Lecture Notes in Electrical Engineering 1250

Pengfei Gu · Yang Xu · Weihua Chen ·
Zhongqiu Wang · Yongbin Sun ·
Zheming Liu *Editors*

New Energy Power Generation Automation and Intelligent Technology

The Eighth Seminar on Digital Instrumentation and Control Technology for Nuclear Power Plant (Volume 2)

Springer

Lecture Notes in Electrical Engineering 1250

The book series *Lecture Notes in Electrical Engineering* (LNEE) publishes the latest developments in Electrical Engineering—quickly, informally and in high quality. While original research reported in proceedings and monographs has traditionally formed the core of LNEE, we also encourage authors to submit books devoted to supporting student education and professional training in the various fields and applications areas of electrical engineering. The series cover classical and emerging topics concerning:

- Communication Engineering, Information Theory and Networks
- Electronics Engineering and Microelectronics
- Signal, Image and Speech Processing
- Wireless and Mobile Communication
- Circuits and Systems
- Energy Systems, Power Electronics and Electrical Machines
- Electro-optical Engineering
- Instrumentation Engineering
- Avionics Engineering
- Control Systems
- Internet-of-Things and Cybersecurity
- Biomedical Devices, MEMS and NEMS

For general information about this book series, comments or suggestions, please contact leontina.dicecco@springer.com.

To submit a proposal or request further information, please contact the Publishing Editor in your country:

China

Jasmine Dou, Editor (jasmine.dou@springer.com)

India, Japan, Rest of Asia

Swati Meherishi, Editorial Director (Swati.Meherishi@springer.com)

Southeast Asia, Australia, New Zealand

Ramesh Nath Premnath, Editor (ramesh.premnath@springernature.com)

USA, Canada

Michael Luby, Senior Editor (michael.luby@springer.com)

All other Countries

Leontina Di Cecco, Senior Editor (leontina.dicecco@springer.com)

**** This series is indexed by EI Compendex and Scopus databases. ****

Pengfei Gu · Yang Xu · Weihua Chen ·
Zhongqiu Wang · Yongbin Sun · Zheming Liu
Editors

New Energy Power Generation Automation and Intelligent Technology

The Eighth Seminar on Digital Instrumentation and Control Technology for Nuclear Power Plant (Volume 2)

Springer

Editors
Pengfei Gu
Pengfei Valley, China Nuclear Power Design Co., Ltd.
Shenzhen, China

Yang Xu
Department of Engineering Physics
Tsinghua University
Beijing, China

Weihua Chen
China Nuclear Power Design Co., Ltd.
Shenzhen, China

Zhongqiu Wang
China Nuclear Power Engineering Co., Ltd.
Beijing, China

Yongbin Sun
China Techenergy Co., Ltd.
Beijing, China

Zheming Liu
Product Information Committee
China Instrument and Control Society
Beijing, China

ISSN 1876-1100 ISSN 1876-1119 (electronic)
Lecture Notes in Electrical Engineering
ISBN 978-981-97-7054-0 ISBN 978-981-97-7055-7 (eBook)
https://doi.org/10.1007/978-981-97-7055-7

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

If disposing of this product, please recycle the paper.

Preface

In recent years, with the development of domestic research and international exchanges, more and more digital instrumentation and control (I&C) technologies have been applied in Chinese nuclear power plants, such as Firm Sys, a microprocessor-based safety I&C system developed by China General Nuclear Power Corporation (GNPC), and nas pic, a safety DCS developed by China National Nuclear Corporation (CNNC). In order to solve the problems in actual production and application, and to provide a platform for technical discussion. The 8th Seminar on Digital Instrumentation and Control Technology and Application in Nuclear Power Plants focuses on cutting-edge technology issues of concern to the nuclear power industry, such as hardware and software verification and validation and licensing, intelligent maintenance management and digital updating, advanced main control room and HFE, and cyber security. Since 2016, the symposium has become an effective annual technical forum for nuclear utilities, regulators, engineering companies, contractors, research institutes and equipment manufacturers. The 8th Symposium on Digital Instrumentation and Contrsol Technologies and Applications for Nuclear Power Plants was successfully held on 22–23 June 2024 in Shenzhen, China. More than 200 experts, researchers and senior engineers from 34 organisations, including the National Nuclear Safety Administration (NNSA), Tsinghua University, the Ministry of Ecology and Environment (MOE), Beijing Guangli Nuclear Technology Co. Ltd, the State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment (SKLNPME), and the China National Nuclear Power Engineering Corporation (CNPEC), as well as organisations and companies from the aerospace industry, attended the conference. The symposium provided a platform for the exchange of ideas on all aspects of nuclear power plant instrumentation and control systems, and also promoted China's civil-military integration. More than 100 conference papers were presented, covering topics such as digital instrumentation and control technology, electromagnetic compatibility, main control room and human-machine interface design, and software verification and validation. After anonymous peer review and expert selection, 97 excellent papers were finally selected to be included in the proceedings of Springer's Lecture Notes in Electrical Engineering, including 7 critically excellent papers. Keynote speeches were delivered on "Firm Sys-based I&C Island Solutions", "Digital Transformation of I&C Systems", and "Localisation of I&C System Components". These speakers shared with the audience their latest and most important research advances. In fact, many of the topics discussed in the symposium provide important references and strong support for related work in nuclear power plants. We believe that these papers can also benefit the entire nuclear instrumentation and control systems industry. On the occasion of the publication of this paper, we would like to thank the organisers of the workshop for providing a good platform for the nuclear power practitioners. We are also very grateful to the experts who provided support and guidance during the review process. Finally, we would like to thank all the authors, without whose efforts and research this book would never have been successfully published.

Contents

Research on Quantitative Hazard Analysis Method of Safety-Level I&C System Based on Fault Tree

Xin-yue Li[1], Lan-lan Zhang[1](✉), Yuan Xiang[2], Xian-jian He[1], Jing Wen[1], and Zhao Chen[1]

[1] Science and Technology on Reactor System Technology Laboratory, Nuclear Power Institute of China, Chengdu 610213, China
275409921@qq.com

[2] China Nuclear Control System Engineering Co., LTD., Beijing 100176, China

Abstract. Hazard analysis is a key technical link in the verification and validation (V&V) activities, in order to study the quantitative hazard analysis method with strong feasibility for the hazard analysis of hardware V&V activities, so that the hazard analysis work will not have different analysis results due to different analysts, this paper uses the fault tree analysis method (FTA), analyzes the main methods and ideas of constructing fault trees by assuming a determined unexpected top event "PAMS function abnormal". The idea of obtaining product failure rate data and the calculation method of human error probability were deeply studied, then quantitatively analyzed the fault tree, and finally obtain the probability of "PAMS function abnormal". Through the research in this paper, it can be effectively demonstrated that the fault tree analysis technology supported by reliability theory, probability theory, Boolean rule and other mathematical theories is effective in the hardware V&V hazard analysis activities of safety-level I&C system, and can guide the practical engineering application of hazard analysis.

