Proceedings of the Korean Nuclear Society Autumn Meeting
Taejon, Korea, October 1996

A Study on Implementation of Dynamic Safety System in Programmable Logic Controller for Pressurized Water Reactor

Ung Soo Kim and Poong Hyun Seong
Korea Advanced Institute of Science and Technology

Abstract

The Dynamic Safety System (DSS) is a computer based reactor protection system that has fail-safe nature and perform dynamic self-testing. In this paper, the implementation of DSS in PLC is presented for PWR. In order to choose adequate PLC implementation model of DSS, the reliability analysis is performed. The KO-RI unit 2 Nuclear power plant is selected as the reference plant, and the verification is carried out using the KO-RI unit 2 simulator FISA-2.

1. Introduction

The reactor protection system is currently used in nuclear power plant for safety and efficiency. The reactor protection system receives the signals from the reactor and other components, and generates a trip signal with the coincidence logic. Then, the reactor protection system sends the trip signal for the reactor trip. At many Westinghouse type PWRs currently used in Korea, the solid state protection system (SSPS) and 7300 series cards are the main parts of the reactor protection system. The 7300 series cards form 4 independent channels that the analog signals from the reactor and other components pass through, and provide bistable outputs to the SSPS. The SSPS determine reactor trip finally using coincidence logic. This system is a simple logic circuit based reactor protection system. The Dynamic Safety System (DSS) is a computer based reactor protection system that allows much more complex trip algorithm. It has fail-safe nature, and can perform dynamic self testing. The DSS is developed in AEA Technology of the UK and applied to Prototype Fast Reactor (PFR) at first. And then the DSS is applied to Advanced Gas-cooled Reactor (AGR) named Dungness B (1992) with great success. The Dungness system is the first software based protection system to be licensed for use in the UK. However the DSS has to be modified for applying to PWR. The DSS tested in the UK monitors a few parameters, whereas the PWR has many parameters that must be monitored and has more complex trip algorithms.

The KO-RI unit 2 Nuclear Power Plant is selected as reference nuclear power plant, and the reactor protection system using DSS technology is implemented in Programmable Logic Controller (PLC). Reliability analysis is carried out for DSS in PLC and verification is performed using data from the FISA-2 KO-RI unit2 simulator.

2. Design and Reliability Analysis of DSS in PLC

In nuclear power plants, safety is a matter of great significance and most components used in nuclear power plant must be highly reliable. Therefore reliability analysis should be carried out before implementation of DSS in PLC. As shown in Fig. 1, the typical DSS consists of several components such as, Trip Algorithm Computer (TAC), Voting Algorithm Computer (VAC), Pattern Recognition Logic (PRL), and Final Voting Logic (FVL). The TAC perform two tasks. The first task is the determination of reactor trip with input signals from reactor and other components using trip algorithms, and the second task is the control of test signal generator. The VAC receives signals from the TACs and performs voting logic. The PRL compares output pattern from VAC with expected output pattern, and if these two patterns are mismatched, the PRL generates trip signal. The FVL vote PRL output finally.

Applying the DSS technology to the PWR, the structure modification of the DSS and the reliability analysis of the modified DSS are needed. The modified model of the DSS in PLC is classified into 5 categories, and the data of PLC, listed in Table 1, is used and we assume that there is no software fault and use linearly increasing failure rate. The reliability analysis is performed as follows:

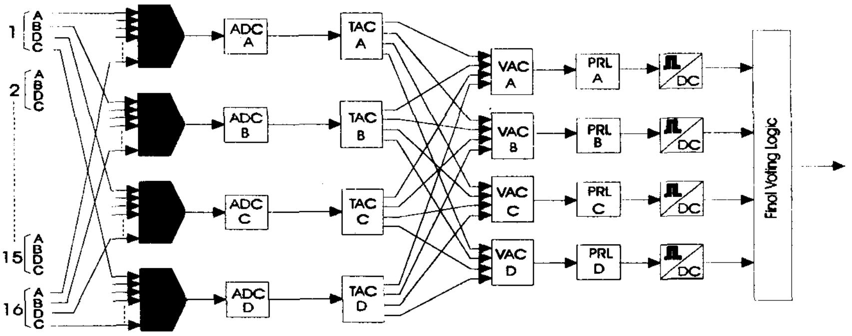

Fig. 1 Block Diagram of DSS

	PLC Component	MTTF (hour)	λ(hour $^{-1}$)
1	AVI 03000	372949	1.12933E-11
2	AVO 02000	307379	1.66254E-11
3	CPS 11400	254978	2.4161E-11
4	CPU 42402	279931	2.00455E-11
5	DDI 35300	228616	3.00543E-11
6	DDO 35300	279425	2.01182E-11

