Reliability Analysis of Nuclear Safety-Class DCS ESFAS Based on FTA

Xu Zhang[1(✉)], Hao Peng[1], Shi-Man Feng[1], Jing-Hua Yang[2], and Shi-Yong Chen[1]

[1] Science and Technology on Reactor System Design Technology Laboratory, Nuclear Power Institute of China, Chengdu 610213, China
zhangxu020354@foxmail.com

[2] PowerChina Sichuan Electric Power Engineering Co., Ltd, Chengdu 610041, China

Abstract. Nuclear safety-class DCS realizes reactor safety protection function, which is directly related to the safe and stable operation of nuclear power plants, so its reliability should be analyzed and optimized. In this paper, the engineered safety features actuation system in nuclear safety-class DCS is analyzed through the control instruction logic flow involved in the structure, according to the components of the series and parallel or voting logic and other logical relations to bulid a fault tree model. Using fault tree model, the reliability degradation trend is obtained, and the minimum cut set, importance degree and other parameters are quantitatively calculated. According to overhaul cycle of nuclear power plant, a maintenance optimization method for engineered safety features actuation system is proposed, and some optimization suggestions are given.

Keywords: FTA · Nuclear Safety-class DCS · Reliability · Quantitative analysis

1 Introduction

Nuclear safety-class DCS in nuclear power plant mainly realizes important functions such as reactor tripping, engineered safety features driving. It is used to ensure the intactness of reactor fuel envelope, reactor coolant loop pressure and safety hulk, and thus the power plant is in a safe state. When the operation parameters of the power plant reach the reading value set by the reactor protection system, the emergency shutdown of the reactor can be triggered safely and reliably, and special safety facilities can be operated when necessary. It can be seen that the reliability of DCS directly affects the safety of the reactor.

Nuclear safety-class DCS typically consists of reactor tripping system (RTS), engineered safety features actuation system (ESFAS), Priority actuator control system (PACS), Gateway system (GW) and maintenance system, et al. Among them, ESFAS and PACS jointly realize safety injection, containment isolation, containment spray, main feed water isolation, main steam isolation, auxiliary feed water start-up and other special functions.

ESFAS generates driving instructions and sends them to PACS. Through the selection logic inside PACS, the driving instructions are finally output to drive the local equipment. ESFAS contains two diverse sub-groups, and the driving instructions of two sub-groups are logical “OR” in PACS.

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 257–268, 2023.
https://doi.org/10.1007/978-981-99-3455-3_25

2 Research Object and Research Status

2.1 Research Analysis

With the improvement of digitization degree of instrument and control (I&C) system in power plant, reliability research of I&C system has gradually become a research hotspot. In literature [1], for the structure of DCS basic components in the thermal power plant, Markov method was adopted to analyze the transition relationship of system space and influence of component repair rate on system reliability. In literature [2], nuclear safety-class DCS was taken as the object to bulid a fuzzy fault tree (FT) model and analyze its reliability parameters, and DCS module level was taken as the research object, however, system level was not analyzed. Literature [3] lists the important reliability parameters of DCS and their calculation methods, and puts forward the parameter verification method of "model + test + evaluation". In view of the fact that the traditional fault tree analysis (FTA) method cannot describe the dynamic interaction during the operation of the I&C system, Dynamic Flowgraph Methodology was used in literature [4] to analyze the sensor failures, output latching device and hot MPU failure, and hot-standby MPU failures of nuclear safety-class DCS. In literature [5], Petri net was used to analyze the influence of periodic tests and maintenance on the reliability of the reactor protection system, and it was verified that Petri net could be well applied to the reliability assessment of the reactor protection system. In this paper, based on the above researches, the reliability analysis of nuclear safety-class DCS ESFAS is carried out.

2.2 Structural Analysis

Generally speaking, in nuclear safety-class DCS, RTS consists of 4 channels (I/II/III/IV), each channel contains two diverse sub-groups. ESFAS consists of two logical trains A/B, each train contains two diverse sub-groups. PACS system receives drive instructions from ESFAS and hardwiring signals from ECP/BUP (emergency control panel/backup panel), DAS (diverse actuation system), NC (non-classified) DCS and other systems, and drives field equipment after selecting the priority logic. The brief architecture diagram of safety-class DCS is shown in Fig. 1.

