# Research and Application of Software Reliability Analysis Method for Safety I&C System in NPPs

Sheng-Chao Wang(✉), Jian-Zhong Tang, and Tao Bai

State Key Laboratory of Nuclear Power Safety Monitoring Technology
and Equipment, I&C Equipment Qualification and Software V&V Laboratory,
China Nuclear Power Engineering Co., Ltd., Shenzhen,
Guangdong 518172, China
18566693557@163.com

**Abstract.** With the extensive application of digital equipment in nuclear power plants (NPPs), computer software plays an increasingly important role in the digital instrumentation and control (I&C) systems of NPPs. However, with the increase of software scale, defect density increases geometrically. Therefore, the reliability of the software must be considered before the digital equipment is put into practical use of the safety I&C systems in NPPs. This research firstly introduces the advantages and disadvantages of software failure modes and effects analysis (FMEA) and software fault tree analysis (FTA), adopts FMEA and FTA comprehensive analysis method for qualitative analysis of software reliability, and establishes the analysis steps and comprehensive analysis principles. On this basis, taking the application software of safety instrumentation and control (I&C) system of nuclear power plant as the analysis object, the analysis model is established, and the key causes of function failure are found out by solving the minimum cut set to make improvement measures. At last, the technical characteristics of FMEA and FTA comprehensive analysis method are summarized to provide reference for the software reliability analysis of I&C systems in NPPs.

**Keywords:** I&C system · Software reliability · FMEA · FTA

## 1 Introduction

With the extensive application of digital equipment in nuclear power plants (NPPs), computer software plays an increasingly important role in the digital instrumentation and control (I&C) systems of NPPs. The scale and importance of software are on the rise. However, with the increase of software scale, defect density increases geometrically. The following Table 1 gives the defect density of some applications. The increase of software defects not only leads to a great increase in the cost of defect location and repair, but also may lead to a large number of software failure and produce serious consequences. Therefore, the reliability of the software must be considered before the digital equipment is put into practical use of the safety I&C systems in NPPs.

Y. Xu et al. (Eds.): SICPNPP 2019, LNEE 595, pp. 541–549, 2020.
https://doi.org/10.1007/978-981-15-1876-8_53

**Table 1.** Defect density of some applications [1].

| Applications | Number | Defect density (100 LOC) |
|---|---|---|
| Airborne | 8 | 1.28 |
| Strategic | 18 | 0.66 |
| Tactical | 6 | 1.00 |
| Process control | 2 | 0.18 |
| Production | 9 | 1.30 |
| Development | 2 | 0.40 |

This research mainly uses the static test technology of software reliability qualitative analysis to detect and eliminate software defects, that is to say, to find and eliminate software defects without actually running the software. Software reliability analysis method is different from the defect detection methods of software testing. This method can be applied to the early days of software development process, find out the defects and the weak link in the software requirements or the software design, to avoid the continuation of defects to the subsequent development stage. In addition, it also reflects the principle of defect detection as early as possible, reducing the cost and time of defect repair. Commonly used software reliability analysis methods include software failure modes and effects analysis (SFMEA), software fault tree analysis (FTA), event tree analysis (ETA) and Petri net analysis.

This research firstly introduces the necessity of software reliability analysis of digital equipment, and then explains the advantages and disadvantages of FMEA and FTA and the principle of comprehensive analysis using the two methods. After that, according to the principle of comprehensive analysis, the application software of I&C system of nuclear power plant is taken as an example, and an analysis model is established to qualitatively analyze the reliability of the software. Finally, the software reliability analysis is summarized and prospected.

## 2 Software FMEA and FTA Comprehensive Analysis

### 2.1 The Advantages and Disadvantages of the Analysis Methods

The software FMEA is a bottom-up single factor failure analysis method, which cannot perfectly express the various logical relationships among failure reasons. In addition, the analysis process and results of the software FMEA are presented in table form, which is not as intuitive as the graphical expression of FTA.

Software FTA is a top-down method of pushing fault causes backward according to tree structure, which may miss potential key top-level failure events and fault causes, affect the importance ranking of bottom events, and thus affect fault control and judgment of implementing improvement measures. The tree structure of FTA is not as detailed as the form of FMEA in describing the analysis results and other information.

