Analysis for Periodic Test Interval of Digital I&C System for NPP Based on PSA Technology

Sun Wei(✉) and Li-Ming Zhang

State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment,
China Nuclear Power Engineering Co., Ltd., Shenzhen 518172, China
sunw@cgnpc.com.cn

Abstract. At present, digital control technology is widely used in safety I&C system of nuclear power plant. In addition to improving the self-diagnosis coverage of the equipment to increase the reliability of the system, periodic tests are also widely used, but how to determine the test interval of the safety I&C system in theory has gradually become a new research direction. Base on this, this article models the periodic test interval from the beginning of design and combines with the PSA technology by analyzing the initial events of a typical NPP, and integrates it into plant PSA models. Through the analysis of calculation results, the weakness of the test interval is identified and the improvements are given. After that a set of design process for periodic test interval are summarized and ultimately enhance the overall safety and reliability objectives of NPP.

Keywords: PSA · Reliability · Periodic test interval · Digital control technology

1 Introduction

PSA technology is a safety evaluation method based on probability theory and risk assessment. It identifies and analyzes unexpected faults, abnormalities or consequences in the system operation process, and carries out risk analysis and evaluation on this foundation. PSA method is one of the two safety analysis methods for nuclear power plants (deterministic theory and probability theory). Its advantage lies in analyzing the relationship and interaction between various factors, which can quantitatively evaluate the safety of nuclear power plants and identify the weak links in the design, construction and operation of nuclear power plants.

PSA evaluation is divided into two aspects, namely, analyzing the frequency of unwanted events and the consequences of unwanted events. The result of both frequency and consequence is risk. For nuclear power plant, such undesirable events refer to core damage, radionuclide leakage into the environment, public casualties and property losses. Different from the deterministic analysis method, probabilistic safety assessment is a systematic analysis method. The input of this analysis is as real information as possible about power plant design, operation practice, personnel behavior, and component reliability, physical process of core damage, Containment behavior and environmental conditions. The foundation of this analysis is probability theory, and the output of

Y. Xu et al. (Eds.): SICPNPP 2020, LNEE 779, pp. 551–562, 2021.
https://doi.org/10.1007/978-981-16-3456-7_53

this analysis is the probability and consequence of various accident sequences, various radioactive material releases and various health effects [1].

IAEA has also played an important role in the research and promotion of PSA. PSA has been implemented for different reactor types, and the development and application of PSA technology have been systematically studied. IAEA has put forward requirements for the implementation of PSA auxiliary system design: PSA requirements are described in NS-R-1 [2]: "When Safety Analysis is carried out on unit design, both deterministic analysis method and probability analysis method shall be used. Then take this analysis as foundation to formulate and verify the design basis for safety important items." After that, PSA was taken as part of the decision-making process in NS-G-1.2 [3], and the following requirements were put forward: PSA results should be taken as part of the design process to evaluate the safety level of the unit.

The key technology of Digital Control System in Nuclear Power Plant is the "nerve center". It provides more advanced control and management methods and is an important equipment to ensure the safe and reliable operation of the nuclear power plant. From design to manufacture, the system needs to meet the requirements of reliability, security, system complexity, interface processing and other aspects, and integrates many technologies such as computer, communication, display and control. Traditionally, in the design stage, the reliability of the I&C system is only improved by improving the reliability of DCS equipment, such as the manufacturing level of process equipment, software and hardware identification level, Quality Assurance, etc. During the operation phase, the high reliability of the equipment is ensured through the periodic test. How to calculate and analyze the system reliability and periodic test interval on this foundation through quantitative evaluation method is somewhat different from the mainstream requirements in the world.

Based on this, this paper is oriented to engineering practice application. Through PSA method, the equipment reliability data and periodic test period are coordinated. Through quantitative reliability numerical calculation, the periodic test interval of safety I&C system is calculated, and the design scheme is improved or optimized to enhance the overall safety goal of Nuclear Power Plant. On this foundation, a set of Nuclear Power Plant digital I&C Periodic Test interval design method based on PSA technology is explored to meet the needs of subsequent engineering practice.