Keywords: Hardware V&V · Hazard analysis · Fault tree · Product failure rate · Human error probability

1 Introduction

Hazard analysis is a system engineering activity which identifies hazardous conditions that may lead to adverse consequences by analyzing system design, operating conditions, system physical constraints, and rules. The cause of the hazard may be random hardware failure, human causes or unfriendly environmental factors.

At present, the hazard analysis of safety level I&C system mainly uses the Preliminary Hazard Analysis (PHA), Failure Mode and Effects Analysis (FMEA), Fault Tree Analysis (FTA) and Markov Analysis (MA), these technologies have their own limitations and advantages and disadvantages. For example, PHA can be used in all aspects of the system and is simple to use, but only applicable to the preliminary system design phase. FMEA is easy to implement and can provide meaningful analysis results, but

P. Gu et al. (Eds.): SICPNPP 2024, LNEE 1250, pp. 1–12, 2024.
https://doi.org/10.1007/978-981-97-7055-7_1

the analysis process is limited to single component failure mode, and the analysis of combined failure mode, human error, and external environment is less, which is easy to miss when analyzing complex instrument control systems. MA is a complex system modeling tool involving timing, sequence, redundancy and fault tolerance, which can be used for probabilistic calculation of various system states, but the modeling and calculation are very complex, it is very difficult to apply to nuclear safety-level I&C systems. While FTA is between the above analysis techniques, the modeling difficulty is lower than that of MA, but its probability calculation results are almost equivalent to those of MA model, and it is suitable for large-scale complex system modeling. However, there are also technical difficulties in the application of FTA, such as the acquisition of bottom event failure probability data. This paper focuses on the modeling methods and ideas of FTA in the nuclear safety-level I&C system hardware V&V activities, as well as the research of quantitative analysis methods, providing ideas for obtaining random hardware failure probability data, giving common hardware product failure rate data, and detailing the calculation method of human error probability.

2 Overview of Fault Tree Analysis

Fault tree analysis (FTA) is a systematic analysis technology used to determine the root cause and occurrence probability of an undesired top-level event (top event), and connect all the causes or events that cause the occurrence of the top event through Boolean algebra and logical relations. The fault tree is a collection of all events (failure mode, human error, and normal state) that can cause a top event to occur [1]. Fault tree analysis is applicable to any phase of the system life cycle from the concept phase to the handover phase. Entire systems including systems, subsystems, components, hardware, software, processes, environments, and human errors can be modeled and analyzed.

The construction of a fault tree is an iterative process, starting at the top event and continuing down through all branches. The build process needs to distinguish between “ state of the system” (SS) events and “ state of the component” (SC) events, the “ state of the system” event needs to identify the “immediate (I), necessary (N), and sufficient (S)” causes or events for which cause the event occurred; The “ state of the component” event needs to determine the “primary (P),subsequent (S), and command (C)” causes or events that cause the event to occur until all events are decomposed into basic events that can no longer be decomposed (hardware failure, software failure, human error, etc.), this is the FTA cut set.

As one of the key products of FTA, cut set and minimum cut set contain all paths to trigger the top event. Top-down algorithm (MOCUS algorithm) and bottom-up algorithm (reverse MOCUS algorithm) can be used to calculate the minimum cut set of the top event for FTA qualitative analysis. The probability and reliability theory can be also used in FTA quantitative analysis to determine the probability of top event occurrence and the importance of cut set.

3 Construction of Fault Tree

The process of fault tree construction is to use causality, starting from the top event, top-down, and gradually listing the direct cause of the upper event (the basic event). The construction of the fault tree assumes that the failure rate of terminals, hardware lines, and PCB lines is 0, and does not consider the impact of hardware and software design errors and site environment factors on the system. This paper takes "PAMS function abnormal" as the top event of the pre-fault tree, and the top event is SS event. The I-N-S concept is adopted in the fault tree construction. It is analyzed that the causes of the top event may be "acquisition unit error", "operation unit error", "transmission unit error" and "display unit error". The primary and subsequent causes should be considered in the construction of intermediate fault tree and bottom fault tree. In summary, the example of the fault tree "PAMS function abnormal" is shown in Fig. 1.

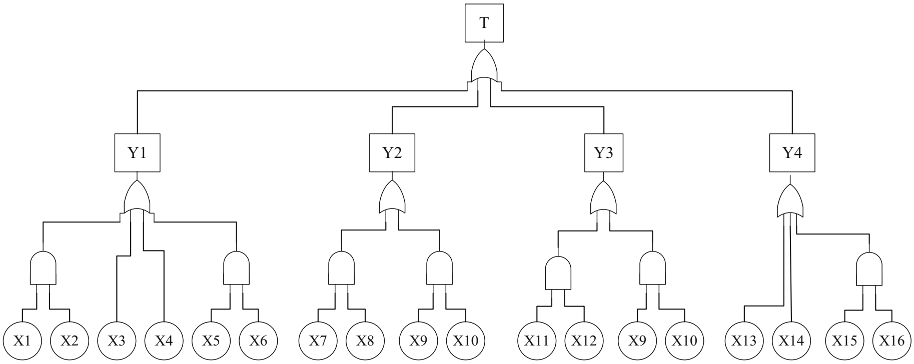


Fig. 1. Example of "PAMS Function Abnormal" fault tree

Table 1 shows the comparison relations of event codes and event contents in the fault tree.

Table 1. Event code and event content comparison table

Event code	Event content	Event code	Event content
T	PAMS function abnormal	X7	A Main control module fault
Y1	Acquisition unit error	X8	B Main control module fault
Y2	Operation unit error	X9	C Power module fault
Y3	Transmission unit error	X10	D Power module fault

(*continued*)

Table 1. (*continued*)

Event code	Event content	Event code	Event content
Y4	Display unit error	X11	A Communication module fault
X1	Human error (alarm not responding)	X12	B Communication module fault
X2	Human error (test not recovered, etc.)	X13	Human error(Misread signals, misread numbers, etc.)
X3	Acquisition module fault	X14	SVDU unit fault
X4	Isolation module fault	X15	E Power module fault
X5	A Power module fault	X16	F Power module fault
X6	B Power module fault		

4 Qualitative Analysis

The qualitative analysis of FTA is to determine the cut set and the minimum cut set of the fault tree. The minimum cut set refers to the set of the smallest basic events that can cause the occurrence of the top event. The more the minimum cut set, the greater the probability of the system's occurrence of danger [2].

