Annals of Nuclear Energy 111 (2018) 73–81

Contents lists available at ScienceDirect

Annals of Nuclear Energy

journal homepage: www.elsevier.com/locate/anucene

Availability analysis of safety grade multiple redundant controller used in advanced nuclear safety systems

Kwang Seop Son [a,b,*], Dong Hoon Kim [a], Gee Yong Park [a], Hyun Gook Kang [c]

[a] Nuclear ICT Research Division, Korea Atomic Energy Research Institute, Republic of Korea
[b] Department of Nuclear and Quantum Engineering, Korea Advanced Institute of Science and Technology, Republic of Korea
[c] Mechanical, Aerospace, and Nuclear Engineering (MANE), Rensselaer Polytechnic Institute, 110 Eight Street, Troy, NY, USA

ARTICLE INFO

Article history:
Received 9 September 2015
Received in revised form 26 July 2017
Accepted 25 August 2017

Keywords:
Multiple redundant architecture
Availability
Markov model
System unavailability rate

ABSTRACT

We analyze the availability of the Safety Programmable Logic Controller (SPLC) having multiple redundant architectures. In the SPLC, input/output and processor module are configured as triple modular redundancy (TMR), and backplane bus, power and communication modules are configured as dual modular redundancy (DMR). The voting logics for redundant architectures are based on the forwarding error detection. It means that the receivers perform the voting logics based on the status information of transmitters. To analyze the availability of SPLC, we construct the Markov model and simplify the model adopting the system unavailability rate. The results show that the fault coverage factor should be $\geq$0.8 and Mean Time To Repair (MTTR) should be $\leq$100 h in order to satisfy the requirement that the availability of the safety grade PLC should be $\geq$0.995. Also we evaluate the availability of SPLC comparing to other PLCs such as simplex, processor DMR (pDMR) and independent TMR (iTMR) PLCs used in the existing nuclear safety systems. The availability of SPLC is higher than those of the simplex, pDMR but is lower than that of iTMR for one month which is the periodic off-line test and inspection. That's why the number of redundant modules used in PLC is more dominant to increasing the availability than the number of fault masking methods such as voting logics used in PLC on the assumption that operation time is in the early stage. But the availability of iTMR, which has many redundant modules but has only a voting logic fast decrease and eventually is the lowest after 8000 h. Also if the MTTR of each module in PLC is required to be increased to 200 h, the availability of SPLC would be better than iTMR.

1. Introduction

Nuclear safety systems monitor the safety variables and perform the safety functions such as a reactor trip and operation of safety pumps and valves when the monitored safety variables are out safe operation range (Son, 2011). Most existing nuclear safety systems have been operated with analog and relay components until recently however the use of digital components in nuclear safety systems has been considered seriously because of decline or halt in the production of analog components. Digital safety systems based on a Programmable Logic Controller (PLC) have been installed in nuclear power plants since Hanul 5&6 in Korea, which began commercial operation in 2005(Kwon et al., 2007).

PLCs are widely used in process control systems and typically perform the desired control functions with modules that can be programmed and assembled. The development process for safety grade PLCs in the nuclear safety system must be carried out in compliance with strict nuclear safety requirements unlike that for industrial PLCs. In particular, since high dependability such as reliability, safety and availability is the important factor of the PLCs for the nuclear safety systems, various redundant architectures are designed to enhance the dependability.

The simplex, processor-dual modular redundancy (pDMR) and independent triple modular redundancy (iTMR) PLC are used in the existing nuclear safety system. In the simplex, all modules are configured as single module except for a power module configured as the DMR. In the pDMR, both a processor and power module are configured as the DMR and the others are configured as single module (Hwang et al., 2010). In the iTMR, three simplex PLCs are independently configured as the TMR and final value is selected by a voter (Tricon Systems, 2006).

In this paper, the Safety PLC (SPLC) using multiple redundant architectures is introduced and its availability is analyzed using the Markov model. In particular, we simplify the Markov model

* Corresponding author at: Nuclear ICT Research Division, Korea Atomic Energy Research Institute, Republic of Korea.
E-mail address: ksson78@kaeri.re.kr (K.S. Son).