Table 1 The data of PLC for reliability calculation

2.1 Dual Voting (2/4, 2/4) using 9 PLC Drops

This model is typical to DSS employed in AGR, and the structure of implementation in PLC is shown in Fig 2. Dual voting is performed, and the system reliability is calculated as follows :

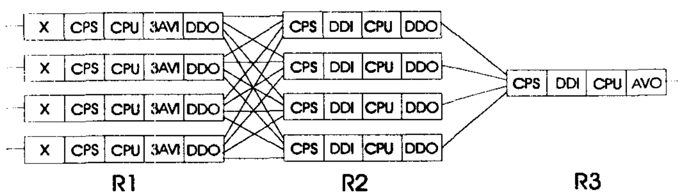

Fig. 2 Dual Voting (2/4, 2/4) using 9 PLC Drops

$$R_1(t) = Xe^{-(\lambda_3+3\lambda_1+\lambda_4+\lambda_6)t^2/2} = Xe^{-4.9102\times 10^{-11}t^2}$$

$$R_2(t) = e^{-(\lambda_3+\lambda_5+\lambda_4+\lambda_6)t^2/2} = e^{-4.71895\times 10^{-11}t^2}$$

$$R_3(t) = e^{-(\lambda_3+\lambda_5+\lambda_4+\lambda_2)t^2/2} = e^{-4.54431\times 10^{-11}t^2}$$

$$R_{trip}(t) = R_3\left\{ \sum_{n=0}^{2} {}_4C_n\, R_1^{\,4-n}(1-R_1)^n\right\}\left\{ \left(\sum_{m=0}^{2} {}_4C_m\, R_2^{\,4-m}(1-R_2)^m\right\}$$

$$R_{normal}(t) = R_3\left\{ \sum_{n=0}^{1} {}_4C_n\, R_1^{\,4-n}(1-R_1)^n\right\}\left\{ \left(\sum_{m=0}^{1} {}_4C_m\, R_2^{\,4-m}(1-R_2)^m\right\}$$

2.2 Dual Voting (1/2, 1/2) using 6 PLC Drops

This model is to BWR reactor protection system using one-out-of-two-taken-twice trip logic, and the structure implemented in PLC is shown Fig. 3. The reliability calculation is as follows :

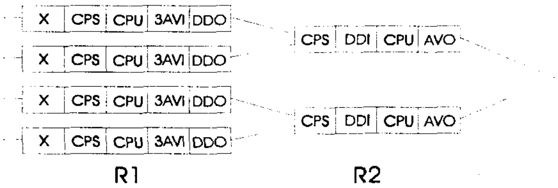

Fig. 3 Dual Voting (1/2, 1/2) using 6 PLC Drops

$$R_1(t) = Xe^{-(\lambda_3+3\lambda_1+\lambda_4+\lambda_6)t^2/2} = Xe^{-4.9102\times 10^{-11}t^2}$$

$$R_2(t) = e^{-(\lambda_3+\lambda_5+\lambda_4+\lambda_2)t^2/2} = e^{-4.54431\times 10^{-11}t^2}$$

$$R_{trip}(t) = R_2 \sum_{n=0}^{3} {}_4C_n\, R_1{}^{4-n}(1-R_1)^n + 2R_2(1-R_2)(\ R_1{}^4 + 4\ R_1{}^3(1-R_1) + 5\ R_1{}^2(1-R_1)^2 + 2R_1(1-R_1)^3)$$

$$R_{normal}(t) = \ R_1{}^4\ R_2{}^2$$

2.3 Single Voting (2/4) using 5 PLC Drops

This model is to PWR reactor protection system using two-out-of-four trip logic, and the PLC implementation structure is shown Fig. 4. The reliability calculation is as follows :