4.1 Calculate Cut Sets and Minimum Cut Sets

Using MOCUS algorithm solve the cut set and the minimum cut set of the fault tree "PAMS function abnormal", and the minimum cut set is { X1, X2}, { X3}, {X4}, {X5,X6}, { X7,X8}, { X9,X10}, { X11,X12}, { X13}, {X14}, {X15,X16}.

4.2 Qualitative Analysis Conclusion

According to the results of qualitative analysis, the fault tree of "PAMS function abnormal" has 10 minimum cut sets, and the occurrence of PAMS function abnormal must be the result of all the basic events of a certain minimum cut set occurring at the same time, where {X3}, {X4}, {X13}, {X14} are the cut sets of a single basic event. The occurrence of a single event will directly lead to the occurrence of a top event, so it is necessary to focus on the failure rate of a single event in practical application. In addition, according to the analysis above, human error also should be attention, in the man-machine display interface, test procedures and other aspects of technology or management methods to reduce the occurrence of human error.

5 Quantitative Analysis

Qualitative analysis of FTA is an intuitive judgment without data support, and its credibility is relatively low. Therefore, quantitative analysis based on qualitative analysis can effectively improve the credibility of FTA. Quantitative analysis includes calculating the occurrence probability of the top event and cutting set importance analysis. The calculation of the top event probability depends on the accuracy of the basic data, so the enrichment of the basic event failure probability data is the key to the wide application of fault tree analysis technology.

5.1 Research on Basic Event Failure Rate Data Acquisition

5.1.1 Research on Failure Probability of Hardware Products

The essence of hardware product failure is the failure of integrated circuits or components that make up hardware products. In the life cycle of hardware products, failure is subject to some objective law of probability distribution, known as the bathtub curve, as shown in Fig. 2.

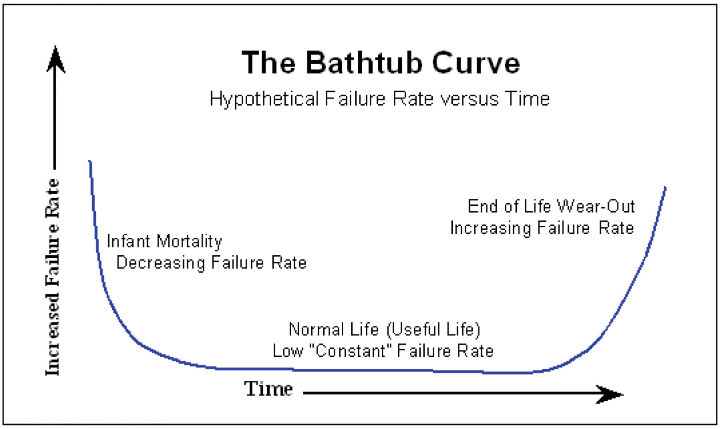


Fig. 2. Bathtub curve

The failure of hardware products can be divided into three stages with time, namely, early failure period, accidental failure period and wear-out failure period. In the early stage of the product being put into use, the product failure rate is high, and it rapidly decreases with time according to a specific function law. At this stage, the product can enter the accidental failure period immediately after being put into use by changing temperature and humidity, vibration and other ways to accelerate aging. The accidental failure period is the main working time of the product, during which the failure rate is maintained at a low level and in a stable state. The failure rate can be approximated as a constant, and the failure in this stage occurs randomly, also be called as the random failure stage. The last stage of the product life cycle is the wear-out failure period, due to natural aging, wear, corrosion and other wear factors, resulting in a rapid increase in the failure rate of the product over time. To sum up, the service life of hardware products is the second stage of product life cycle, the method and way of obtaining product failure rate data during accidental failure period is the focus of this paper.

5.1.2 Collection Channels of Hardware Product Failure Rate Data

In the safety level I&C system hardware V&V hazard analysis activities, hardware components as the smallest analysis unit, usually divided into two categories, one is the safety level I&C equipment supplier self-developed hardware products, the other is general engineering materials, such as circuit breakers, relays, wiring terminals and so on. The failure rate data acquisition channels of the above products are divided into user data, manufacturer data, MTBF data, calculated value, and expert experience value according to the use priority.

1) User data

User data is the market failure rate data collected based on a large number of samples of products in different application scenarios. The data is relatively objective and suitable for relevant analysis. User data is usually collected by the product manufacturer or product agent which includes maintenance and replacement records in using, failure logs, spare parts library use and other data, then analyze the product failure rate data within a certain time range.

2) Manufacturer data

Manufacturer data is the theoretical data that manufacturers estimate the reliability of products under given working conditions based on the reliability prediction model. Reliability prediction data is a process from part to whole and from small to large. The prediction process uses previous engineering experience, fault data, combined with the current technical level, and is based on the failure data of components. The predicted data has sufficient theoretical support and high reliability, and can be directly used for hazard analysis.

3) MTBF data

MTBF data is the failure rate that is based on the MTBF data in the product manual prepared by the product manufacturer, and calculated according to the formula.

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

4) Calculation value

In the case that the product failure rate cannot be obtained by the above three methods, for electronic components, reliability related calculations can be carried out according to the reliability prediction methods and data of electronic equipment given by SN29500 (Failure Rate of Components), IEC61709 (Electric components-Reliability-Reference conditions for failure rates and stress models for conversion) and other standards. For mechanical devices, reliability related calculations can be performed using Monte Carlo method based on the structure of the product itself.

5) Expert experience value

Expert experience value is in the case that the basic data of components cannot be found, through some evaluation means to determine the necessity of continuing to find the basic data or whether the fact that there is no component is acceptable, or whether to take expert advice, and finally give the product failure rate data.

5.1.3 Data of General Hardware Product Failure Rate

By investigating the manufacturers and dealers of switching power supply, relay, air switch, terminal, fiber optical and other products, the failure rate of PCB integrated circuit, terminal, fiber optical, wire and other hardware products without components is approximately 0. Table 2 shows the specific series product failure rate data of some manufacturers, which can be directly used for hazard analysis and can also be used as a reference index for product failure rate analysis.

