Lifetime Evaluation of Digital Engineered Safety Features Actuation System Using Reliability Block Diagram

Joo Hyun Park, Dong Young Lee, Jong Gyun Choi, Jae Bok Han

Korea Atomic Energy Research Institute,
P.O. Box 105, Yusong, Daejon, 305-600, Korea
Tel. 82-42-868-2923, Fax. 82-42-868-8916
E-mail: joohyun@kaeri.re.kr

Jun Lyou

Chungnam University Electronics CIS Lab,
Goong-Dong 220, Yusong-Gu, Daejon, Korea
E-mail: jlyou@cnu.ac.kr

ABSTRACT

The Digital Engineered Safety Feature Actuation System (DESFAS) of nuclear power plants actuates safety systems to mitigate severe accidents occurred in nuclear power plants. The reliability of the system should be evaluated in order to meet the reliability criteria of nuclear power plants. In this work, we have calculated and evaluated the lifetime of DESFAS by using Reliability Block Diagram (RBD) and failure rates of digital control components. Surveillance test is assumed in the evaluation. The result shows that the digital control component can be used in DESFAS system.

I. Introduction

The DESFAS of nuclear power plants is a very important system because the system actuates safety systems to mitigate severe accidents when these are occurred in nuclear power plants (NPPs). The system requires for a very high reliability and safety. EPRI-URD requires the reliability of instrumentation and control systems in NPPs as follows.

'Mean time between forced outage (MTBFO) caused by failures of MMIS equipment shall be greater than fifty reactor operating years over the entire design life of the MMIS equipment. The meaning of forced outage includes shutdowns that result directly from the failure, and shutdowns the operators must perform to avoid violation of plant Technical Specification due to these failures.'[1]

The system has been implemented with analog components such as a relay, an analog comparator. Recently, the system has been changed to digital components due to an aging problem and lack of a stock of analog components.[2,5] The reliability of digital instrumentation and control (I&C) systems, therefore, should be compared with it of analog I&C system.

The reliability of a system is defined to be the probability that a system will perform a required function without failure under stated conditions for a stated period of time.[3] To develop the highly reliable system, it is imperative that the reliability analysis should be performed over the life cycle of the system including requirement phase, design phase, and implementation phase. The reliability analysis such as failure mode effect analysis (FMEA) and fault tree analysis (FTA) can identify imbalances in the system design and be used as feedback data for improving the system design.[4,5]

The most of the instrumentation and control (I&C) systems implemented in nuclear power plants in Korea were analog technology based systems. It was reported that the number of the forced outages of the plant due to the failure of the I&C system is one time or more per year. The number of the forced outages of the plant can be reduced by the employ of digital technology because the various fault tolerance strategies such as the redundant design, automatic self-diagnosis, and the bypass of the failed component is integrated into the I&C system. For example, the reactor protection system that consists of four channels working on a basis of 2-out-of-4 votes for a reactor trip operates properly if the three channels out of four channels operate properly. If the digital technology is employed for developing the reactor

protection system, the failed channel in the reactor protection system can be detected and repaired more quickly compared with the analog system. Therefore, the number of forced outage of the plant can be substantially reduced. [6]

With consideration of the advanced digital technology, the requirement of 50 operating years for MTBFO was issued for the aspect of utility for stable operation of the reactor without scram caused by an I&C system failure.

Fault Tree Analysis (FTA) has been introduced to quantitatively evaluate the reliability of NPP I&C systems. FTA, however, cannot properly consider the effect of maintenance. In this work, we have reviewed quantitative reliability evaluation techniques and applied the Reliability Block Diagram and failure rates to the evaluation of mean time between failures of DESFAS. In section II, MTBFO calculation models with a periodic maintenance are derived from a RBD model and a Markov chain model. The structure of DESFAS and the results of MTBFO are described in section III and IV respectively.