2 Overview of PSA Technology

According to the classification of research levels, PSA is usually divided into 3 levels. The purpose of the first-level PSA is to calculate the core damage probability (CDF). Core damage refers to "the Reactor core is exposed and heated to the extent that long-term cladding oxidation or serious fuel damage is expected to occur, and the core part involved is sufficient to cause large radioactive release". The secondary PSA is based on the foundation of the analysis results of the primary PSA to study the accident process and Containment response after the core is damaged, and to evaluate the release amount and frequency of various radionuclides to the environment. Three-level PSA further studies the diffusion of radioactive substances in the environment and estimates its impact on public health and social environment [4].

The scope of discussion in this paper is level 1 PSA, which explains the analysis process, basic framework and elements of probabilistic safety assessment in the application of Nuclear Power Plant [5] (Fig. 1):

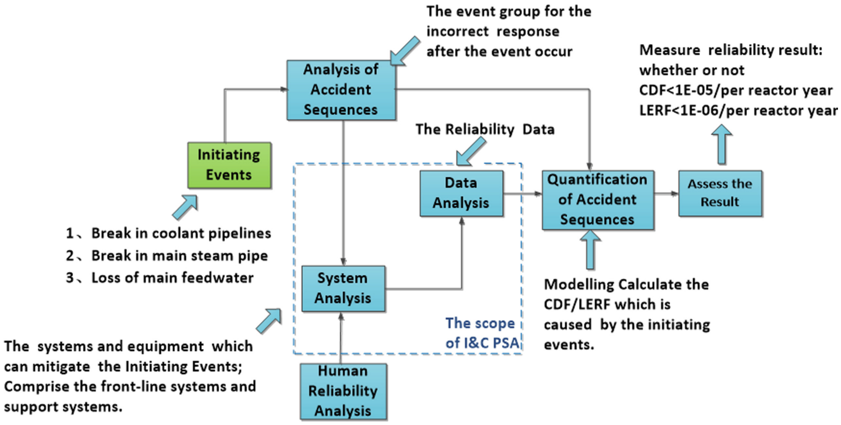
The event group for the incorrect response after the event occur
Analysis of Accident Sequences
Measure reliability result: whether or not CDF<1E-05/per reactor year LERF<1E-06/per reactor year
The Reliability Data
Initiating Events
Data Analysis
Quantification of Accident Sequences
Assess the Result
1、Break in coolant pipelines
2、Break in main steam pipe
3、Loss of main feedwater
System Analysis
Modelling Calculate the CDF/LERF which is caused by the initiating events.
The scope of I&C PSA
The systems and equipment which can mitigate the Initiating Events; Comprise the front-line systems and support systems.
Human Reliability Analysis

Fig. 1. General process of level1 PSA for NPP digital I&C

1) Initial event analysis: identify events that may lead to Nuclear Power Plant anomalies and require successful response from Nuclear Power Plant equipment and personnel to prevent core damage;
2) Success Criteria Analysis: Determine the minimum requirements for each Safety Function (and the system used to perform these functions) required to prevent core damage after the initiation event occurs;
3) Accident sequence analysis: modeling different event processes (event sequences) that successfully mitigate or cause core damage after the event occurs in time sequence (event tree model);
4) System analysis: Determine various failure combinations that may cause the system to fail to perform its functions. The model includes hardware, instrument and human failure events that may lead to system failure. The development of events should be detailed enough to take into account various correlations (fault tree model);
5) Data analysis: Evaluating the frequency of originating events, equipment failure probability;
6) Personnel reliability analysis: identifying and quantifying human error events and their probability under accident conditions;
7) Quantify the accident sequence: calculating the total CDF accord to the CDF obtained by each originating event category;
8) Analysis results: Identify the main contribution categories (qualitative plus quantitative) classified by originating events, accident sequences, equipment failures and human error events.

