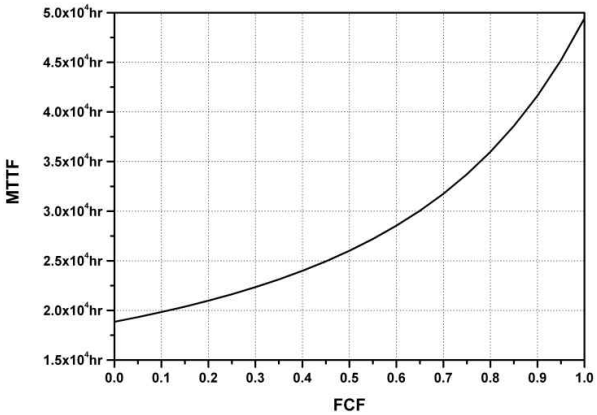

Fig. 4 MRC MTTF vs. FCF

Fig. 4 shows the MTTF of SPLC depending on FCF when the failure rate of each module is the failure rate in [5]. When FCF = 0 and 1, the MTTF becomes about 19,000 hours and 50,000 hours, respectively. The MTTF increases by 4 months as FCF increases by 0.1. Thus, it is necessary that the diagnostic ability influencing Fault Coverage Factor (FCF) significantly has to be strengthened.

4. Conclusions

In this paper, the architecture of MRC for nuclear safety systems is described. The MRC is configured for multiple modular redundancy (MMR) composed of dual modular redundancy (DMR) and triple modular redundancy (TMR). Markov models for MRC architecture was developed, and then the reliability was analyzed by using the model. From the reliability analyses for the MRC, it is obtained that the failure rate of each module in the MRC should be less than 2×10^{-4}/hour and the MTTF average increase rate depending on FCF increment, i.e. ΔMTTF/ΔFCF, is 4 months/0.1.

REFERENCES

[1] S. J. Hwang, S. H. Song, Y. H. No, D. H. Yun, G. M. Park, M. G. Kim, K. C. Choi, U. T. Lee, "The Interface Between Redundant Processor Modules of Safety Grade PLC Using Mass Storage DPRAM", Transaction of the Korea Nuclear Society Autumn Meeting, p.1209-1210, Oct.2010.
[2] (2012). [Online]. Available:Iom.invensys.com/EN/pdfLibrary/ProductSpec_Triconex_Tricon_03-10.pdf
[3] K. S. Son, D. H. Kim, "Development of Broadband-Nuclear Safety Data Network (B-NSDN)", NuPIC Symposium in Korea, Autumn, 2011.
[4] Barry W. Johnson, Design and Analysis of Fault-Tolerant Digital Systems, Addison-Wesley Publishing Company, 1989
[5] C. J. Choi, Reliability Analysis Report of Safety Grade PLC (POSAFE-Q), Technical Report in KAERI(Korea Atomic Energy Research Institute), 2008