II. MTBFO of Redundant Systems

1. MTBFO of the repairable duplex system modeled by RBD

A reliability block diagram is a pictorial way of showing the successful operation of a system. The system and its components are assumed to be only in one of two states, good (or UP) and bad (or DOWN). A group of components that are essential for the successful operation of the system (or a specific mission o the system) are drawn in series. Redundant components that can substitute for other components are drawn in parallel. In the block diagrams, the boxes represent the components. The reliability block diagram is not a schematic diagram of the system showing the physical connections, but it is a logical diagram indicating the functional relationships between events such as the successful operation of a system and the satisfactory functioning of its components.

For a repairable component, the probability that the component fails in time period t is as

follows:

$$F(t) = 1 - e^{-\lambda t} \cong \lambda t, \tag{1}$$

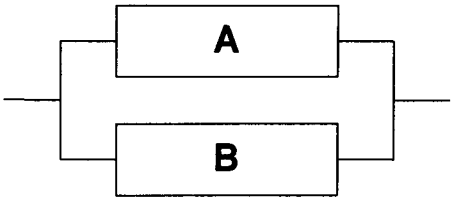


Figure 1. RBD model of Duplex System

where the failure of the component is assumed exponentially distributed and λ is the failure rate of the component. The unavailability of the component is as follows:

$$U_{component} = \lambda(T_D + T_R) + T_I / T_{TI} + T_M / T_{MI}, \tag{2}$$

where λ is operating failure rate, T_D time to detect failure, T_R time to repair failure, T_I time to test component, T_{TI} test interval, T_M time to maintain component, and T_{MI} maintenance interval respectively. Equation (2) can be simplified if it is assumed that there is no periodic test and maintenance. Additionally, if T_D, time to detect failure, is very short, the equation (2) is modified as follows:

$$U_{component} = \lambda T_R. \tag{3}$$

For repairable duplex system as shown in the figure 1, the system failure occurs when, given that the one of the two components is failed, the other component is also failed during the repairs of the failed component. Therefore, the system failure probability is as follows:

$$P_{AB}(t) = U_A\lambda_B t + U_B\lambda_A t \approx \lambda_A T_{RA}\lambda_B t + \lambda_B T_{RB}\lambda_A t \tag{4}$$

If both the components have the same failure rate and repair time, the equation (4) is simplified as follows:

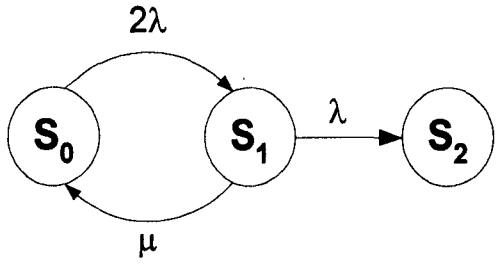
$$P_{AB}(t) = 2\lambda^2 T_R\, t = 2\lambda^2 MTTR\, t \tag{5}$$

Therefore, the failure rate of the repairable duplex system can be approximated as follows:

$$\lambda_{SYS} = 2\lambda^2 MTTR$$

2. MTBFO of the repairable duplex system modeled by Markov Chain

A powerful tool for analyzing complex probabilistic systems is the Markov process model. The two central concepts of such models are the state and the state transition. The state of a system represents all that must be known to describe the system at any instant. A simple model for a component is a Markov model with two states representing the UP state (where the component is functioning satisfactorily) and the DOWN state (where the component has failed and is possibly undergoing repair). In the case of a complex system with a number of components, each state represents a distinct combination of working and failed components. For a system with N components, the number of states is 2^N. As time passes, the system goes from state to state. This change of states is called sate transition.



S_0 Normal state in which both of the two components are functioning properly
S_1 State in which one component has failed
S_2 State in which both of the two components are have failed
λ Failure rate of the component
μ Repair rate of the component