http://dx.doi.org/10.1016/j.anucene.2017.08.065
0306-4549/

Nomenclature

Table of acronyms

A	Availability
A_{iTMR}	Availability of iTMR PLC
A_{pDMR}	Availability of pDMR PLC
$A_{Simplex}$	Availability of simplex PLC
A_{SPLC}	Availability of SPLC
AI	Analog Input Module
AO	Analog Output Module
BUS	Backplane Bus
C	Fault Coverage Factor
CCF	Common Cause Failure
CRC	Cyclic Redundancy Check
DI	Digital Input Module
DMR	Dual Modular Redundancy
DO	Digital Output Module
iTMR	independent TMR
MTTR	Mean Time To Repair
pDMR	processor DMR
PLC	Programmable Logic Controller
PRO	Processor Module
PWR	Power Module
R_{SPLC}	Reliability of SPLC
RTOS	Real Time Operation System
SCC	Safety Critical Communication Module
SPLC	Safety PLC
SSC	Safety Status Communication Module
TMR	Triple Modular Redundancy
Λ_{AI}	System unavailability rate of AI
Λ_{BUS}	System unavailability rate of BUS
Λ_{DI}	System unavailability rate of DI
Λ_{iTMR}	System unavailability rate of iTMR PLC
Λ_{SSC}	System unavailability rate of SSC
Λ_{PWR}	System unavailability rate of PWR
Λ_{pDMR}	System unavailability rate of pDMR PLC
Λ_{PRO}	System unavailability rate of PRO
Λ_{SCC}	System unavailability rate of SCC
$\Lambda_{Simplex}$	System unavailability rate of simplex PLC
Λ_{voter}	System unavailability rate of voter

as adopting the concept of the system unavailability rate. Also the availability is evaluated as comparing the other PLCs having different redundant architectures as described above.

2. SPLC architecture

2.1. Redundant architecture

The SPLC is composed of analog input/output, digital input/output, processor, and communication, backplane bus and power module like industrial PLCs. The analog input/out, digital input/output and processor modules are configured as the TMR and communication, bus and power modules are configured as the DMR as shown in Fig. 1 (Son, 2013).

In Fig. 1, the process values from sensors that could be either a digital or analog value are transmitted to the TMR analog/digital input(AI/DI). After signal conditioning, the outputs are sent to the TMR processor (PRO) through the DMR backplane bus (BUS). Each PRO selects one out of two normal BUS and performs the voting logic with the three results from the TMR AI/DI as depicted in Fig. 2 The result of voting logic of the TMR PRO is transmitted to the TMR AO/DO through the DMR BUS. Like TMR PRO, each AO/DO selects one out of two normal BUS and performs the voting logic with the three results from TMR PRO. Finally the voter selects the final value using its voting logic.

2.2. Redundant voting logic

In SPLC, the outputs of precedent modules (Transmitters) are selected by the successor modules (Receivers) using the redundant voting logics based on the status information of precedent modules such as heartbeat and cyclic redundancy check (CRC). The methods of voting logic for the DMR and TMR are as in the following.

2.2.1. DMR

The DMR modules are composed of the primary and secondary module. The voting for the DMR is performed by a receiving module as described above. The receiving module makes a judgment whether the failures of transmitter's primary and secondary occur or not using the status information. Without any failures in both the primary and secondary, the receiving module selects the value of the primary. But the receiving module selects the value of secondary when the failure of primary is detected. If failures of both primary and secondary are detected, the receiving module generates a predefined constant value, which generally implies the actuation of safety functions.

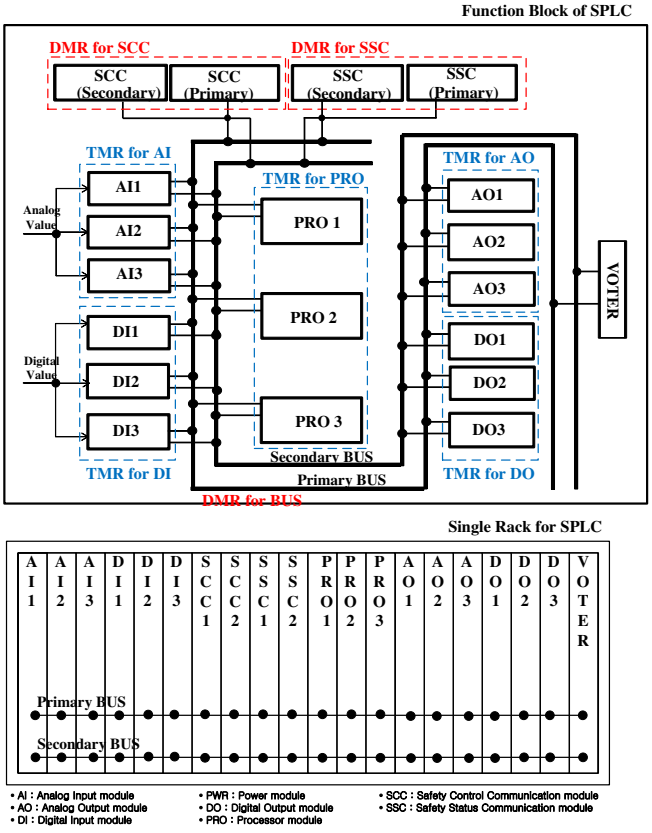

Fig. 1. SPLC Architecture in advanced nuclear safety system.

2.2.2. TMR

The voting logic for the TMR is shown in Fig. 2.