Table 2. Data of general hardware product failure rate

Sequence Number	Classification	Manufacturer	Model/Series	Failure Rate
1	Power	PLUS	QS10.241,QS10.241-A1/-C1/-D1	$1.72 \times 10^{-6*1}$
2	Power	PHOENIX	QUINT4-PS/1AC/24DC/20	$1.49 \times 10^{-6*2}$
3	Power	MORNSUN	LIMF240-23B** Series	$1.14 \times 10^{-6*3}$
4	Relay	OMRON	MY /MYK/MYQ/MYH Series	$1.00 \times 10^{-7*4}$
5	Relay	PHOENIX	PLC-RSC-24DC-21	$3.34 \times 10^{-6*5}$
6	Air Circuit Breaker	SCHNEIDER	iC65N Series	$2.00 \times 10^{-6*6}$
7	Air Circuit Breaker	ABB	S202M Series	$2.00 \times 10^{-6*7}$
8	Air Circuit Breaker	CHINT	DZ47–60	$1.60 \times 10^{-4*8}$

Remarks *1: Data comes from product manual MTBF@40°C (SN29500,IEC 61709);
*2: Data comes from product manual MTBF@40°C (SN29500, IEC 61709);
*3: Data comes from product manual MTBF@40°C (MIL-HDBK-217F);
*4: Data comes from product manual failure rate P value (Switching frequency of 120 times/min);
*5: Integrated product attributes, characteristics, manufacturer survey data, according to the component and mechanical switch reliability prediction model given expert values;
*6: Integrated product attributes, characteristics, manufacturer survey data, according to the mechanical switch reliability prediction model given expert values;
*7: Integrated product attributes, characteristics, manufacturer survey data, according to the mechanical switch reliability prediction model given expert values;
*8: The data were calculated by Monte Carlo method[3].

5.1.4 Research on Failure Probability of Human Error

So far, human reliability Analysis (HRA) has been developed into the third generation. The first generation of human reliability analysis mainly obtains human error probability data through statistical accident cases, mainly human error evaluation and reduction technology (HEART), human cognitive reliability (HCR), human error probability prediction technology (THERP), etc. These methods are based on expert judgment, and analyzed from the perspective of complexity and difficulty of tasks. People are regarded as part of the hardware, but they fail to understand the internal mechanism of human behavior. The second generation human reliability analysis method focuses on studying how situational environmental factors affect human behavior, trying to find ways to prevent human error from the production mechanism of human behavior [4], which mainly includes ATHEANA method and CREAM method. With the development of computers, the third generation HRA method, dynamic HRA method based on simulation, has gradually emerged, which uses virtual environment and virtual people to simulate human performance in the actual environment, and explains the characteristics of dynamic interaction between complex human-machine systems[5], including BN-CREAM model.

5.1.5 Calculation of Human Error Probability

Considering the difficulty, advantages and disadvantages of various human reliability methods, this paper adopts cognitive reliability and error analysis method (CREAM) [6] to calculate the probability of human factor error. CREAM method, as a typical method in the second generation of human factor reliability analysis, mainly considers the influence of the situation environment on human behavior, quantifies it through Common Performance Conditions (CPC), and calculates the probability of human error 。

CREAM prediction analysis method includes basic law and extended law. The basic law calculates the probability interval of human error, which can only be used to roughly estimate the probability of human error. Therefore, this paper adopts the extended law to calculate the probability of human error, and the process is as follows:

1) Identify the cognitive activity (one or more) involved in this activity or operation according to E. Hunnagel's cognitive activity classification map [6].
2) According to the contrast relationship between cognitive activities and cognitive functions [6] and Table 3 below, determine the cognitive functions corresponding to these cognitive activities as well as the most likely failure modes and the basic probability of occurrence (called the failure probability of cognitive functions) which is recorded as $\mathrm{CFP}_{\mathrm{C}}$ by expert judging.
3) According to the environment of the accident site, determine the levels of 9 CPC factors as shown in Table 4 by experts.
4) Rough method or detailed method can be chosen in this step, this article uses detailed method for calculation. According to Table 4, the weight of cognitive function (cognitive function included in cognitive activity) corresponding to each determined CPC factor level was multiplied to obtain the weight of each cognitive activity, denoted as

ω, and then multiplied by the basic probability to obtain the corrected probability of cognitive function failure, $\mathrm{CFP}_{\mathrm{r}} = \mathrm{CFP}_{\mathrm{C}} \times \omega$.

5) Finally, according to the logical relationship diagram of cognitive activities in Fig. 3, the final probability of cognitive function failure can be determined, which is denoted as $\mathrm{CFP}_{\mathrm{T}}$.

Table 3. Cognitive function failure mode and the basic values of failure probability

Cognitive function	Failure mode	Basic values of failure probability
Observe	Observation target error	0.001
	Error identification	0.007
	Observation not made	0.007
Explain	Diagnostic failure	0.2
	Decision error	0.01
	Delayed interpretation	0.01
Plan	Priority error	0.01
	Inappropriate planning	0.01
Performance	Wrong mode of action	0.003
	Action time error	0.003
	Action target error	0.0005
	Wrong sequence of action	0.003
	Omission of action	0.03

5.2 Top Event Probability Calculation

The first term approximation method is used to calculate the top probability, that is, the probability of the top event is the sum of the probabilities of all the smallest cut sets of the fault tree, and the calculation formula is as follows:

$$P(\mathrm{T}) \approx \sum_{j=1}^{n} \prod_{X_i \in \mathrm{K}_j} q_i \tag{2}$$

Calculate: $\mathrm{P(T)} = 9.14 \times 10^{-5}$, which is the probability of the occurrence of the determined unexpected event “PAMS function abnormal”.

5.3 Cut Set Importance Analysis

Cut set importance refers to the influence on the probability of top event occurrence when the event of cut set occurs. Importance is divided into structural importance (also

Table 4. CPC and the corresponding weight values of cognitive function

CPC name	Level	cognitive function and its weight values			
		Observe	Explain	Plan	Performance
Organizational integrity	Very effective	1	1	0.8	0.8
	Effective	1	1	1	1
	In vain	1	1	1.2	1.2
	Poor effect	1	1	2	2
Working condition	Superiority	0.8	0.8	1	0.8
	Normal	1	1	1	1
	Mismatch	2	2	1	2
Man-machine interface and operational support completeness	Support	0.5	1	1	0.5
	Sufficient	1	1	1	1
	Tolerable	1	1	1	1
	Inadequacy	5	1	1	5
Availability of procedures/plans	Proper	0.8	1	0.5	0.8
	Acceptability	1	1	1	1
	Inadequacy	2	1	5	2
The number of targets that appear simultaneously	Below human processing capacity	1	1	1	1
	Match the person's current abilities	1	1	1	1
	Above human processing capacity	2	2	5	2
Available time	Sufficient	0.5	0.5	0.5	0.5
	Temporary insufficiency	1	1	1	1
	Continuous insufficiency	5	5	5	5
Duty period	Daytime (adjustment)	1	1	1	1
	Night (not adjusted)	1.2	1.2	1.2	1.2

(*continued*)

Table 4. (*continued*)