Figure 2. Morkov chain model of repairable duplex system

The Markov chain model of the repairable duplex system is shown in the figure 2. The state of the system is in initial state, S_0, if it is assumed that both of the two components are functioning properly when the system starts initial operation. If the one component of the two components

is failed, the state of the system goes from S_0 to S_1. When the system is in state S_1, the system can go to state S_0 or state S_2. If the failed component is repaired before the failure of the other component, the system goes to state S_0. If during the repairs of the failed component the other component is failed, the state of the system goes from S_1 to S_2. The state S_2 means the failure of the repairable duplex system. Therefore, the failure probability of the system is the probability that the system is in state S_2. On the contrary, the reliability of the system is the probability that the system is in state S_0 or S_1. The each state probability of the system modeled by Markov chain is formalized as the differential equations:

$$\begin{aligned}
\frac{dP_0}{dt} &= -2\lambda P_0 + \mu P_1 \\
\frac{dP_1}{dt} &= 2\lambda P_0 - (\mu + \lambda) P_1 \\
\frac{dP_2}{dt} &= \lambda P_1
\end{aligned} \tag{7}$$

where the P_0 is the probability that the system is in state S_0, P_1 the probability that the system is in state S_1, and P_2 the probability that the system is in state S_2.

Equations (7) are solved as follows:

$$\begin{aligned}
P_0(t) &= \frac{1}{2x}\left[\left\{\lambda - \mu + (\mu - \lambda)xe^{xt}(1+e^{xt})\right\}e^{-\frac{1}{2}(3\lambda+\mu+x)t}\right], \\
P_1(t) &= \frac{2\lambda(e^{xt}-1)e^{-\frac{1}{2}(3\lambda+\mu+x)t}}{x}, \\
P_2(t) &= 1 + \frac{1}{2x}\left[\left\{3\lambda + \mu - (3\lambda+\mu)e^{xt} - x(1+e^{xt})\right\}e^{-\frac{1}{2}(3\lambda+\mu+x)t}\right],
\end{aligned} \tag{8}$$

where $x = \sqrt{\lambda^2 + 6\lambda\mu + \mu^2}$

The reliability of the system is formalized as follows:

$$R(t) = 1 - P_2(t) \tag{9}$$

The mean time to failure is formalized as follows:

$$MTTF = \int_0^\infty R(t)dt = \int_0^\infty (1 - P_2(t)dt = \frac{\mu + 3\lambda}{2\lambda^2} \quad (10)$$

The mean time between failures is formalized as follows:

$$MTBF = MTTF + MTTR = \frac{\mu + 3\lambda}{2\lambda^2} + \frac{1}{\mu} = \frac{\mu^2 + 3\lambda\mu + 2\lambda^2}{2\lambda^2\mu} \cong \frac{\mu}{2\lambda^2} \quad (11)$$

Therefore, the approximated failure rate of the repairable duplex system is as follows:

$$\lambda_{SYS} = \frac{1}{MTBF} \cong \frac{2\lambda^2}{\mu} = 2\lambda^2 MTTR \quad (12)$$

III. DESFAS Description

DESFAS receives initiation signals from Digital Plant Protection System (DPPS) and transmits the output signals to Plant Control System (PCS). The output signal makes equipments operate in order to mitigate the accident in NPP. DESFAS generates the signals to run the following six systems.

- Safety Injection Actuation System
- Containment Isolation Actuation System
- Containment Spray Actuation System
- Recirculation Actuation System
- Main Steam Isolation System
- Auxiliary Feedwater Actuation System

DESFAS is comprised of two independent and redundant trains, train A and train B, of equipments housed in separate auxiliary cabinet. Even if only a train is alive, DESFAS can perform its safety functions. The hardware configuration of each train is shown in Figure 3. Each train is composed of programmable logic controllers (PLCs).

The DESFAS block diagram, which shows the interface between the DESFAS and various

other systems including the DPPS, is shown in Figure 4 for a typical train. DESFAS initiation signals are received from the DPPS by fiber optic receivers (FOR) to maintain channel independence. Each train is composed of two pump processors, two valve processors, one communication and interface processor, two power modules, and devices for a signal transmission as shown in Figures 3 and 4.

