Lecture Notes in Electrical Engineering 1055

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

New Energy Power Generation Automation and Intelligent Technology

Proceedings of the Seventh Seminar on Digital Instrumentation and Control Technology for Nuclear Power Plant

Springer

Lecture Notes in Electrical Engineering 1055

Series Editors

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 ·
Rigang Chen · Yongbin Sun · Zheming Liu
Editors

New Energy Power Generation Automation and Intelligent Technology

Proceedings of the Seventh Seminar on Digital Instrumentation and Control Technology for Nuclear Power Plant

Springer

Editors
Pengfei Gu
China United Heavy Duty Gas Turbine Technology Co., Ltd.
Shanghai, China

Yang Xu
Department of Engineering Physics
Tsinghua University
Beijing, China

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

Rigang Chen
China Nuclear Power Engineering Co., Ltd.
Beijing, China

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

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

ISSN 1876-1100 ISSN 1876-1119 (electronic)
Lecture Notes in Electrical Engineering
ISBN 978-981-99-3454-6 ISBN 978-981-99-3455-3 (eBook)
https://doi.org/10.1007/978-981-99-3455-3

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

Contents

Application of Lightning Protection Measures for Outdoor Instruments in Nuclear Power Plants

Hai-rong Lu(✉), Bo Yao, Xu-tao Bai, and Xiao-chen Zhang

Suzhou Nuclear Power Research Institute Co., Ltd., Suzhou 215004, Jiangsu, China
luhairong041@sina.com

Abstract. Taking the reactor dome flow monitoring instrument as an example, analysis and comparison is made on the routine lightning protection measures such that lightning protection devices are added in the design of signal acquisition circuit to improve the lightning protection availability of equipment and circuits and reduce the effect on DCS (digital control system). The practical application shows that this approach brings about minor effect on the signal acquisition circuit, features a flexible layout, convenient maintenance, and strong resistance to multiple lightning strikes, and is available for offering reference in the lightning protection of other equipment and apparatus.

Keywords: Outdoor instrument · Lightning protection devices · Signal acquisition circuit · Nuclear power plant

1 Introduction

Chinese nuclear power plants are mainly distributed in the southeast coastal areas of China, which suffer from extreme weather conditions such as typhoons, lightning strikes, and rainstorms all the year round. The working conditions of nuclear power units are restricted by the climatic environment in its vicinity. Therefore, the prevention and resistance of typhoons, lightning strikes and rainstorms (abbreviated as "three prevention countermeasures") is one of the important disaster prevention and mitigation activities necessary for each nuclear power plant. Among them, lightning strike has attracted more attention due to its unpredictability, which might bring about severe consequences for power and electronic system and components, especially for the weak current system and components, with constraints on the stable operation of nuclear power plants.

The flow monitoring instrument installed on the reactor dome of a nuclear power plant is mainly used to measure the flow rate of the exhaust gas discharged from the nuclear power unit into the atmosphere, and to calculate the total amount of radioactive substances exhausted. The front end of the instrument is installed on the guardrail of the dome chimney maintenance platform, which is among the instruments installed in the toppest elevations all over the plant. In its initial design, considerations are made on the arrangement of chimney with complete lightning protection grounding measures. The

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 1–9, 2023.
https://doi.org/10.1007/978-981-99-3455-3_1

instrument is only designed to shield the signal lines for grounding, whereas, in its actual operation, the lightning protection pattern shows a poor effect, and there have been some cases on signal fluctuations of DCS system and even damages of the acquisition boards inside cabinet in nuclear power plants caused by lightning strikes.

Taking the flow monitoring instrument, a typical outdoor and high-altitude equipment, installed on the reactor dome of a nuclear power plant as an example, it discusses and analyzes several different improvement approaches, with considerations of factors concerning field implementation, lightning protection effects and availability, routine maintenance and repairs, etc., an approach by adding a lightning protection device in the lines is selected to improve the lightning protection availability of the entire data acquisition circuit and apply it on site.

2 Analysis of the Effect of Lightning Strikes on Instruments

Lightning is a common natural phenomenon, which is mainly the discharge between thunderstorm clouds or between thunderstorm clouds and the ground, that is, the phenomenon of lightning strikes. Usually, according to the different characteristics of lightning generation and harms caused, direct lightning strikes, lightning inductions (including electrostatic induction, electromagnetic induction), electromagnetic pulse interference, lightning surge intrusion, etc. [1–3]. Lightning strikes have a great effect on the power and electronic system and components, especially the current control system, communication system, instrumentation components, etc., which apply a large number of integrated circuits and high-sensitivity electronic components, making it difficult for systems or equipment to withstand the damage caused by lightning strikes.

Generally, the main hazards of lightning strike to instruments are as follows: 1. Equipment damage directly suffered from lightning strike; 2. Lightning induction occurs during lightning strikes, and impulse current/voltage is instantaneously generated on the line, resulting in damage to instruments or signal acquisition devices or fluctuation of acquired signals. The flow monitoring instrument installed on the reactor dome of a nuclear power plant, which is among the instruments installed at the highest elevations in the whole plant, is a kind of accident-prone equipment with failures due to lightning strikes. A nuclear power plant in Guangdong Province of China once experienced many times during operation that large fluctuations occurred in the instrument signals under lightning strikes, and even the back-end DCS system acquisition boards were damaged [1–3].

Comprehensive analyses are conducted on the previous events of alarm and equipment damages caused by lightning strikes occurred in the flow monitoring instruments installed on the reactor domes of a nuclear power plant as example [1]:

(1) The probability of damage to the instrument is very low, as the dome chimney has been equipped with lightning protection devices such as lightning rods and lightning strips. The probability of lightning strikes with direct damage to the instruments is very low, and the current can be discharged quickly through the existing configuration, which caused limited harms to the instruments.

(2) The measurement signal fluctuations of the instruments and even the damage of the acquisition boards is directly caused by lightning induction/electromagnetic interference. After lightning strikes the lightning rods, the instantaneous current generates induced current or voltage to the instrument signal line and shielded line through the grounding wires, which causes the measurement signal fluctuations in case of coupling interference. When the over-limit induced current/voltage enters the back-end system along the lines, it is easy to do harm to related equipment.
(3) As simulating damage to the instruments caused by lightning strikes in the laboratory, when the lightning rods and lightning strips are connected with lightning, abnormal signals can be detected in the signal line and the shielding line of instrument signals, and the data shows that there are fluctuations or even exceeding the limit values.

3 Optimization Plan and Analysis

3.1 Improve Circuit Grounding

In view of the lightning strike interference problems exposed, the requirements of shielding, grounding and equipotential bonding in *GB 50057-2010 Code for design protection of structures against lightning* are given: "In the space requiring protection, when shielded cable is used, the shielding layer shall be at least at both ends, and equipotential connection shall be made at the junctions of lightning protection area. When the system only requires equipotential connection at one end, two layers of shielding or steel pipes shall be used for laying, and the outer shielding or steel pipes shall be at least at both ends, and equipotential connection shall be made at the junctions of lightning protection area." The on-site grounding pattern should be checked and the grounding circuit should be improved as follows [3]:

(1) Connect the instrument body and protective cover to the dedicated grounding point near the dome chimney;
(2) Install metal sleeve or galvanized steel pipes for the circuit signal shielding cables that do not enter the cable tray, and form the continuous grounding together with the cable tray.

By improving the grounding of the signal circuit, the effect of loop interference shielding is increased, however, this method is not enough to eliminate the effect of lightning strikes, only available to reduce the interference to a limited extent, and further improvement measures are needed (Fig. 1).

3.2 Add Signal Isolation Device

Based on the consideration of preventing damage to the DCS boards, a signal isolation device can be added to the signal loop, and the conversion (electrical signal – optical signal - electrical signal) of the intermediate measurement signal can be used to isolate and block the possible electromagnetic interference that may be generated in the signal loop, so as to realize the purpose of protecting cabinet equipment [1], as shown in Fig. 2.

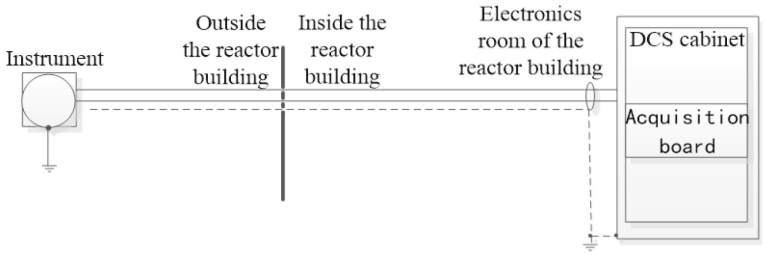


Fig. 1. Indication of ground loop

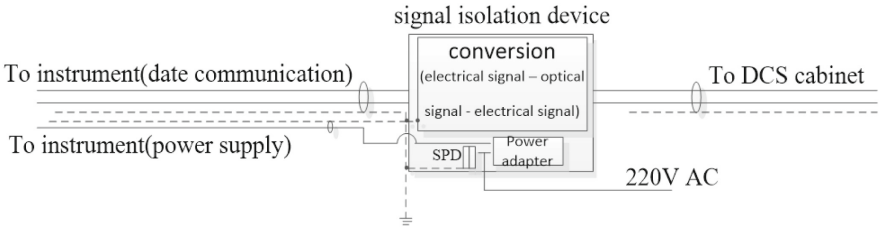


Fig. 2. Add signal isolation device

This approach is available to effectively prevent the damage of over-limit current/voltage to the DCS system and effectively protect the important components of the system, whereas, several problems remain:

(1) The instrument acquisition system is nuclear grade, which needs to meet the nuclear grade K3 identification in the design specification, and special research and development activities shall be done on such a device.
(2) This approach solves the problem of equipment protection, however, some more risk points are induced in the circuit:
   ① The signal isolation device isolates the power supply of the instrument at the same time, and a stable power supply meeting the requirements shall be specially provided.
   ② As for its practical application, a photoelectric converter means a relatively high damage rate in the case of lightning strikes, while it is easy to replace.

3.3 Add Lightning Protection Device

Similarly, in consideration of equipment protection, lightning protection device is added to the signal loop to limit the possible electromagnetic interference that may be generated in the signal circuit through the SPD (Surge Protective Device) and thermistor in the device, which can resist multiple lightning strikes, and realize the purpose of protecting cabinet equipment, as shown in Fig. 3.

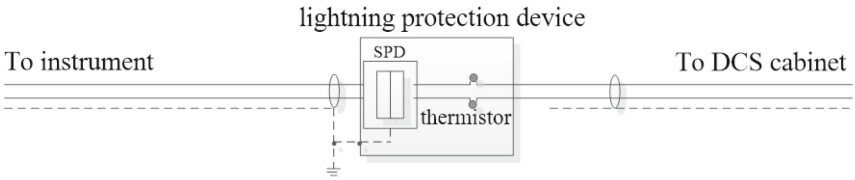


Fig. 3. Add lightning protection device

The main functions of adding lightning protection device are as follows:

(1) Current release: the current generated by lightning strikes is divided into the ground, removing most of the energy of lightning strikes, so that the lightning pulse cannot reach or only rarely reaches the upstream equipment.
(2) Voltage limiting: When lightning strike-caused overvoltage enters, both ends of the surge protector will maintain a certain voltage (residual voltage), which is within the tolerable range of the equipment.
(3) Current limiting: The thermistor limits the passing current in a proper range based on its characteristics, so that the over-limit current is isolated.

This approach can also effectively prevent the damage of over-limit current and voltage to the upstream equipment, but it also requires special research and development and K3 level identification of the device, and the circuit is considered as a fault point.

3.4 Add Lightning Protection Device and Signal Isolation Device

The scheme combines the advantages of lightning protection device and signal isolation device to maximize the safety of equipment under lightning strikes. In contrast to the devices implement separately, this configuration is possessed of such advantages as follows [1]:

(1) As the first layer of protection, lightning protection device is available to timely discharge and limit voltage/current to the surge current generated by direct lightning strikes and induction of lightning, so as to reduce the damage of pulse to equipment.
(2) Signal isolation device, as the second layer of protection, further “filters” the input current and voltage to isolate related risks. Meanwhile, the protection function of lightning protection device improves the ability of signal isolation device to withstand lightning strikes and further improves its reliability.

The protection capability of this scheme has been further improved, but the K3 level identification, power supply, and difficulty of implementation need to be comprehensively considered.

4 Analysis and Implementation

4.1 Comparison and Confirmation of Different Schemes

Based on the foregoing analyses and the temporary measures on site, a summary is made as in Table 1:

Table 1. Comparison of different schemes

Number	Schemes	Advantage	Defect
1	improve circuit grounding	easy to implement	Unavailable to fundamentally solve the problem
2	instrument displacement	reduce the effect of lightning strikes	difficult to implement, and the extension of sampling pipeline has an effect on measurement. Basically, the instrument is still at altitude outdoors, which is unavailable to fundamentally solve the problem
3	signal isolation	available to avoid the effect of lightning strikes and easy to maintain	Consider more fault risk points and independent power supply, difficult to implement, and invulnerable to withstand multiple lightning strikes, and necessary for the requirements of nuclear grade K3 identification
4	lightning protection device	available to avoid the effect of lightning strikes and easy to maintain	Consider fault risk points, easy to implement, and available to withstand multiple lightning strikes, and necessary for the requirements of nuclear grade K3 identification
5	lightning protection device and signal isolation	available to avoid the effect of lightning strikes and easy to maintain	Consider more fault risk points and independent power supply, difficult to implement, and available to withstand multiple lightning strikes, and necessary for the requirements of nuclear grade K3 identification

Based upon the comparative analyses of schemes 1–5, with comprehensive considerations in the difficulty of on-site implementation and resource inputs, the lightning protection device added in scheme 4 is relatively balanced in all dimensions, which is recommended for field application, and meanwhile the grounding is reasonably optimized with reference to scheme 1.

4.2 Effect Analysis

4.2.1 Compliance Analysis on Specification

According to the design criteria of the grounding standard for a nuclear power island: "The signal and low-voltage cables of the instrument control system that are introduced from outside the protection area and might suffer direct lightning strikes, and cables or components that are protected against direct lightning but not induced lightning, should adopt surge protection devices." And also, the *RCC-E Rules for design and construction of nuclear electrical equipment in island* requires: "The protection attenuation approach for sensitive equipment especially includes the installation of secondary protection against overvoltage (surge protector)", the scheme configuration meets the requirements of relevant provisions of the standard specifications for nuclear island grounding.

According to *GB50343-2012 Technical code for protection of building electronic information system against lightning*, "On the basis of external lightning protection measures, the electronic information system of buildings should select equipotential connection and grounding, electromagnetic shielding, reasonable wiring, and surge protection according to the situation." The scheme configuration is also available to meet the relevant external and internal lightning protection measures.

4.2.2 Effect Analysis on Instrument Measuring Circuit

1. Effects of instrument load driving capacity

The field instruments adopt the transmitters of Rosemount 3051 series. According to the load characteristics of transmitters in Fig. 4, it is regarded that when the power supply voltage is about 24 V, the maximum loop load is 600 Ω. As the DCS system uses the Mitsubishi current signal acquisition card (MLPJ-02) and the sampling resistance is about 250 Ω, it can be inferred that the single-line impedance should not exceed 125 Ω, and the device bus group should not exceed 350 Ω. The actual lightning protection device meets the requirements of line resistance control.

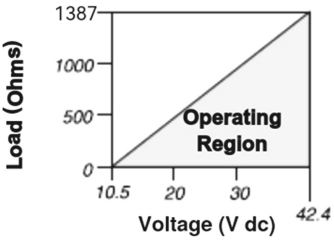


Fig. 4. Instrument load characteristics

2. Shielding grounding effect

According to the requirements of shielding, grounding and equipotential connection in *GB50057-2010 Code for design protection of structures against lightning*, and

GB5027-2007 Design Code for Power Engineering Cables, "The shielding layer of control cables for the analog signal circuit of the computer monitoring system shall not constitute two or more points of grounding, and shall be grounded at one point in a centralized manner", and "When the interference of electromagnetic induction is large, two-point grounding should be adopted, and meanwhile when the interference of electrostatic induction is large, one-point grounding can be adopted. Double shielding or composite overall shielding is proposed to adopt one-point and two-point grounding for the inner and outer shields respectively". At present, the instrument has realized double-layer shielding through the optimization and improvement of circuit grounding, in which the inner cable is grounded at one end and the outer layer is a combination of cable tray with metal sleeve or galvanized steel pipe, forming continuous grounding and multi-point grounding in form, which meets the specification requirements.

3. Effect of response time

The surge protector and thermistor in the added lightning protection device are both resistive loads and have extremely minor effects on the current signal transmission. At the same time, the DCS system does not have high requirements for analog signal acquisition and response. Therefore, the added device would not affect the signal acquisition response time of the whole circuit.

5 Implementation

Based on the above analyses of the lightning protection measures for the flow monitoring instrument on the reactor dome, a nuclear power plant in Fujian Province of China conducted grounding investigation and improvement of the shielded lines of signal circuit upon receiving feedback from the instrument suffering lightning strikes. However, considering that such a measure was not enough to eliminate the risk of lightning strike interference, the plant continued adopting the lightning protection device to optimize and improve the signal circuit, and the relevant transformation was completed in July 2016. The technical parameters of lightning protection device are shown in Table 2.

Table 2. The technical parameters of lightning protection device

Working voltage	24 V
Voltage protection level	≤300 V
Interruption voltage	80 V
Working current	4–20 mA
Single-line impedance	≤75 Ω
Electeic shock	2 kA
Total inrush current	20 kA
Response time	≤5 ns
Identification level	K3 (GB/T 2423&GB/T 13625)

Up to now, the dome flow monitoring instrument has experienced several seasons of high incidence of multiple lightning strikes, and there has not been a large fluctuation of data caused by lightning strike interference or damage to DCS panels. At the same time, according to the results of the cross-comparison of measurement data in the regular verification of annual instruments, instrument error is controlled within a prescribed range, and there is no instrument degradation or failure.

6 Conclusion

Taking the reactor dome flow monitoring instrument as an example, the conventional lightning protection measures are analyzed for comparison, and the approach by adding lightning protection devices to the line is adopted to improve the lightning protection capability of the entire data acquisition circuit. Upon the implementation of the lightning protection measures completed, the outdoor instruments are available to effectively deal with the interference of lightning strikes, and the effects on the DCS system could be reduced. Practice proves that such a lightning protection measure offers a relatively economical and convenient solution against the interference of lightning strikes for nuclear power plants, which is available for reference with applicable values in the lightning protection of other instruments.

References

1. Lin, G.: Lightning protection improvement of chimney flow-meter in the nuclear power plant. Scientific and Technological Innovation, no. 23, pp. 165–166 (2020)
2. Li, F, Ji, T., Chen, Y.: Understanding the new development of lightning disaster – britf-talk on the harmfulness of lightning to CATV and computer network system. CATV Technology, no. 3, pp. 49–51 (2001)
3. Ye, X.: Lightning protection engineering design for instrument and control system. Automation in Petro-Chemical Industry, vol. 56, pp. 1–9 (2020)
4. Standardization Administration, China. Technical code for protection of building electronic information system against lightning. GB50343-2012
5. Standardization Administration, China. Code for design protection of structures against lightning. GB50057-2011
6. Standardization Administration, China. Code for design of cables of electric engineering. GB5027-2008
7. AFCEN, EDF, FRAMATOME. Rules for design and construction of nuclear electrical equipment in island. RCC-E (2008)
8. Zhong, S.: Anti-interference design of lightning protection and grounding of instrument and control system in nuclear power plant. Scientific and Technological Innovation and Application, no. 30, pp. 112–113 (2017)
9. Zhang, Z., Gao, W., Wang, H.: Discussion on lightning protection of physical protection system in nuclear power plant on lightning effect. Science & Technology Vision, no. 34, pp. 290–291 (2015)
10. Yang, Y., Wang, C., Du, J.: Analysis of the factors influencing coordination effectiveness of SPD in substation surge protection. Electric Safety Technology, no. 11, pp. 36–39 (2020)

Study on High Flux at Shutdown Alarm Setpoint Automatic Update Logic

Wen-Qing Yang(✉), Xiao-Fei Li, Wen-Qian Liu, Chao Wang, Bo Lv, Ji-Kun Liu, and Hao Luo

State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment, China Nuclear Power Engineering Co., Ltd., Shenzhen 518172, Guangdong, China
vencentyoung@gmail.com

Abstract. The source range of the nuclear instrumentation system (RPN) is used to monitor the reactor neutron flux from shutdown to initial startup. When the count rate measured by source range detector is higher than the set value, a "high flux at shutdown alarm" will be triggered. This alarm alerts the operators that positive reactivity has been added to the core, such as unexpected dilution or control rods withdrawal. This paper analyzes the source range high flux at shutdown alarm setpoint update logic of a nuclear power plant. It is found that the setpoint will be updated to a low value after the source range is automatically put into operation, resulting in false triggering of the alarm. This paper discusses the avoidance measures of alarm false triggering from the perspective of operational administration and control logic optimization. The results show that both measures are feasible.

Keywords: RPN · High flux at shutdown alarm · Operational administration

1 Introduction

The nuclear instrumentation system continuously measures and monitors the nuclear power of the reactor. Since the nuclear power measurement range spans multiple orders of magnitude, the RPN is divided into three ranges: source range (SR), intermediate range (IR) and power range (PR). The implementation of different ranges improves the measurement accuracy [1].

The source range channel is used for the core neutron flux measurement from the refueling to the initial start-up stage. The boron-coated proportional counter tube is used as the neutron detector for SR, and the neutron flux level is characterized by the count rate output by the channel.

This paper analyzes the high flux at shutdown alarm logic of RPN source range channel in a NPP, and discerns that the automatic update function of the alarm setpoint in this logic has the problem of false triggering of the alarm after the channel is put into operation.

In this paper, two feasible measures are proposed to prevent false triggering of the alarm, and both the advantages and disadvantages of different measures are analyzed.

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 10–17, 2023.
https://doi.org/10.1007/978-981-99-3455-3_2

2 High Flux at Shutdown Alarm

The RPN source range channel is equipped with an alarm function of high neutron flux rate in shutdown. This alarm reminds the operators that the sub criticality of the reactor is reduced, and the core has the risk of approaching criticality. With this alarm, operators can find out the mis-dilution of the boric acid in coolant or the accidental extraction of the control rods timely.

According to the conclusion of the safety analysis, if the threshold of the high flux at shutdown alarm is set within 3 times the current count rate, the operator will have enough time to intervene in the state of the unit to avoid accidental criticality approaching [2]. Considering the statistical fluctuation of the count rate at low flux level [3], the alarm setpoint is generally set to a value which is 2 to 3 times the current count rate.

The triggering logic of the high flux at shutdown alarm is shown in Fig. 1. If the alarm is not manually blocked, once the count rate exceeds the alarm setpoint, while the source range protection function is not blocked, the alarm is triggered. The alarm information on screen and the alarm light remind operators to intervene. At the same time, a horn inside the reactor building sends out an alarm sound to remind the personnel to evacuate [4].

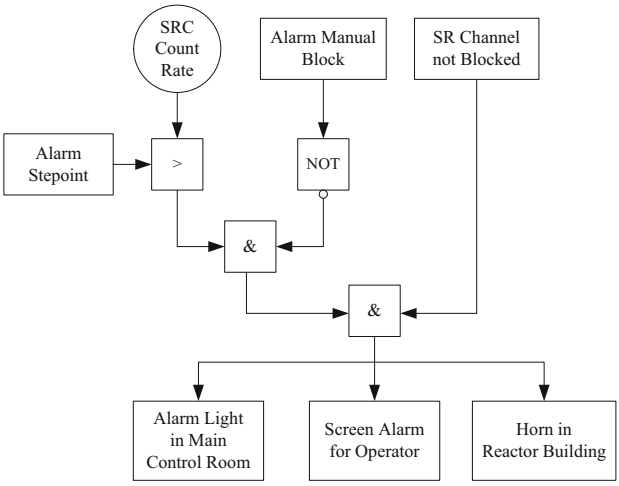


Fig. 1. High Flux at Shutdown Alarm Logic

3 Alarm Setpoint Automatic Update Logic

3.1 Setpoint Update Manually During the Startup Phase

During the start-up, the source range count rate continues to increase with the adding of positive reactivity. In the process of count rate increase, if the alarm setpoint is automatically updated, the setpoint will be continually greater than the measured value,

so that the alarm cannot be triggered. Therefore, the setpoint should not be automatically updated during the flux increasing stage. The operator needs to update the setpoint manually when the measured count rate is close to the alarm setpoint. After manual update, the alarm setpoint is set to 2.5 times the current count rate.

During power operation, after the current measured by the intermediate range exceeds the P6 setpoint (P6 indicates that the reactor has reached its criticality), it is allowed to block the source range to prevent the SR detector from operating at excessively high flux level. In addition to the initial criticality after refueling, when the P10 signal (P10 indicates that the reactor power is 10% of full power) appears during normal operation, the source range will be blocked automatically.

3.2 Setpoint Update During Shutdown Phase

After the reactor is shut down, due to the decay of the delayed neutron precursor nucleus, the neutron flux will decrease exponentially with a period of about -80s after the shutdown, until it stabilizes at the subcritical breeding equilibrium level [5]. When the current value measured by intermediate range drops below the setpoint of the P6 which means the core is now subcritical. Once the NOT P6 signal is triggered, the source range channel is automatically put into operation. At this time, the count rate of the source range channel still shows an exponential downward trend. Figure 2 shows the trend of the count rate after the source range is put into operation during the reactor trip.

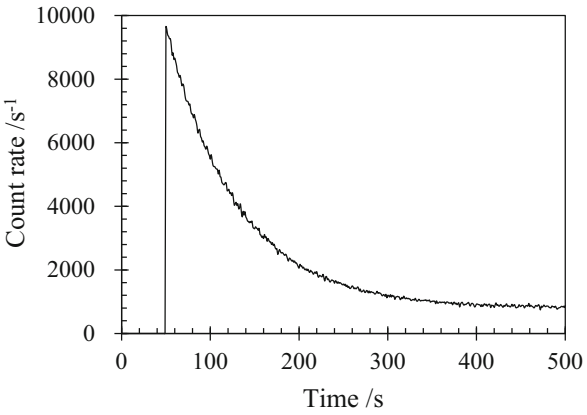


Fig. 2. SRC Automatic Re-Used After Reactor Trip

Due to the continuous decrease of the count rate after the shutdown, in order to achieve immediate protection, the system will trigger an automatic update when the alarm setpoint exceeds 2.8 times (2.50×1.12) the current count rate. After the automatic update, the alarm setpoint is set to 2.5 times the current count rate. The automatic update function ensures “dynamic tracking” of the alarm setpoint to the measured count rate in the flux drop phase. The specific logic is as follows (Fig. 3):

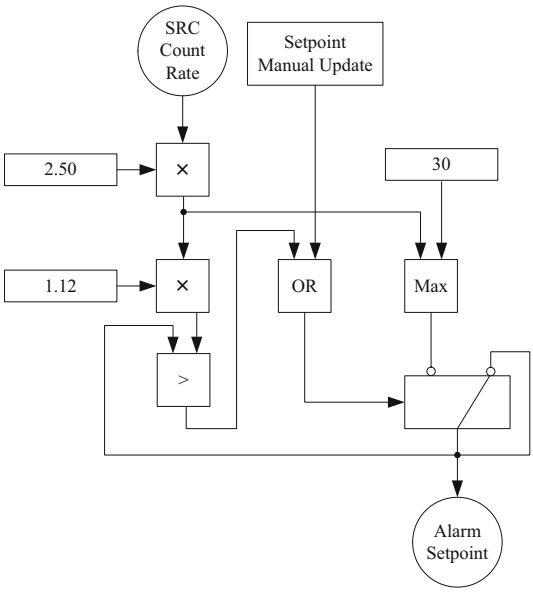


Fig. 3. High Flux at Shutdown Setpoint Updating Logic

3.3 Analysis of False Triggering of Alarm

The source range detector adopts a boron-coated proportional counter tube, and the detector needs to work with a certain high voltage. Under the condition that the external neutron flux rate is constant, the curve of the detector count rate and high voltage is called the detector high voltage plateau curve [6], as shown in the Fig. 4.

It can be seen from the high voltage plateau curve that the detector can only output the count rate when the high voltage exceeds a certain amplitude, and as the high voltage approaches its setpoint, the count rate continues to increase.

After the source range is put into operation, the high voltage of the detector gradually returns to the working voltage. During the high voltage recovery process, the count rate of the source range gradually increases from the lower limit of the range according to the trend of the high voltage plateau curve.

In the initial stage of high voltage establishment, the source range count rate is low, and 2.8 times of the count rate is less than the alarm setpoint which was set before SRC blocking, so the alarm setpoint automatic update logic will be triggered, and the setpoint is updated from the higher value to a lower value. As the high voltage establishment process continues, the source range count rate continues to increase until it reaches the current flux level count rate (about 10^5 s^{-1}). During the increase of the count rate, the high flux at shutdown alarm is falsely triggered.