In main feed water isolation function of train-A sub-group 1 (ESFAC-A1), the control instruction of TFM031VL of main feed water loop 1# steam generator (SG1) is taken as an example. ESFAC-A1 receives local tripping signal from four channels of RTS and take 2 out of 4 logic, and then takes "OR" logic with other logic, and output the driver instruction of TFM031VL. A brief logic diagram is shown in Fig. 2.

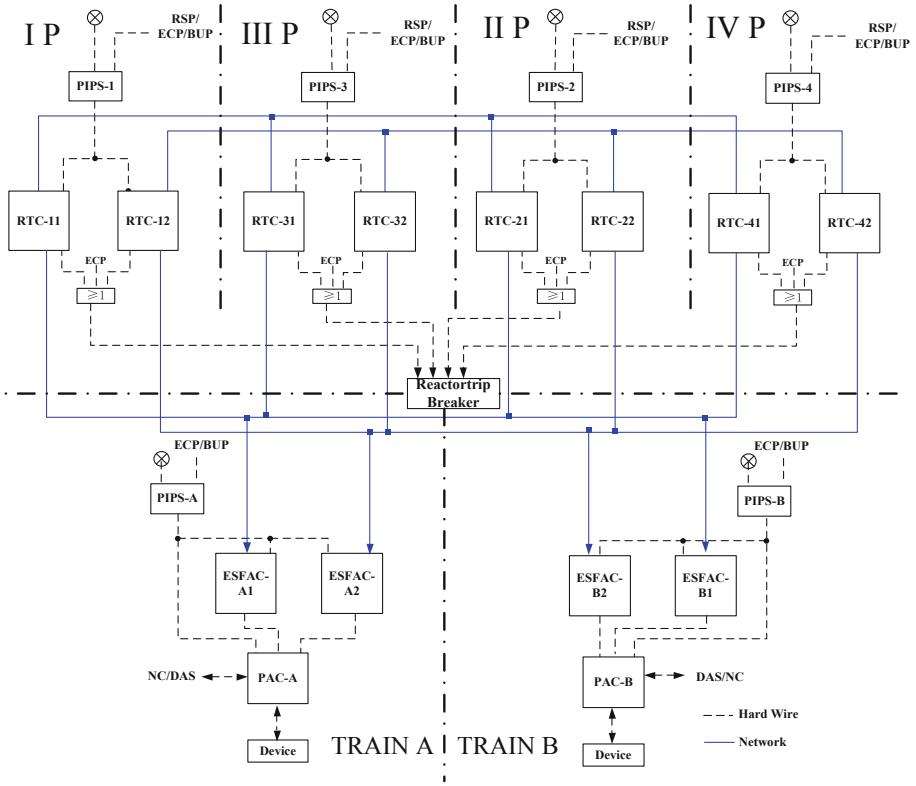

Fig. 1. Schematic Diagram of Safety-class DCS

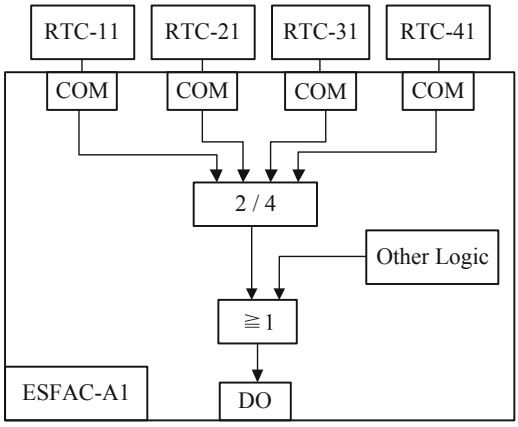

Fig. 2. Logic Diagram of TFM031VL Close Driver Command

3 ESFAS System Reliably Model

3.1 FTA Method

FT is a special logical causality diagram of inverted tree. FTA takes a product failure event as the top event, through top-down in strict accordance with the level of fault causal logic analysis, find out a proximate cause of the failure event of necessary and sufficient step by step to draw the FT, finally all possible causes and combination of causes leading to occurrence of the top event can be found out, and the probability of top event and the importance degree of bottom events can be calculated when basic data is available. The FT analysis method has a good ability to describe and express the internal structure relations and organizational level of the analyzed object. FT usually uses logic such as "AND" gate, "OR" gate to describe the relationship between events, and determine the calculation expression from bottom to top according to the relationship. The bottom event is usually selected with a clear reliability model and known reliability parameters, and the probability of the event is calculated layer by layer based on the reliability parameters of the bottom events. FTA is widely used in various industrial fields due to its clear expression and strong expansibility [6].

3.2 Reliably Parameters Calculation Method

MTBF (Mean Time Between Failure) refers to the average time for a product or system to work correctly within the interval between failures, which is a commonly used reliability calculation parameter for repairable products. The main components of nuclear safety-class DCS are electronic products, and the life distribution can adopt the general analysis method of electronic products, which is generally considered to conform to the exponential distribution. The failure rate can be expressed as the formula (1).