CPC name	Level	cognitive function and its weight values			
		Observe	Explain	Plan	Performance
Adequacy of training and experience	Full, experienced	0.8	0.5	0.5	0.8
	Full, limited experience	1	1	1	1
	Inadequacy	2	5	5	2
The cooperation quality of team members	Very effective	0.5	0.5	0.5	0.5
	Sufficient	1	1	1	1
	Tolerable	1	1	1	1
	Inadequacy	2	2	2	5

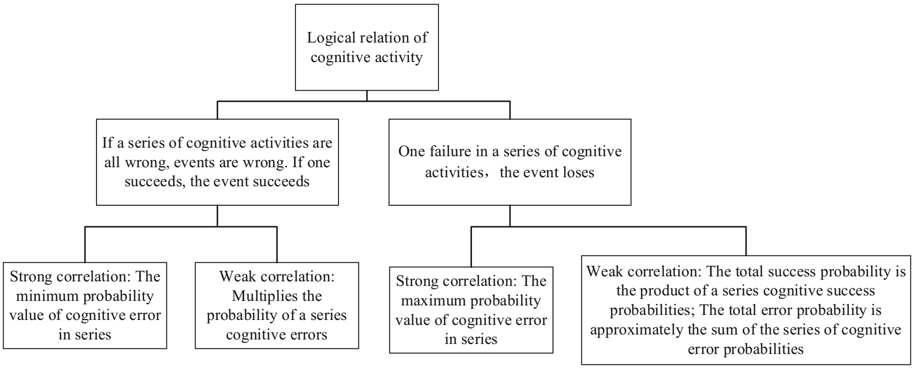

Logical relation of cognitive activity
If a series of cognitive activities are all wrong, events are wrong. If one succeeds, the event succeeds
One failure in a series of cognitive activities， the event loses
Strong correlation: The minimum probability value of cognitive error in series
Weak correlation: Multiplies the probability of a series cognitive errors
Strong correlation: The maximum probability value of cognitive error in series
Weak correlation: The total success probability is the product of a series cognitive success probabilities; The total error probability is approximately the sum of the series of cognitive error probabilities

Fig. 3. Logical diagram of cognitive activity

known as probability importance), critical importance and component importance. In the optimization design of the system and the identification of weak links, priority should be given to structural importance. Therefore, this paper selects structural importance for analysis. Structural importance can be explained mathematically as the difference between the probability of the top event when the *i* event occurs and the probability of the top event when the *i* event does not occur [7].

$$I_i^B = \frac{\partial g(q)}{\partial q_i} = g(1_i, q) - g(0_i, q) \tag{3}$$

where g is the probability of the top event, q_{i} is the probability of the bottom event, i = 1,2,3… 16.

Order by calculated importance:$I_3^B = I_4^B = I_{13}^B{=}^B_{14} > I_9^B{=}I_{10}^B{>}\ I_1^B = I_2^B = I_5^B{=}\ I_6^B = I_7^B = I_8^B = I_{11}^B{=}\ I_{12}^B = I_{15}^B{=}I_{16}^B$

From the ranking of the importance of basic events, it can be intuitively seen that human error and modules with no redundant configuration are the most influential factor on the occurrence probability of top events.

5.4 Quantitative Analysis Conclusion

According to the above, it is concluded that the probability of "PAMS function abnormal" is 9.14×10^{-5}. Among the causes of PAMS function abnormal, the human error contribution degree is the highest. In the design of I&C system, measures such as anti-human error design, redundancy, increasing protection and isolation devices, and configuring different modules should be taken to reduce the probability of high-contribution events. In addition, when troubleshooting faults, it can be ranked from large to small according to the importance, which can efficiently troubleshoot the cause of the top event failure.

6 Conclusion

By assuming that " PAMS function abnormal" is the top event, constructing a fault tree, and the fault tree is analyzed qualitatively and quantitatively, the following conclusions are reached: As a hazard analysis technology, FTA has a complete set of theoretical system as guidance and support, and the fault tree construction method is simple and easy to operate. In particular, the bottom event probability calculation is used in the quantitative analysis process, which reduces subjective judgment in the analysis process and makes the analysis results more accurate. This quantitative analysis method is effective in the hazard analysis of safety level I&C system.

References

1. Ericson, C.A.: Hazard analysis techniques for system safety, pp. 168–207. National Defense Industry Press, Beijing (2012)
2. Jing, Y.: Risk assessment of elevator unintended car movement based on fault tree. China Elevator **33**(21) (2022)
3. Zhang, W.: Reliability analysis and evaluation of operating mechanism in miniature circuit breaker. Zhejiang Sci-Tech University (2015)
4. Yang, L.: A improved human reliability analysis method and its application. University of South China (2011)
5. Li Pengcheng, Chen Guohua,ZhangLi, Dai Licao. Research Review and Development Trends of Human Reliability Analysis Techniques[J]. Atomic Energy Science and Technology,2011,45(03):329–340
6. Erik Hollnagel. Cognitive Reliability and Error Analysis Method. Elsevier Science Ltd, 1998:122–130
7. SUN Hongmei, MU Mingming, Gao Lei. Research on the Qualitative and Quantitative Analysis of Fault Tree Analysis[J]. Electronic Product Reliability and Environmental Testing,2023,41(03)

Exploration of Factory Testing Requirements Analysis Methods for Nuclear Safety Class DCS

Jing-yin Li, Cheng-yong Wu, Jing Wen, and Zhao Chen(✉)

Science and Technology On Reactor System Design Technology Laboratory, Nuclear Power Institute of China, Chengdu 610213, China
1224339553@qq.com

Abstract. The safety class DCS of nuclear power plants is an important component of the DCS, and ensuring its system reliability and stability is crucial. The factory test provides the most powerful guarantee for the reliability of the safety class DCS. To fully cover all design requirements and improve the coverage and adequacy of factory testing, this article takes the analysis of factory testing requirements for the safety class DCS of the "Hualong One" unit of China National Nuclear Corporation as an example. It proposes different types of principles for analyzing test requirements for large-scale and complex systems, clarifies the corresponding analysis elements, and manages test requirements using a requirements traceability matrix. This provides a framework for analyzing test requirements for factory testing activities to enhance the coverage and adequacy of factory testing for the safety class DCS.

Keywords: Digital instrument and control system · Test requirement analysis · Factory testing · Requirement Tracking Matrix

1 Introduction

With the proposal of the dual-carbon goal, in order to build a clean, low-carbon, safe and efficient energy system, accelerate the adjustment and optimization of industrial structure, and promote energy conservation and carbon reduction in key areas, China actively promotes green and low-carbon development and increases the construction of nuclear power. According to the assessment of the National Development and Reform Commission, there will be 40 to 50 sets of nuclear power units under construction in the next few years. The quality of nuclear power equipment and nuclear safety have also received increasing attention from all relevant parties. Among them, nuclear safety level DCS is the "central nervous system" of nuclear power plants, is an important system to ensure the three safety barriers of nuclear reactors, and its reliability and stability are key factors affecting nuclear safety [1].