According to the above analysis, after the normal shutdown or accidental reactor trip, due to the existence of the automatic update logic of the alarm setpoint, the automatic operation of the source range will lead to the triggering of the high flux at shutdown alarm when the reactor is shut down. False alarm is interference information for the operator, which will affect the operator's normal judgment on the state of the unit. Especially in

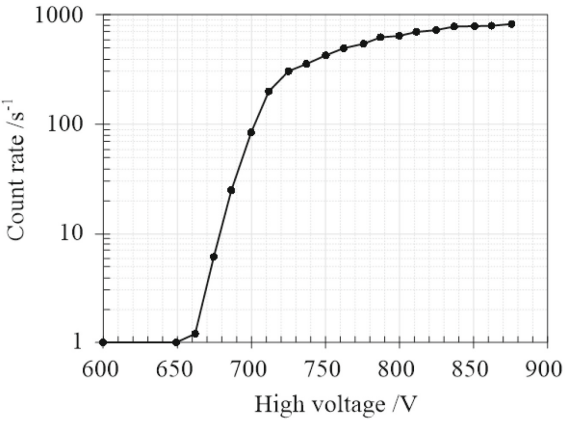


Fig. 4. SRC Detector High Voltage Plateau Curve

the transient stage after the unit accidental reactor trip, the false alarm may also interfere with the ongoing accident procedures.

According to feedback, the high flux at shutdown alarm was falsely triggered during the zero power physical test after the first critical in a third generation unit for this reason.

4 Measures to Avoid False Alarm of High Neutron Flux Rate in Shutdown

The purpose and applicable stage of the high flux at shutdown alarm in shutdown are discussed, and the following avoidance measures are proposed.

4.1 Operational Administration

The purpose of setting the high flux at shutdown alarm is to remind the operator that abnormal positive reactivity is introduced to the core in the shutdown state. When the unit is ready to start, the "shutdown state" assumption of the alarm no longer exists. At this time, the introduction of positive reactivity is to make the unit reach the critical state. During this process, the increase of the neutron flux is an expected event, so the high flux at shutdown alarm is unnecessary for the critical process.

In order to reduce the unnecessary manual update of the alarm setpoint by the operator, the alarm can be blocked by a hardware key before the normal start-up. After the alarm is blocked, the corresponding protection function is realized by the SR high flux reactor trip.

After planned shutdown or the accidental reactor trip, the "stable shutdown" state cannot be reached immediately due to the neutron flux continued to decrease slowly. When the source range count rate reaches the stable count rate in the shutdown state, update the alarm setting manually before the unlock of the alarm by key switch release.

4.2 Setpoint Update Logic Optimization

Since the operation of the source range detector involves the process of high voltage establishment, it is considered to block the alarm during the establishment process. After the count rate has returned to a higher level after the establishment, the count rate will be updated once by a pulse signal.

After the source range is put into operation again, the high flux at shutdown alarm will take effect after a delay of 10 s. Even if the alarm setpoint is brushed to a low value during the voltage establishment process, the alarm will not be triggered within 10 s (Fig. 5).

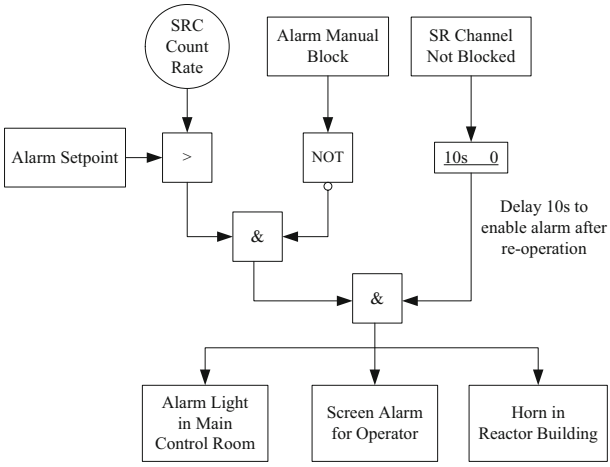


Fig. 5. Alarm Enabled Delay After SRC Re-Used

The disappearance of the detector high voltage loss signal indicates that the voltage establishment process has been completed and the detector count rate has recovered. After the high voltage loss signal disappears, a delay of 3 s (enough time to stabilize the high voltage) triggers a pulse to update the alarm setting, which can automatically update the current setpoint (updated during the high voltage establishment process, lower value) to a normal value (Fig. 6).

Under the premise of not affecting the original automatic update logic, the above optimization avoids the false triggering of the alarm after the source range is put into operation again due to the high voltage establishment process.

4.3 Comparison of the Two Measures

The way of avoiding false triggering of alarms through operational administrative management is consistent with the requirements of the current second-generation reactor operation procedures, and there is no need to modify the control logic. The disadvantage is that it needs to manually block the alarm every time the reactor starts up, and manually unblock the alarm after shutdown. The blocking of the alarm reduces the protection coverage to some extent.

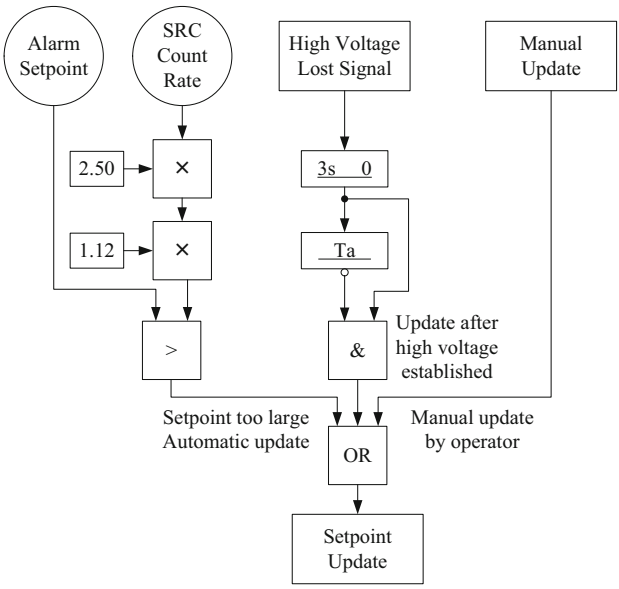


Fig. 6. Alarm Setpoint Update Logic Optimization

The optimization of the setpoint update logic can solve the problem of false alarm triggering from the source, and there is no need to block the alarm, which is equivalent to expanding the coverage of the protection.

In a EPR plant, during the start-up physical test, when the IR current decreased below P6 set-point, the SR was put into operation automatically. Almost at the same time, the SR high flux at shutdown alarm was trigged. After the modification of the control logic and onsite verification, the defect of the control logic has been fully eliminated.

5 Conclusion

From the point of view of the alarm purpose, it is feasible to apply administrative control measures, which can completely avoid false triggering of the alarm. Starting from the working principle of the source range, adaptation of the alarm delay and the update logic after the voltage is established can solve the problem of false triggering from the source. The choice of the two measures should be made according to the requirements of the technical specification and accident analysis for the availability of alarm.

References

1. Mao, H., Xiong, W., Que, J., et al.: The principle and engineering practice of ex-core nuclear instrumentation system in nuclear power plant. Nucl. Electron. Detect. Technol. **34**(6), 758–761 (2014)
2. Wang, X.: Analysis of Boron Dilution Accident. China Nuclear Power Design Co., ltd, Shenzhen (2014)

3. Li, L., Wang, Z., Guan, Z., et al.: The effect of statistical fluctuation on control operation and the method of its elimination in nuclear gauge. Nucl. Electron. Detect. Technol. **2**, 87–91 (1993)
4. Li, J., Fan, W.: Section 6.2 Alarm Card of Nuclear Instrumentation System (RPN) System Design Manual. Shenzhen CGN Engineering Design Co., Ltd. (2019)
5. Xie, Z., Wu, H., Zhang, S.: Physical Analysis of Nuclear Reactors, pp. 240–242. Xi'an Jiaotong University Press, Xi'an (2004)
6. Tang, B., Ge, L., Fang, F., et al.: Principles of Nuclear Radiation Measurement, pp. 120–125. Harbin Engineering University Press, Harbin (2011)

Experimental Research on Data Management Method of Instrument and Control Emulation System

Hao Peng(✉), Xu Zhang, Lei Tang, Yan-qun Wu, Yu Zhang, and Meng-bing Zheng

Science and Technology on Reactor System Design Technology Laboratory, Nuclear Power Institute of China, Chengdu, China
tonghuaph@qq.com

Abstract. The instrument and control (I&C) emulation system that developed based on virtual technology is an effective mapping of physical I&C system. It can realistically reflect the properties of physical system, and can be applied to verify profit intelligent control strategies. In the stage of solution design, it is definitely necessary to analyze data storage and interaction procedures of each process or thread that represents various functions in system. Moreover, some simulation functions, for instance, saving and loading initial conditions, involve the management for various data types. Therefore, overall management for internal and external data is indispensable. Refer to above requirements, this paper proposes a set of data management methods that include interface design and process optimization for data interaction in I&C system. The method has been proven to be beneficial for data management in physical system, and it should have significant engineering application value in I&C system.

Keywords: DCS · I&C emulation system · Data management

1 Introduction

The instrument and control (I&C) emulation system that applies virtual technology is the virtualization of physical system. The system gets rid of the dependence on traditional controller hardware, making it possible to run slave computer software in desktop computer environment [1–4].

Physical I&C system consists of several independent running control stations. These stations communicate with each other by asynchronous communication. Based on this special feature, the control station can be virtualized as an independent-running process and named as the Virtual Control Station (VCS). The inter-communication between VCSs adopts asynchronous inter-process communication (IPC). To improve system authenticity, VCS should realize functions of core modules in physical DCS control stations, mainly including Virtual Main Processing unit (VMPU), Virtual Data Acquisiton unit (VDA), Virtual Data Output unit (VDO), Virtual Communication (VCOM), etc.

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 18–30, 2023.
https://doi.org/10.1007/978-981-99-3455-3_3

As above, VMPU is used to analyze and calculate the control algorithm of process system. To enable functions of external command, data interface, malfunction setup and data override, as well as reducing resource consumption, the process named Data Management Service (DMS) can be added to realize the overall scheduling function. Besides, the MS (maintenance station) used for data monitoring and maintenance can be established as same as the physical one, which connects with VCS in TCP/IP communication mode. Therefore, the system architecture of I&C can be summarized as shown in Fig. 1.

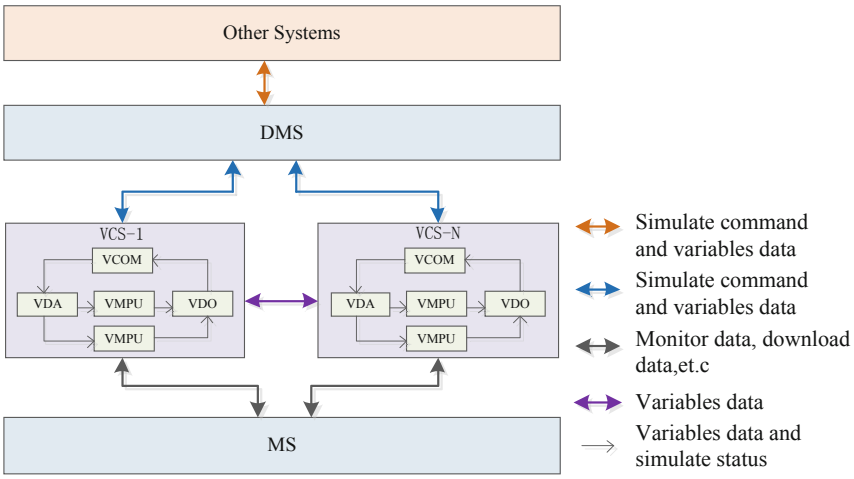


Fig. 1. I&C System Architecture

The processes represent different functions in I&C emulation system, and there is a large amount of data interaction between these processes. Meanwhile, various simulation functions have a significant relationship with data management. Appropriate data management methods can reduce communication load and storage capacity, improve system operating efficiency, and reduce the risk of response delay or system shutdown caused by data overload. As the result, the described I&C emulation system is taken as the experimental object, and its data management function is investigated.

2 Data Interaction Management in I&C Emulation System

2.1 Data Interaction Management Between DMS and VCS

The data management between DMS and VCS includes variable lists, calculated input value and calculated output value per cycle. The variable configuration of a VCS can be downloaded by operations in MS. After collecting the type and quantity of variables, VCS will only transfer variable information to DMS during initialization so that the capacity of data interaction can be kept at a reasonable level. Since VCS and DMS can be configured at the same or different simulation hosts, a communication method

"socket" belonging to IPC mode is selected to exchange data. During normal operation, VCS acquires input data from DMS that will be involved in the operation of VMPU. After each cycle calculation finished by VMPU, VCS will send output data and virtual module status to DMS.

The data package that sent from VCS to DMS includes not only status information of each virtual module, but also output data of algorithm computing. To reduce CPU load and improve transmission efficiency, the buffer area is set up. The data only will be sent to DMS when buffer area is full or data collection is completed. Similarly, specific buffer area is set for each VCS. According to different data types,buffers can be divided into three types:

Data sending buffer: io_send_buffer;
Data receiving buffer: io_recv_buffer;
Status buffer: status_buffer.

The setting and corresponding relationship of buffer areas in DMS and VCS are indicated in Fig. 2. As shown in it, the data in sending buffer can be sent along with that in status buffer, which will reduce time consumption of CPU scheduling.

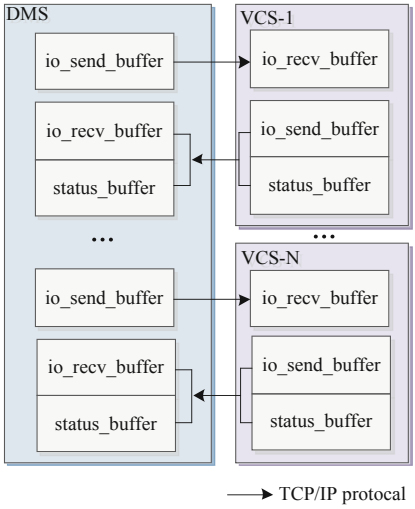


Fig. 2. Data Interaction Relationship between DMS and VCS

2.2 Data Interaction Management Between VCS and Virtual Modules

In order to decrease switching consumption between processes, the virtual modules such as VMPU, VCOM and VDA can be treated as threads in VCS processes, and each thread shares the memory space of its own process. The shared memory comprises data shared memory and status shard memory. The data shard memory is used as data storage space of virtual modules in VCS. When VCS is started, firstly it obtains variable configuration

lists of this VCS, calculates the required memory space and then creates corresponding memory space that shared by virtual modules such as VMPU.

Figure 3 and Fig. 4 indicate the architecture of data shared memory of VDA respectively.

Data_Shared_Memory（Analog Variable Card）

Channel 1	Original Data 4 Bytes	Engineering Data 4 Bytes	Status 1 Byte
Channel 2	…	…	…
Channel 3	…	…	…
…	…	…	…

Fig. 3. Schematic Diagram of Data Shared Memory (VDA, Analog Input)

Data_Shared_Memory（BinaryVariable Card）

Channel 1	Engineering Data 1 Byte	Status 1 Byte
Channel 2	…	…
Channel 3	…	…
…	…	…

Fig. 4. Schematic Diagram of Data Shared Memory (VDA, Digital Input)

The status shared memory is implemented as storage space for emulation information and operation mode, which includes current emulation status, emulation instructions, current initial condition (IC) name, operation mode and LCD display content of VMPU, etc. Its detailed structure is shown in Fig. 5.

2.3 Data Interaction Management Between VCSs

In I&C emulation system, the communication function between one VCS and another is achieved by VCOM. Because different VCSs can be configured at the same or different simulation hosts, IPC socket communication method can be applied by VCS for data exchange. During the initialization of VCOM, VCOM can acquire IP of destination VCS and establish TCP connections by analyzing download configuration files, which enables data transfer between stations. To achieve the requirement of communication

Status_Shared_Memory
（For one station）

sim_status	4 Bytes	vmpu_status	4 Bytes
sim_command	8 Bytes	vmpu_mode	4 Bytes
sim_command _param	16 Bytes	vmpu_lock	2 Bytes
ic_name	32 Bytes	vmpu_lcd	8 Bytes
master_ slot	1 Byte	vmpu_cycle _end	1 Byte

Fig. 5. Schematic Diagram of Status Shared Memory

determinacy for safety class I&C system, the communication between different VCSs should be periodic, and the data format should be fixed in every communication. Figure 6 shows a typical communication data format between various VCSs.

Digital Value 1	Engineering Value 1 Byte	Status 1 Byte
Digital Value 2	Engineering Value 1 Byte	Status 1 Byte
Analog Value 1	Engineering Value 4 Bytes	Status 1 Byte
Analog Value 2	Engineering Value 4 Bytes	Status 1 Byte

Fig. 6. Communication Data Format between Various VCSs

2.4 Data Interaction Management Between MS and VCS

The data management between MS and VMPU mainly includes the data related to monitoring, downloading, maintenance and other functions. As the physical I&C system, VMPU has three operation modes: normal, maintenance and download mode.

When VMPU is in normal mode, it is quite necessary to have monitoring function so that real-time computing conditions of VMPU can be accurately captured by MS. At a time, VMPU only sends one type of data to MS, following the sequence of equipment information, algorithm input data and algorithm output data, original input data, mandatory area data, parameter data, and optimized input data. At the same time, for the sake of facticity improving, the communication mechanism between VMPU and MS should be in consistent with that in physical system, at least in the aspect of transmission rate and transmission date type. For instance, in physical system, only one type of data with maximum size limit of 12K can be sent in one cycle. If the data size exceeds 12K, then

this type of data will be sent separately by cycles. After all types of data being sent, a completed monitoring unit that contains monitoring information will be generated, and eventually analyzed by MS.

When VMPU is set to download mode, the data can be downloaded to it and saved to the corresponding path of the local PC where VCS processes running.

The maintenance function includes variable forcing and parameter modification. The similarity of them is that data modification commands come from MS while VMPU works in maintenance mode. In terms of variable forcing, the information of forcing operation is sent from MS to VMPU, following from that, the forced variable is copied to mandatory area in which will be marked as true. After these operations, VMPU will send the feedback to MS, indicating that the forcing operation is done. The variables belonging to mandatory area are as follows: parameter variables, IO variables, network variables and flags. It needs to be emphasized that forcing operation is a kind of operations applied on computer memory, so it is easier to be invalid when power is failure. Compared to variable forcing function, the difference of parameter modification function is that the modified parameter would be copied to parameter area, which is written to hard disk and saved permanently.

2.5 Data Synchronization Management Between VMPUs

Generally speaking, for one VCS of physical I&C system, there are two main processing units which might be operated either on hot standby redundancy or parallel redundancy. Therefore, data synchronization management between two VMPUs that are in a pattern of redundancy configuration becomes pretty important. When VMPUs are in normal operation mode, these two VMPUs will capture data from shared memory respectively. If VMPUs are configured as hot standby redundancy, the standby VMPU will synchronize with the master one to get output data, and only data in shared memory of master VMPU will be acquired by VDO and VCOM. If VMPUs are in parallel redundancy, they will not synchronize the output data, while data will be selected by VDO or VCOM depending on the status of VMPUs. Besides, data synchronization management will not occur when VMPUs are in maintenance mode.

3 Data Interaction Management with Third-Party System

3.1 Data Interaction Management with Process Model

As shown in Fig. 1, the data in VCS can also derive from the third-party system, such as process model and human machine interface. In order to reduce resource consumption and unify the interface, DMS serving as the master interface of sending or receiving external data is developed to interact data uniformly with third-party system [5]. The override function can be enabled to change the data sent by I&C system to external, or the data transmitted from the external to I&C inside. Whether to select data from DMS or MS is determined by the force flag transferred by MS in VCS. Figure 7 represents the data flow between VCS and third-party system when override function is triggered.

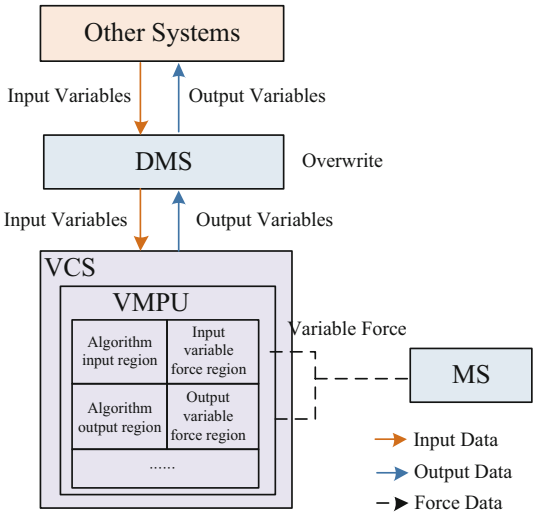


Fig. 7. Data Flow Diagram of Variable Forcing and Override Function

3.2 DataManagement of Saving and Loading IC

The IC refers to the completed data and status of the system at a certain time. In practical application, some particular ICs need to be saved and loaded repeatedly, which means that the I&C system should have the function of saving and loading ICs. The data of ICs mainly include all data in VCS, information in DMS, as well as information entries of corresponding ICs that saved in system database.

The IC files are saved in hard disk with a special format of block length and block content. When an IC is loaded, its format will be analyzed at first and then data will be assigned at specified position as format required. The simulation information of ICs that stored by DMS includes override and malfunction information, ID of each VCS, and data in DMS send buffer. The function of storing DMS send buffer is to enable VCS to start operation with the correct variable value when loading the IC. The schematic diagram of saving IC is shown in Fig. 8.

3.3 DataManagement of IC Calibration Function

In practice, if configuration files are changed, the case might be happened that saved ICs are unavailable. The reason for this is that the offset address of variables or algorithm blocks in configuration files is changed and thus it cannot correspond with the one that saved earlier. In this case, engineers have to carry out ICs again, which will bring huge workload and time consumption.

In order to solve this problem, the IC calibration function is introduced, so that the unchanged part of saved ICs, backtracks or scenarios can still be correctly loaded into the corresponding position of the original variable or algorithm block when configuration changes. This function brings convenience to the person who in charge of debug work, which is not only conducive to locate the algorithm changing position, but also makes

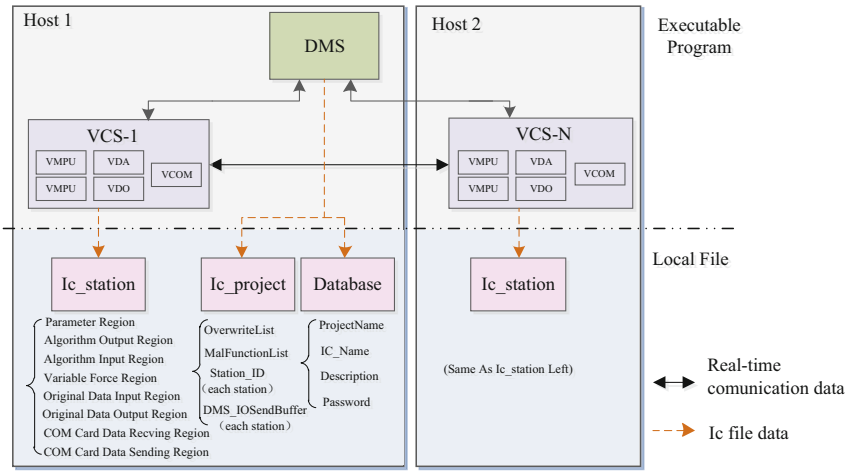


Fig. 8. Schematic Diagram of Saving IC

the debugging personnel avoid reworking every time when algorithm configuration is slightly changed. Data management of IC calibration involves input and output variables, time-dependent algorithm blocks and time-independent algorithm blocks with parameters. By parsing the file with its name and offset, the offset address of each variable or algorithm block is recorded, and the corresponding value can be loaded into the correct variable or algorithm block when loading ICs, backtracks or scenarios.

4 Experimental Study

Take the load reduction condition in the HPR 1,000 Megawatts pressurized water reactor (PWR) nuclear power plant as an example. To ensure the accuracy of the experiment, the selected digital reactor model needs to comprehensively consider the reactor neutron dynamics model, thermal hydraulics model and reactivity model [6, 7]. The system architecture of semi-physical closed-loop simulation system is shown in Fig. 9. The physical or virtual DCS collects data through a digital sensor model, and the data comes from the calculated results of the reactor model. Control instructions are transmitted through actuator models such as digital control rods and act on the calculation process of reactor and primary loop models [8–11].

To verify whether the data management function is valid after applying simulation function, the experiment of power regulation process is implemented as follows.

In following figures, the signal sp represents the setpoint value of nuclear power reactor, the signalpv-DMS is the measured value obtained by DMS (emulation system), and the signalpv-MS is the nuclear power measured value read by engineer workstations (physical DCS).

Experiment 1: Pseudo-authenticity Experiment.

The closed-loop full scope simulator with the participation of the I&C emulation system should have a high degree of pseudo-authenticity with that composed of physical

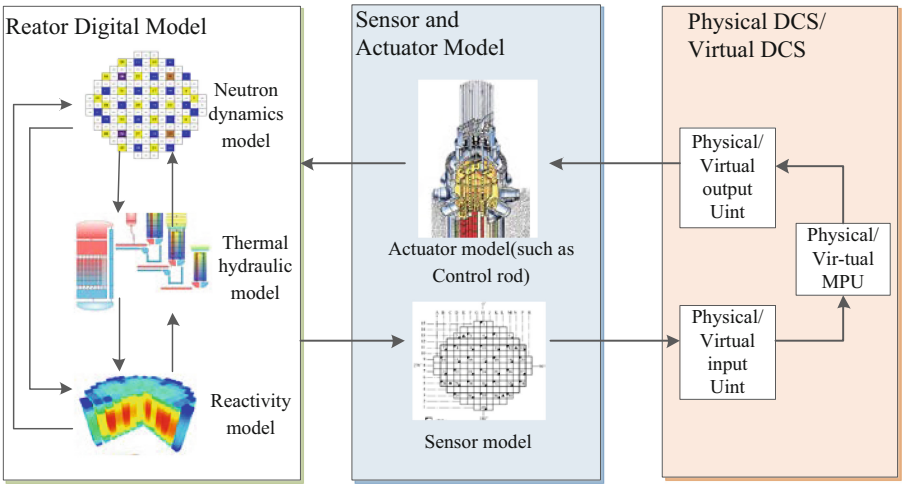


Fig. 9. System architecture of semi-physical closed-loop simulation system

system. By comparing the adjustment time, overshoot and other parameters in the power regulation process, the pseudo-authenticity of emulation system can be investigated and proved. The IC selected for experiments should have certain complexity and high sensitivity to algorithm and time. For this reason, the control loop mainly based on digital value calculation cannot be selected.

Taking the start-up IC as an example. The nuclear power of the reactor is increased from 0% full power (FP) to 40% FP. This power regulation process is implemented by two closed-loop systems, the one is composed of process model and physical control system, while the other is made up of emulation system instead. The experimental results are shown in the Fig. 10.

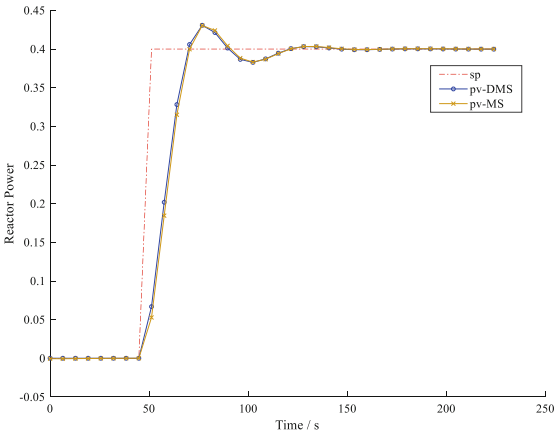


Fig. 10. Simulation Experiment of Pseudo-authenticity for the Start-up Condition

The results prove that the emulation system has pseudo-authenticity.

Experiment 2: Freezing Function Experiment.

Freezing is a basic function. The experiment is taken by increasing the reactor power from 30% FP to 50% FP, and freeze the project after the parameters are stable. From the above analysis, it can be seen that after freezing the project, the value sent from DMS to the third-party system should be unchanged, but MS cannot obtain variable values any more since VMPU operation is suspend and thus its connection with MS should be interrupted. The experimental results are indicated in the following Fig. 11. The locations indicated by arrows in the figure are the timing of freezing begins and operations continues respectively, MS cannot obtain data between the two timing.