$$\lambda = \frac{1}{MTBF} \tag{1}$$

Product reliability R(t) can be expressed as formula (2) [7].

$$R(t) = e^{-\lambda \times t} = e^{\frac{-t}{MTBF}} \tag{2}$$

Thus, the trend of the reliability of the analyzed object with time can be obtained.

3.3 FT Model

The TFM031EL1 instruction realized by control station ESFAC-A1 must meet the requirements of normal operation of communication, MPU and output module. Among them, the communication takes 2 out of 4 configuration, each channel has two communication modules redundancy, and MPU takes hot-standby redundancy mode. The architecture is as shown in Fig. 3.

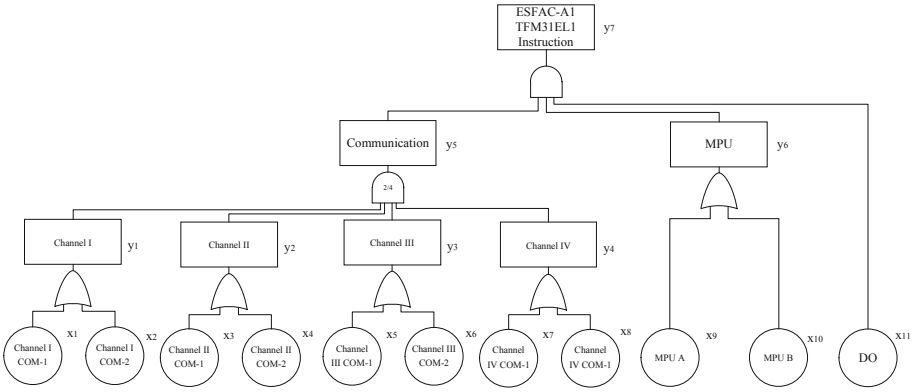

Fig. 3. Logic Diagram of TFM031EL1 Instruction in ESFAC-A1

According to the instruction analysis, the top event (y7) was recorder as the TFM031EL1 instruction failure event of ESFAC-A1. The bottom events are the failure of various components, including hot-standby MPU, redundant COM modules, DO module. For the station ESFAC-A1, the bottom events are denoted as x1–x11 respectively, and the corresponding component number of ESFAC-A2 is similarly calculated. The redundant COM modules in each channel constitute the communication failure, which is denoted as event y1–y4; At least two of the four channels are required to be in normal operation, that is, communication fault y5 is the result of 3 out of 4 voting (y1–y4); The hot-standby MPU take redundant relationship, and MPU fault event is denoted as y6; Communication fault, MPU fault and DO fault together constitute the top event ESFAC-A1 TFM031EL1 command failure, which is denoted as y7. For fault of redundant system, "AND" gate is used to represent the relationship between upper and lower layers, such as single channel communication failure. For series system faults, "OR" gate is used for to represent the relationship between upper and lower layer, such as single cabinet control command failure event.