As mentioned above, the respective advantages of FMEA and FTA make up for each other's shortcomings. In order to better reflect the completeness of software reliability analysis process and results and the intuitiveness of logical expression, find out the potential defects or problems as early as possible and improve the quality of software reliability analysis, this research comprehensively applies the two analysis techniques to case analysis.

## 2.2 The Principle of the Comprehensive Analysis

By referring to the general steps of software reliability qualitative analysis of nuclear power plant safety system in GB/T 9225, the analysis steps in Fig. 1 are formulated [2].

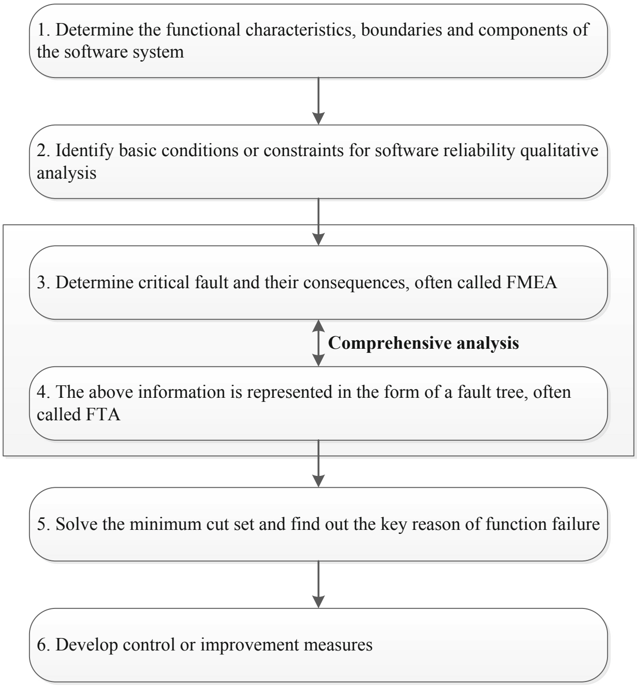
1. Determine the functional characteristics, boundaries and components of the software system
2. Identify basic conditions or constraints for software reliability qualitative analysis
3. Determine critical fault and their consequences, often called FMEA
Comprehensive analysis
4. The above information is represented in the form of a fault tree, often called FTA
5. Solve the minimum cut set and find out the key reason of function failure
6. Develop control or improvement measures

**Fig. 1.** Qualitative analysis steps of software reliability.

Among the steps, the most important analysis steps are the comprehensive analysis of FMEA and FTA (see Fig. 2). Starting from the failure mode of a certain function of the analysis object, the failure impact is firstly obtained through the software FMEA analysis. The failure impact can be used as the source of the top event of the software FTA, and the priority of the analysis of the software FTA can be determined according to the impact degree. It can also analyze the fault mode of the object as an intermediate event, and conduct downward analysis of the fault cause of software FTA. Based on the software FMEA, the tree structure is used to construct a more intuitive logic relationship between fault causes. Then, according to the constructed tree logic relationship, the minimum cut set is solved to judge the importance ranking of bottom events, and the key fault modes and their causes are found so as to formulate control or improvement measures.

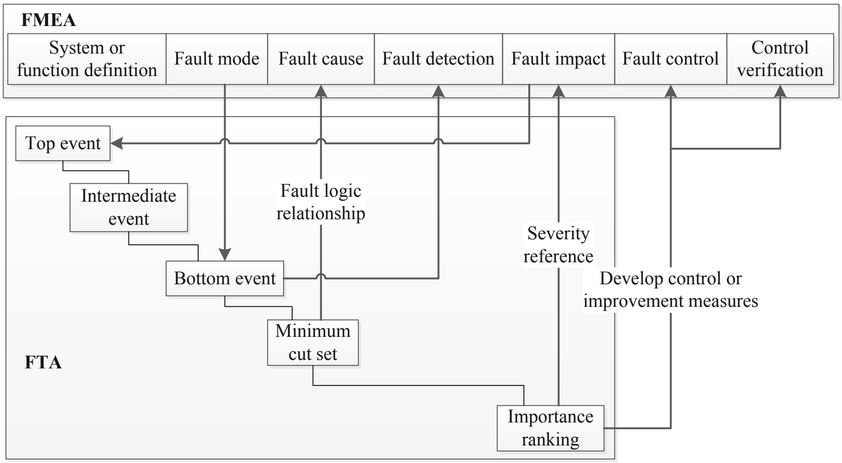

**Fig. 2.** Principle of FMEA and FTA comprehensive analysis [3, 4].

# 3 Modeling and Application

## 3.1 System Function and Structure

In order to facilitate analysis and modeling, the schematic diagram of reactor trip protection system (RTS) shown in Fig. 3 is presented. The system consists of two mutually redundant protection channels, which acquire the same sensor analog signals respectively, and send them to each other's voting logic through network communication at the same time. After the voting logic processing, both channels get the digital signal of trip protection and output it to the actuators or the reactor trip breakers.