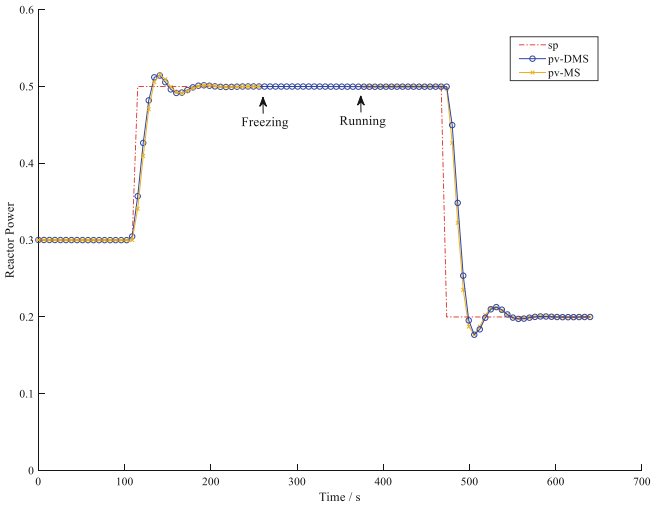


Fig. 11. Freezing Function Experiment

The experimental results conform to the above analysis. After freezing the project, the third-party system continues obtain the remaining unchanged value from DMS while MS cannot take the value. After restoring the running state of the project, the value received by the third-party and MS both return to normal.

Experiment 3: Override Function Experiment.

In this experiment, the reactor power is increased from 30% FP to 50% FP. After the operation is stable, the value of override function is setup to 40% FP. From the above analysis, it can be seen that the pvshould still be 50% FP because the override value is an output data, and it does not affect the calculation process inside the simulation system. The third-party system takes the value of 40% FP from DMS, which also means the calculation of process model is based on PV of 40% FP. After clearing the override state, the pvvalue at DMS should return to 50% FP. The measured results are shown in Fig. 12.

As presented above, after setup override function, the value of the third-party system has been changed, and the value inside the simulation system remains unchanged. After

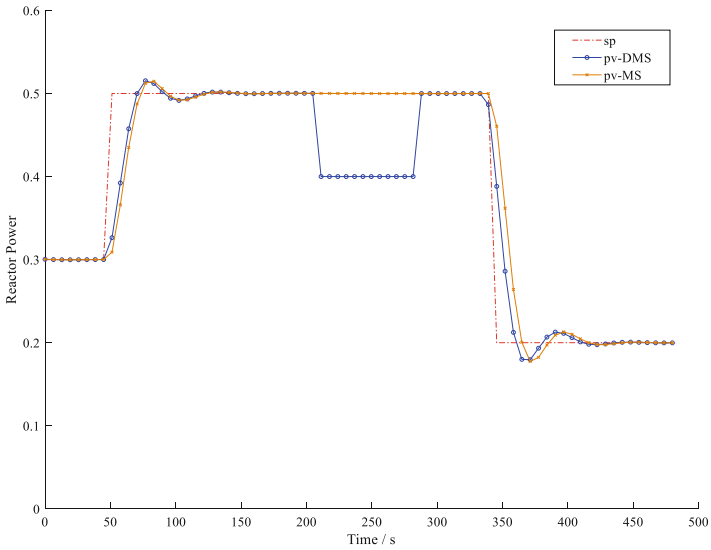


Fig. 12. Override Function Experiment

the override is restored, the output value is switched to the internally calculated value by the simulation system without disturbance.

Experiment 4: Saving and Loading IC Experiment.

In this case, the IC is created with the reactor power at 60% FP. Afterwards, dramatically reduce spvalue to 20% FP until all parameters are stable, and finally restore the previous saved IC. It can be expected that when 60% FP is stored, all data information under 60% FP should be recorded.

The system should enter frozen state after IC being loaded. When the IC of 20% FP is loaded back to replace that of 60% FP, the system will change to frozen state, the input signal spbecome back to 60% FP, and the output signal pvis still 20% FP. After running the project, the output signal pvwill recover to 60% FP.

After the loading IC instruction is issued, the project is in frozen state. Whether the input value and the output value are loaded back is related to the project running state. This is because the storage locations of the input variable and the output variable are different. The value of input variable is sent to VCS by DMS, and its value is recorded in the sending buffer area sent to VCS by DMS. When saving IC, this area is saved and it will be backfilled to DMS when loading IC (the project is in frozen state). Therefore, when the project is in frozen state and the loading instructions is issued, the value of input variable that can be obtained through DMS by the third-party system should be the value that preserved by the saving IC operation. In addition, the value of output variable is stored in a file that copied from VMPU's cache area. When the project is loading but not in running state, this value can be only loaded back to the VMPU's cache area. When the project is frozen, there are no periodic operations for VMPU and the value will not be written to the shared memory by VMPU. At this time, even though VCS continues to send output data, but it is the data that saved before loading ICs. As a result, the

third-party system cannot obtain data from DMS until the project is switched to running state.

The experimental results are shown in Fig. 13.

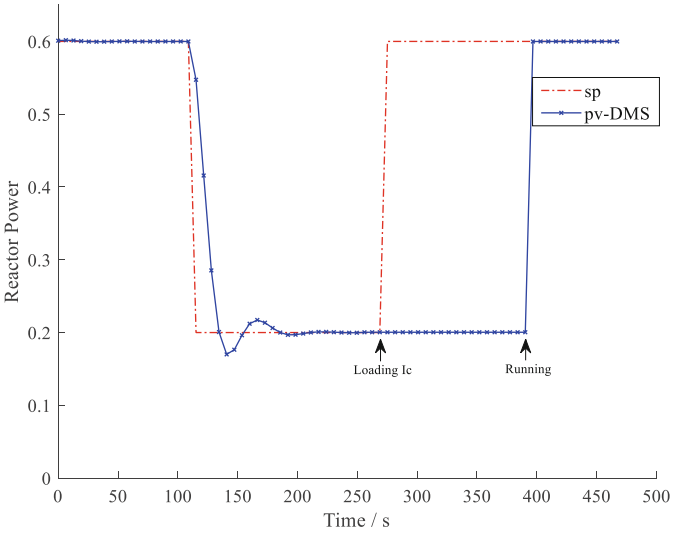


Fig. 13. Saving and Loading IC Experiment

5 Conclusion

The data management of I&C emulation system is closely related to its logic operation and simulation features. Based on the analysis of system architecture and simulation function for a specific emulation system, this paper introduces a new data management method, and its effectiveness has been verified in various experiments by combining the simulation function.

Funding. The project was funded by Sichuan Provincial Science and Technology Fund for Distinguished Young Scholars (2020JDJQ0068).

References

1. Zhang, X., Ma, Q., Chen, Q., Wang, K., Peng, H., Liu, G.-H.: Design and optimization of communication in nuclear safety class emulation system. In: Xu, Y., Sun, Y., Liu, Y., Wang, Y., Gu, P., Liu, Z. (eds.) SICPNPP 2019. LNEE, vol. 595, pp. 430–440. Springer, Singapore (2020). https://doi.org/10.1007/978-981-15-1876-8_43
2. Gao, H., Qu, M., Li, Q., et al.: Research and design on virtual DCS process control plat-form in nuclear power plant. Comput. Integr. Manuf. Syst. **34**, 144–149 (2017)
3. Peng, H., Zhang, X., Deng, Z., et al.: Design and verification of virtualization transplantation method for distributed control system. J. Shanghaijiaotong Univ. **53**, 118–122 (2019)

4. Sun, Y., Zhang, Y., Pang, Z.: A validation and verification method of I&C software of nuclear power station based on FSS. Comput. Integr. Manuf. Syst. **31**, 147–150+272 (2014)
5. Zhang, X., Xu, H., Wang, K., et al.: Interface design of safety-class instrument control simulation system. Mod. Comput. **25**, 69–72 (2019)
6. Lin, M., Yang, Z., Hou, D., et al.: Applying engineering simulator to verification and validation of digital I&C in nuclear power plant. In: International Conference on Nuclear Engineering 17th, pp. ASME, Brussels, pp. 729–733 (2009)
7. Hou, D., Lin, M., Xu, Z., et al.: Development and application of an extensible engineering simulator for NPP DCS closed-loop test. Nucl. Eng. Des. **38**, 49–55 (2010)
8. Zhang, J., et al.: Nuclear Reactor Control. China Atomic Energy Press, Beijing (2016)
9. Zhang, X., Deng, Z., Li, J., et al.: Design and verification of reactor power control based on stepped dynamic matrix controller. Sci. Technol. Nucl. Install. **2019**, 1–11 (2019)
10. Deng, Z., Lu, X., Jian, Y., et al.: Application of SDMC developed based on SCADE in core power control. Process Autom. Instr. **40**, 103–106 (2019)
11. Wang, G., Wu, J., Zeng, B., et al.: Model predictive control method for core power control in pressurized water reactor. Atomic Energy Sci. Technol. **51**(3), 480 (2017)

Analysis and Treatment on Control Rod Measured Position Fluctuation

Wen-Qing Yang(✉), Xiong-Wei Cheng, Chao Wang, Chu-Hao Huang, Zheng-Dong Huang, Ji-Kun Liu, and Qiao Wei

State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment, China Nuclear Power Engineering Co., Ltd, Shenzhen 518172, Guangdong, China
vencentyoung@gmail.com

Abstract. Core reactivity control and shutdown margin are provided by control rod clusters, which makes it a crucial system for reactor control and protection. The physical position of control rod is measured by rod position indication system (RPI). After equipment type change of rod control and rod position indication system (RGL) in a plant, an issue that fluctuation of measured position occurred even with a stable physical position, during the system commissioning. It will seriously interfere with the surveillance of control rod position. The root cause of measured position fluctuation is ascertained by measurement principle and circuit analysis, and a practical solution is proposed also. By acquisition of detector signals and development of analysis algorithm, the issue was solved. At the same time, optimization suggestions at the hardware level for the root cause are proposed.

Keywords: Control rod · Rod position measurement · Circuit analysis · System Commissioning

1 Introduction

The control rod position measurement is realized by the rod position detector and post-processing circuit. The measured rod position indicates the real physical position of the control rod inside the reactor core. The CPR1000 nuclear power plants adopt the differential transformer measurement principle to measure the rod position [1].

When a new type rod control and rod position measurement system (RGL) was applied in a power station for the first time. It was found that compared with the old type, the new equipment had the phenomenon of measuring rod position fluctuation, that is, the measured rod position fluctuates frequently when the real rod position remained unchanged.

Frequent fluctuation of the measured rod position will falsely trigger the rod position deviation alarm [2]. The rod position deviation alarm is used to indicate that the control rod is accidentally dropped or out of step, false alarm affects the operator's judgment on the state of the unit.

This paper analyzes and studies the principle of rod position measurement, the difference analysis of new and old equipment with the original data collected on site, and analyzes the reasons for the fluctuation of control rod measurement rod position.

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 31–43, 2023.
https://doi.org/10.1007/978-981-99-3455-3_4

2 Control Rod Position Measurement Principle

The power station adopts a differential transformer as the rod position detector. Inside the detector, the secondary coil is excited by the alternating current flowing through the primary coil. When the control rod shaft moves, the induced voltage of the secondary coil changes. 5 sets of secondary coils generate different induced voltage combinations at different control rod positions. The combined signal is sent to the rod position measurement cabinet for filtering and shaping to obtain the GRAY code representing the rod position. The GRAY code is decoded by the PLC software in the rod position processing cabinet to obtain the control rod position [1, 3]. The structure of the rod position detector is shown in the following figure (Fig. 1):

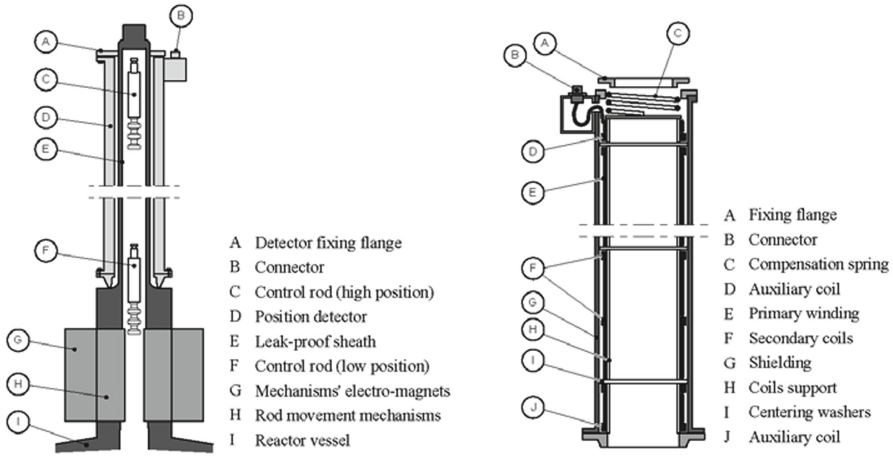
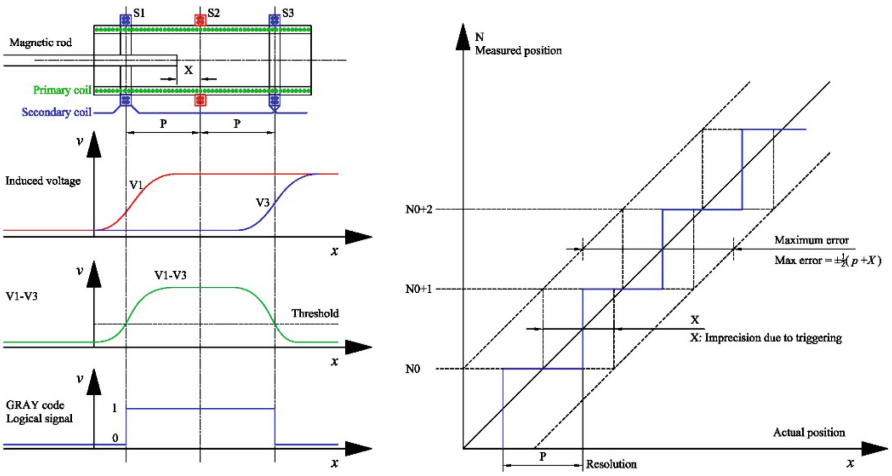
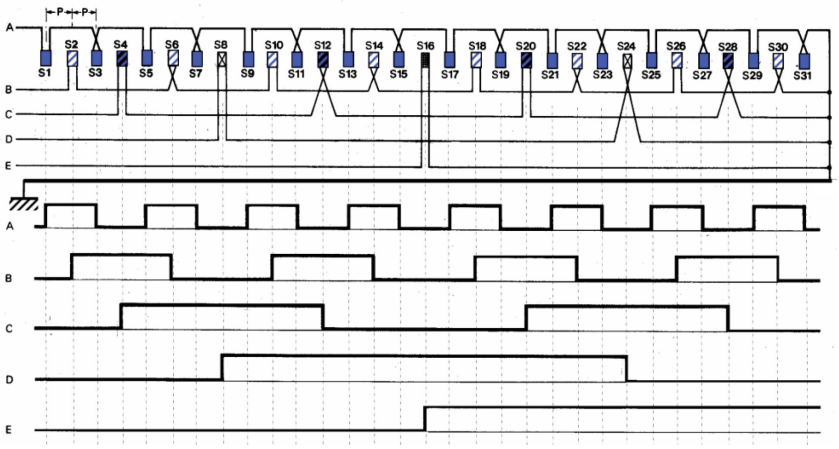


Fig. 1. Rod position detector structure

Secondary coils of different groups are staggered, and each group of coils is connected by differential connection. When the driving shaft of the control rod passes through an even number of coils in the same group, the induced potentials of the subcoils cancel each other out, which is characterized as a low voltage. On the contrary, when the driving rod passes through the odd number of coils in the same group, the output of the whole coil is characterized as high voltage. The relationship between coil arrangement and GRAY code signal combination is shown in the following figure [1] (Fig. 2):



a) Rod position detector operating principle



b) Generation of GRAY code

Fig. 2. Rod position measurement principle

The induced voltage of the secondary coil of the rod position detector is conditioned by the rod position measurement signal processing circuit and compared with the threshold value to obtain the GRAY code, and then the GRAY code is converted to measured position. Due to the quantity limitation of the coils, the measuring rod position is not a continuous mechanical step, but a discontinuous point related to the coil spacing. The measuring interval of the rod position detector equipped in this power plant is equivalent to 8 mechanical steps. The conversion lookup table from GRAY to rod position is shown in the following table [1] (Table 1):

Table 1. Lookup table of gray code and measured position

GRAY code					Rod position	GRAY code					Rod position
E	D	C	B	A		E	D	C	B	A	
0	0	0	0	1	0	1	1	0	0	0	120
0	0	0	1	1	8	1	1	0	0	1	128
0	0	0	1	0	16	1	1	0	1	1	136
0	0	1	1	0	24	1	1	0	1	0	144
0	0	1	1	1	32	1	1	1	1	0	152
0	0	1	0	1	40	1	1	1	1	1	160
0	0	1	0	0	48	1	1	1	0	1	168
0	1	1	0	0	56	1	1	1	0	0	176
0	1	1	0	1	64	1	0	1	0	0	184
0	1	1	1	1	72	1	0	1	0	1	192
0	1	1	1	0	80	1	0	1	1	1	200
0	1	0	1	0	88	1	0	1	1	0	208
0	1	0	1	1	96	1	0	0	1	0	216
0	1	0	0	1	104	1	0	0	1	1	224
0	1	0	0	0	112	1	0	0	0	1	232

3 Reason Analysis for Rod Position Fluctuation

The direct cause of the rod position fluctuation is that a certain GRAY code signal has a bit flip change between the two states of high and low level. According to the working principle of the signal processing circuit, when the comparator threshold and hysteresis remain unchanged, the only reason for the fluctuation is that the amplitude of the induced voltage in the secondary coil of the detector has changed greatly.

rod position detector is essentially equivalent to a transformer. The induced voltage of the secondary coil is proportional to the voltage of the primary coil. The power supply for the primary coil is provided by the power supply module which realizes the primary coil a 50 Hz AC power supply through the R-C (resistor and capacitor) oscillator circuit [1].

The induced voltages on the primary coils of the three control rods were recorded during the rod drop test on the 50%FP (Full Power) level in a plant which equipped with the same type of rod position measurement system [4]. Comparing the waveform data collected by the power plants equipped with different types of rod position measurement systems under the same test conditions, the voltage amplitude of the domestic equipment has large fluctuations in the steady state. Spectrum of the primary coil induced voltage signal is analyzed by using fast Fourier transform [5], and the results are as follows (Fig. 3):

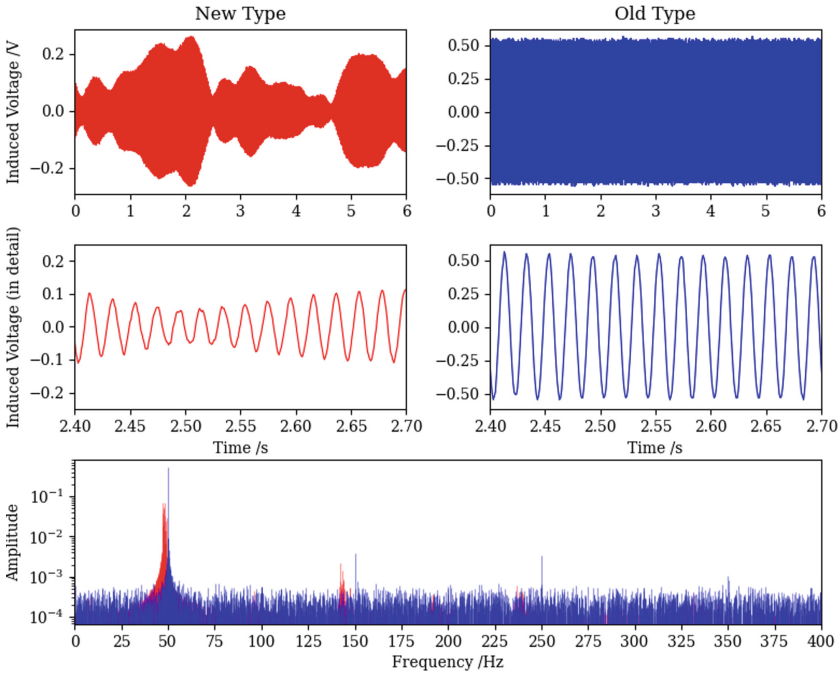


Fig. 3. Induced voltage of detector primary coil

The amplitude of the induced voltage of the new equipment fluctuates greatly and the frequency is scattered in the range of 49 ± 3Hz. The amplitude frequency of the induced voltage oscillation of the old equipment is relatively stable, and the frequency distribution is concentrated at 50 Hz. The voltage of the measured coil comes from the induction of the electromagnetic field established by the primary coil of the surrounding detectors. When the power supply frequency of the surrounding detectors is inconsistent, the amplitude of the induced voltage of the measured detector will oscillate.

Compared with the transformer amplitude modulation power supply of the old equipment, the new equipment uses direct current to generate alternating current through the R-C oscillator circuit [6]. The R-C oscillator circuit is built by components such as capacitors and resistors. Due to the inherent manufacturing deviation between electronic components, the oscillation amplitude and phase of the alternating current generated by them must be different, and the frequency is not concentrated enough. This causes the amplitude of the superimposed alternating current to oscillate.

For older equipment with transformers, all primary coils can be equivalent to the secondary side of the transformer inside the cabinet. According to the electrical characteristics of the transformer, if the same AC power supply is used on the primary side, the induced voltages on the secondary side will have the same frequency and phase, and will still be a standard sine wave after superposition even if there are differences in the electromagnetic parameters of the secondary coils.

The original signal of the secondary coil is processed by the signal processing card, which can be divided into two parts: rectification and comparison. The rectifier circuit converts the induced AC voltage into a DC signal, and then sends it to the hysteresis comparator for comparison with the threshold to generate a digital signal as the GRAY code of the coils set. The signal processing in this part is not much different from the old type. The principle of the detector signal processing card is shown in the following figure (Fig. 4):

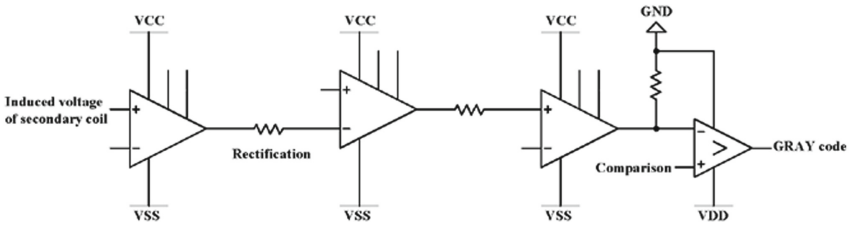


Fig. 4. Schematic diagram of signal processing card

Circuit simulation of the rod position measurement is carried out. When multiple sinusoidal signals of different frequencies and different phases are used to superimpose the induced voltage of the secondary coil, the DC voltage output by the rectifier circuit fluctuates, and the GRAY code signal output by the comparator appears fluctuation, which is consistent with the situation on site. When a sine signal with a fixed frequency is used to simulate the working conditions of the old equipment, the DC voltage is stable after rectification, and there are no Gray code fluctuations. The simulation results are as follows (Fig. 5):

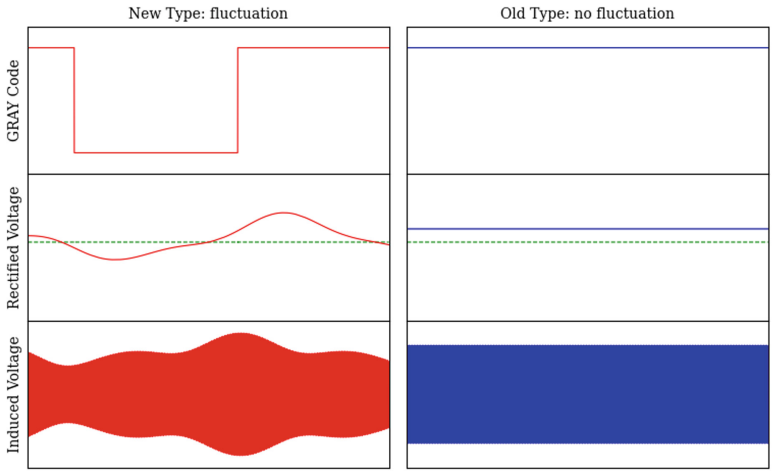


Fig. 5. Simulation of rod position fluctuation

According to the above principle analysis and simulation results, it can be seen that the root cause of the position fluctuation is the frequency and phase difference of the primary coil power supply among the detectors after the equipment changed. This difference in power supply leads to fluctuations in the amplitude of the induced voltage on the secondary coil, which are processed by the rectifier circuit and manifest as fluctuations in the value of the DC voltage. When the hysteresis of the comparator fails to envelop the voltage amplitude, the Gray code signal fluctuates, resulting in the measurement rod position falsely change.

4 Rod Position Detector Calibration

4.1 Operation Guidelines for Rod Position Detector

The purpose of rod position detector calibration is to limit the deviation between the measured position and the real rod position within the allowable range. At the same time, for the withdrawal and insertion process, the deviation of the turning point of the measurement rod position needs to be within 1 mechanical step [6].

Take the following figure as an example. During the withdrawal process (red line), the measured position becomes 32 when the real position is 31, and becomes 40 after the real position reaches 37. The measurement deviation of the corresponding 32-step position is −1/+5 steps respectively. For the insertion (blue line), the measured position changes to 32 when the real position is 36, and changes to 24 after 30 steps of the real position. The deviation of the corresponding 32-step position is −2/+4 steps respectively, which has 1 step deference from the withdrawal, that is, the hysteresis is 1 step (Fig. 6).

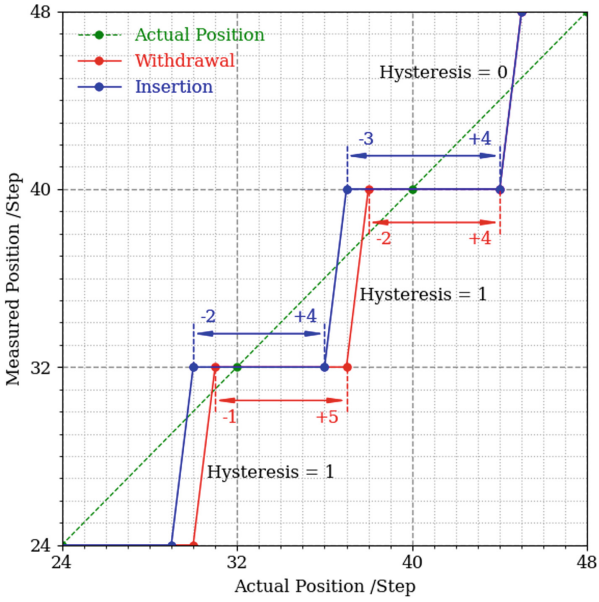


Fig. 6. Measured position accuracy analysis

It is required that in the process of withdrawal and insertion, the change direction of the measured rod position is consistent with the moving direction of the control rod, that is, there is no position fluctuations.

4.2 Rod Position Detector Calibration Principle

The rod position detector signal processing card provides a measurement interface for the output voltage of each coil. By measuring the voltage of each coil in the process of moving the rod, the threshold value can be calculated according to the voltage measurement value at the theoretical turning point.

Due to the interference of the CRDM operating current and the influence of signal noise, the induced voltage of the secondary coil inevitably has disturbances. Setting the hysteresis in the comparator can prevent the rod position fluctuation caused by the signal interference. An inappropriate hysteresis may cause the turning point of the withdrawal and insertion to be inconsistent. If the threshold hysteresis is set too large, the rod position deviation of the withdrawal and insertion will exceed the standard requirement of 1 mechanical step. A reasonable threshold hysteresis should be able to suppress the disturbance while ensuring that the position deviation of the turning point does not exceed the limit.

Coil A Adjustment Method

Influenced by the CRDM coil, the induced voltage of the A coil does not change monotonically when the control rod moves. The induced voltage of the A coil during the movement of the control rod is acquired and shown in the following figure for both withdrawal and insertion (Fig. 7):

It can be seen from the actual waveform that the voltage change is not monotonous during the withdrawal and insertion, and the waveform is superimposed with wavelet peaks and wavelet troughs. According to the working principle of the hysteresis comparator, refer to the system operation manual, use the maximum value of the wavelet peak V_1 and the maximum value of the wavelet trough V_2 to calculate the voltage deviation $V_0 = V_1\text{-}V_2$, and the A coil threshold V_A can be carried out by [1]:

$$V_A = \begin{cases} \dfrac{V_0 - a}{b}, & V_0 > p \\ \dfrac{V_0 - c}{d}, & V_0 \le p \end{cases} \tag{1}$$

where a, b, c, d, p are adjustment coefficients.

According to the above method, by recording the rectified value of the induced voltage of the A coil during the process of moving the rod the threshold value of the A coil can be obtained by calculation.

Coil B/C/D/E Adjustment Method

According to the characteristics of the rod position detector, the theoretical turning point of the coil is the midpoint of the two measurement steps. Taking the voltage at the midpoint position as the threshold value can ensure the minimum deviation between the measured rod position and the actual rod position at each turning step (Fig. 8).