Compared with the traditional deterministic method, PSA method has the following characteristics [6]:

a) PSA not only studies the physical phenomenon, process and consequences after the occurrence of an event, but also carries out quantitative evaluation of risks on this basis;
b) In the analysis of PSA, a variety of complex correlations among systems, equipment and personnel that exist in the design are considered;
c) In the PSA model, the short-term unavailability of equipment brought by periodic tests and maintenance is considered;
d) PSA adopts more realistic assumptions to reflect the actual situation of nuclear power plants, and its evaluation results are closer to reality.

To sum up, PSA method can make up for the deficiency of traditional determination method to a great extent. Comprehensive use can make safety analysis and reliability analysis more comprehensive, objective and reasonable.

3 Digital Control System

Nuclear power plant digital control system (DCS) is a distributed control system based on computer and network communication. DCS system not only has the measurement and control function of conventional industrial process instrument, but also has extremely strong data processing capacity and high-speed information communication rate. The main advantages are decentralized control, centralized management, high reliability, data acquisition and process control functions are decomposed, implemented by multiple functional computers, independent work, to avoid the common mode failure risk caused by centralized control. Its main features are as follows:

1) With high control accuracy and strong logical operation processing and computing capability, it can significantly improve the comprehensive performance of the I&C system, and complete the complex logic operation processing and calculation functions that cannot be achieved by the analog I&C system in the past;
2) Communication network is used to connect each system equipment, which greatly reduces the number of connecting cables and improves the reliability of data transmission;
3) It can conveniently and effectively realize multiple redundancy, fault security and fault tolerance, and improve the system availability and reliability;
4) It can be conveniently and effectively realized with system on-line inspection and self-diagnosis function, which is helpful for fault analysis and judgment;
5) The system has good extension flexibility, strong configurability and easy maintenance;
6) It has powerful data processing and storage capacity, and improves the man-machine interface.

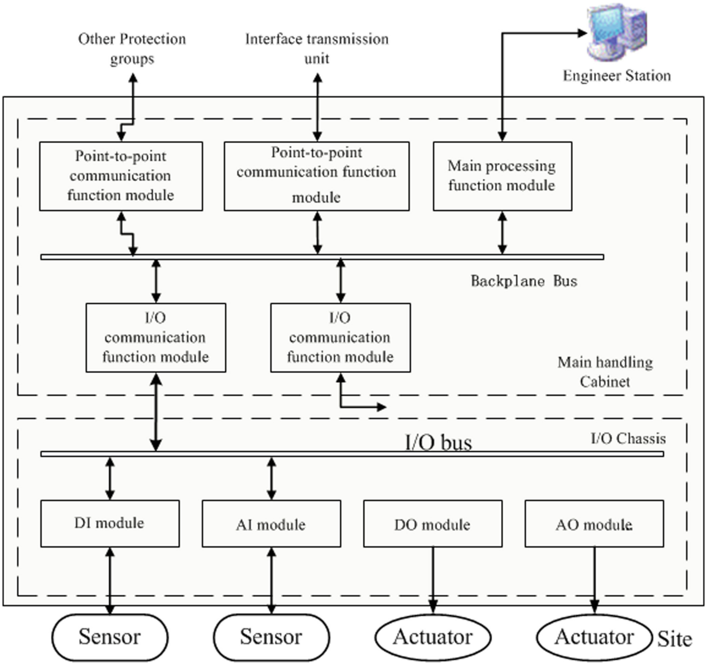
Other Protection groups
Interface transmission unit
Engineer Station
Point-to-point communication function module
Point-to-point communication function module
Main processing function module
Backplane Bus
I/O communication function module
I/O communication function module
Main handling Cabinet
I/O bus
I/O Chassis
DI module
AI module
DO module
AO module
Sensor
Sensor
Actuator
Actuator
Site

Fig. 2. Internal architecture of typical NPP digital I&C cabinet

DCS mainly includes the first-floor equipment such as master controller, communication module and I/O module, and the second-floor equipment such as operator station. The typical internal structure diagram of the cabinet is shown in Fig. 2.