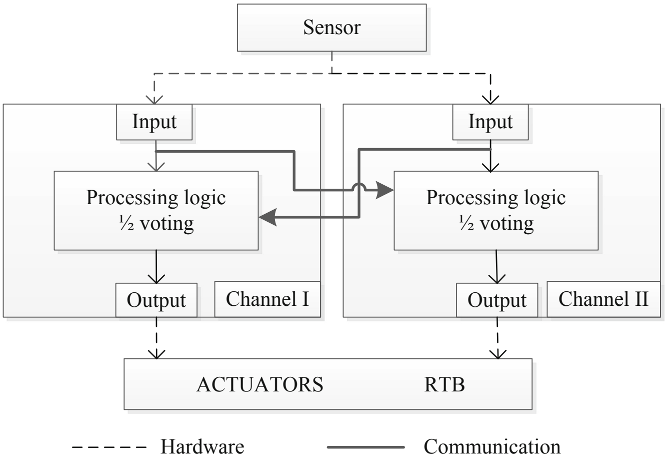

**Fig. 3.** The schematic diagram of RTS.

### 3.2 Basic Conditions and Constraints

Based on the system characteristics of RTS, the corresponding basic conditions or constraints should be given before the software reliability analysis. Specific as follows:

1. For software common cause failure (CCF) that may affect RTS protection or critical safety functions, additional diversity system is set up to mitigate and protect.
2. Communication between the channel processors is confirmed by the receiving processor and, if necessary, the data defaults to a secure state.
3. If the processor loses the current signal, the processor replaces it with the last known valid signal in its history.
4. In the event of a single fault, the system operates normally and without bypass.
5. For a device that outputs trip/no-trip status signals, when it loses power or signal, the final output signal will be the RT safety status signal.

### 3.3 FMEA and FTA Comprehensive Analysis

According to the comprehensive analysis principle in Fig. 2, combining with the characteristics, basic conditions and constraints of the software system, the fault state or reason of the processor that may reduce the system reliability is identified by taking the software of the case system as the research object. At the same time, the fault states related to hardware are eliminated, and the software reliability is qualitatively analyzed based on the software fault mode. The analysis mainly includes five aspects: input fault mode, program fault mode, output fault mode, communication fault mode and human error. In the reliability analysis, the software system can only be accurately modeled when human factors are considered [5]. The analysis of software fault mode is shown in Table 2.

**Table 2.** Software fault mode analysis [6].

| Function name | Fault mode | Fault cause | Fault detection | Fault impact | Fault control | Control verification |
|---|---|---|---|---|---|---|
| Reactor trip protection | 1. No input received<br>2. Error input received<br>3. Value below/above acceptable range | Software/hardware interface defects | Channel check test system self-diagnosis | Voting logic degradation, RT signal is fault safety status value | Channel redundancy | Software testing, system validating testing |
| Reactor trip protection | 1. Communication delays or stops receiving<br>2. Net transmission error<br>3. Net signal itself wrong | Software/hardware error | Heartbeat signal detection system self-diagnosis | Voting logic degradation | Channel redundancy | Software testing |
| Reactor trip protection | 1. Parameter setting error<br>2. Wrong formula or equation | Programming error | Channel check test Trigger function test system self-diagnosis | Voting logic degradation, RT signal is fault safety status value | Channel redundancy | Software testing |

(*continued*)

**Table 2.** (*continued*)

| Function name | Fault mode | Fault cause | Fault detection | Fault impact | Fault control | Control verification |
|---|---|---|---|---|---|---|
| | 3. Program cannot start/terminate<br>4. Program runs abnormally<br>5. Program runs in endless loop | | | | | |
| Reactor trip protection | 1. Boolean jump | Software/hardware interface defects | Channel check test system self-diagnosis | Voting logic degradation, RT signal is fault safety status value | Channel redundancy | Software testing, system validating testing |
| Reactor trip protection | 1. No local channel processor program is downloaded<br>2. Incorrect program version is downloaded | Human error | Management review CRC check | Voting logic degradation, RT signal is fault safety status value | Channel redundancy | Software testing |

Based on the software fault mode analysis in Table 2, by analyzing the causes of failure of software execution functions, FTA identifies various logical relationships among the causes of failure, finds out the key causes of failure of software function, judges the effectiveness of measures to correct and prevent failure causes, and qualitatively evaluates the reliability of software.