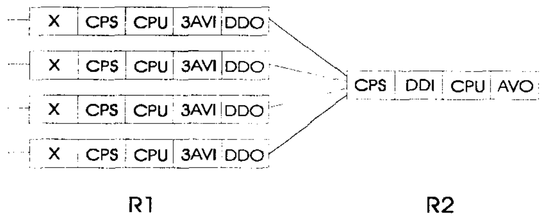

Fig. 4 Single Voting (2/4) using 5 PLC Drops

$$R_1(t) = Xe^{-(\lambda_3+3\lambda_1+\lambda_4+\lambda_6)t^2/2} = Xe^{-4.9102\times 10^{-11}t^2}$$

$$R_2(t) = e^{-(\lambda_3+\lambda_5+\lambda_4+\lambda_2)t^2/2} = e^{-4.54431\times 10^{-11}t^2}$$

$$R_{trip}(t) = R_2 \sum_{n=0}^{2} {}_4C_n\, R_1{}^{4-n}(1-R_1)^n$$

$$R_{normal}(t) = R_2 \sum_{n=0}^{1} {}_4C_n\, R_1{}^{4-n}(1-R_1)^n$$

2.4 Single Voting (2/4) using 1 PLC Drop

This model is the same as above, but using 1 PLC drop. The structure is shown in Fig. 5 and the reliability is calculated as follows :

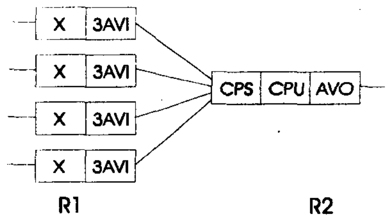

Fig. 5 Single Voting (2/4) using 1 PLC Drop

$$R_1(t) = Xe^{-3\lambda_1} = Xe^{-1.694\times 10^{-11}t^2}$$

$$R_2(t) = e^{-(\lambda_3+\lambda_4+\lambda_2)t^2/2} = e^{-3.00191\times 10^{-11}t^2}$$

$$R_{trip}(t) = R_2 \sum_{n=0}^{2} {}_4C_n\, R_1^{\,4-n}(1-R_1)^n$$

$$R_{normal}(t) = R_2 \sum_{n=0}^{1} {}_4C_n\, R_1^{\,4-n}(1-R_1)^n$$

2.5 Dual Voting (2/4, 1/4) using 8 PLC Drops

This model is the same as typical DSS model except Final Voting Logic. As shown in Fig. 6, the first voting is the two-out-of-four, but the second voting is the one-out-of-four. The reliability is calculated as follows :

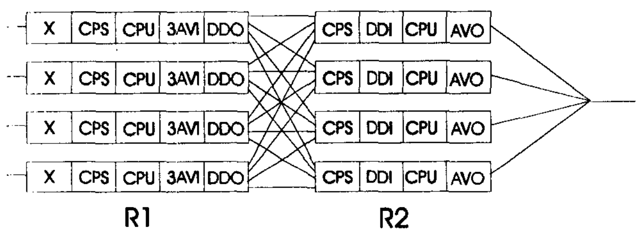

Fig. 6 Dual Voting (2/4, 1/4) using 8 PLC Drops

$$R_1(t) = Xe^{-(\lambda_3+3\lambda_1+\lambda_4+\lambda_6)t^2/2} = Xe^{-4.9102\times 10^{-11}t^2}$$

$$R_2(t) = e^{-(\lambda_3+\lambda_5+\lambda_4+\lambda_2)t^2/2} = e^{-4.54431\times 10^{-11}t^2}$$

$$R_{trip}(t) = \left\{ \sum_{n=0}^{2} {}_4C_n\, R_1^{\,4-n}(1-R_1)^n \right\}\left\{ \left(\sum_{m=0}^{3} {}_4C_m\, R_2^{\,4-m}(1-R_2)^m \right\}$$

$$R_{normal}(t) = R_2^{\,4} \sum_{n=0}^{1} {}_4C_n\, R_1^{\,4-n}(1-R_1)^n$$

2.6 Result of Reliability Analysis

Fig. 7 and Fig. 8 show the results of reliability analysis. As R_{trip} becomes higher the safety is increased and as R_{normal} becomes higher the economical efficiency is increased. As shown in figures, the model in 2.2 and 2.5 has very high reliability in trip state however the economical efficiency is lower than other models. The model in 2.4 is appropriate as PLC implementation model for the safety and the economical efficiency.