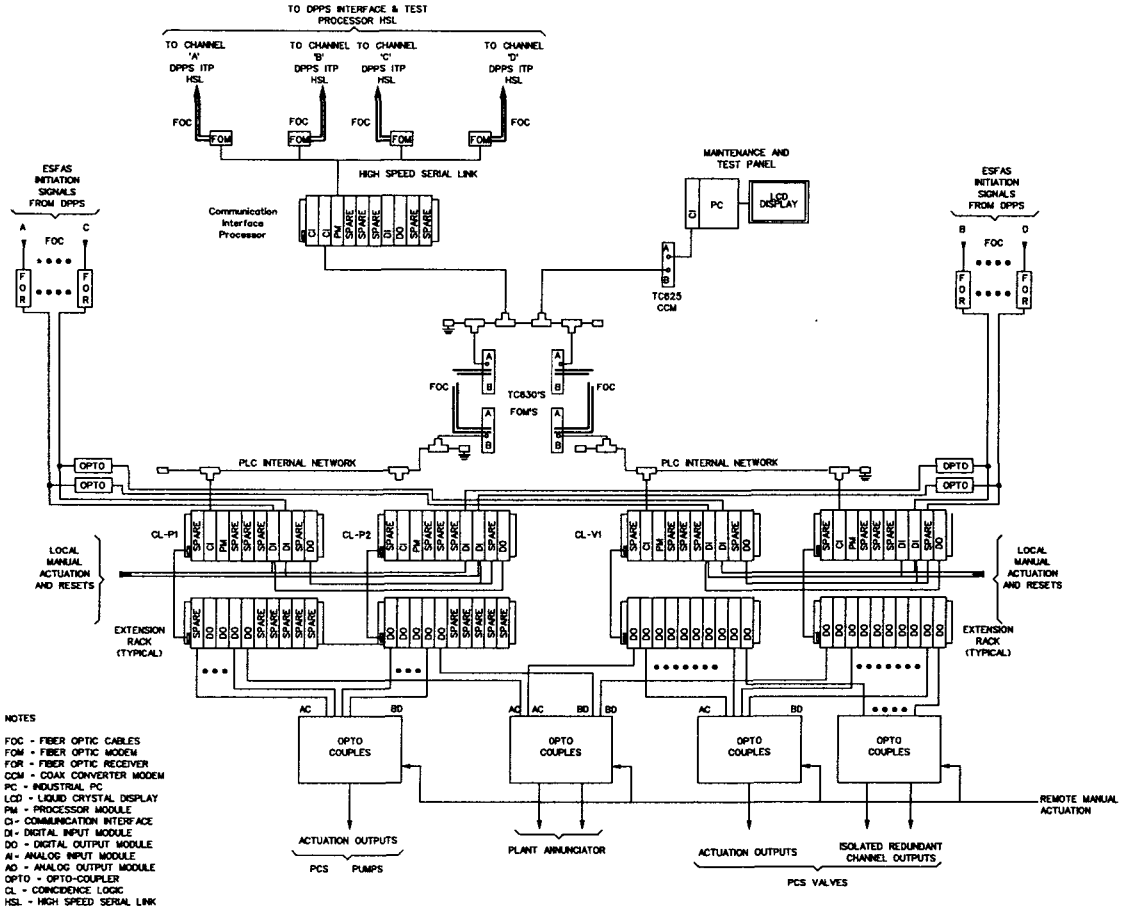


Figure 3. DESFAS Configuration

The initiation signals are distributed so that trip actuation signals for pumps may be processed by one set of PLCs and trip actuation signals for valves may be processed by another set of PLCs. Coincidence logic is implemented in each the sets of PLCs for the pump and the valve actuation.

Each train of DESFAS performs a selective 2 out of 4 logic using 4 signals transferred from 4 DPPS channels. This logic is implemented in each set of controllers for the pump and valve groups. Each set of controllers is composed of two PLCs. In each set, a signal A and a signal C of DPPS is combined using "OR" logic in one PLC and a signal B and a signal D of DPPS is combined using "OR" logic in another PLC. The actuation signal of the pump or the valve is initiated by using "AND" logic with two combined signals generated from each PLC in OPTO Couplers. The initiation signals are transferred to the plant computer system (PCS) and make engineering safety equipments run.