As shown in the Fig. 4, the implementation logic of reactor trip (RT) function is 1/2 voting logic. In order to invalidate this function, the signal of two redundant channels shall be invalidated or the software common cause failure occurs between channels. The failure of single channel signal means that the processor of the channel is not available. Failure of hardware is not analyzed in this research. Software failure can be caused by input fault or program fault or output fault or communication fault or human error. Each fault mode can be subdivided into specific bottom events, as shown in Fig. 4.

### 3.4 Solve the Minimum Cut Set

According to the fault tree model obtained in Fig. 4, the logical relationship between various bottom events has been obtained, and the downlink method is adopted to solve the minimum cut set.

The analysis rules of the downlink method are:

1. The order of cut set is increased when "and" gate is encountered (the number of base events contained in cut set), and;
2. The number of cut sets is increased when "or" gate is encountered.

The solution of the minimum cut set for the failure of RT function is shown in Table 3. It needs to be particularly noted that the two channels of the RTS are mutually redundant, so the intermediate event A3 is not further subdivided.

According to the data in the fifth column of Table 3, the number of cut sets in which RT function failure is 16.

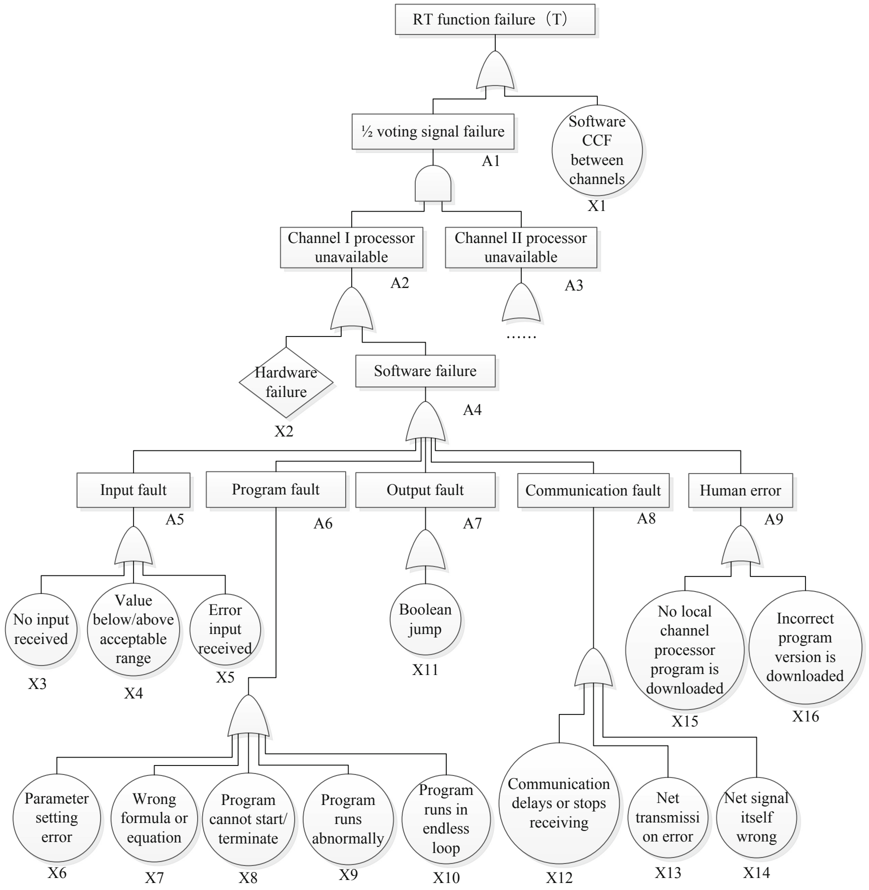

**Fig. 4.** Fault tree model of RT function failure.

**Table 3.** The downlink method to solve the minimum cut set.

| Step | 1 | 2 | 3 | 4 | 5 | 6 (decomposition A3) |
|---|---|---|---|---|---|---|
| Process | A1 | A2, A3 | X2, A3 | X2, A3 | X2, A3 | …… |
| | X1 | X1 | A4, A3 | A5, A3 | X3, A3 | …… |
| | – | – | X1 | A6, A3 | X4, A3 | …… |
| | – | – | – | A7, A3 | X5, A3 | …… |
| | – | – | – | A8, A3 | X6, A3 | …… |
| | – | – | – | A9, A3 | X7, A3 | …… |
| | – | – | – | X1 | X8, A3 | …… |
| | – | – | – | – | X9, A3 | …… |
| | – | – | – | – | X10, A3 | …… |
| | – | – | – | – | X11, A3 | …… |

(*continued*)

**Table 3.** (*continued*)

| Step | 1 | 2 | 3 | 4 | 5 | 6 (decomposition A3) |
|---|---|---|---|---|---|---|
| | – | – | – | – | X12, A3 | …… |
| | – | – | – | – | X13, A3 | …… |
| | – | – | – | – | X14, A3 | …… |
| | – | – | – | – | X15, A3 | …… |
| | – | – | – | – | X16, A3 | …… |
| | – | – | – | – | X1 | …… |

The cut set is used to judge the importance of bottom events, and the influence of the occurrence of bottom events on the occurrence of top events is only analyzed from the fault tree structure without considering the probability of bottom events.

Basic principles of importance (I$\varphi$) analysis of ground events:

1. Only all basic events that appear in the same minimum cut set have equal importance;
2. In the minimum cut set, the fewer the number of basic event, the more important the basic event is;
3. The more times the basic event appears in different minimum cut sets, the more important it is.