In addition, the structure of the I&C system is vertically divided into four layers by function: process system interface layer (Level 0), automatic control and protection layer (Level 1), operation and management information layer (Level 2), and plant technical management layer (Level 3).

1) Level 0 is the interface layer of instrument control and process system, mainly composed of sensors, actuators and other field equipment.
2) Level 1 mainly includes reactor protection system (RPS), reactor power control system (RPCS), plant standard automation system (PSAS), special I&C subsystem system, Diversity Actuation System (DAS), Serious Accident I&C system (SA I&C), etc.
3) Level 2 is mainly composed of power station computer Information and Control (KIC) equipment, emergency operation device (ECP), display screen (LDP) and so on. These devices are located in the main control room (MCR), remote shutdown station (RSS) and Technical Support Center (TSC).
4) Information management (level 3) (Fig. 3).

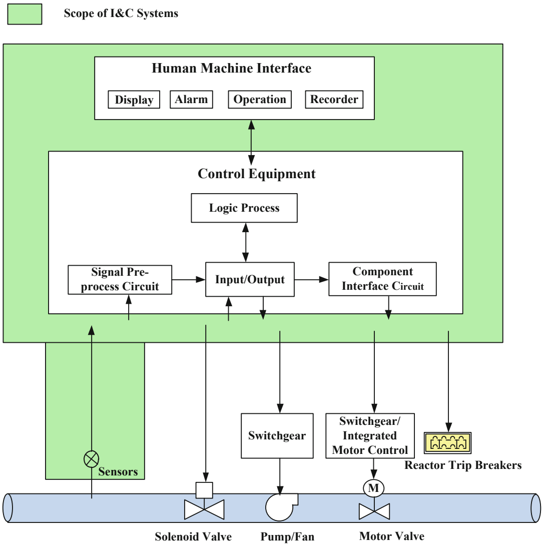

Fig. 3. Typical architecture of NPP digital I&C

4 Self-diagnosis of Safety I&C System and Periodic Test

In order to improve the reliability of digital I&C system, self-diagnosis and periodic test are generally adopted in control system. Based on this, the safety level system should be capable of conducting tests during the normal operation of the plant as well as during the outage. The types of tests include operational tests, channel calibration and response time tests.

The safety system shall be tested to include as many sensors, signal processing equipment, logic devices and final drivers as possible without compromising the continuous normal operation of the plant. When selecting all parts of a protection system, consideration should be given to experiment ability. In the case that the complete test cannot be realized, the method of segmental overlapping test can be adopted.

4.1 Self-diagnosis Design

Self-diagnosis refers to the inspection performed by the device itself, including online continuous self-diagnosis, device triggered self-diagnosis and manual triggered self-diagnosis. The application of self-diagnosis in the computer-based protection system can improve the reliability of the system and extend the cycle of periodic test s. The self-diagnosis design features are as follows:

1) The coverage of self-diagnosis should be as comprehensive as possible, including memory function and integrity test, data link diagnosis, etc.
2) The fault detected by self-diagnosis should be prompted to the operator of the power station by means of alarm and information instruction;

3) The software and hardware used to realize the self-diagnosis function shall not affect the independence, system integrity and single fault criteria of the redundant channel;
4) Self-diagnosis cannot affect the execution of safety functions or cause false actions of safety functions;
5) The interface design between the self-diagnosis software and the security function software should have minimal impact on the logic and data structure of the security function software;
6) A proper balance should be maintained between resources for self-diagnosis (such as cycle time, etc.) and computer performance.