To prove that the nuclear safety grade DCS final product meets the requirements, a high quality development process is largely relied upon, and full life cycle Verification and Validation activities are required to ensure the reliability and correctness of the system. Factory testing is an important activity for V&V, providing objective evidence

P. Gu et al. (Eds.): SICPNPP 2024, LNEE 1250, pp. 13–24, 2024.
https://doi.org/10.1007/978-981-97-7055-7_2

that the safety functions of the system can be performed as expected under all operating conditions, including various abnormal operating conditions [2].

In guideline HAD102/10–2021, how are V&V activities related to design and development activities in the whole life cycle process of a nuclear safety-grade instrument control system from the perspective of the "V model" [3].

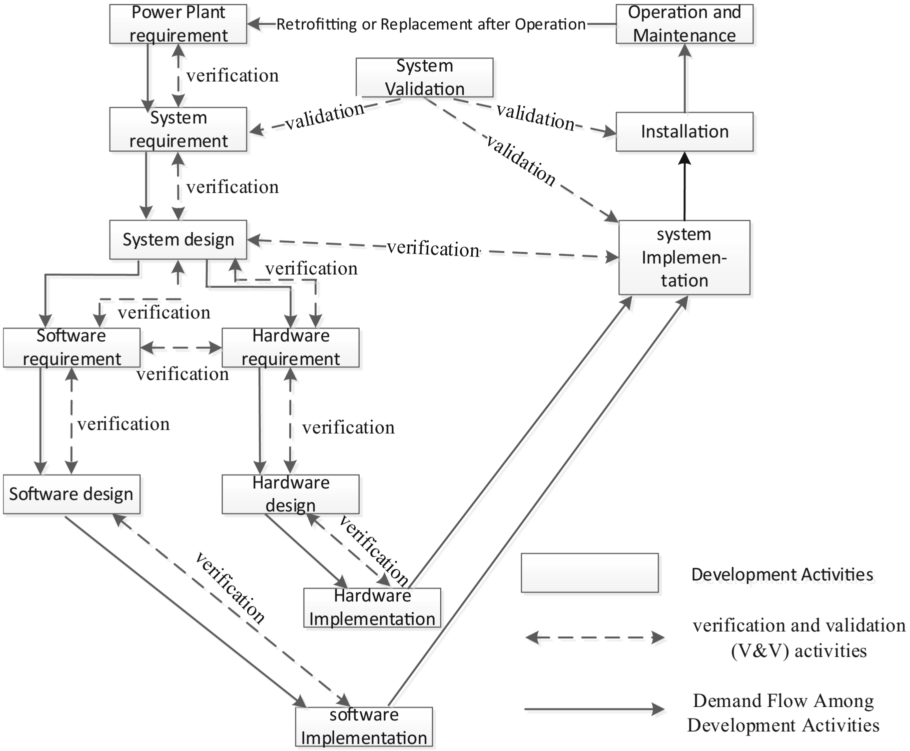


Fig.1. Typical relationship between the lifecycle process of the I&C system and verification and confirmation activities

In Fig. 1, solid lines represent the development activities of the instrumentation and control system, while dashed lines represent the Verification and Validation (V&V) activities. Factory testing activities for the safety class DCS are conducted after system integration, with the aim of confirming whether the functional performance of the entire instrumentation and control system meets the system requirements. System requirements are communicated to suppliers in the form of requirement documents derived from plant needs, and suppliers collectively refer to these documents as user requirements. In order to ensure the integrity and correctness of user requirements in the final product, factory testing activities need to be carried out to confirm the functional performance of the product before leaving the factory. The test content and scope of the factory test are determined through the test requirements analysis activity. These test requirements analysis activities are a key task during the test planning phase, and according to the IEEE

1012–2016 standard, they correspond to the requirements phase of the instrumentation and control system lifecycle, as shown in Fig. 2.

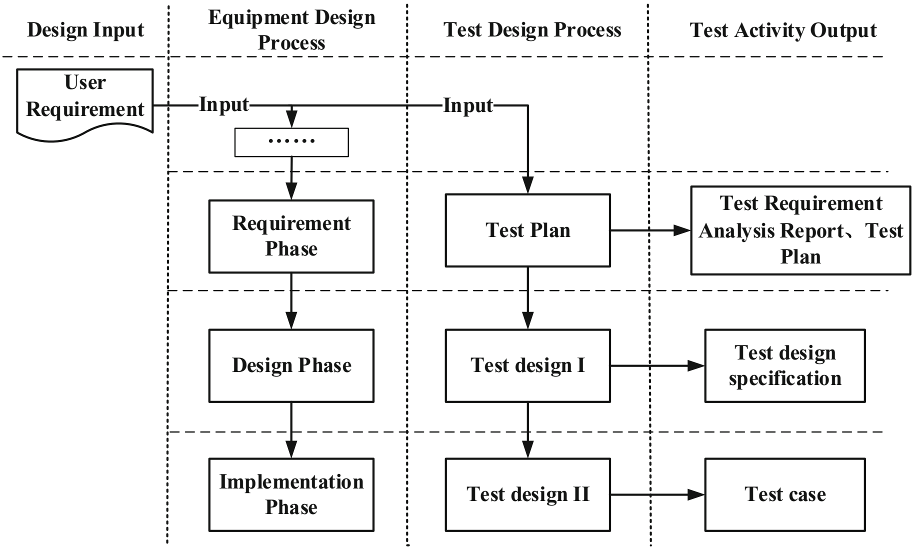


Fig.2. Corresponding diagram of the testing requirement analysis stage

In Fig. 2, the top-level requirements for both the equipment design process and the test design process are user requirements. These two processes are independent of each other and align with the relationship between development activities and V&V activities shown in Fig. 1. The input for the test requirements analysis activity is user requirements, and the output is a test requirements analysis report. To carry out the test requirements analysis activity, first, the user requirements must be obtained. Then, a test requirements analysis is conducted on the obtained requirements. Finally, a requirements traceability relationship is established based on the analysis results.

After investigation, although various literatures have studied the requirement analysis process, these analysis methods cannot be directly applied to the nuclear power industry. For example, Ying Li et al. proposed a scenario analysis method based on INCOSE technical process definition for system requirement analysis [4], and Yunling Shen proposed a software test requirement management process based on TMMi level 3. Among them, the use of test requirement analysis criteria and the establishment and reuse of common test requirement assets can significantly promote the quality of software test requirements [5]. Renyuan Wang et al. adopted the tracking matrix for demand management, which promoted the management to be more efficient and has reference significance [6]. At present, the suppliers of nuclear safety DCS system carry out the analysis of factory testing requirements by relying on their own experience, and the analysis principles and analysis elements have not formed a unified consensus in the industry. On this basis, combined with the experience of "Hualong One" project, this paper proposes a method and principle of nuclear safety DCS factory test demand analysis to ensure that user requirements can be confirmed completely and effectively, so as to improve the quality of nuclear safety DCS products and ensure nuclear safety.