To sum up, the importance (I$\varphi$) order of the bottom event of RT function failure is:

$$I\varphi(X1) > I\varphi(X2) = I\varphi(X3) = I\varphi(X4) = I\varphi(X5) = I\varphi(X6) = I\varphi(X7) = I\varphi(X8) = I\varphi(X9) = I\varphi(X10) = I\varphi(X11) = I\varphi(X12) = I\varphi(X13) = I\varphi(X14) = I\varphi(X15) = I\varphi(X16)$$

## 3.5 Develop Control or Improvement Measures

According to the order of the bottom event and its importance in the above cut set, it analyzes whether the RTS and its software have designed corresponding corrective and preventive measures to mitigate or eliminate the impact of the bottom event, as shown in Table 2.

Control or improvement measures have been taken to reduce or avoid the occurrence of top event for bottom events that may lead to the failure of RT function of top event (see Table 2). A single fault will not lead to the harmful consequences of the software, but the software common cause fault adopts a diversity system to provide protection, and the trip protection function achieved by the software design of the system has high reliability.

## 4 Conclusions

By combining the advantages and disadvantages of FMEA and FTA, this research adopted the qualitative reliability analysis method of FMEA and FTA comprehensive analysis to study the reliability of the software of nuclear power plant trip protection system. According to the principles and steps of comprehensive analysis, the FMEA analysis form and FTA fault tree model are established. On this basis, the importance ranking of the bottom event is obtained, and the corresponding prevention or improvement measures are designed to ensure the reliability of the studied software system according to the importance ranking. In conclusion, the research may probably conclude that the software of this RTS has high reliability. A whole set of qualitative and comprehensive analysis methods of software reliability proposed in this research can achieve quantitative evaluation of software reliability if the occurrence probability of bottom events can be obtained.

## References

1. Pham, H.: System Software Reliability. Springer (2006)
2. GB/T 9225: General Principles of Reliability Analysis for Nuclear Power Plant Safety Systems. The State Bureau of Quality and Technical Supervision (1999)
3. Lu, M.Y., Ai, J., Li, Q.Y.: Software Reliability Engineering. National Defense Industry Press (2015)
4. Liu, B.B.: Research on Comprehensive Analysis Methods of Software FMEA and FTA. Master’s thesis of Beijing University of aeronautics and astronautics (2008)
5. Gu, P.F., Wang, Z.F., Zhang, J.B.: A study on human reliability about human machine interface in accident situation of nuclear power plant. In: International Conference on Nuclear Engineering (2010)
6. GJB/Z 1391: Guide to Failure Mode, Effects and Criticality Analysis. General Armament Department of the People’s Liberation Army (2006)