4.2 Periodic Test Design

Periodic tests refer to tests performed at scheduled intervals to detect faults and check runnability, including manual tests or manually triggered automated tests. The main design features of periodic test s are as follows:

1) The periodic test device and its interface with the protection system shall not affect the independence of the redundant channel, the integrity of the system and the single fault criterion;
2) During the periodic test, the response ability of the protection system to real signals shall be maintained;
3) Each redundant channel shall be allowed to conduct periodic tests independently, and measures shall be taken to prevent periodic bypass multiple channels at the same time;
4) If a part of the protection system is tested by bypass or exits from operation, continuous and clear instructions shall be provided in the control room, and measures shall be provided to enable the operator to confirm that the tested equipment has been restored to its normal operation mode after the completion of the test;
5) The periodic test should simulate the path of normal signal as practically as possible;
6) Measures shall be taken to prevent unauthorized personnel from triggering periodic tests.

Taking the periodic test of a nuclear power plant as an example, the main test activities of the safety level I&C system are as follows:

a) Channel inspection;
b) Shutdown and ESFAS functional test;
c) Shutdown circuit breaker action test;
d) Specially designed action test;
e) Output control loop test;
f) Drive test;
g) Connection test between the protection system and the third-party system;
h) Human-machine interface test;
i) Response time test.

According to the requirements of reliability technical characteristics, on the one hand, if the periodic test interval is shortened and the frequency of periodic test is increased, the reliability of the system can be improved. But on the other hand, the reliability of high frequency increases the workload of maintenance personnel, and is easy to introduce human risk, but reduces the reliability of the system. Therefore, it is particularly important to determine the periodic test interval scientifically (Fig. 4).

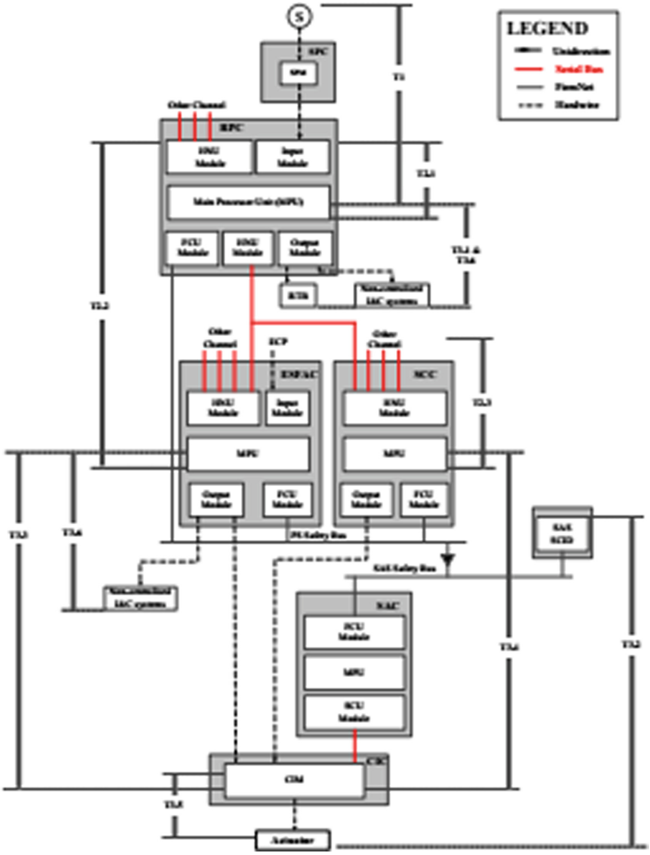

Fig. 4. Periodic testing overlap diagram of safety I&C system

4.3 Periodic Test Cycle Analysis and Calculation

During the operation of DCS equipment, there are two fault modes as follows:

1) Self-detected Failure (DF): DCS system itself has loop detection function, which can detect and detect some faults detected by the self-diagnosis system when the hardware device fault is detected;

2) Undetected Failure (UF): Some failures are beyond the self-detected range of DCS and cannot be detected by DCS self-detected system. These failures are usually potential failures detected in unit operation which can be detected by periodic tests (Fig. 5).