Based on the above analysis, the TFM031EL1 instruction failure FT model is shown in Fig. 4.

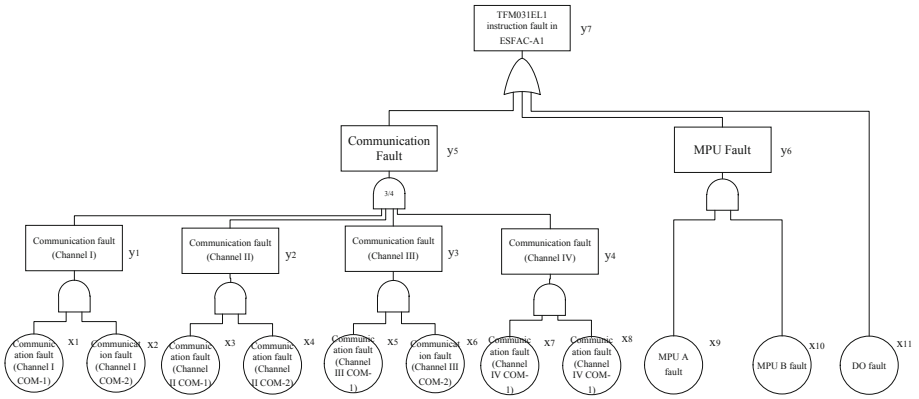

Fig. 4. FT Model of TFM031EL1 Instruction Fault in ESFAC-A1

4 Simulation Experiment

4.1 Reliability Parameter Calculation

The components involved in the case include the MPU, COM module and DO module. The specific module parameters and MTBF are shown in Table 1.

Table 1. Equipment Model and failure rate (λ)

Component Name	Component Cate-gory	λ
MPU	SAMC31	1226.4×10^{-9}
COM	SACO31	825.1×10^{-9}
DO	SADO21	1875.9×10^{-9}

It can be obtained from formula (2) that the reliability functions of MPU, COM and DO are as shown in formula (6)–(8).

$$R_{MPU} = e^{-1226.4\times10^{-9}\times t} \tag{6}$$

$$RCOM = e^{-825.1\times10^{-9}\times t} \tag{7}$$

$$R_{DO} = e^{-1875.9\times10^{-9}\times t} \tag{8}$$

Thus, the function of reliability decay over time of the above components was obtained, and the reliability decay curves of MPU, COM, and DO module were further obtained, as shown in Fig. 5.

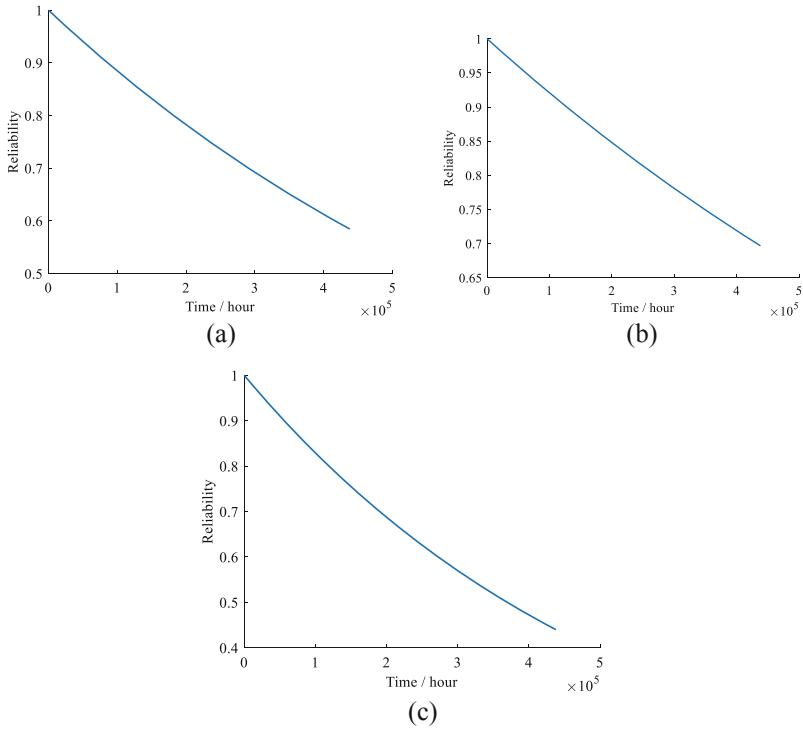

Fig. 5. Simulation Results of Equipment Reliability

The reliability of all kinds of components generally shows a declining trend over time. According to the figure, DO is the weakness of reliability parameters in various components.