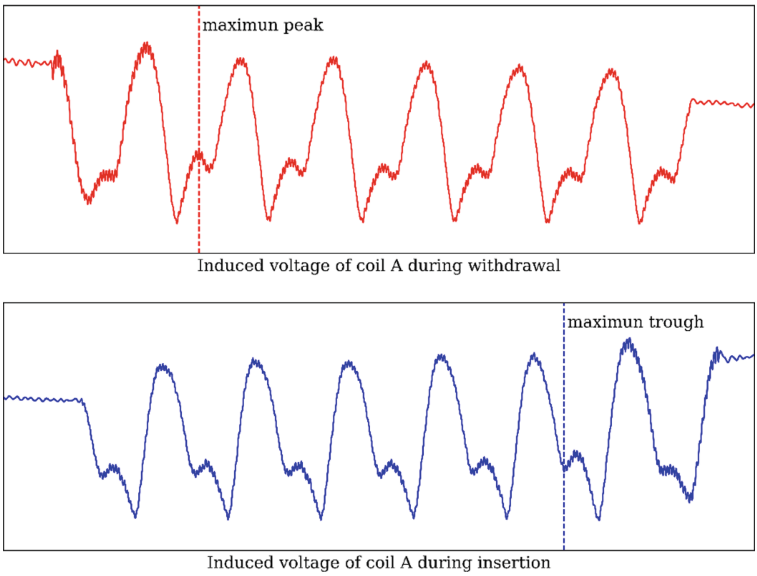


Fig. 7. Rectified induced voltage of coil-a during rod movement

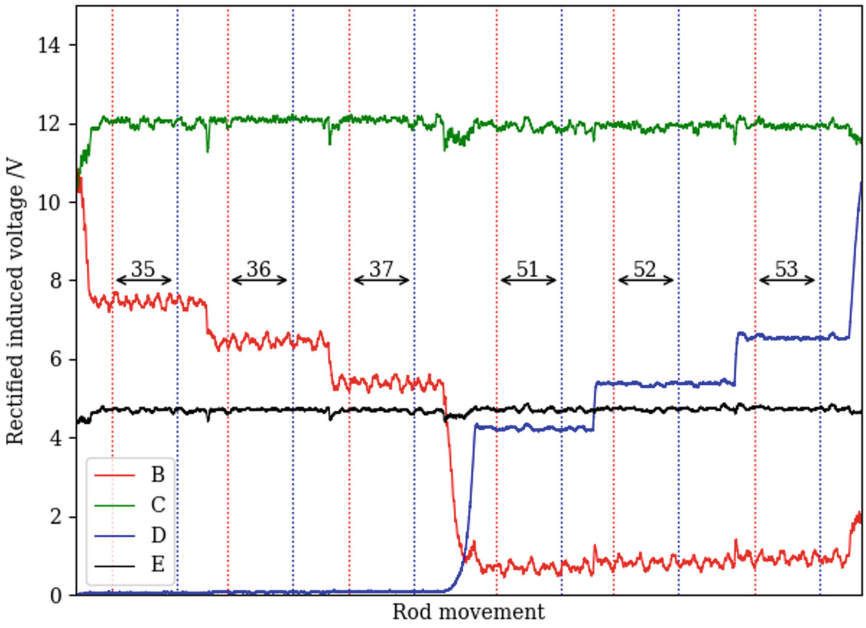


Fig. 8. B/C/D/E coil rectified induced voltage during rod movement

Let the operator move the control rod to the theoretical position turning point, record the voltage rectification value of the coil corresponding to the theoretical turning point of

the control rod, and calculates the average value of the voltage V_{avg} of each theoretical turning point for each coil. Use the following equation to calculate the coil threshold using V_{avg} as a reference: [1]

$$V_{BCDE} = \frac{V_{avg} - e}{f} \tag{2}$$

where e and f are the adjustment coefficient.

On-site measurement found that relying only on the measurement data of the theoretical turning point will lead to inaccurate calculation of the B/C/D/E coil thresholds. Therefore, by adding the data of each step before and after the theoretical turning point and calculating the average value, the applicable range and the accuracy of the calculated threshold is improved.

4.3 Rod Position Detector Calibration Implementation

Since the old equipment does not have the problem of mutual interference between detectors caused by the inconsistency of power supply, the thresholds of each coil are well consistent, and the preset parameters provided by the manufacturer are generally used for adjustment. The correctness of the parameters is verified by slow and fast rod moving, and individual channels are fine-tuned according to the test results if needed.

For the new type of equipment, due to the mutual interference of the power supply among the detectors, the working conditions of the detectors are now very different, and the parameters of each detector need to be adjusted separately according to the previous description. By continuously withdrawing and inserting the control rod and recording the induced voltage output of the A coil, the calibration of the A coil can be completed. B\C\D\E coil calibration can be accomplished by moving the control rod to a series of specific theoretical turning points and measuring the corresponding coil induced voltage output.

The signal acquisition system is shown in the figure below. The coil induced voltage is measured by connecting output interface of the signal processing card to the signal acquisition instrument through the connecting wire. By developing data processing software and reading the data collected and recorded by the signal acquisition instrument, the calculation of the calibration parameters of the rod position detector can be completed automatically (Fig. 9).

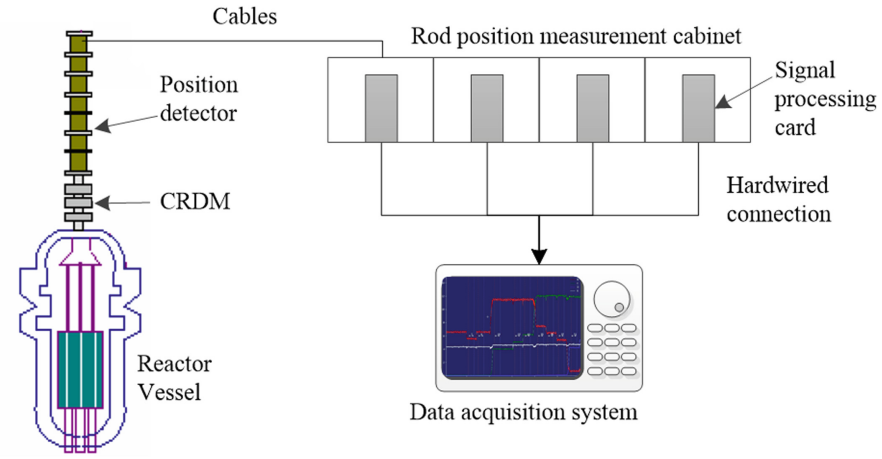


Fig. 9. Data acquisition for position detector calibration

4.4 Suggestions on the Optimization of the Power Supply

According to the analysis above, the root cause of the rod position fluctuation is that the power supply frequency and phase of the primary coil of the detector are inconsistent. The frequency and phase consistency of the power supply of the detector can be achieved by optimizing the design of the power supply circuit.

A feasible solution is to use 220VAC factory power distribution as power supply for each division of cabinets, and the send power supply to each detector after voltage transformation through transformer and amplitude modulation by control circuit.

It can be considered that the transformers and modulation circuits do not change the frequency and phase of the alternating current. The secondary side of the transformer, that is, the power supply of the detectors, has the same frequency and the same phase (Fig. 10).

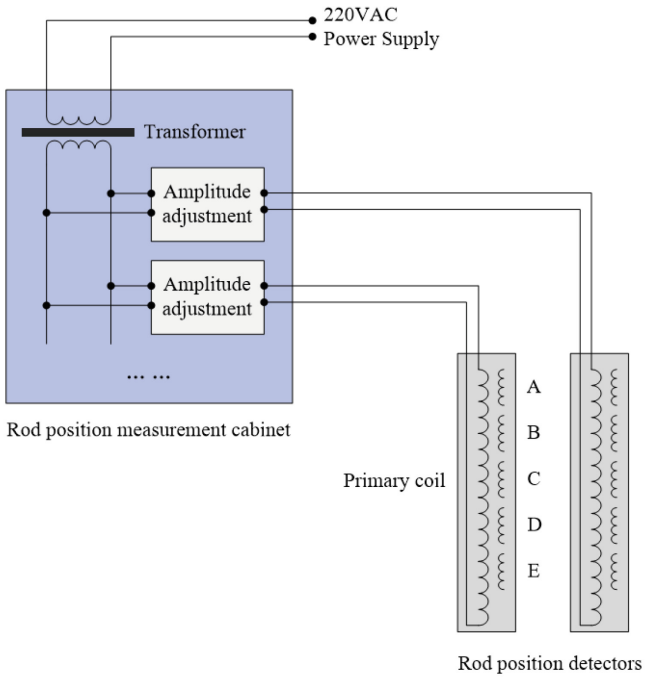


Fig. 10. Power supply circuit optimization

5 Conclusion

This paper analyzes the fluctuation of the measured rod position in a plant. Through the analysis of the rod position measurement principle, the comparison of the difference between the old and the new equipment, and the analysis of the onsite data, it is determined that the root cause of this issue is the fluctuation of the induced voltage output of the secondary coil which caused by the inconsistent power supply of the primary coil of the detector. The theoretical threshold and hysteresis cannot effectively cover the signal fluctuations.

According to the working principle and signal characteristics of the detector coils, the detector calibration method is determined, the special detector calibration data processing software is developed, and the calibration test of the rod position detector in this plant is completed.

The determination of the root cause of the measured rod position fluctuation has reference significance for subsequent equipment upgrades and design optimization. At the same time, the calibration method can be applied to equipment operation, maintenance and commission of power plant which uses the same type of equipment.

References

1. Xu, Y.-L.: Operation and Maintenance Manual of Rod Position System Equipment, pp. 14–22. China General Nuclear Power Research Institute Co., Ltd., Shenzhen (2018)
2. Shang, J.: RGL-Rod Position Indication and Rod Control System Manual, pp. 19–21. China General Nuclear Power Engineering Co.,Ltd., Shenzhen (2018)
3. Zhou, Q.: Processing Cabinet Software Design Manual, pp. 4–15. China General Nuclear Power Research Institute Co., Ltd., Shenzhen (2017)
4. Xu, X.-X.: Core Physical Test Commissioning Procedure, p. 19. China General Nuclear Power Research Institute Co., Ltd., Shenzhen (2018)
5. Zou, L.-H.: Digital Signal Processing, pp. 133–162. National Defence Industry Press, Beijing (1985)
6. Laurent, A.: RPI-Equipment Operation & Maintenance Manual, pp. 20–22. Rolls-Royce (2015)

Anti-interference Study of Wireless Sensor Networks in Nuclear Power Plants

Zhi-guang Deng(✉), Qian Wu, Xin Lv, Mei-qiong Xiang, Tao Xu, Yue Qin, Yong-sheng Sun, and Ye-shun Peng

Science and Technology on Reactor System Design Technology Laboratory, Nuclear Power Institute of China, Chengdu 610213, China
dzg7400613@163.com

Abstract. The compatibility and anti-interference capability of wireless sensor networks within nuclear power plants in complex electromagnetic environments are the most essential elements to ensure reliable operation and effective combat of equipment within nuclear power plants in harsh environments. Interference signals generated by electrical, rotating and communication equipment and sensors attached to nuclear power plants, as well as malicious enemy interference sources, cause their electromagnetic environment to become increasingly complex. For the complex interference environment of nuclear power plant compartment, this paper firstly adopts supervised and unsupervised learning for interference cognition, and after obtaining the features of wireless interference sequences, anti-interference decision based on deep reinforcement learning and array antenna multi-domain anti-interference based on intelligent decision are implemented. From the intelligent interference simulation based on the physical transmission system, it can be seen that the proposed method can effectively identify and resist typical interference signals, which can bring reference to the anti-interference of nuclear power plants.

Keywords: nuclear power plant · wireless sensors · interference perception · anti-interference

1 Introduction

As a new sensing and detection technology that has emerged in recent years, wireless sensors and sensing networks have been widely used in the fields of intelligent detection, situational awareness, equipment operation, industrial manufacturing and environmental monitoring. The application of wireless sensors in the monitoring of nuclear power plant electrical/mechanical equipment can greatly enhance the flexibility of monitoring equipment arrangement, significantly reduce the cable laying and termination workload during the construction of nuclear power plant, help improve the level of information technology and automation of nuclear power plant and the integration and miniaturization of the overall equipment, and help reduce construction and operation costs.

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 44–56, 2023.
https://doi.org/10.1007/978-981-99-3455-3_5

The wireless environment of the compartment of the nuclear power plant has strong specificity, such as complex compartment structure, high-power electromechanical equipment instantaneous start and stop and other electromagnetic radiation on the wireless sensor network of the wireless transmission process will have interference effects. In addition, the wireless communication environment in the nuclear power plant compartment is characterized by a small metal confined space, a large number of sensor nodes in the proximity range, an extremely complex electromagnetic environment, multipath interference in the compartment, multi-user interference, serious co-channel interference, and large randomness of transmission delay [1]. These characteristics pose a great challenge to the application of wireless sensor networks. Compared with traditional wireless sensor networks in wide area space, wireless sensor networks in complex ship cabin communication environment, wireless sensor networks put forward extremely high requirements for communication quality, the need to minimize the possibility of sensitive sensors subject to electromagnetic interference, reduce the impact of various interference on the BER performance, improve the quality of information transmission (Quality-of-Service) reliability, improve the Time-sensitive sensing and detection equipment on the requirements of time delay, etc.

The interference faced by wireless sensor networks in nuclear power plant compartments is not only strong and dense, but also the types of interference are diversified, complex and new, and the interference signals are constantly changing in multiple dimensions over time, such as time domain, frequency domain and air domain. Therefore, some existing interference identification methods that extract feature parameters in a single dimension only for common interference types are no longer sufficient to meet the demand. There is an urgent need to study an intelligent interference cognition technique with multi-dimensional feature parameters, diverse recognition means and better robustness.

Machine learning-based cognitive radio technology is a new intelligent and reliable wireless communication technology that uses machine learning techniques to enable sensor terminal devices to achieve interference suppression and reliable wireless transmission by sensing, understanding, learning and evaluating the surrounding electromagnetic environment, and using the wireless background knowledge obtained by interacting and fusing with the wireless environment to adjust system decision parameters and transmission parameters in real time [2–4]. Cognitive-based intelligent anti-interference technology is the future development direction of intelligent anti-interference technology. At the receiving end, through the monitoring, sensing and identification of the electromagnetic environment, the interference is automatically sensed, identified and classified from the time domain, frequency domain, air domain, power domain and waveform domain, respectively, and the receiving end then takes the best anti-interference measures based on the sensing and identification results. For interference signal classification, the commonly used classification algorithms are Decision Tree (DT), Support Vector Machine (SVM), Deep Neural Network (DNN), etc. [5–11]. The flexibility, real time, intelligence, and ability of machine learning techniques to interact adaptively with the surrounding environment make it a great application for intelligent interference cognition.

The combination of machine learning cognitive technology, time/frequency domain anti-interference technology (fast/slow frequency hopping technology) and air domain

anti-interference technology (array antenna technology) in the nuclear power plant shipboard sensor nodes and the wireless sensor network they form, this intelligent multi-domain combined hybrid communication regime can compensate for the shortcomings of any single technology and significantly improve the wireless sensor network's ability to resist complex electromagnetic interference [12–16].

In this paper, based on Lora protocol, the wireless anti-interference of nuclear power plant is studied in terms of wireless anti-interference cognition, anti-interference intelligent decision, and multi-domain anti-interference for the special electromagnetic interference environment of nuclear.

2 Intelligent Anti-interference for Nuclear Power Plants Based on Machine Learning

2.1 Intelligent Anti-interference Architecture

The intelligent anti-interference system is based on machine learning algorithms and constitutes an anti-interference "intelligent loop" of cognition-decision-measure-evaluation. The training server uses the historical experience data in the machine learning knowledge base for training, so that the system has the ability to learn independently and continuously optimize the anti-interference performance. The intelligent anti-interference architecture is shown in Fig. 1.

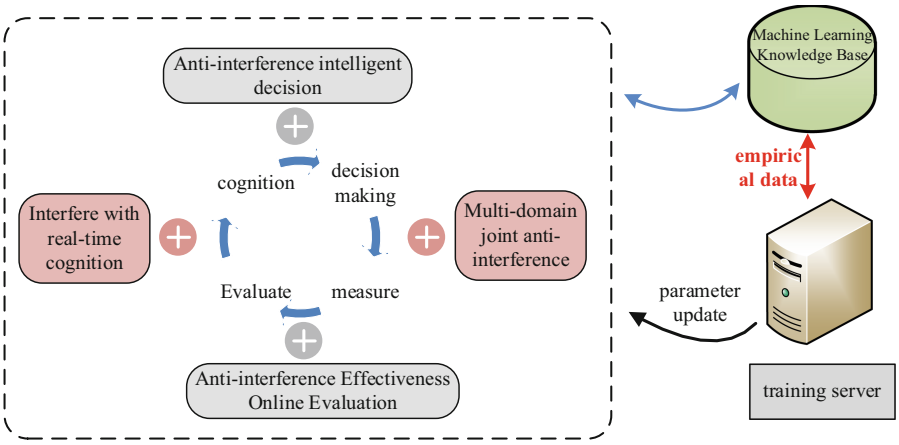


Fig. 1. Schematic diagram of intelligent anti-interference architecture

1) Cognition: Interference cognition is to realize real-time cognition of various kinds of interference in the working environment, combining the deep neural network algorithm of supervised learning and the clustering algorithm of unsupervised learning, to give full play to the advantages of machine learning algorithm in processing fuzzy uncertain signals, and does not rely on the results of interference feature extraction. At the same time, the fast matching classification and clustering mechanisms are used to improve the cognitive ability of complex and variable interference.

2) Decision-making: Intelligent decision-making is to realize the selection of system working mode and anti-interference strategy. Decision-making is based on deep reinforcement learning algorithms, taking into account machine learning knowledge base information such as interference, system capabilities, and task requirements. The decision result is the state setting and parameter setting of each unit of the system including the anti-jamming function, which will directly determine the anti-jamming capability and business operation capability of the system. Based on machine learning algorithms, it is equipped with a training server with powerful processing capabilities. Through self-learning, it continuously optimizes the decision-making process and improves decision-making performance.
3) Measures: Anti-interference measures are the state settings and parameter settings of each unit of the system according to the decision-making results, as measures to combat interference and ensure normal business operation. The anti-jamming functions of the system include array antenna intelligent anti-jamming, adaptive interference cancellation, link parameter adjustment, etc.
4) Evaluation: Intelligent evaluation is to evaluate the working state of the system, reflecting the effectiveness of the anti-interference measures selected under the current interference situation, which can assist the system in decision-making optimization.

2.2 Intelligent Interference with Cognition

In this paper, we consider a study of clustering algorithms based on supervised learning algorithms combined with unsupervised learning algorithms. The unsupervised learning algorithm is capable of clustering novel disturbances beyond the library of disturbance types and adapts to the requirements of complex disturbance environments for the system.

The interference awareness architecture used by the system combining supervised and unsupervised classification is shown in Fig. 2.

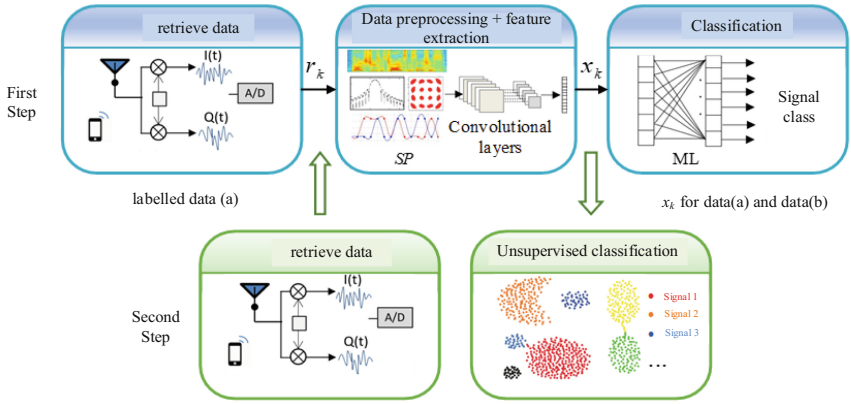


Fig. 2. Interference cognitive architecture combining supervised and unsupervised classification

Supervised classification uses the Inception network structure of CNN. The input layer uses a sample size input of 1024 × 1 × 12 or 1024 × 1 × 3 then a network consisting of two layers of convolution, activation function, pooling, and batch normalization then a network consisting of four layers of modified Inception, pooling, and batch normalization and finally a fully connected layer with Softmax for classification.

The unsupervised classification uses the K-Means iterative clustering algorithm, and the main processes include cluster assignment and moving cluster centers. The algorithm accepts an unlabeled data set and then clusters the data into different groups.

2.3 Anti-interference Intelligent Decision Making

In order to improve the response time of decision making and the success rate of interference protection, in order to improve the response time of decision making and the success rate of interference protection, we fully consider the information of multiple dimensions such as equipment information, interference characteristics, spatial posture, interference protection means and effectiveness evaluation algorithm, and at the same time make full use of the powerful information processing capability of ground station. In this paper, a reinforcement learning algorithm based on deep deterministic policy gradient (DDPG) is used to implement anti-interference decision making, as shown in Fig. 3.

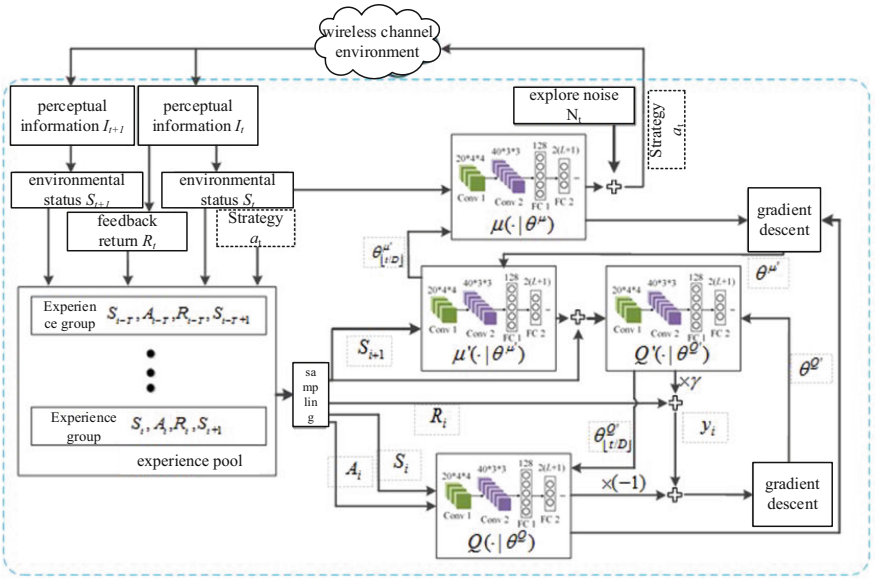


Fig. 3. Intelligent decision making based on DDPG reinforcement learning algorithm for anti-disturbance

The implementation of anti-interference decision making based on DDPG reinforcement learning algorithm mainly includes four parts: feature information pre-processing

and environment state representation, design of anti-interference strategy set, payoff function design, and deep network design and training.

1) The feature information is pre-processed, and then multidimensional information such as local device information and interference features are jointly constructed with the environment state information.
2) The anti-interference strategy set is constructed based on the interference suppression means in the link, including link parameter adjustment, array antenna anti-interference, multi-domain joint interference suppression and other anti-interference strategies.
3) The design of the return function determines the optimization direction of the DDPG algorithm. In this paper, the return function is designed according to the link communication quality assurance of the link, such as the signal-to-noise ratio.
4) Deep neural networks make anti-interference decisions based on environmental state information, and in this paper, convolutional neural networks (CNN) will be used as the decision unit for anti-interference strategies. The state matrix reflecting the dynamics of disturbances in the link environment outputs policy specific parameters through this neural network. Finally, the training of the neural network is completed based on the empirical information constructed from historical empirical information, including state information, current take strategy, payoff function value and transfer state information.

2.4 Multi-domain Anti-interference

As shown in Fig. 4, multi-domain anti-interference contains array antenna intelligent anti-interference, link parameter adjustment, adaptive interference pair elimination and other RF domain, air domain, time domain, transform domain anti-interference techniques.

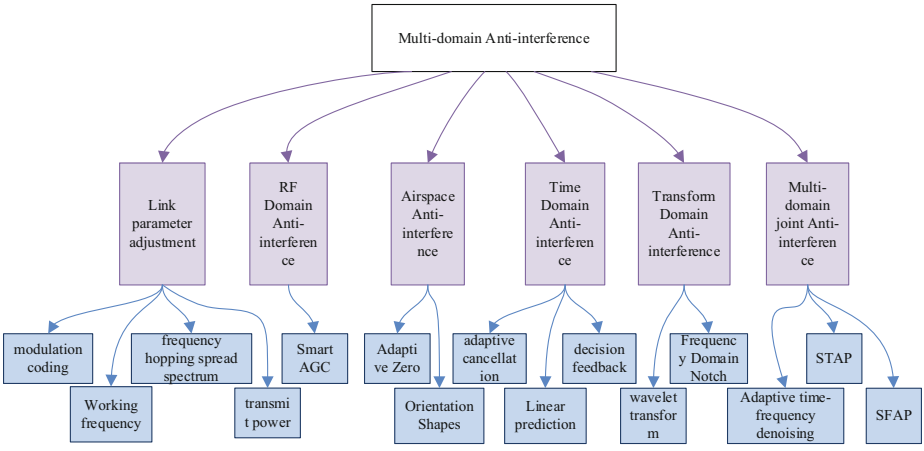


Fig. 4. Multi-domain anti-interference design

1) Array antenna intelligent anti-interference design

In this paper, we use the subarray-level beamforming based technique and combine the intelligent decision results to achieve the adaptive anti-interference capability under different interference environments. The block diagram of the adaptive anti-interference design of the array based on this method is shown in Fig. 5.

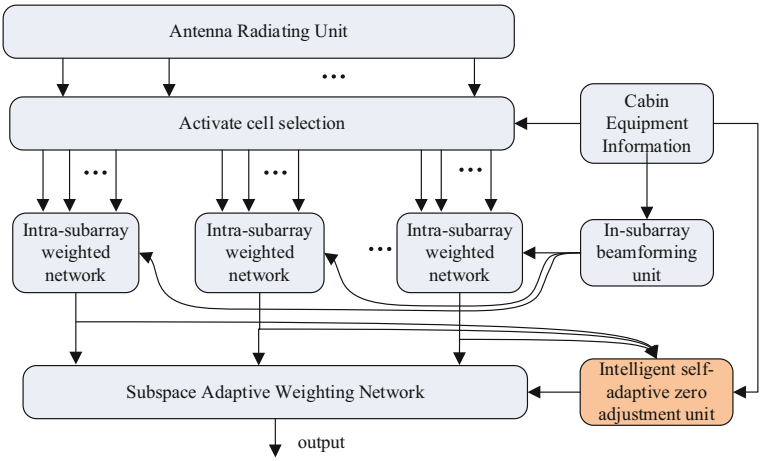


Fig. 5. Block diagram of the anti-interference design of the array antenna

The intra-sub-array weighting network outputs the data to both the adaptive zeroing unit and the inter-sub-array adaptive weighting network after weighting the sampled data of each array element within the sub-array. The intelligent adaptive zeroing unit uses the input real-time data, as well as the sensed interference parameters for adaptive weight calculation, and simultaneously outputs the calculated weights to the inter-sub-array adaptive weighting network, and finally, the inter-sub-array adaptive weighting network uses the input real-time data and the weight vector to complete the weighting of the received data, and outputs the final anti-interference data afterwards.

2) Adaptive Interference Pair Elimination

Adaptive interference cancellation takes advantage of the significant characteristic difference in the frequency domain energy of the interfering signal and the desired signal, reconstructs the interference at the receiving end, and then cancels it with the interfering signal, which has good anti-interference effect on audio interference and multi-access interference existing in systems using spread spectrum mode, etc.

The principle of signal reconstruction and parallel interference cancellation is shown in Fig. 6. The demodulation, signal reconstruction, interference cancellation, and demodulation again are all performed in parallel for K users, and the BER of the information obtained from the demodulation again is lower than that of the information obtained without interference cancellation by the above process, which achieves first-level interference cancellation.