2 Acquisition of User Requirement

2.1 Definition of User Requirement

Referring to the software engineering standard terminology of the Institute of Electrical and Electronics Engineers (IEEE), user requirements are defined as the conditions that meet the user's usage needs (user usage requirements) and the conditions that satisfy the needs specified in the document (document-specified requirements)[7].

2.2 Acquisition and Classification of User Requirement

The user requirements for nuclear safety class DCS suppliers are derived from documents transmitted through the Interface Control Manual (ICM) and contract attachments. These documents are reviewed and confirmed to form the project's design input baseline list, which serves as the basis for requirement acquisition. Taking the standard "Hualong One" unit safety class DCS information provision documents as an example, the files in the design input baseline list are classified into the following six categories based on their content:

1) General requirement documents, such as system requirement specifications and equipment technical specifications, are used to outline the overall requirements for the system's functional performance;
2) Specialized requirement documents, such as default value principles and information security requirement specifications, are used to provide supplementary explanations for the design requirements of a specific aspect or sub-function of the system;
3) Guidelines/principles, such as design guidelines and coding principles, are used as instructive documents to standardize the design process;
4) Manuals for process systems, such as FD/SAMA diagrams, IO lists, and setpoint manuals for process systems like compressed air production systems and equipment cooling water systems;
5) Contract attachments primarily contain technical content related to the system, including equipment technical specifications as well as explanations of deviations and clarifications contained within them;
6) Clarification documents, providing technical clarification explanations for all documents mentioned in 1) to 5).

3 Test Requirement Analysis

3.1 Test Requirement Characteristics

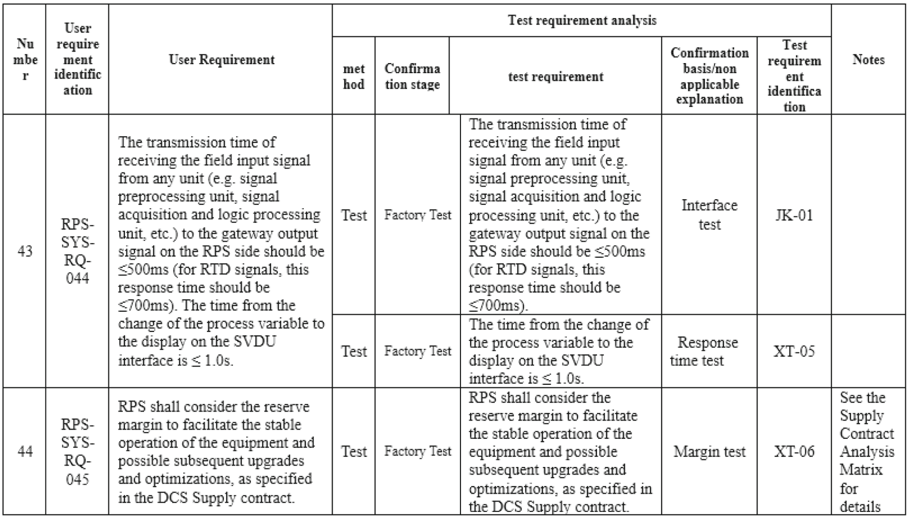
Test requirements are formed after analyzing and organizing user requirements (the extracted description should be consistent with the original text). Test requirements define the content of testing, including the test objects and test scope [8]. Therefore, test requirements possess the following characteristics:

1) Traceability: Each test requirement is bi-directionally traceable to user requirements and vice versa, as well as to the test content.。
2) Testability: Each test requirement must be testable.
3) Clarity: Each test requirement should be clear and explicit (i.e., the test requirement should be able to map to a specific test content).
4) Unique Identification: Each test requirement should have a unique identifier.

3.2 Principles of Test Requirement Analysis

Test requirements analysis is divided into two stages: initial analysis and detailed analysis. During the initial analysis, user requirements that require detailed analysis are screened out. During the detailed analysis, specific test content is analyzed and organized from the user requirements. Combining the characteristics of test requirements, the analysis principles for the six types of user requirement documents are summarized as follows:

1) General Principle: For documents that only require initial analysis, a brief description of the initial analysis results is required. For documents that require detailed analysis, the analysis and organization should be conducted based on the demand identification number or section number as the unit.
2) General Requirements Category: Such documents are analyzed in detail by requirement number or chapter number according to the general principle. The analysis example is shown in Fig. 3.



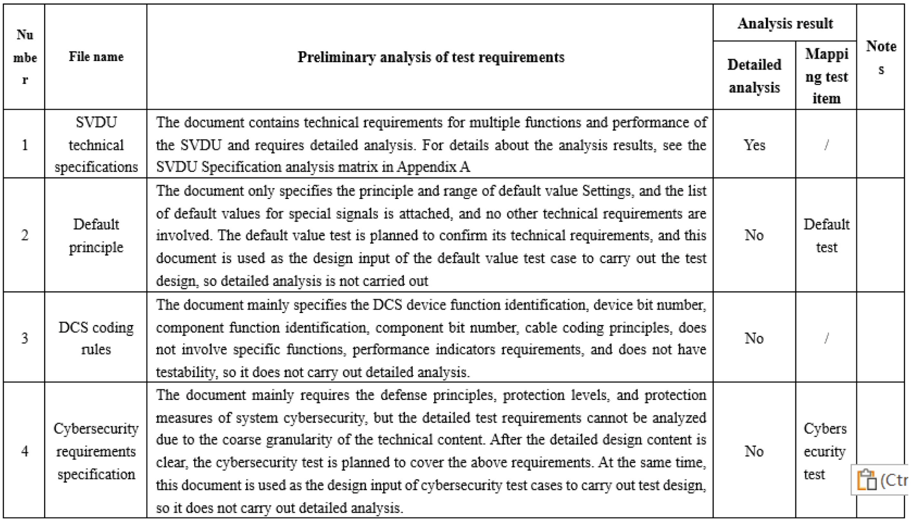
Number	User requirement identification	User Requirement	Test requirement analysis					Notes
			method	Confirmation stage	test requirement	Confirmation basis/non applicable explanation	Test requirement identification	
43	RPS-SYS-RQ-044	The transmission time of receiving the field input signal from any unit (e.g. signal preprocessing unit, signal acquisition and logic processing unit, etc.) to the gateway output signal on the RPS side should be ≤500ms (for RTD signals, this response time should be ≤700ms). The time from the change of the process variable to the display on the SVDU interface is ≤ 1.0s.	Test	Factory Test	The transmission time of receiving the field input signal from any unit (e.g. signal preprocessing unit, signal acquisition and logic processing unit, etc.) to the gateway output signal on the RPS side should be ≤500ms (for RTD signals, this response time should be ≤700ms).	Interface test	JK-01	
			Test	Factory Test	The time from the change of the process variable to the display on the SVDU interface is ≤ 1.0s.	Response time test	XT-05	
44	RPS-SYS-RQ-045	RPS shall consider the reserve margin to facilitate the stable operation of the equipment and possible subsequent upgrades and optimizations, as specified in the DCS Supply contract.	Test	Factory Test	RPS shall consider the reserve margin to facilitate the stable operation of the equipment and possible subsequent upgrades and optimizations, as specified in the DCS Supply contract.	Margin test	XT-06	See the Supply Contract Analysis Matrix for details