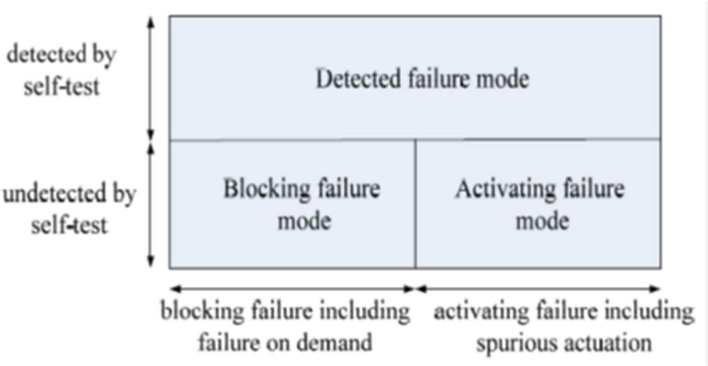

Fig. 5. Failure mode synthesis

In accordance with GB 9225 general Principles for Reliability Analysis of Nuclear Power Plant Safety Systems, the steady-state availability concept is used for repairable or replaceable items (calculations may assume an infinite maintenance time to simulate an unrepairable situation). A repairable or replaceable item works until it fails, is repaired, works again, fails again, and is repaired ("repair," meaning repair or replacement). In an infinite time, availability is related to the average running time and maintenance time. The formula is as follows:

$$\text{Availability} = \frac{\text{average working time}}{\text{average working time} + \text{Unavailable time}} \tag{1}$$

There are two situations to be considered. One is that an item is found to be out of order as soon as it fails (self-display) and is repaired immediately (without time delay). In this case, it can be assumed that the time out of service is equal to the time to repair. In another case, the fault is not self-displaying and can only be detected by periodic test s. Then the non-working time is the time interval between failure and the next test plus the maintenance time.

In general, availability is a complex mathematical function that depends on the probability distributions of test intervals, run times, and repair times.

1) If the following assumptions are met:
2) There is a constant items λ failure rate;
3) Faults can only be detected by periodic tests;
4) The test interval is constant T;
5) λT small enough;
6) Maintenance time plus logical delay time is far less than the test interval time;

Items are in a working state at the beginning of each test interval, and faulty items must be tested and repaired. The test will not cause item failure, nor will it change the item failure rate. Equation (5) can be simplified as: $\overline{A} = \lambda T / 2 A\cdot$

According to the above analysis, periodic test cycle T, as an input variable of reliability, needs to meet the overall reliability target requirements, which can be determined by adopting iterative design.

Taking a certain power plant as an example, PSA method is adopted to design the periodic test cycle of iteration safety level I&C system. Table 1 shows the DCS failure data of the equipment.

Table 1. Failure rate of DCS equipment

Equipment	MTBF	Failure rate (/hour)
CPU power supply	1.39E+05	7.17E−06
Optical electric converter	9.80E+06	1.00E−07
Redundancy management equipment	3.60E+05	2.76E−06
Master management unit	3.08E+05	3.24E−06
Bus interface unit	1.74E+05	5.74E−06
CPU processing unit	2.05E+05	4.88E−06
I/O interface card	5.96E+05	1.67E−06

Through the above analysis, the reliability calculation formula is as follows:

$$U = 1 - \big(\mathrm{MTBF}/\big(\mathrm{MTBF} + \mathrm{MTTR} + (1 - P) \times T_{pt}/2\big)\big)$$

U: Mean Availability (Failure on Demand)
MTBF: Mean time between failures (hour)
MTTR: Average repair time (hour)
P: Probability of successful self-diagnosis after equipment failure
Tpt: Periodic Test Period (hour)

Taking CPU as an example, after substituting its invalid data into the public display, it can be calculated that:

$\mathrm{MTBF}_{\mathrm{CPU}} = 2.654 * 10^8$ h (configure CPU in switch mode)
MTTR = 4 h
P = 0.99
Tpt = 12 month
U cpu $= 6.933 * 10^{-6}$

Taking this as an example, the DCS function, acquisition module and output module are calculated, and then substituted into the PSA model of the power plant, the core failure probability can be lower than 10^{-04}, which meets the requirements of the first-level PSA index of the power plant. Therefore, the established 12-month periodic test period meets the requirements.