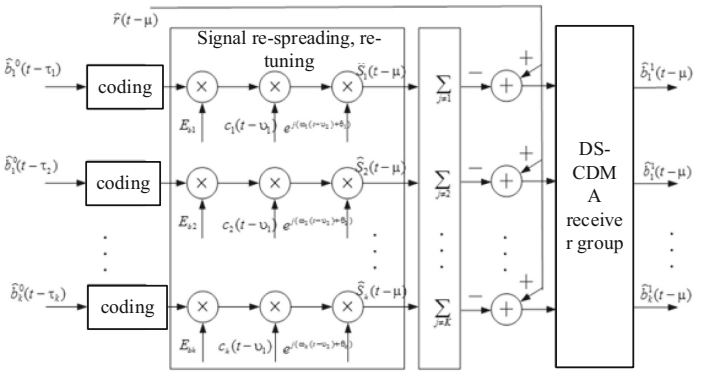


Fig. 6. Block diagram of parallel interference cancellation principle

3 Simulation Verification

After developing the anti-interference program based on tensorflow2.0 in the upper windows system, this paper uses STM32Cube.AI to convert the trained neural network model to C/C++ and run it to the underlying embedded system, and finally builds a physical demonstration system as shown in Fig. 7, the demonstration system includes STM32F767IGT6 embedded controller The demonstration system includes STM32F767IGT6 embedded controller, SX1278 LoRa module, and two types of sensors: temperature and humidity sensor DHT11 and smoke sensor MQ-2.

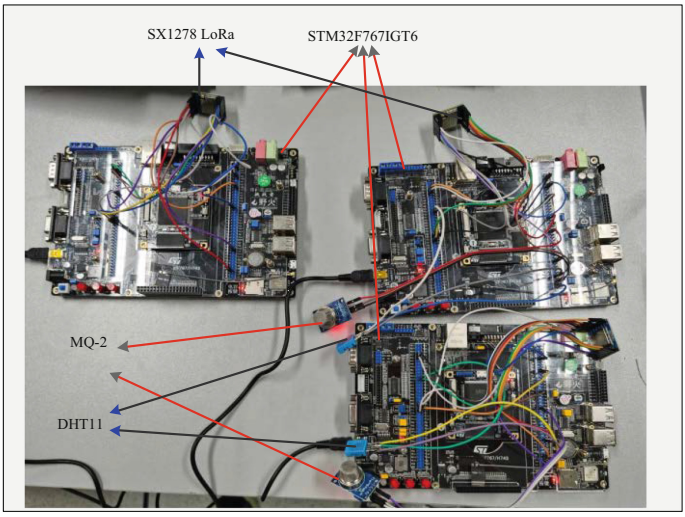


Fig. 7. Wireless transmission test physical system diagram

3.1 Intelligent Interference Cognitive Simulation

1) Classification results for single disturbances

The signals to be identified are: single-tone interference, multi-tone interference, partial band interference, noise FM interference, Gaussian pulse interference, linear sweep interference, CDMA signal, Gaussian noise (no interference).

In the simulation, the JNR of the training sample signal is −10 to 20 dB, with 1 dB JNR interval, and the number of samples per signal at each JNR is 300; the JNR of the validation sample signal is 0 to 20 dB, with 1 dB JNR interval, and the number of samples per signal at each JNR is 100; the JNR of the test sample signal is −10 to 20 dB, with 2 dB JNR interval, and the number of samples per signal at each JNR is 300. The number of samples per signal under each JNR is 300.

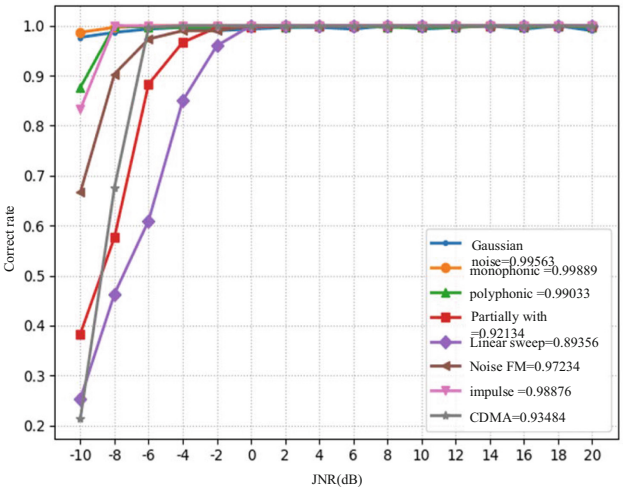


Fig. 8. Correct recognition rate of a single interference signal

As can be seen from the Fig. 8, the recognition rates of different interfering input signals are all high, and the signal recognition rates are close to 100% when the JNR is greater than 0dB.

2) Coexisting interference classification results

The actual work process, the link can not only receive a single interference signal, that is, the usual received interference signal is likely to be a variety of interference in the form of co-existence. Therefore, there is a need to classify cases where multiple interferences are mixed together. Here, three relatively similar interference signals are selected as examples.

The signals to be identified are: partial band interference, noisy FM interference, linear swept interference and their two-by-two combinations, in six categories.

In the simulation, the JNR of the training sample signal is −10 to 20 dB, with 1 dB JNR interval, and the number of samples per signal at each JNR is 300; the JNR of the validation sample signal is 0 to 20 dB, with 1 dB JNR interval, and the number of samples per signal at each JNR is 100; the JNR of the test sample signal is −10 to 20 dB, with 2 dB JNR interval, and the number of samples per signal at each JNR is 300. The number of samples per signal under each JNR is 300. The correct recognition rate of coexisting interference is shown in Fig. 9.

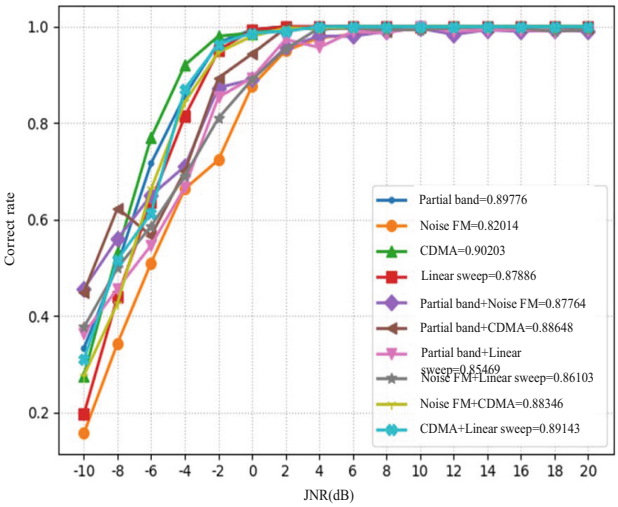


Fig. 9. Coexistence interference correct recognition rate

The confusion matrix, also known as the error matrix, is a standard format for representing accuracy evaluations. The confusion matrix of the concurrent interference signals is shown in Fig. 10.

It can be seen from Fig. 10 that when the interference-to-noise ratio is greater than 2 dB, the recognition rate of co-existing interference signals is close to 100%. When the interference-to-noise ratio is less than 2 dB, the misclassification of interference signals is almost concentrated in the interference signals related to its own signal. The complex coexisting interference signal provides reference and reference.

3.2 Anti-interference Intelligent Decision Simulation

In the simulation we assume the existence of two sources of interference, Interference 1 uses cyclic sweep interference with a sweep width of 20 sub-channels. Interference source 2 uses smart jamming, in which the source interferes with probability to the channel being used by the ground console and interferes with other subchannels at

random with probability. The DQN algorithm for behavioral selection using discrete transmit power and the DDPG algorithm for continuous transmit power selection are experimented in the simulation, and the return values of each learning using the DDPG algorithm and using the DQN algorithm are recorded.

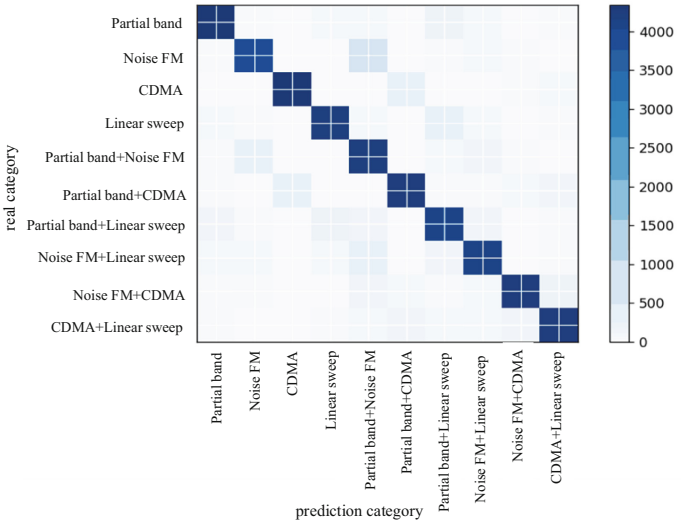


Fig. 10. Coexisting interference confusion matrix

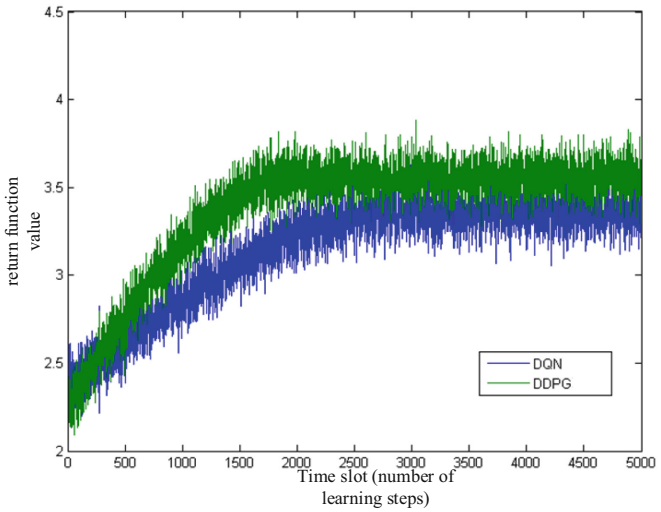


Fig. 11. Convergence of the cumulative return function in the link for the DDPG and DQN intelligent anti-interference algorithms

As can be seen in Fig. 11, the implementation of interference policy selection using reinforcement learning can all optimize the link performance. Since the approach using DQN requires quantization of the sub-channel transmit power will cause gain loss in optimal performance DDPG due to the DQN algorithm. At the same time, the algorithm starts with a better return function value than the DDPG algorithm because the DQN algorithm has a smaller retrieval space after strategy space quantization.

4 Conclusion

This paper addresses the complex electromagnetic environment problems faced by the application of wireless sensor networks in nuclear power plants, and carries out multi-domain interference signal detection in the time domain, frequency domain and air domain, interference feature parameter extraction through supervised and unsupervised strategies, and focuses on the effectiveness of multi-domain anti-inhibition of interference signals under the conditions of multipath fading (interference), partial band interference and multi-tone interference in the compartment of nuclear power plants. Through the research of this paper, we strive to reduce (or even eliminate) multiple electromagnetic interferences in large-scale wireless sensor networks from time/frequency/space multi-dimensions, and at the same time enhance the large-scale networking capability of sensor networks, form a study on intelligent interference signal feature identification, adaptive antenna array beamforming, and multi-domain interference suppression, and verify the feasibility and effectiveness of the proposed intelligent anti-interference based on its learning through physical simulation analysis. Through physical simulation analysis, the feasibility and effectiveness of the proposed intelligent anti-interference based on its learning are verified, and the theoretical basis is laid for the application of wireless sensor networks in nuclear power plants.

References

1. Lanhai, Fang, L., et al.: Shipboard Electrical Power Systems, 2nd edn. National Defence Industry Press, Beijing (2016)
2. Bkassiny, M., Li, Y., Jayaweera, S.K.: A survey on machine-learning techniques in cognitive radios. IEEE Commun. Surv. Tutor. **15**(3), 1136–1159 (2013)
3. Jayaweera, S.K.: Machine learning in cognitive radios, in signal processing for cognitive radios. Wiley Telecom (1), 768–770 (2015)
4. Chu, G.-S.: Research and implementation of modulation identification of non-collaborative communication signals. Chongqing University, Chongqing (2017)
5. Li, J.D., Feng, X.: Modulation recognition algorithm based on support vector machine and cyclic accumulation. Syst. Eng. Electron. Technol. **4**, 520–523 (2007)
6. Cai, Z.W., Li, J.D.: Individual identification of communication radiation sources based on dual spectrum. J. Commun. **28**(2), 75–79 (2007)
7. Guiguan, Wang, Y., Huang, H.: Deep learning-based physical layer wireless communication technology: opportunities and challenges. J. Commun. (40), 19–23 (2019)
8. Sun, M., Zhao, T., Guo, Y., et al.: Decision tree based modulated signal automatic identification algorithm and its DSP implementation. J. Guilin Inst. Technol. (1), 115–118 (2005)

9. Xiang, F., Hongbo, Y.: A hierarchical modulation classification algorithm based on higher-order cyclic accumulation and support vector machine. Telecommun. Technol. **52**(6), 878–882 (2012)
10. Li, J.-J., Lu, M.-Q., Feng, Z.-M.: A support vector machine based hierarchical modulation identification method. J. Tsinghua Univ. (Nat. Sci. Ed.) **46**(4), 500–503 (2006)
11. Feng, X.Z., Luo, F.L., Yang, J., et al.: Wavelet-based support vector machine for digital communication signal modulation identification. J. Electron. Measur. Instrum. **23**(3), 87–92 (2009)
12. Yuanbo, C., Chunyu, Z.: Short-range wireless communication technology and applications. Electronic Industry Press, Beijing (2015)
13. Gross, F.: Smart Antenna for Wireless Communications. McGraw Hill (2009)
14. Duan, C., Zhang, L.J.: Interference suppression method for frequency hopping systems based on adaptive antennas. Radio Wave Sci. **19**(6), 726–729 (2004)
15. Hongxia, W., Chengsheng, P.: Interference suppression study of satellite frequency hopping system based on beamforming. J. Astronautics **32**(8), 1793–1798 (2011)
16. Lee, Y., Jan, Y., et al.: Using hopping technique for interference mitigation in modulated scattering array antenna system. IEICE Exp. **7**(12), 839–843 (2010)

Research on Application of High Temperature and High Pressure Radar Liquid Level Measurement in Nuclear Power Plant

Zhi-guang Deng(✉), Bi- wei Zhu, Qian Wu, Xue-mei Wang, Si- jie Xu, Jia-liang Zhu, Chen-long Dong, and Yong-sheng Sun

Science and Technology on Reactor System Design Technology Laboratory, Nuclear Power Institute of China, Chengdu 610213, China
dzg7400613@163.com

Abstract. At present, the water levels of high-temperature and high-pressure vessels such as voltage stabilizers and steam generators on ships' nuclear power plants are measured by the pressure principle. Affected by the load conditions in the vessels, the differential pressure water level measurement has problems of low accuracy and low reliability. The radar type liquid level gauge has the advantages of high precision and high reliability, and is an effective means of measuring the liquid level of high temperature and high pressure containers. In this paper, a FMCW system split guided wave radar based on the principle of frequency domain reflection (FDR) is proposed for liquid level measurement. The antenna probe part and the electronics part adopt a split structure, and the electronics part is installed in the secondary instrument cabin with better environmental conditions., the radar is easy to meet the index requirements of shock, vibration and irradiation. The high-frequency signal emitted by the radar antenna is conducted along the coaxial rod probe, and the signal will be reflected only when it encounters the surface of the material, which effectively eliminates the influence of obstacles such as the heating plate in the container, the internal reference pipe water replenishment device and the reference pipe connection. Non-blind zone measurement of liquid level to meet the liquid level measurement requirements of high temperature and high pressure vessels in ship nuclear power plants.

Keywords: nuclear power plant · high temperature · high pressure · radar level gauge

1 Introduction

The water level of high-temperature and high-pressure vessels such as regulators and steam generators on naval nuclear power plants is the most direct parameter to characterize the amount of water installed in a circuit or two circuits, and has been used as an important control parameter or even protection parameter, directly its measurement reliability and accuracy requirements are very high, at present the above water level measurement is generally measured using the differential pressure principle [1–5]. Affected

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 57–72, 2023.
https://doi.org/10.1007/978-981-99-3455-3_6

by the operating conditions of nuclear power plant, the water in the vessel is basically in a two-phase state, and pressure, temperature, etc. also changes with the operating conditions, the hull tilt and sway, etc. will also have an impact on the measurement, the above factors make the differential pressure water level measurement has low accuracy, reliability is not high, especially in mobile and special operating conditions or even a significant change in water level or unavailable, seriously affecting the manipulation of the nuclear power plant by the operator.

The electromagnetic wave emitted by the radar level meter has a stable propagation speed in the same medium, so it is not affected by temperature, density, dust, pressure, etc. It can work stably and accurately in a complex environment, and has the advantages of high accuracy and reliability, which is an effective means of high temperature and high pressure vessel level measurement. The existing mature industrial products [6–9], in the use of environmental conditions, structure type and other aspects of the nuclear power plant high-temperature and high-pressure vessel level measurement needs there is still a big gap, the application to nuclear power plant is facing great problems.

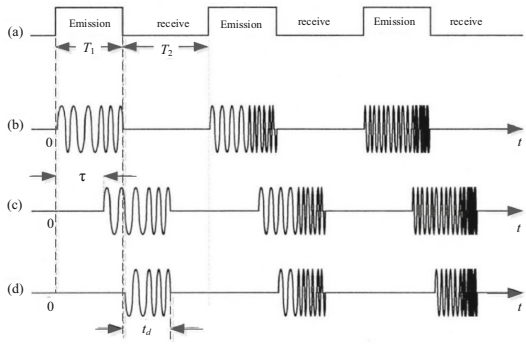
According to the classification of the emission signal system, the measurement method of radar level meter has two methods: pulse method [10] and frequency modulated continuous radar wave (FMCW) measurement [11]. According to the classification of radar antenna form, radar level meter can be divided into intelligent radar and guide wave radar two kinds [12, 13]. Pulse method radar is to transmit radar pulses in an intermittent manner, and the radar waves propagate in free space at the speed of light. The distance from the reflecting surface to the probe is calculated by measuring the time from the radar wave being emitted to being accepted. Frequency modulated continuous wave radar level meter continuously emits radar wave signal, it is important that the frequency of radar wave is continuously changing, the rate of change of radar wave frequency is constant in one measurement cycle, strictly speaking, frequency modulated continuous wave radar level meter measures the time travel by measuring the frequency deviation. Intelligent radar transmits microwave signals through the antenna, the signal propagates in space at the speed of light and encounters the surface of the measured medium, part of its energy is reflected back and received by the same antenna to achieve non-contact measurement of the object surface. Based on the time domain reflection (TDR) principle, the guided wave radar emits high frequency pulses through the probe and conducts them along the cable or rod probe. When the pulses meet the material surface, they are reflected back and received by the receiver inside the instrument, and the distance signal is converted into the level signal. Since it is based on the principle of guided wave, the guided wave radar has strong suppression ability to dust, steam and foam, and even the environment with a large amount of steam does not affect its measurement accuracy.

In this paper, we carry out research on high precision radar level measurement technology for high temperature and high pressure vessels of nuclear power plants, propose a split type level measurement radar solution applicable to the nuclear power environment conditions of ships, break through the transmitting and receiving technology of level measurement radar system, long distance radar signal transmission and signal processing technology, and key process technology of high precision radar level meter; develop the level measurement radar prototype and complete the functional performance test verification.

2 Frequency Modulated Continuous Radar Wave (FMCW) Split Guided Wave Radar Liquid Level Measurement Based on Frequency Domain Reflectometry (FDR)

2.1 Large Dynamic Range Signal Reception Based on FM Interrupted Continuous Wave

The liquid level measurement radar uses a frequency modulated interrupt continuous wave technology to solve the isolation problem between the transceiver. A gating switch is configured in the radar transmitter and receiver. Within the time width of the chirp pulse transmitted by the radar, the transmit gating pseudo-random sequence is used to modulate the amplitude of the radar transmit signal, and the received echo signal is also used for amplitude modulation. The receive gated pseudo-random sequence is amplitude modulated. That is, when the radar signal is transmitted, the receiver does not receive it, and when the radar signal is turned off, the receiver receives it, as shown in Fig. 1. This scheme can not only solve the transceiver isolation problem of LFM system radar, but also effectively reduce the requirements on the dynamic range of the receiver.



(a) Transmit and receive timing (b) Transmit signal waveform (c) Echo signal waveform (d) Receive signal waveform

Fig. 1. Schematic diagram of the working of FMICW radar

The typical transmit gate waveform and receive gate waveform are shown in Fig. 2, and the corresponding average received signal function waveform is shown in Fig. 3. It can be seen from Fig. 3 that the use of the FMICW scheme can greatly suppress the transceiving direct-coupled signal and the echo amplitude in the vicinity, and has the effect of time-varying gain similar to the time-domain shock pulse radar.

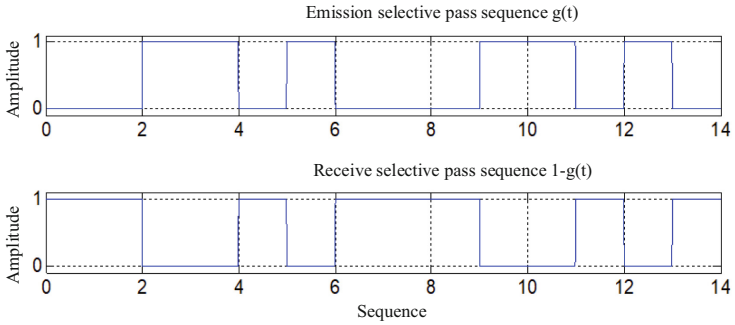


Fig. 2. M-sequence strobe waveform of length 7

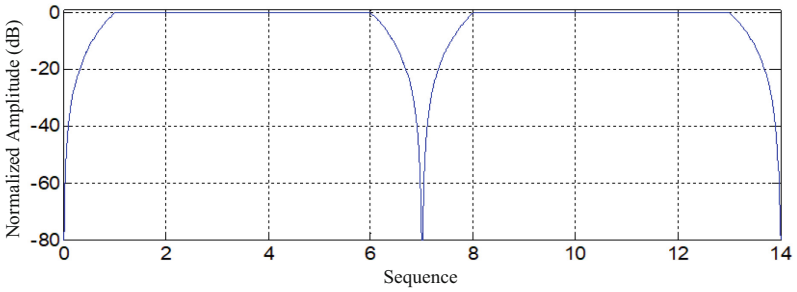


Fig. 3. The average received signal waveform of the M-sequence gated waveform of length 7

2.2 Large Dynamic Range Signal Reception Based on FM Interrupted Continuous Wave

Linear frequency modulation signal (LFMCW) is generally obtained by phase-locked loop and voltage-controlled oscillator (VCO), and there are usually two schemes: open-loop and closed-loop. The closed-loop scheme adds the phase-locked loop to lock and track the phase information, which can realize the automatic calibration of the frequency. Therefore, the closed-loop scheme is adopted in this paper.

The liquid level measurement radar works in the L-band. Due to the relative bandwidth limitation of the existing VCO devices, the ultra-wideband LFMCW signal required by the system cannot be directly generated. In this paper, the down-conversion method is used to realize the L-band LFMCW signal generation. First, the LFMCW signal with the required bandwidth is generated in a higher frequency band, and then the required ultra-wideband LFMCW signal is realized by down-conversion. Because the linearity of the voltage control curve of the VCO is poor and will drift with temperature, it cannot guarantee the output of a high linearity FM signal. The DDS output signal with the constant temperature crystal oscillator as the clock is used as the reference signal, and the linearity of the output FM signal is corrected in real time through closed-loop feedback.

The principle of the LFMCW transmitter in the L-band is shown in Fig. 4. Two PLLs are used in the transmitter, in which PLL1 and VCO generate the LFMCW signal of C-band, which is amplified and filtered and sent to the RF input of the mixer. L-band LFMCW. The output signal is divided into two channels after power division, one of which is amplified and filtered and then fed into the circulator to be fed to the antenna probe unit, and the other is amplified as the local oscillator signal of the receiver.

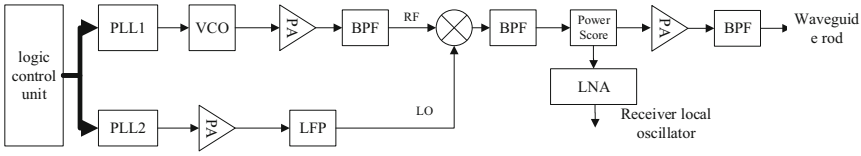


Fig. 4. Schematic diagram of the signal source of the liquid level radar

2.3 Long-Distance Signal Transmission and Signal Processing

There is a long distance between the split-type liquid level measurement radar antenna probe and the electronic part. The transmitted signal needs to be transmitted from the transmitter to the probe, and the received signal needs to be transmitted from the probe to the receiver. There are generally two methods for realizing long-distance microwave signal transmission: optical fiber transmission and coaxial cable transmission.

Optical fiber transmission first uses an electro-optical conversion module to convert the microwave signal into an analog optical signal so that it can be transmitted in the optical fiber, and then uses a photoelectric conversion module at the receiving end to restore the analog optical signal to a microwave signal. Because the loss of the fiber is very low, it can transmit long distances. However, in practical applications, the electro-optical conversion module has a loss of about 30 dB, and the photoelectric conversion module has a loss of about 10 dB. Therefore, the microwave signal has a differential loss of 80 dB in the sending and receiving transmission path, and the photoelectric conversion module installed at the antenna end is the same as the electro-optical conversion module. There is a risk of strong radiation, and it can be seen that it is not feasible to use optical fiber for long-distance microwave signal transmission in this paper.

Compared with optical fiber transmission, although the loss per unit length of microwave signal transmitted by coaxial cable is larger, the loss is directly related to the signal frequency. As the frequency decreases, the loss also decreases rapidly, and there is no additional loss introduced by the photoelectric conversion module. Therefore, this paper chooses ultra-low loss 50 Ω coaxial cable to realize long-distance signal transmission. In order to further reduce the signal loss, the operating frequency of the radar is selected in the L-band, and the cable loss in this frequency band is about 6dB/100ft. After theoretical calculation, it can meet the signal transmission requirements of the liquid level measurement radar.

This paper not only needs to adapt to use in various complex environments, but also needs to meet the requirements of high measurement accuracy and real-time performance. In view of the shortcomings of the existing high-precision ranging algorithms

such as slow calculation speed or poor anti-noise performance, non-uniform spectrum is used for signal processing. The refinement algorithm (NSZT), by judging the signal frequency range and finally narrowing the range, obtains high-precision signal frequency information, in exchange for the anti-noise performance of the algorithm at the expense of increasing the amount of calculation, and NSZT can use parallel algorithms, The computational efficiency can be greatly improved. Real-time distance measurement is achieved while ensuring the ranging accuracy. Simulation and experiments show that the method can be used for high-precision ranging applications.

3 Analysis of Liquid Level Composition of Split Guided Wave Radar

The traditional radar level gauge adopts an integrated structure, and the radar electronics part is installed on the top of the container, which is directly connected to the antenna in the container. The environmental parameters of the liquid level measurement of the nuclear power plant of the ship are extremely harsh and have a very strong radiation dose, which far exceeds the index requirements of radiation-resistant and hardened electronic components. The electronic part is structurally shielded, and the effect is often unsatisfactory. At the same time, it brings huge weight overhead, and it is difficult to meet the index requirements such as shock and vibration. Therefore, the liquid level measurement radar studied in this paper is planned to use a split structure, and the electronic part is installed in the secondary instrument cabin with better environmental conditions, so that it is easy to meet the requirements of shock, vibration and irradiation indicators.

High temperature and high pressure containers such as pressure stabilizers have liquid surface boiling phenomenon, causing liquid level fluctuations and forming foam on the surface of the liquid medium. Fluctuations in the liquid level will cause deviations in the direction of the echoes, making the antenna of the traditional radar level gauge unable to receive. The foam can both absorb microwave signals and reflect them, attenuating the transmitted signal and causing measurement errors. It can be seen that the antenna type radar liquid level gauge commonly used in the industry cannot measure normally when the liquid level is boiling. For the measurement of the boiling liquid level, the still-pipe installation method should be selected, or a guided-wave radar level gauge should be used. The still-pipe is used for collecting waves and preventing liquid level fluctuations, which can avoid the influence of obstacles and foam in the container on the measurement. Guided wave radar uses a probe to guide radar waves. The electromagnetic wave emission and reception of this radar are carried out along the probe. It is suitable for measuring media with foaming, boiling surface or turbulent flow. Strong inhibitory power, measurement is not affected. In addition, FMCW radar has the advantages of miniaturization and low radiation power. Therefore, this paper proposes a FMCW system split guided wave radar based on the principle of frequency domain reflectometry (FDR) for liquid level measurement. The schematic diagram of the system is shown in Fig. 5.

Liquid level measurement radar consists of electronic unit, coaxial probe, cable assembly and other parts. Among them, the electronic unit is installed in the secondary instrument cabin, and the coaxial probe is installed in the container under test.