Fig.3. Example of Document Analysis for a General Requirements

3) Specialized Requirements Category: This category of documents requires judgment during the initial analysis. If the content of the document involves multiple technical requirements, detailed analysis should be conducted. However, if the content of

the document only involves design requirements for a single function/performance, only the corresponding test items will be mapped during the initial analysis, and no detailed analysis will be conducted. For example, the “SVDU Technical Specification” requires multiple technical indicators such as functionality, graphics, and response time, which require detailed analysis. The analysis process is similar to Fig. 3. On the other hand, the “Default Value Principles” only requires the design of default values and does not include other technical indicators. Therefore, after mapping the test items, detailed analysis is not required. The analysis example is shown in number 2 in Fig. 4.

4) Principles/Guidelines Category: As these documents are not related to specific system functional performance and are not testable, they are not subject to detailed analysis. Instead, a brief description is provided during the initial analysis stage, such as the “DCS Coding Rules.“ The analysis example is shown in number 3 in Fig. 4.



Number	File name	Preliminary analysis of test requirements	Analysis result		Notes
			Detailed analysis	Mapping test item	
1	SVDU technical specifications	The document contains technical requirements for multiple functions and performance of the SVDU and requires detailed analysis. For details about the analysis results, see the SVDU Specification analysis matrix in Appendix A	Yes	/	
2	Default principle	The document only specifies the principle and range of default value Settings, and the list of default values for special signals is attached, and no other technical requirements are involved. The default value test is planned to confirm its technical requirements, and this document is used as the design input of the default value test case to carry out the test design, so detailed analysis is not carried out	No	Default test	
3	DCS coding rules	The document mainly specifies the DCS device function identification, device bit number, component function identification, component bit number, cable coding principles, does not involve specific functions, performance indicators requirements, and does not have testability, so it does not carry out detailed analysis.	No	/	
4	Cybersecurity requirements specification	The document mainly requires the defense principles, protection levels, and protection measures of system cybersecurity, but the detailed test requirements cannot be analyzed due to the coarse granularity of the technical content. After the detailed design content is clear, the cybersecurity test is planned to cover the above requirements. At the same time, this document is used as the design input of cybersecurity test cases to carry out test design, so it does not carry out detailed analysis.	No	Cybersecurity test	

Fig.4. Example of Preliminary Analysis for Test requirements

5) Process System Category: This category of documents involves drawings, setpoint manuals, and other materials that require detailed analysis. The analysis method involves identifying on the drawings the specific functional test scripts that correspond to each confirmed logical function. Since the specific test scripts for logic confirmation cannot be identified during the test requirements analysis phase, the labeling work for this category of documents is carried out during the test design phase. However, during the test requirements analysis phase, only a brief description is provided in the initial analysis. An example of the final test design phase labeling is shown in Fig. 5.

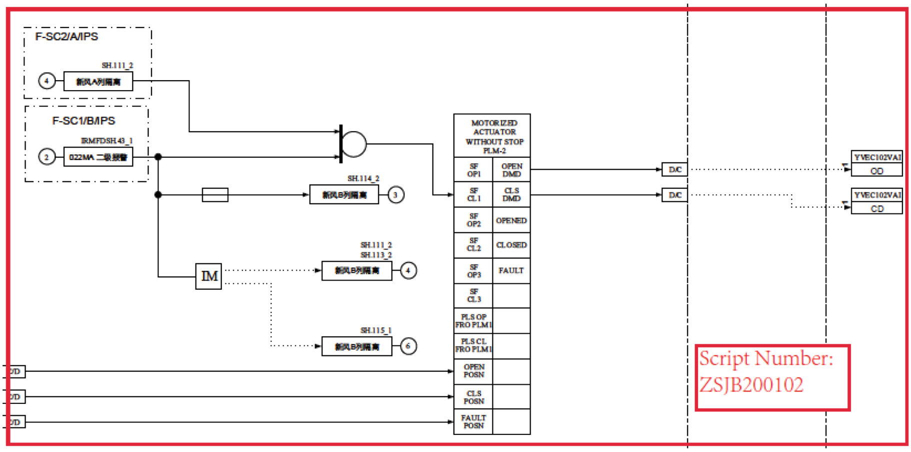


Fig.5. Example of Document Identification for Process System Manual

6) Contract Attachments: Only the equipment technical specifications and their deviation and clarification statements involving technical content in the contract attachments shall be analyzed. The analysis shall be conducted in detail according to the general principles.
7) Clarification Documents: When analyzing clarification documents, they should be considered as an integral part of the source documents they clarify, and no separate analysis or explanation should be conducted.
8) Other Principles: Among the user requirement documents listed from 1) to 7), if a document is found to require detailed analysis during the initial analysis stage but the extracted test requirements are not clear due to the coarse granularity of its content (i.e., unable to map out specific test items or criteria), then it is acceptable to indicate in the initial analysis stage that detailed analysis will not be conducted for that document. However, appropriate test items should be identified and planned to ensure that the requirement is confirmed in the final stage. For example, the "Information Security Requirement Specification" states: "Adopt technical means to ensure that only authorized devices can access the instrumentation and control system network." This requirement does not specify the specific technical means and protective devices, and it is not possible to extract clear test requirements. Therefore, detailed analysis may not be conducted during the test requirements analysis, but information security functional testing should be mapped during the initial analysis stage for final confirmation. The analysis example is shown in number 4 in Fig. 4.

3.3 Elements of Test Requirement Analysis

Based on the principles of test requirements analysis, when conducting a detailed analysis of user requirement documents, it is necessary to proceed on a clause-by-clause and sentence-by-sentence basis according to the user requirement identification numbers, and extract and organize the test requirements therefrom. To ensure the completeness of the confirmation of user requirements, the traceability of test requirements, and a clear