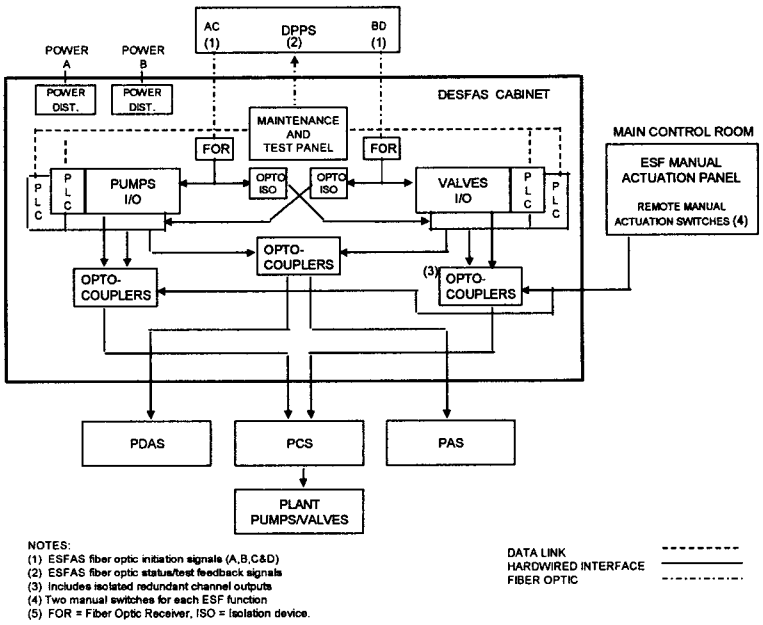


Figure 4. DESFAS Block Diagram

Each PLC operating pumps is put in two racks and has one processor module, one communication module, two digital input modules, six digital output modules, and nine spare modules as shown in Figure 5 (a). The modules related to the generation of DESFAS initiation signals are one processor module, one communication module, two digital input modules, and six digital output modules as shown in Figure 5 (b).

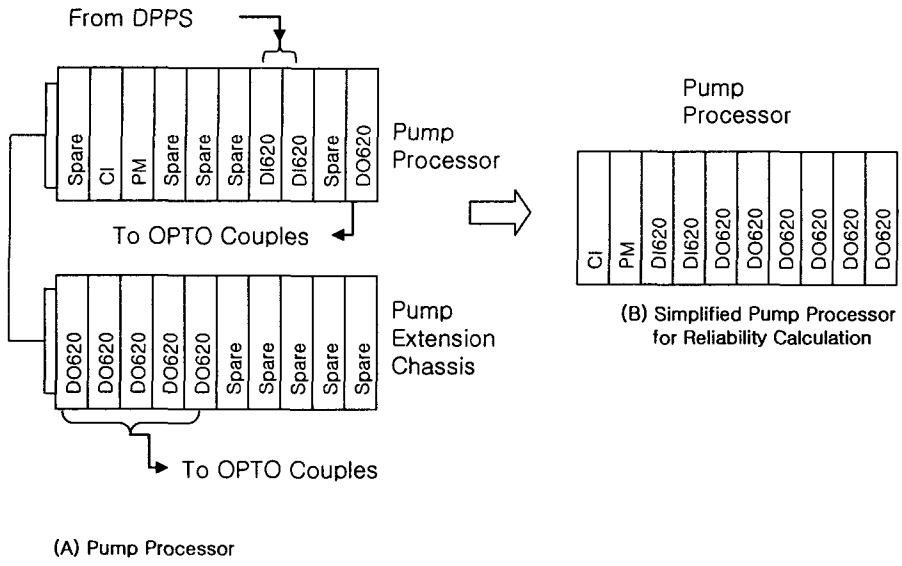


Figure 5. Structure of Pump PLC

Each of PLC to operate valves is put in two racks and has one processor module, one communication module, two digital input modules, eleven digital output modules, and five spare modules as shown in Figure 6 (a). The modules related to the generation of DESFAS initiation signals are one processor module, one communication module, two digital input modules, and eleven digital output modules as shown in Figure 6 (b).