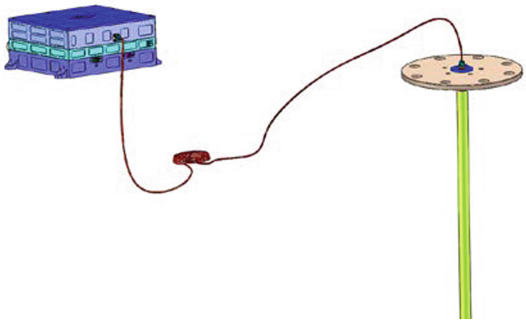


Fig. 5. Structure diagram of liquid level measurement radar equipment

3.1 Electronics Unit

The block diagram of the electronic unit of the guided wave radar for liquid level measurement based on FDR is shown in Fig. 6, which is controlled by the distributor, reference clock module, chirp source, transmitter circuit, circulator, receiver RF, receiver IF, acquisition and processing unit composition. The system uses a high-stability, constant temperature 100 MHz crystal oscillator as the reference frequency source, and generates two reference frequencies through the phase-locked crystal oscillator (PLO), which are used as the data acquisition clock and the reference FM signal generation clock respectively. The linear frequency modulation signal source generates a fast and stable frequency multiplication signal of the reference frequency modulation signal through a VCO oscillator and phase-locked loop technology, which meets the linearity requirements of the frequency sweep signal. After the FM signal is amplified and the amplitude is regularized, most of the energy is transmitted to the probe through a long distance and radiated. A small part of the signal is sent to the receiver through the directional coupler for mixing with the received signal, the difference frequency signal is taken out, and the data is collected after amplification. Finally, after real-time data processing, the liquid level measurement results are uploaded to the remote terminal for display and storage.

3.2 Waveguide Rod

The flange of the radar level gauge, the inner core rod and the outer conductor tube of the coaxial still-pipe are all made of stainless steel. The brass connector ensures good conduction, and the structure of the flange end is shown in Fig. 7. The total length of the stainless steel outer conduit and the inner core rod is divided into 4 sections, each section is 1 m long, and the total length is 4m. The overall schematic diagram of the probe is shown in Fig. 8. The diameter of the inner pipe is 30 mm, and each pipe is threaded through the inner pipe connector. The diameter of the outer pipe is 60 mm, and the pipes are connected by thread. The detailed connection is shown in the figure. The inner and outer pipes are coaxially and insulated between pipes through polyimide connecting pieces, and the connecting pieces and the outer conduit are tightly connected by the external structure support, and are connected with the inner core rod through threads. Pressure equalizing holes are opened on the outer wall of the outer conductor

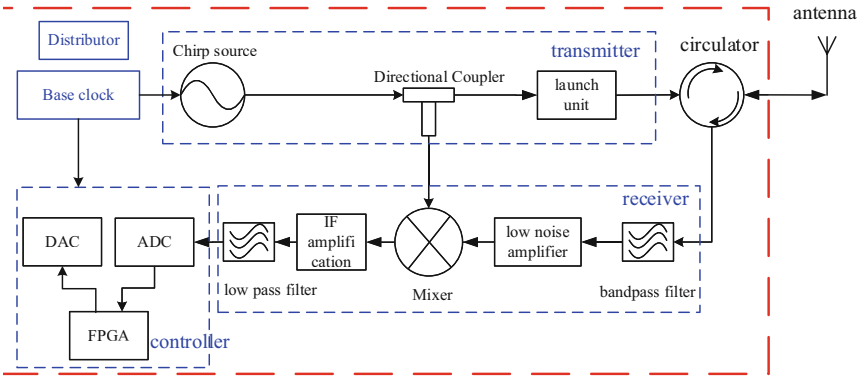


Fig. 6. Block diagram of electronic unit of liquid level measurement radar

tube of the top section near the flange to ensure the same water level inside and outside the probe. The annular connecting piece of the inner and outer tubes is a hollow part with four fan-shaped holes on it to ensure the same pressure between each section of the probe.

The mechanical simulation analysis of the probe shows that the current structural design can meet the requirements of the working pressure difference of 17.2 MPa inside and outside the tested vessel, which verifies the effectiveness of the structural design scheme.

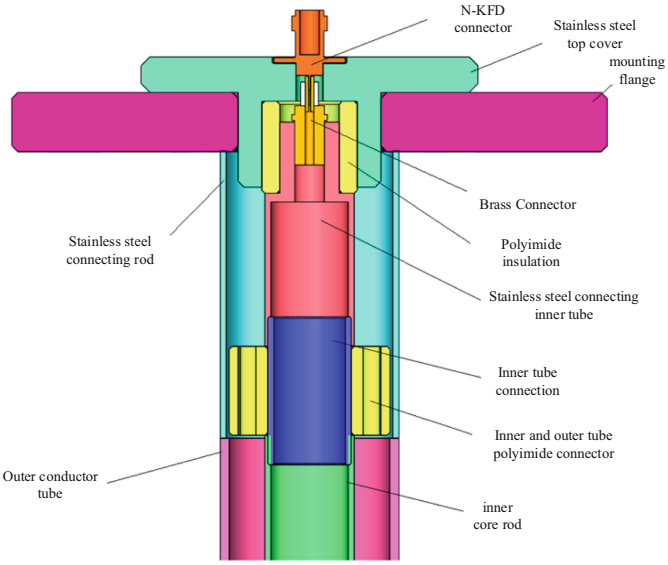


Fig. 7. Schematic diagram of the structure of the still-pipe of the liquid level gauge

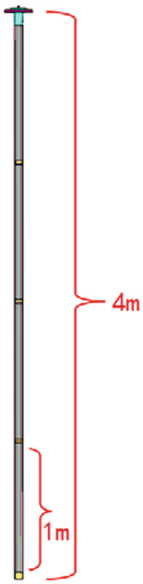


Fig. 8. Overall schematic diagram of the probe

4 Test and Validation

4.1 Simulation Analysis

The transmission and reflection of signals on a coaxial probe can be explained using transmission line theory, and Fig. 9 shows how it works. According to the transmission line theory, the guided wave coaxial can be equivalent to a transmission line. The characteristic impedance of the transmission line is directly related to the electrical properties of the medium it fills. The calculation of the reflection coefficient in the process of signal propagation is as follows:

$$\Gamma = \frac{Z_t - Z_0}{Z_t - Z_0} \tag{1}$$

Among them, Zt is the impedance at a certain point of the guided wave coaxial, and Z0 is the characteristic impedance of the coaxial.

In order to analyze the working characteristics of the coaxial probe segment, a simulation model is established using the electromagnetic simulation software HFSS, as shown in Fig. 10. In the model, the inner conductor diameter of the coaxial rod segment is 26 mm, the outer conductor diameter is 60 mm, the insulating collar material is polyimide composite material or ceramic, and the dielectric constant is 6.0. The S11 and S21 simulation results of the probe segment are shown in Fig. 11 and Fig. 12, respectively. It can be seen that in the working frequency band of the liquid level radar, the reflection coefficient of the single-section probe is less than -6dB, and the transmission coefficient is greater than -1.5dB.

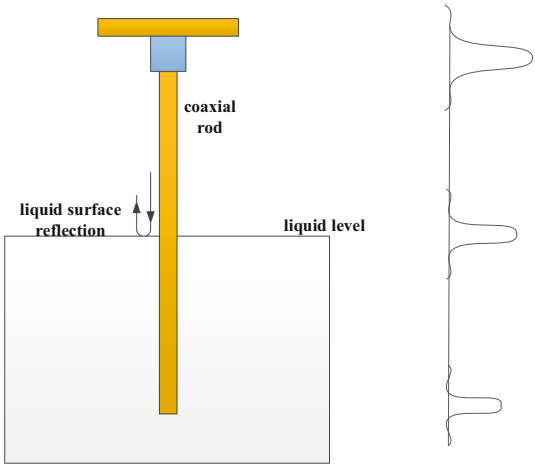


Fig. 9. Working principle of coaxial probe

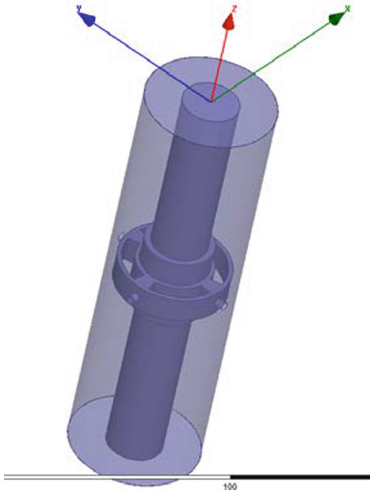


Fig. 10. Probe segment model

Use ADS RF simulation software to simulate the probe segment without insulating collar, and obtain the characteristic impedance of the probe to be 50.1 Ω. Then simulate the probe segment filled with liquid water between the inner and outer conductors to obtain the guided wave. The characteristic impedance of the rod is 5.6 Ω. According to the calculation formula of the reflection coefficient, the reflection coefficient of the electromagnetic wave at the liquid surface is -1.9 dB.

In addition, the length of the selected high-frequency cable SYV-50-3-5 is 30 m. After considering the loss of the conversion connector, the one-way attenuation in the L-band is about 15dB. According to the above analysis, the strongest echo signal of

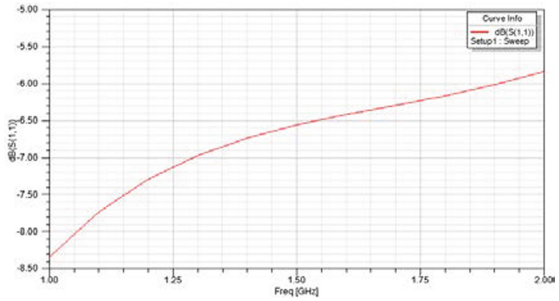


Fig. 11. Segmented S11 curve of the probe

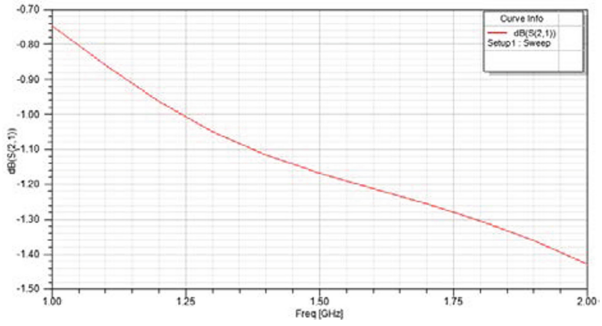


Fig. 12. Segmented S21 curve of the probe

the liquid level radar is the reflected signal of the insulating collar in the topmost probe section, and the signal power is 0 dBm–15 dB–6 dB–15 dB = –36 dBm; the weakest echo is the liquid level The reflected signal of the liquid level at the lowest time, the signal power is 0 dBm–15 dB–10 × 1.5 dB–1.9 dB–10 × 1.5 dB–15 dB = –62 dBm.

In order to further analyze the working characteristics of the coaxial rod guided wave radar, a simulation model is established using the electromagnetic simulation software CST. The amount of full-wave simulation grids is large, and the calculation is time-consuming. In order to reduce the calculation time, a smaller simulation model is used for calculation. The length of the coaxial rod is 0.7 m, the distance from the liquid level to the port is 0.6 m, and the distance from the bottom of the liquid level to the port is 0.8 m. The liquid is water (dielectric constant 81, conductivity 0.01 S/m). In the simulation, the feed signal is a Gaussian pulse signal with a pulse width of about 2 ns.

Figure 13 shows the feed pulse signal and a series of reflected signals received by the port. It can be seen from the figure that the first reflected signal is the strongest, that is, the reflected echo of the feed port; the second reflected signal is the same as the first reflected signal. The time interval of the first reflection signal is 4 ns, which is consistent with the two-way time of the liquid surface reflection echo, so it is the liquid surface echo; the time difference between the third reflection signal and the first reflection signal is 8.5 ns, which is reflected from the end of the coaxial rod. The two-way time of the echo is the same (the water volume in the simulation is small, and the effective dielectric

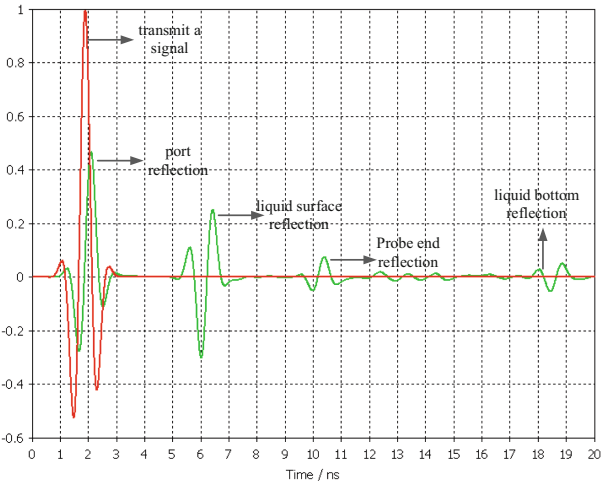


Fig. 13. Feed signal and reflection signal of coaxial probe port

constant is less than 81), so it is the echo reflected from the end of the coaxial rod; the time difference between the fourth reflected signal and the first reflected signal is about 16 ns, which should be Reflected signal for the bottom of the liquid surface. The simulation results show that the coaxial probe can be used for effective measurement of liquid level.

4.2 Experimental Verification

1) Measurement range verification test.

A special water level test device with a height of 4 m is processed, and the probe is placed in the test device, and the whole is in a vertical state. The measurement range of the radar level gauge is confirmed by injecting or draining water and measuring the water level, as shown in Fig. 14.

When measuring, firstly inject water into the water level measuring device until the water level is flush with the bottom end of the probe, observe and record the reading of the radar level gauge, and compare and confirm with the actual liquid level. Then fill the water level measuring device with water until the water level is close to the flange position, observe and record the reading of the radar level gauge again, and compare it with the actual liquid level to confirm. The reading range of the two measurements is the measurement range of the radar level gauge, the data are recorded in Table 1 as shown.

2) Measurement Accuracy Verification Test.

The probe is placed in the water level test device, and the whole is in a vertical state. The water level is changed by injecting or draining water, and the comparison is performed at 1 to 2 points per meter, and the difference between the radar level gauge reading and the actual liquid level is compared to verify. The water level measurement accuracy of the radar level gauge. For each measurement, it is necessary to wait for the

Fig. 14. Functional performance test test device

Table 1. Measurement range verification test

Test items	Ruler to measure liquid level (cm)	Radar level gauge reading (cm)	In line with the situation
Low water level measurement	0	0.7	Conformity
High water level measurement	379.6	380.5	Conformity

water level and radar level gauge readings to stabilize before recording. The ruler level and radar level gauge readings and errors are shown in Fig. 15.

It can be seen from the figure that the standard deviation of the difference between the reading of the radar level gauge and the actual liquid level is less than 20 mm, and the measurement accuracy test of the radar level gauge is qualified.

3) Response time test

The response time of the radar level gauge is the time from 10% of the sudden change of the liquid level range to the stable display of the radar level gauge reading. During the test, the liquid level in the water level test device is abruptly changed by at least 0.4 m by injecting water. After the water level is stable, the timing is started, and the reading of the radar level gauge is observed. After the reading is stable, the timing ends, and the measured time difference is the radar level gauge. The response time, three test records are shown in Table 2.

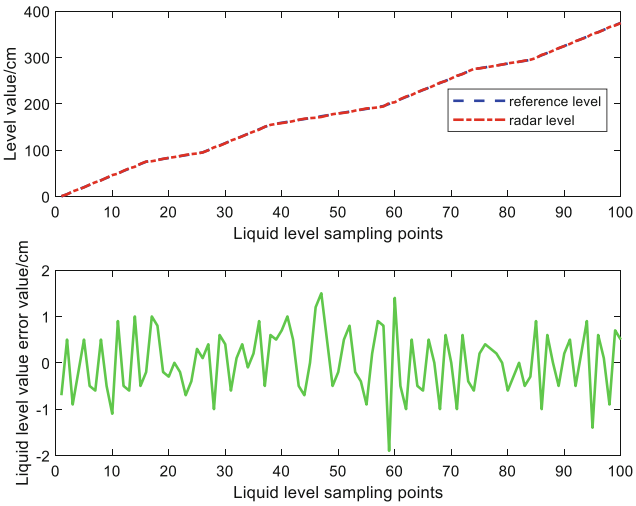


Fig. 15. Ruler level and radar level gauge readings and errors

Table 2. Response time verification test

No	Response time (s)	Qualification status	Notes
1	1.5	Qualified	Radar level meter response time is less than 2s, the test is considered qualified
2	1.7	Qualified	
3	1.3	Qualified	

4) Dynamic water level detection test

The probe is placed in the water level test device in a vertical state, and the dynamic water level detection performance of the radar level gauge is confirmed by injecting or draining water and continuously measuring the water level. Within the measurement range of the water level test device, within 4 m, the water level is raised and lowered for two whole journeys with a water level rate of 20 ~ 40 cm/min, and the comparison is carried out at 1 ~ 2 points per meter. Compare the difference between the radar level gauge reading and the actual level.

When the standard deviation of the difference between the reading of the radar level gauge and the actual liquid level is less than 20 mm, the dynamic water level detection test of the radar level gauge is qualified. The test results are shown in Table 3, and it can be seen that all reading points are qualified.

Table 3. Dynamic water level detection test

No	Ruler level (cm)	Radar level gauge reading (cm)	No	Ruler level (cm)	Radar level gauge reading (cm)
1	30	30.6	2	50	49
3	70	70.79	4	90	90.44
5	110	109.2	6	130	129.7
7	150	149.8	8	170	169.5
9	190	190.4	10	209.6	210.1
11	229.6	230.2	12	249.6	248.5
13	269.6	269.9	14	289.6	289.5
15	319.6	320.3	16	339.6	339.1
17	359.6	359.6			

5 Conclusion

In order to overcome the problems of low precision and low reliability caused by the differential pressure measurement method of high temperature and high pressure vessel water level on the nuclear power plant of ships. This paper proposes a FMCW system split guided wave radar based on the principle of frequency domain reflectometry (FDR) for liquid level measurement, which has the advantages of miniaturization, low radiation power, high range resolution, and high echo signal-to-noise ratio. Key problems such as signal generation and signal transmission are solved by methods such as large dynamic range signal reception of FM interrupted continuous wave, broadband low phase noise and high stability signal source generation, long-distance signal transmission and signal processing. At the same time, the key process and structure design of the split guided wave radar level gauge are carried out. Through simulation analysis and a series of functional performance tests such as measurement range, measurement accuracy, and response time, it is shown that the split guided wave radar level gauge proposed in this paper is proposed in this paper. Under the working pressure of 17.2 MPa and the working temperature of 350°C, the key indicators such as the measurement accuracy of not less than ± 20 mm (±0.5%FS) and the measurement distance of not less than 10m have been achieved, which verifies the feasibility of the proposed radar level gauge and reliability.

References

1. Wenqiang, Z., Yong, H., Lide, Z., Chuanqing, W., Shoujie, Z., Tiancai, H.: Research and design of water level measurement system for marine pressurized water reactor. Small Medium Enterp. Manag. Technol. **06**, 140–143 (2019)
2. Dapeng, L., Zhidong, Y., Yansong, Z.: Improvement of soft sensing technology of evaporator double reference tube water level measurement system. Comput. Measur. Control **13**(11), 1186–1188 (2005)

3. He, B., Wu, Q., Yong, H.: Design of a signal processing circuit for water level measurement of a dual-reference tube regulator. Instrum. User **25**(12), 81–84 (2018)
4. Wu, Q., Xu, T., Zhu, J., He, P., Chen, X., Chen, J.: Research on steam generator water level measurement technology based on automatic correction. Sci. Technol. Vision. **2019**(12), 4–5+43 (2019)
5. Yang, Z., et al.: Research on water level measurement technology of steam generators in surface nuclear power plants. Nucl. Power Eng. **40**(05), 156–159 (2019)
6. Conghui, T., Wei, W., Min, G.: Application of SAAB radar level gauge in LPG storage tank. Res. Dev. **04**, 97–98 (2016)
7. Lei, Z., Deyin, L.: Application and improvement of guided wave radar level gauge in Fuqing nuclear power plant. Autom. Instrum. **40**(6), 16–19 (2019)
8. Lijun, C.: Application of radar level gauge in oil tank measurement. Instrum. User **26**(6), 38–41 (2019)
9. Jia, B.: Application of improved radar liquid level gauge in tank liquid level measurement. Autom. Instrum. **38**(11), 60–63 (2017)
10. Wang, H., Yang, D.: Application and error analysis of pulse radar liquid level gauge. Petrochem. Autom. **6**, 72–75 (2015)
11. Lu, J., Wu, L., Zhao, D.: Design of FMCW radar water level gauge. Mech. Des. Manuf. **3**, 178–181 (2018)
12. Zeng, K.: Research on microwave radar level measurement technology. University of Electronic Science and Technology of China (2017)
13. Cheng, C.: Design and application of guided wave radar liquid level gauge in petrochemical plant. Petrochem. Autom. **57**(S1), 146–149 (2021)

Fault Analysis and Condition Monitoring of Drum Screens in Nuclear Power Plants

Fei Yu(✉), Xiang- Jie He, Xing-Bing Lv, and Wei-Hua Zhou

China Nuclear Power Design Co., Ltd., Shenzhen, China
89631670@qq.com

Abstract. As nuclear safety equipment for nuclear power plants, the drum screen can ensure the safety of the cold source of the nuclear power plant by arresting small debris in seawater. The drum screen is prone to failures such as corrosion of metal parts, large vibration of the driving device, and fracture of structural connecting bolts. In actual operation, due to the lack of automatic monitoring means, the operating personnel only rely on regular inspections to identify equipment operating failures, resulting in untimely detection of equipment failures, which will affect the reliability and safety of the cooling source of the unit.

In this paper, by analyzing the operation failure types and root causes of the drum screen, the fault monitoring method of the drum screen is studied, and the vibration, stress, and corrosion monitoring system scheme of the drum screen is proposed; From the aspects of operation and maintenance, cost-effectiveness, etc., the feasibility of the condition monitoring of the drum screen is analyzed. This scheme can be used for safety monitoring and early warning of cold sources in nuclear power plants, realize the intelligentization of daily operation and maintenance of drum screens and reduce the operation and economic risks of nuclear power plants.

Keywords: drum screen · fault analysis · condition monitoring

1 Introduction

As a key equipment of the seawater filtration system of the nuclear power plant, the drum screen performs the function of filtering the influent water of the nuclear power plant to ensure that the water quality meets the operation requirements. At present, the preventive maintenance methods for the operation of the drum screen in nuclear power plants are mainly based on regular visual inspection, and it is difficult to detect equipment failures in a timely and accurate manner, which may lead to the "sick operation" of the drum screen. It will lead to serious failures, thereby affecting the reliability and safety of the cold source of the unit, and causing huge economic losses. Therefore, the condition monitoring of the drum screen has become one of the problems that must be solved.

This paper summarizes the operating failure types of drum screen equipment in domestic nuclear power plants, analyzes the root causes of drum screen operating failures in detail, and puts forward suggestions for improving the condition monitoring of drum screen equipment, which can realize early identification of drum screen equipment defects, thereby reducing nuclear power plant operation and economic risks [1].

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 73–81, 2023.
https://doi.org/10.1007/978-981-99-3455-3_7

2 Working Mechanism of Drum Screens

The drum screen is a rotating cylinder with a mesh on the circumference. The water flows through the mesh and then flows out. When the drum screen rotates, the dirt collected on the mesh is lifted to the top of the running platform and rinsed. Water flushes the dirt into the sewage bucket and drains away through the garbage chute. Under normal working conditions, the drum screen is in continuous operation and adopts automatic control mode. The rotation speed increases with the increase of the water level difference before and after the drum screen. When the water difference between the inside and outside of the drum screen is lower than 0.1 mWC, the drum screen always maintains a low-speed operating condition. If the water level difference increases, the drum screen will switch to medium or high-speed operation.

The operating environment of the drum screen is complex, and it is alternately immersed in a seawater or marine humid atmospheric environment. The main structural materials are 316 stainless steel and carbon steel, and the anti-corrosion protection is carried out by the combined method of anti-corrosion coating and external cathodic protection current.

3 Drum Screen Operation Event Analysis

During the operation of the drum screen, a large number of meshes are often blocked suddenly, the metal parts are severely corroded, the driving device vibrates greatly, and the structural connecting bolts are loosened and broken, which cause the drum screen to fail to operate normally. The blockage of the drum screen is caused by the sudden intrusion of a large number of marine organisms such as hairy shrimp and jellyfish. The cause of the event is not the failure of the drum screen body. Such operating events will not be described in this paper. The following will focus on analyzing the main operating events of the drum screen body of domestic nuclear power plants.

3.1 Corrosion of Metal Parts of Drum Screen

Several inspections in the operating power plants found that the different metal parts of the drum screen were corroded in multiple places, such as the spokes of the drum mesh, the I-beam of the gear seat, the pinion of the driveshaft head, and the connecting part of the driveshaft, all of which were severely corroded. The drum screen adopts the double anti-corrosion measures of coating the outer surface with anti-corrosion paint and external current cathodic protection. For the immersion area where the drum screen is under the water surface, the cathodic protection system plays a protective role. For the part of the drum screen that rotates on the water surface, the anti-corrosion coating is used to prevent corrosion. This combined corrosion protection method can effectively protect the drum screen, but corrosion may still occur due to factors such as design, quality control, and improper protection, such as the cathodic protection potential measurement deviation and the inability to identify the inspection potential measurement method. In the absence of monitoring the anti-corrosion effect of the drum screen, it is easy to cause the drum screen to be under-protected or over-protected for a long time, resulting

in serious corrosion of the drum screen. In recent years, there are multiple corrosion operating events in four nuclear power plant. The drum screen of a power plant suffered severe corrosion in a large area, with a maximum corrosion depth of 5 mm, which caused the drum screen to fail to operate normally, and may even lead to collapse.

The main corrosion operating events are shown in Table 1 below.

Table 1. The Corrosion Operating Events

Time	Event overview	Event impact
October 2015	The pinion of the driveshaft of the drum screen and the connecting part of the driveshaft was corroded	Loose bolt failure
September 2016	The coating was partially damaged	Affect the progress of the hot test
September 2017	Improper insulation of cathodic protection	Short-time load reduction
January 2018	several serious corrosion defects	Short-term load reduction

The direct causes of serious corrosion of drum screens in nuclear power plants are the deviation of protective potential measurement of drum screens, over/under cathodic protection of drum screen, and insufficient coating thickness. At present, in-service power plants generally check the corrosion of equipment by regularly monitoring the protection potential of the drum screen, calibrating the measured potential fed back by the cathodic protection power supply device, and strengthening regular inspections. When obvious corrosion or deterioration of the corrosion degree is found, the operation of the cathodic protection system will be checked.

3.2 Breakage and Looseness of Drum Screen Bolts

The fixing parts of the drum screen are connected by locking nuts, and each mesh is installed on the periphery of the outer edge of the drum screen with bolts and nuts. The breakage/looseness of the drum mesh bolts usually occurs when the fixing bolts of the bearing seat at the far end of the driveshaft, as well as the connection bolts between the spokes of the filter screen and the hub, and the connection bolts between the A-beam and the mainframe of the drum mesh are loose. The drive-bearing seat swings due to the loosening of the nut. If it is not found in time, the driveshaft pinion may be separated from the rotating filter screen, damage the driveshaft, bearing, and pinion box, and make the rotating filter screen lose power. If the bolts of the drum screen structure are loose or broken, the structure of the drum screen will be directly damaged, which may cause the main body of the drum screen to be damaged or even collapse. The main bolt fracture and loosening events are shown in Table 2 below.

The looseness of the bolts of the drive-bearing seat is mainly caused by the shaking of the drum screen under the action of the water flow when the drum screen is running. At the same time, the radial direction of the drum screen may produce ovality. Affected

Table 2. The Main Bolt Breakage and Loosening Events

Time	Event overview	Event impact
June 2008	Due to the breakage of the fixing bolts, the upper cover of the bearing seat at the far end of the drum screen driveshaft was missing	Shutdown, maintenance Outage
October 2014	The spokes and rim connecting plates and bolts were broken	Equipment maintenance
January 2015	There were large areas of looseness in the connecting bolts between the drum screen spokes and the hub, and the connecting bolts between the spokes and the main beam	Equipment maintenance
January 2015	The connection bolt between the spoke and the hub is loose	Overhaul
June 2015	The nut of the fixing bolt of the bearing support seat at the far end of the drum screen driveshaft has fallen off	Overhaul
August 2019	The upper fastening bolt of the non-drive end bearing seat of the drum screen driveshaft is loose, and the bearing seat as a whole swings slightly up and down	Mounting bracket
April 2020	There were different numbers of bolts broken during torque verification of the fixing bolts of the rotating filter screen garbage bucket	Overhaul

by the shaking and the ovality, the large ring gear of the drum screen will generate force to the pinion, indirectly making the bearing seat bear the upper and lower thrust. If the bolt and nut are unreliable or the bolt is corroded and the force strength is insufficient, and the bolt is subjected to radial force for a long time, the fixing bolt and nut of the drum screen bearing seat are easy to loosen. In addition, it will also be caused by the corrosion of the bolt or structure, the stress release of the drum screen itself, etc.