4.2 Sub-system and System Reliability Simulation Analysis

Combined with the TFM031EL1 instruction failure FT model, the simulation results of channel communication (I–IV) reliability is analyzed as shown in Fig. 6(a), communication sub-system as shown in Fig. 6(b), and MPU redundant system as shown in Fig. 6(c).

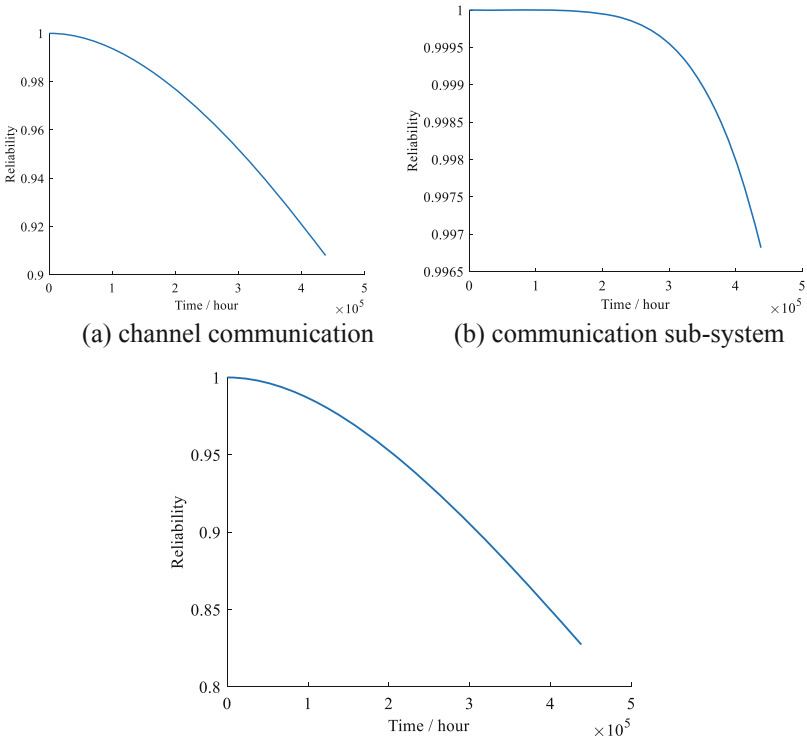

Fig. 6. Simulation Results of Sub-system Reliability

Based on the above analysis, the reliability variation of the command in ESFAC-A1 control station can be obtained, which is as shown in Fig. 7 (Table 2).

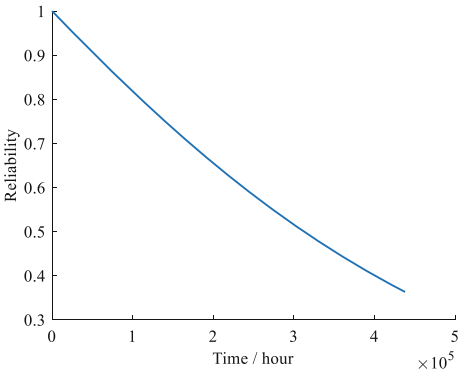

Fig. 7. Simulation Results of Single Control Station Reliability

Table 2. Deterioration of Reliability

Reliability	Time
0.8	110300 h (12.59 years)
0.9	53900 h (6.15 years)
0.95	26700 h (3.05 years)

4.3 Minimum Cut Set and Importance Analysis

4.3.1 Minimum Cut Set Analysis

One of the purposes of FTA is to find out the path or mechanism of event occurrence, so as to put forward optimization methods and take optimization measures. In order to perform this work more efficiently, minimal cut set solution is required. Minimum cut set is one of the basic concepts of reliability statistics. It is the set of bottom events that lead to top event. The occurrence of a group of bottom events (fundamental events) in the FT can cause top event is called the minimum cut set.