3. Implementation in PLC

In PLC the functions of the DSS is implemented with the MODSOFT. The MODSOFT is a programming tool for the PLC. The reference nuclear power plant is the KO-RI unit 2. The trip logic of the DSSs tested in the UK is two-out-of-four, however the trip logic of the KO-RI unit 2 plant is not only two-out-of-four but also some different logic such as, one-out-of-two, two-out-of-three, four-out-of-four, and etc. And the number of monitored parameters differs from each other. Therefore some modification must be carried out in trip and voting algorithm of the DSS, and it is left for future work.

4. Conclusion

The application of the DSS to PWR has a great number of advantages. The inherent self-testing feature and fail-safe design provide a high level of reliability and low spurious trip rate. The software modification makes it possible using more complex trip algorithms.

To meaningfully show how the DSS can replace a current reactor protection system, the verification is needed. Using the KO-RI unit 2 simulator FISA-2, we will verify the correct operation of the DSS implemented in PLC.

Nomenclature

X : input signal reliability

t : time in hours

R_{trip} : system reliability when reactor is in trip state

R_{normal} : system reliability when reactor is in normal state

References

[1] A.B. Keats, "Fail-safe Design Criteria For Computer Based Reactor Protection Systems," *Nuclear Energy*, Vol. 1, No. 6, pp. 423-429, December 1980.

[2] "Programmable Electronic System for Reactor Safety," ATOM 395, September 1989.

[3] B.K. Hajek, D.W. Miller, A. Kauffman, G. Toth, J. Fluhrer, W. Hines, J. Talnagi, C. Strayer, Y. Cai(OSU), G. Adams, P. Harold, I. Smith (AEA Technology, UK), C.D. Wilkinson (EPRI), "Dynamic Safety Systems for BWR Reactor Protection System Replacement," Proceedings of the Ninth Power Plant Dynamics, Control, & Testing Symposium, May 24-26, 1995, Knoxville, TN.

[4] G. Adams, D. Miller, B. Hajek, A. Kauffman, G. Toth, J. Fluhrer, "Emulation of a Dynamic Safety System Reactor Protection System for a US Light Water Reactor," ANS International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human Factor Interface Technologies (NPIC&HMIT'96), May 6-9, 1996, State College, PA.

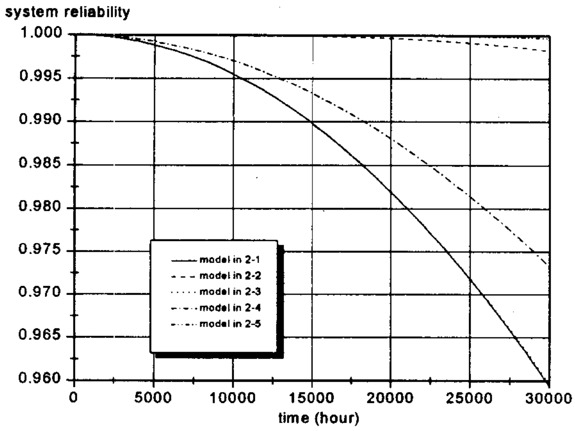

Fig. 7 Reliability when reactor is in trip state

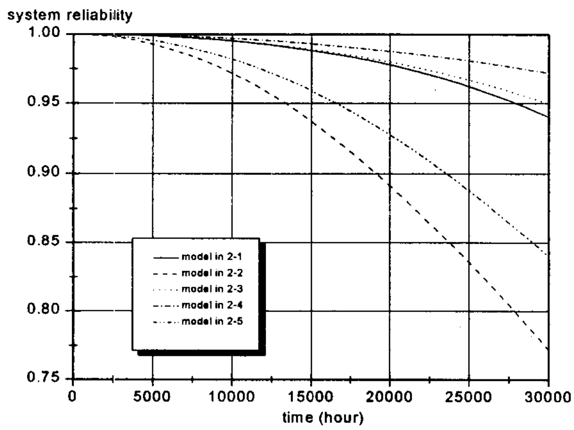

Fig. 8 Reliability when reactor is in normal state