3.3 Vibration of Drum Screen Driving Device

Since the drum screen driving device is suspended and has only one support point, it is easy to cause shaking problems. Long-term shaking will cause damage to rotating parts such as reducer bearings and worms. The motor fixation is strengthened by adding brackets for medium and high-speed motors to prevent the motor from shaking continuously. At the same time, the manual vibration measurement of the reduction box is regularly plotted, but the end vibration cannot be effectively suppressed, which will lead to equipment failures such as fatigue fracture of the fixing bolts of the reduction

mechanism. If the driving device adopts the horizontal arrangement, the seismic performance of the motor reducer can be improved, but the vibration of the drum screen failure vibration transmitted to the reducer through the gear cannot be completely solved. The main driving device vibration events are shown in Table 3 below.

Table 3. The Main Drive Mechanism Vibration Events

Time	Event overview	Event impact
September 2015	The drum screen low-speed motor periodically shakes back and forth horizontally, about once every 30 s	No consequences during the shutdown
December 2016	Two low-speed drive motors shake up and down in the drive gearbox	Overhaul, mounting bracket
March 2017	Low-speed motor shaking twice a minute, and abnormal sound	Overhaul, mounting bracket
April 2017	The gearbox shook and abnormal noises	Overhaul, mounting bracket
May 2017	The motor has obvious intermittent vibration, and there will be four or five consecutive strong vibrations in about 20 s, and the upper bearing temperature was high	Shutdown

The vibration of the drum screen parts caused by equipment rotation, friction, load, etc. is transmitted to the reducer through the pinion, causing the driving device to shake. The unbalanced force generated during the operation of mechanical equipment can also cause stress concentration of components. If the meshing clearance of the drive gear of the reducer is too small, it is easy to cause wear to the drive bearing.

3.4 Summary

Through the above analysis of the operation events of the drum screen in the nuclear power plant, it is identified that the failure types of the drum screen are mainly in the following aspects:

(1) Vibration of the drum screen parts. The operating experience of the drum screen shows that the bolts of the bearing support seat at the far end of the driveshaft are easy to loosen, the driveshaft bearing seat swings up and down slightly, and the drum screen driving device shakes, and the motor vibrates. Due to the continuous rotation of the drum screen, the rotating parts are prone to vibration, which will cause dynamic fatigue of the parts, stress concentration, local damage, and even cause the structure to sink, resulting in periodic fatigue of the equipment, reducing the strength of the equipment, and affecting the life and safety of the equipment.

(2) Corrosion of the metal parts of the drum screen. Although the drum screen adopts a joint protection method for corrosion protection, a large amount of corrosion still occurs due to factors such as design, manufacture, installation, quality control, and improper protection. The main spokes, meshes, main shafts, and dirt buckets of the drum screen in multiple power plants are corroded in a large area, which affects the normal operation of the equipment. Serious corrosion will lead to equipment damage or collapse.
(3) Breakage of the drum screen parts. On the one hand, drum screen parts can break due to long-term stress unevenness or localized corrosion. On the other hand, when the drum screen rotates, it shakes due to the action of the water flow, since the ovality of the drum screen may be generated in the radial direction, the drum screen will be affected by shaking and ovality during operation, which will indirectly cause the bearing seat to bear up and down thrust. If the bolts and nuts are unreliable, and the bolts are subjected to radial force for a long time, the fixing bolts and nuts of the bearing seat on the drum mesh side are easy to loosen or break.

4 Optimization Analysis of the Condition Monitoring of Drum Screen

4.1 Optimization Scheme of the Condition Monitoring of Drum Screen

Drum screen that fails, and it is impossible to know the real state of the underwater working of the drum screen only by regular inspection of the important parts of the drum screen. Therefore, it is necessary to use intelligent monitoring and early warning methods to find out early. It can reduce the risk of accidents or economic losses caused by the expansion of equipment defects.

To ensure the normal operation of the drum screen, based on the operation event type of the drum screen, consider optimizing on the basis of the existing monitoring technology of water level monitoring inside and outside the drum screen and comprehensive fault alarm of the drum screen motor, include:

(1) Monitoring of drum screen spindle and driving device, including vibration, shaft displacement, rotational speed, eccentricity, and auxiliary health parameters such as motor load and bearing temperature. By monitoring the vibration of mechanical equipment and motors under different operating conditions, combined with the motor starting current and winding temperature, the operating status and failure trend of the drum screen body and the driving device can be monitored; By monitoring the shaft displacement of the main shaft and the driveshaft, the axial displacement of the two ends of the drum screen and the radial displacement of the drum screen, combined with the operating parameters of the drum screen, the overall ovality deformation fault of the drum screen can be detected.
(2) Intelligent video corrosion condition monitoring on both sides of the drum screen. Based on a large number of image data collection, the early corrosion of the mesh surface is identified by the image recognition technology.
(3) Stress monitoring of structural weak points such as drum screen spindle, driving device, wheel hub, spokes, bolted connections, etc. By monitoring the stress and

distribution changes of the force-bearing parts of the drum screen body, the safety analysis is carried out according to the change of the drum screen load conditions.

The main monitoring points of the drum screen body and the driving device are shown in Table 4.

Table 4. The main monitoring points of the drum screen body and the driving device

Drum screen parts	Monitoring points	Failure modes
Spindle	Shaft displacement monitoring; Shaft vibration monitoring; Stress monitoring of the bearing housing bolts at both ends; Protection rod stress monitoring;	Deformation of the drum screen spindle, Breakage and looseness of bearing bolts, and damage to the spindle protection rod
driveshaft	Shaft displacement monitoring; Speed monitoring; Shaft vibration measurement; Stress measurement of bearing housing bolts;	Failures such as misalignment, unbalance and wear of the bearing of the drive device, Breakage and looseness of bolt
motor	Motor vibration monitoring; Motor starting current, winding temperature measurement	Vibration fault of a motor; used for shaft trajectory and dynamic balance analysis, monitoring motor temperature high fault
reducer	Reducer housing vibration measurement; Stress measurement of reducer foundation bolts	Reducer gears, wear on assembly surfaces, looseness of bolts, fracture failures
drum screen body	Drum mesh face and radial displacement measurement	Axial and radial deformation of the drum mesh, bearing imbalance, misalignment, and wear
mesh	Intelligent Video Monitoring	Corrosion of the mesh and blockage of the drum mesh surface

4.2 Feasibility Analysis of the Condition Monitoring of Drum Screen

(1) Safety of the cold source

The addition of drum screen condition monitoring means realizes the monitoring of the drum screen body and the full life cycle of the driving device and fault prediction. When the drum screen is abnormal at the initial stage, the problem can be found in time, equipment damage can be avoided, and the unplanned shutdown of the nuclear power plant caused by the drum screen failure can be reduced.

As the last large-scale filtering equipment of the cold source, the condition monitoring of the drum screen can effectively reduce the risk of unit load reduction operation or shutdown due to the failure of the drum screen.

(2) Operation and maintenance of the drum screen

The condition monitoring of the drum screen optimization scheme sends monitoring signals and equipment failure information to the main control room for prompting, does not directly interfere with the system operation, and has no impact on the original control operation and maintenance.

It can provide the operators with the prediction of the operation status for the drum screen, shorten the troubleshooting time, reasonably optimize the maintenance and provide auxiliary decision-making for the maintenance plan.

(3) Maintenance cost of the drum screen

By the condition monitoring of the drum screen, defects such as deformation of the main body, loose bolts, and vibrations can be found early, to avoid the failure to expand to the main part of the drum screen for dismantling and maintenance and reduce the cost of maintenance.

Through the optimization of the drum screen monitoring technology, it can provide online full-cycle monitoring of common failures of drum screen, reduce the workload of inspection personnel, and reduce labor costs.

5 Conclusion

To realize the condition monitoring and fault warning of the drum screen and improve the operation reliability of the key equipment of the cold source, this paper proposes to add vibration monitoring, stress monitoring, and corrosion monitoring methods to the drum screen body and the driving device, and gives the specific monitoring points and monitoring parameters. It can provide a reference for the subsequent development and test verification of the condition monitoring of the drum screen system.

(1) By summarizing and analyzing the operating failure characteristics of the drum screen, it is determined that vibration of the drum screen parts, corrosion of the metal parts of the drum screen and breakage of the drum screen parts is the main failure types of the drum screen.

(2) For the above types of drum screen operation failures, it is recommended to add monitoring of shaft displacement, shaft vibration, and stress on the drum screen main shaft and driveshaft, to add vibration, current and winding temperature monitoring in motors, to add vibration and stress monitoring in reducers, to add displacement monitoring on drum mesh face and radial, and to add intelligent video monitoring of the mesh on both sides of the drum mesh.

(3) The condition monitoring of drum screen can be used by operators to identify equipment failures in advance to improve the safety of the cold source system and improve the operation and maintenance of the power plant. At the same time, it can also reduce the cost of maintenance and labors.

References

1. Xu, K.: Assessing the state of cathodic protection to circuiting water drum screen of nuclear power plant. Total Corros. Control **30**(01), 49–52 (2016)

2. Li, X.: Analysis and research on frequency conversion control fault and overcurrent trip of high-speed motor of circulating pump drum screen of column B in power plant. Sci. Publ. 000(010), 9–11 (2021)
3. Bing, T.: Analysis and suggestions on corrosion causes of drum screen in a nuclear power transfer stage. Power Eng. 2–3 (2019)

Discussion on the Application of Advanced On-Line Monitoring Technology for Drum Screen in Nuclear Power Plant

Xiang-jie He(✉), Xun Zhang, Fei Yu, Jing Xie, and Yue-ming Fu

China Nuclear Power Engineering Company Ltd., Shenzhen 518172, Guangdong, China
173358960@qq.com

Abstract. The drum screen is a coastal nuclear power plant commonly used water filtration device for the nuclear power plant cooling sea water, is one of the important equipment for cold source safety of the nuclear power plant. Due to the harsh operating environment and technical limitations, there are been a lack of systematic online monitoring methods on the status of drum screen. With the application and development of various new technology application in the nuclear power plant, it is possible to increase online fault monitoring of drum screen in order to meet the needs of information and intelligence on safety of nuclear power plant. This paper analyze the principles of different advanced measurement technologies such as the vibration monitoring, optical fiber/optical grating monitoring, the application adaptability and design of these various technologies on drum screen monitoring are discussed, and puts forward the main problems needing attention in the application of online monitoring of drum screen in nuclear power plant.

Keywords: Monitoring technology · optical grating · vibration · strain · drum screen

1 Background

Drum screen is commonly used water filtration device in a coastal nuclear power for cooling sea water, is one of the important equipment for cold source safety of the nuclear power plant, as the last-level equipment of "depth-in-defense" system of the cold source in nuclear power plant. The drum screen is safety-related equipment, if not available, it will directly lead to power reduction and even reactor shutdown.

In recent years, due to the excessive marine organisms and artificial dirt entering the drum screen in the operation process, the abnormal shutdown and shutdown of the nuclear power plant units have occurred from time to time, and such incidents have been highly focused by the nuclear safety supervision and energy management departments.

2 Introduction

The drum screen is a rotating filter device with meshes on the circumference of the drum frame, with a huge volume and complex composition and structure of system and equipment. The main body of the drum screen operates underwater for a long time to filter

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 82–89, 2023.
https://doi.org/10.1007/978-981-99-3455-3_8

and clean up sundries and marine organisms from seawater, the operating environment is bad. Under extreme marine conditions, it is more vulnerable to the impact of the accumulation of large sundries and a large number of marine organisms on the body structure.

Taking the drum screen from outside in and inside out with 19m in diameter and 7m in width as an example, its main function is to filter impurities larger than 3mm from seawater and provide large flow cooling sea water (about 32.6 m^3/s design flow) for nuclear power plants. The drum screen adopts a drum frame single A-type structure, is composed of driving device, spindle device, sealing device, drum frame, lubrication device and sewage device, as shown in Fig. 1. Water enters the drum screen from the outside of circumference of mesh surface, and then flows out along one side of the drum screen after filtering through the mesh surface. Driving device is used to drive the drum screen to rotate, spindle device is used to support the weight of the entire drum screen, sealing device is used to form a seal between the drum screen and the water chamber, and drum frame is used to support the mesh structure. The lubrication device is used to lubricate the main shaft bearing, and the sewage discharge device is used to drain the garbage washed away by the backwash water through the sewage tank.

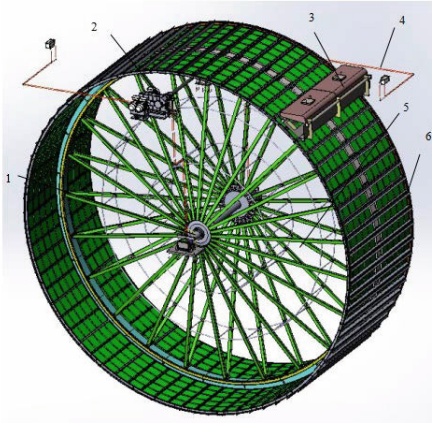


Fig. 1. 3D schematic diagram 1-spindle device, 2-driving device, 3-sewage disposal device, 4-lubrication device, 5- drum frame, 6-sealing device

Driven by the motor, the entire skeleton rotating body structure is alternately in seawater immersion and ocean humid atmospheric environment, and the main shaft may continue to be submerged underwater according to water level changes. The materials used in drum screen mainly include 316 stainless steel, carbon steel and other metal materials. In order to prevent serious corrosion of metal materials under the action of seawater, temporary sacrificial anode block and anti-corrosive coating + external current method for cathode protection are adopted to prevent the corrosion of seawater. However, due to the damage of coating and abnormal polarization, the insufficient protection of drum screen still causes the corrosion of drum screen in some units.

Generally, the drum screen is equipped with a small amount of on-line alarm signal to reflect the running state of the drum screen. Three liquid level gauges are set before and after the drum screen to form 3 groups of water level differential pressure. The high alarm signals of level differential pressure are sent to the DCS in main control room for display and alarm to monitor the blockage of the drum screen. Another, the low oil level alarm of oil level switch of main bearing lubricating oil tank and the drive shaft lubricating oil tank, and drive motor failure comprehensive signals are sent to the DCS in main control room, which is used to monitor the bearing lubricating oil and motor fault status.

During operation of the drum screen, there are various types of failure phenomena such as loose driving bearing bolts, gear wear, metal structure corrosion, large driving device shaking, excessive motor vibration, large area loosening of drum screen structure bolts, and radial arc deformation of the net surface. Most of the failure phenomena are the result of a combination of multiple failures of the equipment. According to the feedback of nuclear power plant design and operation experience, Online vibration and structure monitoring is an important basic technology for drum screen fault monitoring and prediction.

3 Online Monitoring Technology and Application Discussion

According to the technical research of nuclear power plant, marine ships, steel bridges, offshore wind power and other industries, it is shown that advanced technologies such as vibration monitoring, fiber grating monitoring and laser ranging have been gradually developed in online vibration fault diagnosis, bolt loosening stress and structural deformation monitoring [1–4].

3.1 Vibration/displacement Monitoring and Analysis Technology

With the development of computer information technology, fault diagnosis methods of large rotating machinery equipment have been more and more studied and applied, the common methods include expert system, Decision Tree (DT), logistic regression (LR), Bayesian Network, neural network (NN), and so on. They are mainly divided into three categories: fault diagnosis methods based on analytical model, fault diagnosis method based on knowledge and fault diagnosis method based on signal processing.

For the vibration monitoring of large rotating machinery equipment, the state monitoring method based on the traditional speed and acceleration sensor to measure vibration signal has the advantages of simple layout, less damage to the monitoring object and strong anti-interference ability, the advantages of sudden sensitivity to equipment state changes are widely used in vibration monitoring and acquisition systems of rotating equipment (such as pumps, motors, steam turbines and fans) in nuclear power plants, coal-fired power plants and other industries. Fault diagnosis methods based on vibration signals have also developed into the mainstream methods in the field of maintenance and fault diagnosis of rotating machinery and equipment. However, there is no mature systematic product for the analysis of drum screen structure, operating status and fault characteristics and fault warning of intelligent algorithms.

Fault signal processing and feature extraction is the most critical part of fault diagnosis. Through the application of various effective mathematical tools and related technologies, the original signal is transformed, analyzed and processed in multiple fields based on the computer platform. The commonly used analysis methods of signal include: time domain feature Statistics and Analysis, spectrum analysis and feature statistics, wavelet decomposition, etc.

The typical fault simulation test of the drum screen are suggested if could, which can be combined with the sensor fault type, installation method and characteristics to obtain the fault signal samples, these signal provides effective data research for the establishment of the fault library of the drum screen.

The radial and axial displacement of the drum screen can be measured by the non-contact eddy current probe arranged at the radial and axial ends.

At present the laser ranging technology for detection of drum screen is used for off-line inspection in nuclear power plant [2]. Detect the axial displacement of the drum screen, the deviation of the center and position it, which can be obtained by checking the radial run out of the rotation of the drum screen.

Laser ranging technology is a non-contact measurement technology, which uses laser with strong directivity to accurately measure the distance of the target. It is generally divided into phase ranging and pulse method ranging technology. The pulse method is mainly used for long-distance ranging, the accuracy is low, and the phase ranging is suitable for medium and long distances, the accuracy is high, reaching the millimeter level, The bridge deformation monitoring system generally adopt the phase ranging, which emits a beam of fine light to the target through the laser range finder, the photoelectric element receives the laser reflected by the target, and the timer measures the time of the laser beam from emission to reception, and calculates the distance from the observer to the target.

Considering that the operating environment requirements of laser range finder are relatively high, the salt spray generated by backwashing during the operation of drum net will have an impact on it, the operating environment conditions are harsh, as shown in Table 1. When the new drum screen is built, the displacement sensor can be selected for online monitoring. The installation of the laser range finder is more convenient and the technical solution is not complicated. It is suitable to apply to transformation of nuclear power plants with appropriate measures that need to carry out drum net online monitoring.

Table 1. Normal operating environment condition

parameters	Range value
Atmospheric temperature	About -1.9 °C~38.9 °C
Relative humidity	100%
Seawater pH	8.06 ~8.28
Atmospheric salt content	About 3.2%

3.2 Optical Fiber/grating Sensing Technology

The basic structure of optical fiber is very simple, which mainly consists of fiber core, fiber coating, plastic coating, loose sleeve and so on from inside to outside, as shown in Fig. 2. The refractive index of the fiber core is slightly higher than that of the surrounding cladding. When the light enters the fiber core at a certain angle, the difference of refractive index causes the full internal reflection of the light at the interface between the fiber core and the cladding, the guiding light spreads forward in a serrated route inside the core, and finally comes out from the other end [5].

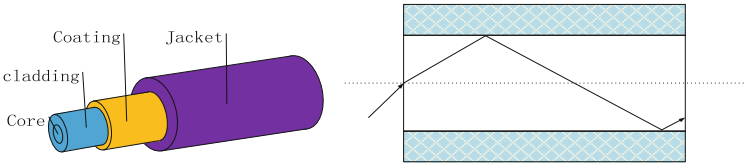


Fig. 2. Basic structure and schematic diagram of optical fiber

Optical fiber sensors generally composed of light source, incident optical fiber, outgoing optical fiber, optical modulator photodetector and demodulator. The light of the light source is sent into the modulation area through the incident optical fiber, and the light interacts with the external measured parameters in the modulation area, making the intensity, wavelength, frequency, the optical properties such as phase change and become the modulated signal light, and then send it to the photodetector and demodulator through the outgoing optical fiber to obtain the measured parameters. Optical fiber sensors can be divided into functional optical fiber sensors and non-functional sensors.

Fiber grating is a space phase grating in the fiber core which distributes axially along the direction of light propagation, and its substantive function is equivalent to forming a narrow band filter in the fiber core. It is based on the principle that the external incident light and the germanium ions in the fiber core interact to cause a permanent change in the refractive index of the fiber core. Fiber grating is widely applied to various sensors, such as temperature, pressure, vibration, concentration, stress and perimeter intrusion detection [4]. At present, the more commonly used fiber grating sensor for structural monitoring is the FBG Bragg fiber grating sensor.

Bragg grating equation,

$$\Delta\lambda_B = 2n_{eff}\Lambda \tag{1}$$

In the formula, $\Delta\lambda_B$ is the offset of the sensor center wavelength, n_{eff} is effective refractive index of fiber core, and Λ is Grating period.

The relationship between wavelength offset and strain to be measured $\Delta\varepsilon$, and the relationship between wavelength offset and temperature change ΔT are as follows,

$$\frac{\Delta\lambda_B}{\lambda_B} = (1 - P_e)\Delta\varepsilon \tag{2}$$

$$\frac{\Delta\lambda_B}{\lambda_B} = (\alpha_f + \xi)\,\Delta \cdot T \tag{3}$$

In the above formulas, P_e is elastic coefficient of optical fiber, and $\alpha_f = \frac{1}{\Lambda}\frac{d\Lambda}{dT}$ is thermal expansion coefficient of optical fiber, $\xi = \frac{1}{n}\frac{dn}{dT}$ is Refractive index temperature coefficient of optical fiber.

Table 2 provide a different wavelength of fiber grating strain sensitivity and temperature sensitivity [4].

Table 2. Different wavelength strain sensitivity and temperature sensitivity.

Wavelength(μm)	strain sensitivity (pm/μ ε)	temperature sensitivity(pm/°C)
0.83	0.64	6.8
1.3	1	10
1.55	1.2	10.3

Research results [4–6] show that the main characteristics of the fiber grating sensor include, a) linearity, also called maximum nonlinear error, is one of the main characteristic parameters of the fiber grating sensor. According to research the smaller the linearity coefficient is, the higher the measurement accuracy of the sensor is. b) Zero drift feature, refers to the change in the zero-point measurement data of the sensor without external load of the structure. The sensor material has good performance and its own zero drift characteristics are relatively stable. The temperature compensation method, packaging method and installation method of the sensor will affect the zero drift performance. c) Strain sensitivity. The strain sensitivity coefficient is only related to the fiber grating material, and has nothing to do with the external working environment. d) Strain repeatability. The intensity of the fiber grating, the strain range of the monitoring point and the way the sensor is installed are all factors that affect the repeatability of the strain.

The main advantages of the fiber grating sensor include, a) when the fiber bends and the light source fluctuates due to the movement of the measured object, the signal measured by the grating sensor will not be affected. b) fiber grating sensors distributed around the measured object can be connected to the same fiber in series to realize distributed measurement of the measured object, and the measurement range can be very large. c) fiber grating sensor can measure the temperature of the structure itself and the strain (deformation) caused by external force, and the measurement accuracy is very high. d) It is easy to multiplexing and network. The multiplexing technology of the fiber grating sensor can not only detect the parameters at the same position, but also detect the parameter changes of different positions at the same time.

4 Issues of Concern

For the selection and application of online monitoring technologies for different nuclear power plant drum screen application scenarios, it is recommended to consider further research on the following issues:

a) The influence of the environment. Because temperature and strain can affect the fiber grating sensing, in the long-term monitoring of the drum screen structure, due to the large changes in the environment temperature of the drum screen, in order to effectively monitor the structure of the drum screen, it is necessary to consider whether to adopt temperature compensation measures to reduce the impact of temperature.

   Fabrication and calibration of fiber grating strain sensor in engineering application.

   Due to the effect of cathode protection current, pay attention to the anti-electromagnetic interference technology and scheme of traditional vibration probe and electronic equipment.

   Underwater monitoring equipment should be waterproof, anti-corrosion, anti-fouling measures.

b) The influence of the installation method. Since the skeleton and spindle are affected by the cathode protection current, the sensor should insulation with the equipment body, and choose the appropriate packaging and installation method. With the external stress and temperature changing, the characteristics of the packaged sensor are tested and studied.

c) Considering that sensor devices need online debugging and troubleshooting during operation, appropriate redundant configurations can be considered for devices that cannot be repaired online.

d) The selection and design of monitoring technology should be carried out simultaneously with the design of the new drum screen, especially for underwater engineering and sensor equipment installed on the skeleton. The power plant transformation should be completed in conjunction with the overhaul progress. Verify the applicability of the technology in the research and development phase.

e) Sufficient data of different operating conditions. In the engineering application phase, it is necessary to collect normal operation and fault operation data under different operating conditions (over 1 operating cycle recommended) to correct the calculation model.

5 Conclusion

The basic principles and characteristics of vibration monitoring and diagnosis technology and optical fiber/optical grating monitoring technology for typical faults of Drum screen, as well as the problems that need to be paid attention to in the selection and application are discussed in this paper. With the construction of intelligent nuclear power, a complete online monitoring and fault warning technical solution will be carried out in-depth research on the characteristics of each equipment of the drum screen.

References

1. Kuang, Y., Chen, Y.: Application of optical fiber sensing system in nuclear power plant. In: Progress Report on China Nuclear Science & Technology, vol. 6, pp.409–413, Baotou (2019)
2. Author, K.: Nuclear power plant drum screen detection system. Power equip. **4**, 20–21 (2018)
3. Author, C.: Design and experimental research of ship structure monitoring and assessment system. Harbin Engineering University, Harbin (2017)
4. Author, L., Author, C.: Theory and Application of fiber grating sensing system for structural health monitoring. Science Press, Beijing (2020)
5. Author, Y., Author, H.: Fiber grating sensing technology and application. Science Press, Beijing (2018)
6. Author, X.: Research on detecting and simulating technology of plate and shell structure based on FBG sensor. Changchun University of Science and Technology, Changchun (2020)

Research on Source Range Channel Disturbance Diagnosis of Nuclear Instrumentation System

Chao Wang(✉), Xiao-Fei Li, Jing Xiao, Jun-Wei Zheng, Wen-Qing Yang, Zheng-Dong Huang, Sheng-Xin Yuan, and Ji-Kun Liu

State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment, China Nuclear Power Engineering Co., Ltd., Shenzhen, Guangdong, China
534784835@qq.com

Abstract. The source range channel of Nuclear Instrumentation System (RPN) of a nuclear power plant provides a neutron flux measurement at shutdown and during initialization phase of the start-up, which is very important to the control and safety of the plant. In order to qualitatively analyze the source range channel disturbance of the CPR1000 nuclear power plant, the article is based on the signal transmission link structure of source range channel, combined with the actual cases on the site, analyzes the easy failure points in the link to the source range one by one. Analyze the influx of the measurement channel, search the cause of the source range channel problem, and formulate corresponding treatment measures. It can not only analyze the safety and stability of the nuclear instrumentation system, and provide relevant information to the operator, but also has important guiding for the subsequent system commissioning, operation and maintenance of RPN system of similar types of nuclear power plants.

Keywords: RPN · source range channel · neutron detector · electromagnetic interference · temperature and humidity · connector

1 Introduction

The CPR1000 nuclear instrumentation system uses neutron flow measurements made by a set of detectors arranged on the outside of the reactor vessel, and controls the evolution through time, the radial and the axial distributions, which directly related to nuclear safety. The RPN system measures neutron flow over about 11 decades, in order to cover this measurement range, the system includes three types of detectors for source, intermediate and power ranges [1]. The source range channel (SRC) supplies a neutron flux measurement during the start-up, and includes two identical and independent channels, which provides real-time monitoring results of neutron flux and has automatic shutdown protection.

During the commissioning, start-up and operation of CPR1000 nuclear power plants, there are many SRC failures, and it is difficult to analyze the causes of failures and deal with the problems. More than ten SRC failures have been accumulated in the past 10 years to China General Nuclear Power, and the failure rate is relatively high. Based on the

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 90–99, 2023.
https://doi.org/10.1007/978-981-99-3455-3_9

characteristics of SRC equipment and experience, this article carries out research on SRC fault diagnosis. According to the fault weak points analyzed by the research, preventive measures are put forward, in order to achieve the purpose of reducing the failure rate of SRC.

2 The Principle of SRC

The SRC monitors the neutron count rate of the reactor under shutdown and startup conditions. When the neutron flux increases unexpectedly, it can trigger a high neutron flux rate alarm, and when the neutron flux changes sharply and exceeds the protection threshold, it directly triggers the reactor shutdown. The Source range detector is a CPNB-44 proportional counter whose high sensitivity allows neutron.

Detection, the incident neutron reacts with ^{10}B, and the neutron flux density can be calculated according to the measured neutron count rate [2]. The structure of boron-coated proportional counter is shown in Fig. 1.