The minimum cut set of TFM031EL1 instruction FT model can be transformed into a reliability block diagram, so that the six minimum cut sets leading to top event include: channel I/II/III/IV fault (3 out of 4); MPU A and B fault; DO fault.

The minimum cut set of TFM031EL1 instruction FT and its probability of occurrence in one year of operation are shown in Table 3.

Table 3. Minimum Cut Set and Probability

Number	Minimum Cut Set	Probabilistic (8760 h)
1	$X_1, X_2, X_3, X_4, X_5, X_6$	1.434271E-13
2	$X_1, X_2, X_3, X_4, X_7, X_8$	1.434271E-13
3	$X_1, X_2, X_5, X_6, X_7, X_8$	1.434271E-13
4	$X_3, X_4, X_5, X_6, X_7, X_8$	1.434271E-13
5	X_9, X_{10}	0.0001151
6	X_{11}	0.016372

4.3.2 Minimum Cut Set Analysis

Nuclear safety-class DCS components are not equally important, in order to facilitate the improvement of system design and maintenance strategy, the concept of importance degree is introduced. In this paper, the probability importance degree of the bottom events of TFM031EL1 instruction is analyzed as an example.

Probabilistic importance is defined as the improvement of system unreliability when a component changes from failure state to normal state.

$$F_{Sys}(F_i = 1) - F_{Sys}(F_i = 0) = \Delta F \tag{9}$$

where i is the number of each component in a minimum cut set, ΔF is probabilistic importance, F_{Sys} is unreliability of the system.

The reliability function of each component is known. Thus, the probabilistic importance of each component can be obtained through calculation, as shown in Table 4.

Table 4. Minimum Cut Set and Probability

Event Name	Probabilistic Importance
MPU A fault	153.580514206704
MPU B fault	153.580514206704
Communication fault (Channel I COM-1)	227.855319902543
Communication fault (Channel I COM-2)	227.855319902543
Communication fault (Channel II COM-1)	227.855319902543
Communication fault (Channel II COM-2)	227.855319902543
Communication fault (Channel III COM-1)	227.855319902543
Communication fault (Channel III COM-2)	227.855319902543
Communication fault (Channel IV COM-1)	227.855319902523
Communication fault (Channel IV COM-1)	227.855319902523
DO fault	100.69223305001

4.3.3 Failure Probability Calculation

The bottom events are calculated step by step according to the logical relationship in FT. The calculated probability of events y_1–y_4, y_5, y_6, y_7 occurring within 8760 h are shown in Table 5.

Table 5. Minimum Cut Set and Probability

Event Name	Probability (8760 h)
ESFAC-A1 TFM031EL1 instruction fault	0.016485332395091
Communication fault	5.73685870712446E-13
Output fault	0.000115218756
Communication fault (Channel I)	5.2345225E-05
Communication fault (Channel II)	5.2345225E-05
Communication fault (Channel III)	5.2345225E-05
Communication fault (Channel IV)	5.2345225E-05

4.4 Control Station Redundancy Design

It is obvious from the reliability decline curve that the reliability decline rate is faster in the early period of use. In order to further improve the system reliability, the same logic is designed in ESFAC-B1, and two output take "OR" logic to achieve logic redundancy and improve system reliability.

Similar to previous analysis, reliability analysis was conducted for the control system composed of ESFAC-A1 and ESFAC-B1, and the results are shown in Fig. 8.