5 Calculation Process of Periodic Test Interval of Safety I&C System

According to the above typical functions and equipment analysis conclusion, the typical flow chart of the periodic test cycle calculation of the safety level I&C system based on the equipment reliability and PSA index of the power plant is as follows, which is divided into eight steps, specifically as follows:

1) Step 1: Determine the system structure, signal transmission mode and other information according to the overall design scheme of DCS, and analyze the implementation scheme of the security-level I&C system based on diversity design, redundancy design and single fault criterion;
2) Second step: function analysis, including protection system function grouping, topology, DCS implementation hardware, signal transmission path and voting logic, etc.;
3) Third, on the basis of complete functional analysis, develop fault mode analysis (FMEA) of DCS equipment. Fault mode analysis refers to the analysis of the system unavailability under the condition of a single hardware failure;
4) The fourth step is to determine the equipment failure mode and failure efficiency;
5) The fifth step is to establish the DCS reliability model based on FMEA and on the basis of the reliability modeling method research.
6) The sixth step is to analyze and debug the model and modify the situation that does not conform to the reality;
7) The seventh step is to calculate the reliability data of the model and analyze whether the data meet the requirements of regulations and contracts;
8) The eighth step is iterative design to analyze whether the current periodic test cycle can meet the reliability target requirements of the I&C system and PSA index requirements (Fig. 6).

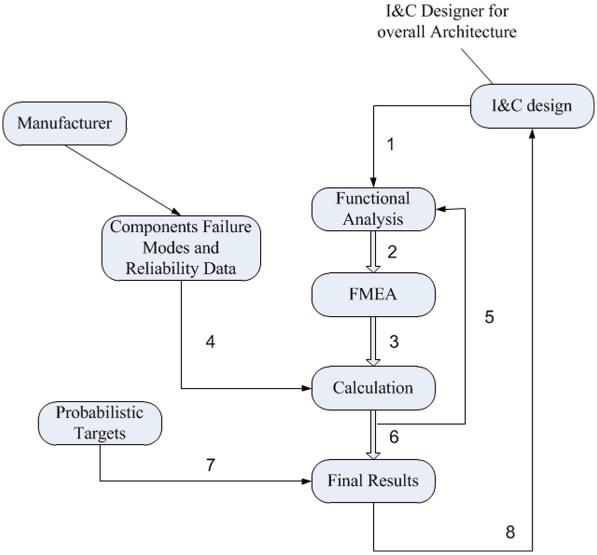

Fig. 6. Calculation flow chart of periodic testing interval of safety I&C system

6 Conclusion

Improving the reliability of the safety level I&C system plays an important role in the reliability of the whole nuclear power plant. In the traditional sense, the reliability of the system is only improved by improving the reliability of the equipment (such as design process, redundancy, manufacturing process, etc.). With the popularization of digital technology, self-diagnosis and periodic test are also important means to improve reliability. Based on this, this paper combined with PSA technology, carried out theoretical calculation of periodic test period, quantitatively analyzed the test period from the perspective of core melting and radioactive release in the whole plant, and gave a typical calculation. On this basis, a set of periodic test interval calculation method of safety level I&C system based on PSA is proposed, which provides beneficial exploration and supplement for similar engineering practice.

References

1. Feng, B.-L.: Probabilistic safety evaluation. Daya Bay Nuclear Power Plant (1), 8 (2006)
2. NS-R-1: Safety of Nuclear Power Plants: Design (2000)
3. NS-G-1.2: Safety Assessment and Verification for Nuclear Power Plants (2005)
4. Chen, J.-F., Guo, J.: Probabilistic safety evaluation. Daya Bay Nuclear Power Plant (1), 18–19 (2006)
5. Jiang, G-J.: Design and application research of digital I&C system based on PSA in nuclear power plant
6. Chen, J.-F., Guo, J.: Review of probabilistic safety evaluation methods. Daya Bay Nuclear Power Plant (1), 18 (2006)