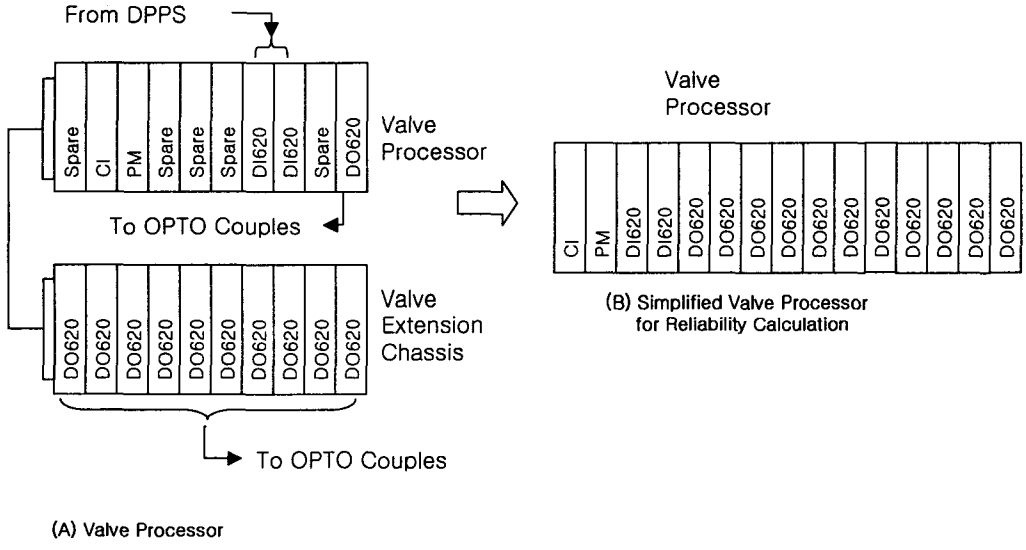


Figure 6. Structure of Valve PLC

IV. RBD of DESFAS

A Reliability Block Diagram is used for assessing the life time of DESFAS. Several assumptions were made for constructing the RBD as follows:

- DESFAS operates properly when both the trains are functioning properly
- DESFAS is comprised of FOR, Valve PLC, Pump PLC and Power supplies
- DESFAS operates properly when both of the valve processor and the pump processor are adequately functioning
- OPTO isolator is not included in the RBD model because the failure rate of the OPTO isolator is very small
- OPTO coupler is not included in the RBD model because the failure rate of the OPTO coupler is very small

The RBD model of the train A in the DESFAS is shown in the Figure 7 and that of the train B has the same architecture. As shown in Figure 7, the RBD of the train A is comprised of signal processing part (Group 1 and Group 2) and power supply part. Due to the each that both of the two parts are essential for proper operation of the DESFAS, two parts are connected in series. The signal processing part is comprised of group 1 and group2. The output signal from train A is transferred correctly to PCS if either modules in the group 1 or modules in group2 are properly functioning. Therefore, modules group 1 and modules in group 2 are connected in parallel. The modules in group 1 (FOR A, FOR C, Valve PLC 1 and Pump PLC 1) are connected in series one another because the modules in channel A and the modules in channel C are essential for the proper operation of the group 1. The modules in group 2 (FOR B, FOR D, Valve PLC 2 and Pump PLC 2) are also connected in series one another due to the same reason as the group 1. Because the train is provided with the duplex power supplies, two power supplies are connected in parallel in the RBD model.