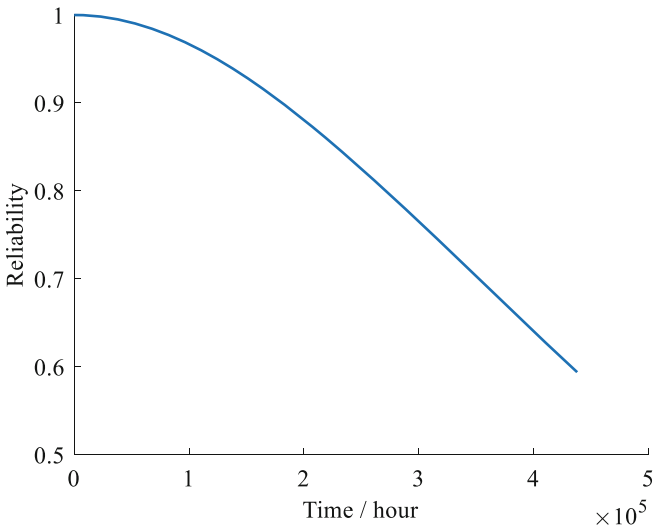

Fig. 8. Control Station Reliability

The decline of system reliability over time is shown in Table 6.

Table 6. Deterioration of Reliability

Reliability	Time
0.8	271300 h (30.97 years)
0.9	181000 h (20.66 years)
0.95	124100 h(14.17 years)

4.5 Maintenance Scheme Optimization

Combined with the above analysis and the actual situation of nuclear power plants, whose typically undergo an 18-month overhaul cycle, the maintenance solution is optimized. In order to maintain the reliability of the system above 0.95, combined with the above

calculation results, the equipment involving TFM031EL1 instruction should be repaired at least once in 9 overhauls (Fig. 9).

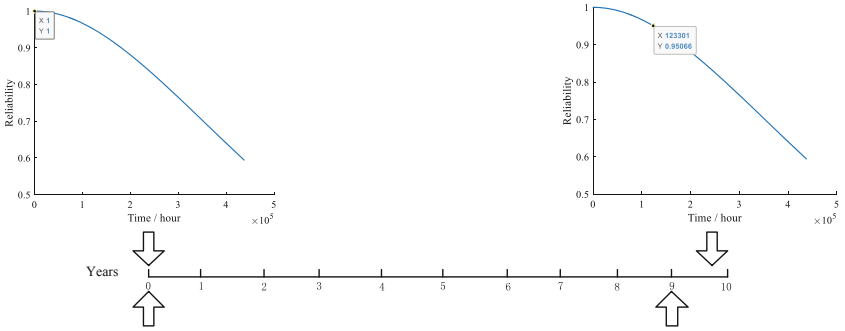

Fig. 9. Schematic Diagram of System Maintenance Scheme Optimization

Similarly, if the reliability requirement is to be improved and the output instruction of single control station is still 0.95, then at least, maintenance shall be performed once in every two plant overhauls.

5 Conclusion

In the paper, the reliability of nuclear safety-class DCS ESFAS is analyzed. Taking TFM031EL1 instruction as an example, the FT method is used and the reliability decline curve with time of different levels and nodes is obtained. Based on the minimum cut set, probability importance and other parameters, the weakness of system reliability is quantitatively analyzed. Combined with the actual situation of nuclear power plant overhaul, the optimization scheme of system maintenance is put forward, and it is also useful for the reliability analysis of other similar control loops in nuclear safety-class DCS.

References

1. Niu, Y., Ma, J., Xia, M., et al.: Reliability modeling and quantify calculation of DCS basic control unit. J. Electron. Meas. Instrum. **25**(6), 506–511 (2011)
2. Zeng, L., Wu, Z., Liu, Z., et al.: A new method for reliability analysis of DCS system output module in nuclear power plants. Ordnance Ind. Autom. **40**(1), 55–59 (2021)
3. Feng, X., Dong, Z.: Typical life and reliability parameters of DCS for nuclear powers. Qual. Reliab. **2020**(3), 35–39, 44 (2020)
4. Zhou, S., Wang, H., Tian, C.: Dynamic flowgraph methodology used in reliability analysis of digital instrumentation and control system in NPP. Nucl. Sci. Eng. **38**(1), 88–98 (2018)
5. Cao, X., Xiong, H., Guo, C., et al.: Dynamic reliability modeling and analysis for reactor protection system. Process Autom. Instrum. **40**(6), 6–10 (2019)