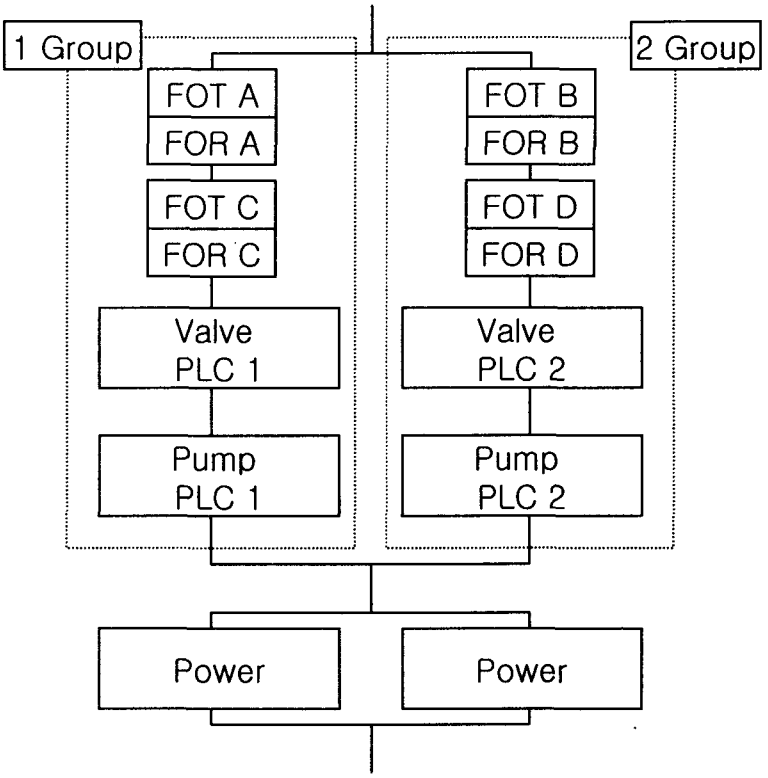


Figure 7. RDB of DESFAS

V. MTBFO of DESFAS

In order to evaluate the MTBFO of DESFAS, the authors used the failure rate data of AC160 PLC, which was applied to DESFAS in Ulchin 5&6 nuclear power plants in Korea. The component failure data of DESFAS is shown in table 1. As mentioned in the previous section, the DESFAS is composed two trains that are connected in serial. One train of DESFAS can be decomposed in three parts, 1-group, 2-group, and a power part. The components in 1-group or 2-group are joined in serial. So, the failure rate of 1-part or 2-part, λ_{1or2}, is calculated as follows:

$$\lambda_{1or2} = 4 \times \lambda_{FO} + \lambda_{VL} + \lambda_{PP}$$

where, λ_{FO} is the failure rate of a fiber optic transmitter (FOT) or a fiber optic receiver (FOR), λ_{VL} is the failure rate of a valve-PLC, and λ_{PP} is the failure rate of a pump-PLC.

Because 1-group and 2-group are connected in parallel as shown in Figure 7, a failure occurs in one group, the whole system is not affected by the failure if another group operates normally

during the repair of the failed group. Thus, the combination failure rate of two groups, λ_{1and2} is calculated as follows:

$$\lambda_{1and2} = {}_2C_1 \times \lambda_{1or2} \times \lambda_{1or2} \times MTTR = 2 \times \lambda_{1or2}^2 \times MTTR$$

where MTTR is a mean time to repair.

Each train of DESFAS uses the redundant electric power supply systems. When one power system operates normally, the electric power is supplied normally in a train even if one power supply system fails. The failure rate of whole electrical power system, λ_P is calculated as follows:

$$\lambda_P = {}_2C_1 \times \lambda_{PW} \times \lambda_{PW} \times MTTR = 2 \times \lambda_{PW}^2 \times MTTR$$

where λ_{PW} is the failure rate of one power supply system.

The failure rate of one train, λ_{Train}, is sum of λ_{1and2} and λ_P. Two trains of DESFAS is connected in serial. The failure rate of DESFAS, therefore, is calculated as follows:

$$\lambda_{DESFAS} = 2 \times \lambda_{Train} = 2 \times (\lambda_{1and2} + \lambda_P)$$

As mentioned before, we use the failure rate data of the Advant 160 PLC, which was applied to DPPS and DESFAS of Ulchin NPP 5&6 in Korea, and 8 hour at MTTR because the time is required in Electric Power Research Institute-User Requirement Document.

The failure rate of the system is calculated as follows.

$$\lambda_{1or2} = 4 \times \lambda_{FO} + \lambda_{VL} + \lambda_{PP} = 1.87E-04/hour$$

$$\lambda_{1and2} = {}_2C_1 \times \lambda_{1or2} \times \lambda_{1or2} \times MTTR = 2 \times \lambda_{1or2}^2 \times MTTR = 5.59E-07/hour$$

$$\lambda_P = {}_2C_1 \times \lambda_{PW} \times \lambda_{PW} \times MTTR = 2 \times \lambda_{PW}^2 \times MTTR = 2.69E-10/hour$$

$$\lambda_{DESFAS} = 2 \times \lambda_{Train} = 2 \times (\lambda_{1and2} + \lambda_P) = 1.12E-06/hour$$

The failure rate of the system which is composed of many components is assumed to have an exponential distribution. The MTBFO is derived from reciprocal number of the failure rate if this assumption is applied to it. Therefore, MTBFO of DESFAS, therefore is calculated as

follows.

$$MTBFO_{DESFAS} = \frac{1}{\lambda_{DESFAS}} = \frac{1}{1.12E-06} = 8.94E5[Hour] = 102.1[Year]$$

As a result, the MTBFO of DESFAS is 102 years. The detail failure rates and MTBFOs of DESFAS are shown in Table 1.

Table 1. Detail failure rate and MTBFO of DESFAS

Description	Part No.	Module Number	Failure Rate /Module	Failure Rate	Unit
(Fiber Optic)					
Fiber Optic Transmitter/Receiver		1	1.23E-05	1.23E-05	
(Pump Logic)					
Processor	PM645	1	9.07E-06	9.07E-06	
Digital Input	DI620	2	2.51E-06	5.02E-06	
Digital Output	DO620	6	6.10E-06	3.66E-05	
Communication Interface	CI532	1	2.90E-06	2.90E-06	
Failure Rate of Single PLC Rack				5.36E-05	
(Valve Logic)					
Processor	PM645	1	9.07E-06	9.07E-06	
Digital Input	DI620	2	2.51E-06	5.02E-06	
Digital Output	DO620	11	6.10E-06	6.71E-05	
Communication Interface	CI532	1	2.90E-06	2.90E-06	
Failure Rate of Single PLC Rack				8.41E-05	
(Faliure Rate of an ESFAS Cabinet W/O Power)					
Failrue Rate of 4 FO, 1 Pump, 1 Valve Logic				1.87E-04	
Failrue Rate of an ESFAS Cabinet without Power module				5.59E-07	
(Power)					
Power Supply(Switch)	SA610	1	4.10E-06	4.10E-06	
Failure Rate of Power Supply				2.69E-10	
(Total Failure Rate)					
Total Failure Rate of an ESFAS Cabinet				5.59E-07	
Total Failure Rate of ESFAS Cabinets				1.12E-06	
(MTBF of ESFAS)					
MTBF of ESFAS Cabinet(Hour)				8.94E+05	Hour
MTBF of ESFAS Cabinet(Year)				102.1	Year

V. Conclusion

The authors have analyzed the DESFAS of Ulchin 5&6 nuclear power plants in Korea and applied component failure rate data of the plants in order to calculate MTBF of the system. We assumed the repair time of DESFAS is 8 hour, which is the minimum time Electric Power Research Institute User Requirement Document (EPRI-URD) requires.

As a result of calculations, the MTBF of DESFAS is about 102 year and it satisfies the 50 year

requirement of EPRI-URD. The result shows that the digital control component can be used in DESFAS system.

References

[1] "Advanced Light Water Reactor Utility Requirements Document", Vol. II, Chapter 10, EPRI, 1990.

[2] N0696-IC-DS564"Design Specification for DESFAS for Ulchin NPP Init 5&6"

[3] Reliable Computer System (Design and Evaluation), Daniel P. Siewiork and Robert S. Swarz, 1998.

[4] 2005842-IC-FM564-30, "Failure Mode and Effects Analysis for DESFAS for Ulchin NPP 5&6"

[5] ST-99-231, "Unavailability Analysis for the Digital Plant Protection System"

[6] KAERI/TR-2047/2002, "Technical Report on Reliability Assessment of the Digital I7C Equipment Using Reliability Block Diagram"