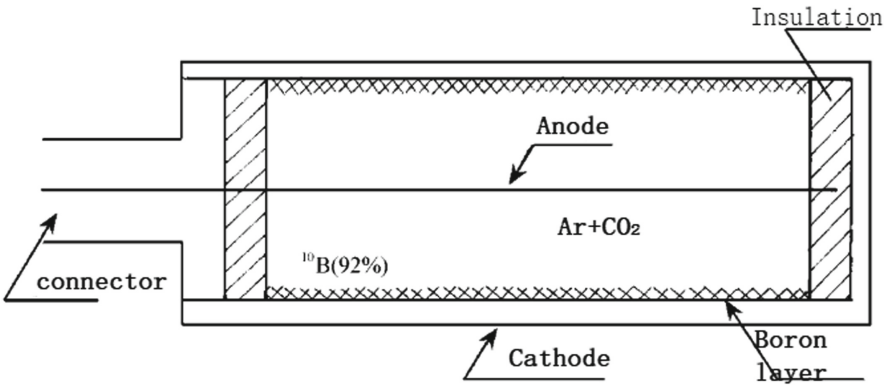


Fig. 1. The structure of boron-coated proportional counter

The processing of the RPN source range signal is shown in Reference [3]. The analog neutron counting pulse signal measured by the detector is transmitted to the I-AIR of the source range cabinet through the cable for primary amplification, and then input to the AIMP5 for secondary amplification and screening. The generated digital pulse signal is then input to the ICTO module to generate the final effective neutron count rate data. The neutron count rate signal is input to the Reactor Protection System (RPS) system for processing, and finally the source range monitoring data and related alarm signals are displayed on the Digital Control System (DCS) [4]. Figure 2 shows the process of the RPN source range signal.

Function of electronic modules is shown in Table 1.

The cable between the source range detector and the connection plate is a mineral cable, and the connector of the cable is an HN-type male connector. This connector has a waterproof function and is insulated from the support. An organic cable with two male connectors is used between the terminal board and the through-piece. An organic cable

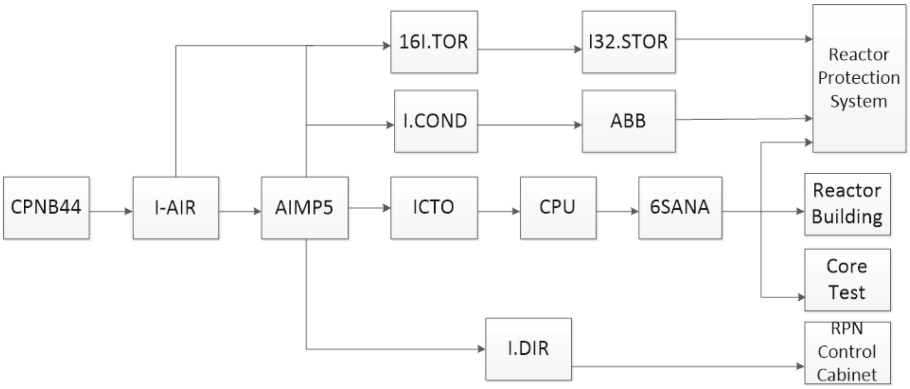


Fig. 2. RPN source range signal

Table 1. Function of Electronic Modules

Module	Type	Function
CPNB44	Source range detector	Measure thermal neutron flux
I.DIR	Audio interface module	Source amplifier module
ICTO	Counting rate module	Measurement of counting rate and interface with the central unit
I.COND	EMC filtering board	Transmission of analogue and digital signals and EMC filtering for all outputs
16I.TOR	16 ON/OFF insulated module	The insulation of inputs and outputs and logic combination
I-AIR	Source range detector	Detection and pre-amplification of pulses and transmission of the high voltage supplied
AIMP5	Audio interface module	Completes the acquisition of pulses and the high voltage supply
6SANA	6 Analogue outputs module	Generate outputs and insulation
ABB	Insulation module	The insulation of outputs
I32.STOR	32 ON/OFF output interface module	provide 32 relays outputs

with two male connectors is used between the penetration and the cabinet [5]. As can be seen from Fig. 3, the connection parts of the penetration side, the connection plate and the cabinet side are the weaker parts of the entire signal transmission. The reliability of the connection will directly affect the signal transmission performance of the system, which in turn affects the availability of the source range. The signal transmission diagram from the source range detector to the signal processing cabinet is shown in Fig. 3.

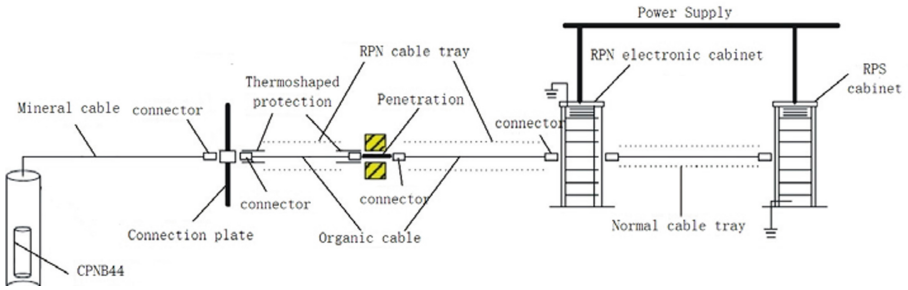


Fig. 3. The signal transmission diagram from detector to cabinet

3 Analysis of SRC Failure

3.1 Electromagnetic Interference

The RPN cabinet is located in the electrical building and the SRC signal is transmitted from the reactor building to the cabinet through penetration for processing. Since the RPN source range signal is a pulse signal, it is susceptible to electromagnetic pulse interference. According to the electromagnetic interference theory, lightning discharge, electrostatic discharge, and the switching action process of the electrical system are all causes of transient interference sources [6]. For example, when the plug of an electrical device is inserted and removed from the power strip, or the conductive path of an electrical device is cut off with a switch, an electric spark will be generated. Therefore, when the inductive load is disconnected and the relay contacts are switched, transient pulse group interference will be generated in the cable circuit, and due to the insulation breakdown of the switch contact gap or the contact bounce, etc., a transient burst will also be generated at the disconnection point. State interference, which will affect the correct transmission of the signal [7].

To prove this theory, a set of comparative experiments were performed on site. Continuously monitor for 24 h when the source range count rate is stable. After confirming that the count rate is stable, select the power-supply cables of two electrical systems close to the source range signal cable, and then intermittently start and stop the power-supply of the two systems within 24 h, the results show a slight fluctuation in the source range count rate. This confirms that the electromagnetic interference caused by the switching action of the power supply of the system will have an impact on the source range. Only two systems are selected to perform in the test. There are dozens of external system power cables on the RPN source range cable path. Strong interference caused by power cables can affect the signal transmission of the source range.

It can be seen that the electrical panels, high-power equipment and other power trays around the cable tray path of the SRC are important factors that cause electromagnetic interference.

3.2 Changes in Temperature and Humidity

The RPN source range cable needs to go through the connection building, penetration and reactor building. The temperature and humidity conditions required by the system manual. In such a case, water molecules may enter into the SRC equipment installed. When the SRC works normally, the high voltage will ionize the water molecules and generate weak signals, which will observe count-rate fluctuations and spikes after amplification.

Fault 1: During the on-site inspection of Unit 2 of A nuclear power plant, it was found that the 401HP sound horn in the 2RPN005AR cabinet (which gives the local sound indication of the neutron count rate) has abnormal sound counts. After checking the log, it was found that the source range detector of the second channel 2RPN024MA exhibited high count rates several times. The channel was examined and no abnormal signal was observed.

Through checking one by one, it was finally confirmed that the cause of the failure was that the ambient temperature and humidity did not meet the standard during the operation of the connector termination, insulation test, and daily debugging, which required the connector to be exposed, causing moisture to enter the connector. After termination, under the action of high voltage, a very small discharge action will become a large pulse after being amplified by 104 times in two stages of the cabinet, which will interfere with the normal signal and cause count-rate fluctuations.

In this regard, the HN connector of the measuring cable was remade, and moisture-proof protection was done. After continuous monitoring for several months, there was no abnormal count. Therefore, in the subsequent production process of the connector, it is required to avoid the connector being exposed in a high humidity environment without protection. Each exposure of the connector must strictly comply with the manufacturer's requirements.

Fault 2: The power range sleeve of Unit 1 of B nuclear power plant entered the water, and then replaced the sleeve, but did not pay attention to the condition of the source range detector. By November, the source range frequently observed count-rate fluctuations and spikes. The inspection found that the insulation of the whole circuit is too low, but the insulation of the source range detector is qualified. After taking the same investigation measures as those of A nuclear power plant, it was found that the connectors on the side of the penetration piece and the connectors at the connecting plate were damp, and abnormal counts no longer appeared after replacement.

From fault 1 and fault 2, it can be seen that RPN, as a nuclear safety level (1E level) system for real-time monitoring of the reactor neutron flux rate, intuitively converts the reactor flux rate into pulse and micro-current signals in real time through the detector, the transmitted micro-current signal strength is at least 10^{-11} A, so it is highly sensitive to external factors, and temperature and humidity have become the inducement of abnormal pulses.

During the construction phase of the project, it is inevitable that the ambient temperature and humidity in the nuclear island will exceed the standard. In the past, the units were installed on the island before the thermal function test. At this time, the ventilation and cooling systems in the nuclear island were not officially put into operation. It may be out of service and cause the temperature and humidity in the island to deteriorate. Therefore, the earlier the RPN equipment is installed on the island, the longer it will be

in the harsh environment, and the greater the possibility of moisture and flooding. This aggravates the impact of unqualified ambient temperature and humidity and inadequate moisture-proof measures on the RPN equipment, and eventually the phenomenon of abnormal counts of source range occurs.

3.3 Faulty Cable Connector

There are many connectors in the signal transmission loop of the RPN source range, and Lines connectors overview is shown in Fig. 4.

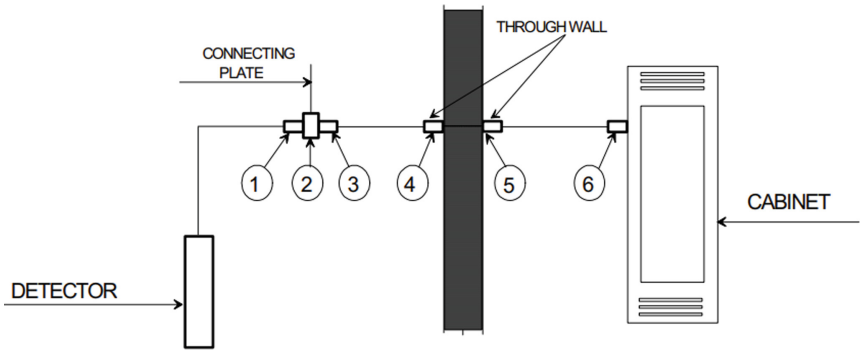


Fig. 4. SGC closing time of K16 during running-in

Type of connectors for source range channel is shown in Table 2.

Table 2. Type of Connectors for Source Range Channel

Identification	Reference	Remarks	Quantity per channel
1	-	Integrated to detector	1
2	-	Integrated to connection plate	1
3	1 410 014	Connector with mineral insulator supplied by manufacturer A	1
4	HN-14J-A	HN Connector supplied by manufacturer B	1
5	HN-14J-F	HN Connector supplied by manufacturer B	1
6	29 713 131BF	Connector with organic insulator supplied by manufacturer A	1

Each source range channel needs to make 4 connectors on site, and they come from different manufacturers, which brings great hidden danger to the connector production.

The connectors at position 3 and position 6 are respectively connected to the integrated cable connector of the detector and the cabinet side, which are well matched in practice and no abnormality is seen in operation. The main problem lies in the connection between the HN-14J-A connector of manufacturer A (the RPN source range is only the mineral cable from the detector to the connection plate, and the other part of the source range cable is nuclear-grade coaxial cable) and the cable connector of manufacturer B. Due to the high precision required for the production of the connector, the following faults occurred on site.

i. When the pins are soldered, the cables are not fixed, causing the soldered pins to be skewed and loose;
ii. The violent construction in the cable connector production process leads to damage to the connector ceramic;
iii. The number of core wires of the cable is not checked, so that the signal cannot be transmitted after soldering the pins;
iv. The connector torque is too small, resulting in unqualified connectivity, and the signal cannot be transmitted.

These connector failures will eventually make the RPN source range signal unable to transmit normally, resulting in source range signal failure.

4 Troubleshooting

4.1 Electromagnetic Interference Countermeasures

The production and installation of RPN cable tray can play a good role in suppressing electromagnetic interference. The production and installation of the cable tray should meet the following requirements.

i. A special, non-perforated solid bottom tray should be used, and a cover should be installed after the cable is laid;
ii. The bending radius of the cable tray should not be less than 30 cm;
iii. Cable trays and brackets should be installed in a dry, vibration-free, chemical-free area, and the ambient temperature does not exceed 80 centigrade;
iv. The edge of the tray should be polished to prevent cable laying Cut the cable during the process;
v. The cable tray is as continuous as possible and closed throughout the process. When passing through different rooms, disconnect the cable tray according to the fire blocking requirements, but the two ends of the disconnection should extend into the fire blocking material in the wall. If the tray must be disconnected due to the cable entering the cabinet or penetration, measures such as installing metal hoses should be taken to achieve full cable closure;
vi. Cable trays should be grounded;
vii. RPN cable trays should be as far away as possible from other metal objects, electrical equipment, and power cables such as lighting. It is forbidden to lay other cables within 15 cm up and down and 10 cm left and right of the RPN cable tray;
viii. Avoid installing large electrical equipment such as switch panels within 2 m around the RPN cable tray.

4.2 Measures to Deal with Changes in Temperature and Humidity

In response to the change of temperature and humidity, the "RPN Temperature and Humidity Prevention Control Plan" has been formulated. By controlling the continuous operation of the reactor pit ventilation system (EVC), container continuous ventilation system (EVR) and nuclear island chilled water system (DEG), the arrangement of heaters, building a temporary work shed and other measures to ensure that the installation environment meets the requirements, through the establishment of a temperature and humidity database to track the environmental changes in the nuclear island, and by adding a desiccant in moisture-proof bag to protect the finished product after installation.

Measure 1: Based on this plan, EVC, EVR, DEG must ensure single-train operation; all work involving EVC, EVR, DEG outage must be included in the three-day rolling plan; RPN detection During and after installation, the EVC, EVR, and DEG systems cannot guarantee single-column operation, referring to the response of the emergency permit mode.

Measure 2: Both the RPN detector and the connection plate are located in the reactor building, and the ambient humidity in this room is high, which makes the equipment at high risk of water immersion and moisture. After on-site inspection and discussion, it was decided to arrange two 30 kW high-power heaters in the reactor pit to heat the air coming from the EVC system, in order to reduce the ambient humidity and improve the non-condensation margin of the equipment.

Measure 3: By coordinating the continuous operation of DEG/EVC/EVR and other systems, the stability of the nuclear island environment is only ensured. If the humidity is still greater than the 65% limit in the installation document, a temporary work shed will be built at the operating point, and temporary The dehumidifier is arranged in the work shed to reduce the ambient humidity and make it meet the requirements.

Measure 4: Regularly conduct RPN equipment inspections to truthfully record the equipment status, and upload the records to the inspection management of the equipment maintenance module in the management information system. If any equipment is abnormal, report it in time and take relevant measures to alleviate the damage to the equipment.

4.3 Countermeasures for Cable Connector Failure

The quality of RPN measurement cable connector production is improved by controlling the connector production process, which is mainly divided into connector production process improvement, production process supervision, production quality inspection, finished product protection and so on. Through continuous tracking and effective control, the source range failure problem caused by the RPN connector manufacturing process is reduced.

Measure 1: Track the connector production process of RPN and refine the work to each step, strictly supervise and check whether each work of the staff is qualified and record the results. Including ambient temperature and humidity inspection and control,

cable diameter inspection, cable shield inspection, post-welding pin inspection, and post-soldering insulation layer flat and inclined inspection.

i. Ambient temperature and humidity inspection and control: The manufacturer's design and installation documents require that the ambient humidity should be less than 65% when the HN connector is made. Since this time period belongs to the engineering construction stage, the humidity in the island cannot meet the installation requirements. By changing the core ring The overall environmental temperature and humidity of the gallery and the small-scale environmental temperature and humidity required for the production of the connector are two methods to prevent the cables and connectors from getting wet during the connector production. The main implementation method is to add two high-power heaters in the R140/R180 room to reduce the humidity of the R440/R480 room, build a temporary work shed and arrange a dehumidifier to reduce the humidity in the temporary work area.
ii. Cable diameter inspection: During the production process of the connector, it was found that the diameter of the cables in the island was irregular, and some of them were in obvious oval shape. Finally, this batch of unqualified cables was replaced by calling other project cables. At the same time, a special team for RPN connector production promotion was established to inspect the cables. Diameter, and report the progress of the work every day.
iii. Inspection of cable shielding layer: Due to the lack of cable insulation layer in the previous unit, feedback this experience to other projects, and carry out special check on the cable shielding layer of other projects.
iv. Check the number of cable core wires: The core wires of the cable are composed of 7 extremely thin copper wires. In order to prevent the core wires from being cut due to operating errors during the connector production process, it is necessary to strengthen the supervision and inspection of this risk.
v. Pin inspection after welding: The core of connector production is how to perfectly weld the pins and core wires together, and at the same time ensure that the pins are not tilted or detached. This work will vary greatly due to the craftsmanship of the workers, so it is necessary to focus on checking the soldering of the pins.
vi. Flat and oblique inspection of the insulation layer after soldering: When the pins are soldered, the cable insulation layer will be dented due to overheating of the soldering iron or too long soldering time, so the insulation layer must be inspected after the pins are soldered.

Measure 2: Take a comprehensive inspection of the finished connector. If one item is unqualified, the connector must be disassembled and remade until it is qualified. The comprehensive inspection mainly includes the following contents.

i. Check whether the contact between the pin and the ceramic insulation bottom of the connector is tight and there is no gap.
ii. Gently shake the pin to check for looseness.
iii. Gently push the pin in to check whether it will retract.
iv. Use a depth meter to measure the depth of the pins to determine whether the installation requirements are met.

v. Measure the cable insulation resistance.

Measure 3: After the connector is made, take corresponding protective measures to prevent the connector from being damaged by moisture. Due to the high humidity in the nuclear island, it is necessary to use HN plugs, silica crystal desiccant, specially customized moisture-proof protection bags to protect the completed connectors from moisture.

5 Conclusion

This paper analyzes the source range channel disturbance of nuclear instrumentation system. The transmission link system of RPN source range channel is analyzed, determines that the main source range failure is electromagnetic interference, temperature and humidity changes and cable connector failure, and proposes countermeasures through the long-term verification effect during the commissioning and start-up of multiple plants, the source range is very stable, and there is no abnormal count-rate fluctuations and spikes, which fully shows that the measures proposed in this paper effectively reduce the probability of the source range failure of the RPN system.

References

1. Ji-long, P.: Daya Bay Nuclear Power Plant Operation Course (Volume 1 and 2) [M], p. 12. Atomic Energy Press, Beijing (1998)
2. Guangdong Nuclear Power Training Center: 900 MW Pressurized Water Reactor Nuclear Power Plant System and Equipment, pp. 255-257. Atomic Energy Press, Beijing (2005)
3. Zhao, C., Qin, H., Shen, H., et al.: Impact analysis of CPR1000+ nuclear power plant RPN channel improvement. Nucl. Sci. Eng. **35**(2), 250–254 (2015)
4. Huan, M., Xiang, W., Ji, Q., et al.: The principle and engineering practice of the nuclear measurement system outside the nuclear power plant. Nucl. Electron. Detect. Technol. **34**(6), 758–761 (2014)
5. Liu, Y., Li, W.: Design of nuclear instrumentation system for Qin-shan nuclear power phase II project. Nucl. Power Eng. **24**(S1), 238–240 (2003)
6. Yang, Z., Wei, Y., Bo, Z., et al.: Diagnosis and characteristic estimation of circuit radiation interference mechanism. Chinese J. Electrotechn. Technol. **25**(10), 6–13 (2010)
7. Liu, S.: Electromagnetic compatibility requirements and evaluation of safety-related instrumentation and control systems in nuclear power plants. Nucl. Sci. Eng. **22**(1), 89–95 (2002)

Analysis for Main Process Variables Control Function Categorization and System Classification in Nuclear Power Plant

Tao Fu[1(✉)] and Ming-Gang Li[2]

[1] State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment, China Nuclear Power Engineering Co., Ltd., Shenzhen 518000, China
futao@cgnpc.com.cn

[2] Shanghai Engineering Science and Technology Co., Ltd., Shanghai 20000, China

Abstract. Each Instrumentation and Control (I&C) system shall be classified according to its suitability to implement I&C functions up to a defined category. At present, there is no uniform requirement for the classification of the Main Process Variables Control System (MVCS).The requirements of International Atomic Energy Agency (IAEA) and International Electrotechnical Commission (IEC) are summarized in this paper. The rationality of main process variables control function categorization and system classification is analyzed by safety analysis, reliability claim analysis and Probabilistic Safety Assessment (PSA) analysis. The analysis results show the reasonable main process variables control function categorization and system classification.

Keywords: Function Categorization · System Classification · Safety Analysis · Reliability Claim · PSA

1 Introduction

There are numerous complex systems and equipment in the nuclear power plant. In order to realize the nuclear safety target of nuclear power plant, it is necessary to classify the I&C function, system and equipment according to the importance of the nuclear safety function. Reasonable safety classification can effectively ensure the safe and stable operation of nuclear power plants, reduce construction investment and in-service maintenance costs. All items are required to determine a reasonable classification of safety to guide the design of the item.

The control functions which are designed to maintain the main process variables within the normal operation range of the nuclear power plant are categorized as safety category 3 in IAEA SSG-30-2014 [4]. This is different from the requirement of IEC 61226-2009 [1] in which these control functions are categorized as Category B. The purpose of this paper is to investigate the function categorization and system classification of main process variables control according to the following three aspects:

- safety analysis.
- reliability claim analysis.
- PSA analysis.

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 100–105, 2023.
https://doi.org/10.1007/978-981-99-3455-3_10

2 Design Scheme

2.1 Function Categorization

The related functions to maintain the main variables of the nuclear power plant within the normal operational range are as follows:

- Provides the functions to maintain core reactivity control;
- Provides the functions to maintain sufficient Reactor Coolant System (RCP) water inventory for core cooling;
- Provides the functions to transfer heat from the reactor coolant to the ultimate heat sink;
- Provides the functions to maintain integrity of the Reactor Coolant Pressure Boundary (RCPB).

These high level safety functions are further decomposed to the following the main process variables control I&C functions:

- Reactor power control

  The reactor power control follow turbine load transients within established limits. It generates signals for actuation of rod during power operation condition.

  The reactor power control obtains the power demand according to different secondary loop conditions, and converts the power setpoint into a rod position setpoint for reactor power control banks.

  The reactor power control compares the measured rod position and the reference position to generate the error signal. The speed and direction of the power control banks are determined based on the sign and magnitude of the rod position error.
- Reactor coolant average temperature control

  The reactor coolant average temperature control continuously compares the measured average temperature and the reference temperature to generate the error signal, and then send the error signal to rod speed program to determine the speed and direction of the reactor coolant average temperature control bank.
- Pressurizer pressure control

  The pressurizer pressure control is in charge of maintaining the primary pressure at a setpoint value in steady state operation and within allowable range around its setpoint. Based on a Proportion-Integral-Derivative controller, the RCP pressure control is performed in the pressurizer by increasing or decreasing the mass of the steam cushion with respectively heaters or spray valves.

  The pressurizer pressure is controlled by the heaters installed at the bottom of the pressurizer and the spraying devices installed at the top of the pressurizer.
- Pressurizer water level control

  The pressurizer water level control function to maintain the pressurizer water level at a setpoint value in steady state operation and within allowable range around its setpoint. During normal operating, the pressurizer level variations are caused by reactor coolant temperature variations, which highly affect the water density of the RCP. When the pressurizer level goes out of the normal operating range, the functions which are designed to prevent reactor trip or to protect equipment are activated.

- Steam generator level control

  The steam generator water level control function is able to ensurea sufficient Steam Generator (SG) water inventory for heat removal from primary to secondary side (including proper operation of SG).

  The SG level control I&C function also has the task of maintaining the SG level at a setpoint value in steady state operation, and within allowable limits during normal operating transients.
- Steam dump control

  Reactor power cannot always be varied as quickly as turbine load. The steam dump control function reduces the magnitude of nuclear steam supply system temperature and pressure transients resulting from large, rapid turbine load reductions, by dumping main steam directly to the condense.

The main process variables control I&C functions are categorized as safety category 3 which is accordance with the IAEA SSG-30.

2.2 System Classification

IEC 615130 states that: "Each I&C system shall be classified according to its suitability to implement I&C functions up to a defined category".

The MVCS is used to implement the main process variables control I&C functions of safety category 3, so the MVCS is classified as safety class 3.

2.3 Reliability Claim

The MVCS need to implements more complex control functions than Protection System (PS). So the MVCS is utilized by a general digital control platform which has reliable application experience. The platform can meet the functional and performance requirements of system and can work in normal and extreme environments in nuclear power plant. The hardware of the platform is qualified according to the requirements of nuclear area and the software is designed and developed according to the requirements of Category C in IEC 62138 [4]. So the reliability of the platform is higher than the general digital control platform used in conventional industry area. Based on the functional safety assessment methodology in IEC 61508 [5], the MVCS utilized by the platform at least corresponds to the reliability of Safety Integrity Level 1. So the reliability target of MVCS is claimed to 10^{-1} Probability of Failure on Demand (PFD).

3 Identified Difference

3.1 Requirement of IEC 61226–2009

The statement of the category for main process variables control function is "If plant process control functions are the only means of control of these variables, these control functions operating so that the main process variables are maintained within the limits assumed in the safety analysis should be assigned to safety category B" in the IEC 61226–2009.

Compared with the statement in IEC 61226-2009, the difference for the category of main process variables control functions is identified. The categorization required by IEC 61226-2009 is higher than the design scheme.

3.2 Design Scheme of Other Projects

The following information is identified as follows:

- In EPR, The main task of the Process Automation System (PAS) is the monitoring and automation of the plant in all normal operation conditions. The PAS is a E2 classified (safety class 3) equipment.

  The Reactor Control Surveillance and Limitation System (RCSL) is mainly devoted to F2 and NC I&C functions that control and monitor the operation of the reactor. This includes in particular:
- Core control functions,
- Core automatic limiting conditions of operation and limitation functions and primary/secondary limitations.

  The specific actuation control functions for the control rods are implemented in the RCSL. The RCSL is a E2 classified (safety class 3) equipment too.
- In UK ABWR, the Plant Control System (PCntlS) is used to control and maintain the plant condition during normal operation. The PCntlS consists of the reactor power control, the reactor water level control and the reactor pressure control, the key functions include the Recirculation Flow Control System (RFC), Rod Control and Information System (RCIS), Electro-hydraulic Turbine Control System (EHC), Feedwater Control System (FDWC) and Automatic Power Regulator (APR). The control system contributes to nuclear safety by keeping the reactor within the intended operational boundaries, avoiding demands being placed on the protection systems. The PCntlS is directly classified as a Class 3 system.

4 Assessment

The assessment is presented as the two aspects:

- Whether the main process variables control functions are needed in the event of an accident by safety analysis and reliability claim analysis.
- Whether the reliability claim meet the requirement of PSA.

4.1 Safety Analysis

The MVCS is classified as safety class 3. The following principles are apply to safety class 3 used in the safety analysis:

- If the transient leads to the actuation of an safety class 3 or NC system, and if the operation of this system would have a beneficial effect with regard to a safety criterion, the safety analysis shall be performed without considering this system.

- If the transient leads to the actuation of an safety class 3 or NC system, and if this system worsens the consequences of the transient with regard to a safety criterion, the safety analysis shall be performed assuming the system is operating normally.

For example: Following loss of main feedwater, the pressurizer main spray should be considered to operate normally when calculating the minimum DNBR.

So the MVCS is not credited in the safety analysis. Even if the MVCS fails, the conclusion of safety analysis is not affected.

4.2 Reliability Claim Analysis

An accident with very low expected frequencies need not be included in the design basis analysis. A accident frequency of 1×10^{-7} pa would be a typical cut-off when applying design basis techniques. The accident whose frequency is more than 1×10^{-7}pa need to be analyzed. This statement means that the frequency of Initiating Event (IE) multiples PFD for I&C systems which mitigate the consequences of IE shall be less than 1×10^{-7}pa. The formula is listed as follows:

$$IE\ frequency \times PFD\ of\ I\&C\ systems < 10^{-7}\ pa$$

Generally the frequency of IE is less than 1/ry. The reliability numeric target of PS and Diverse Actuation System (DAS) is listed as follows:

- PS is claimed to 10^{-4} PFD;
- DAS is claimed to 10^{-3} PFD.

So, it is enough that the IE can be mitigated by PS and DAS independently. Other I&C systems (e.g. MVCS) are not required.

4.3 PSA Analysis

For PSA, the accident sequence analysis aims at studying the plant-specific scenarios which may lead to core damage following each IE. The accident tree model of I&C system is integrated in PSA model for core damage frequency and large release frequency calculation, and the PSA results and risk insights are used to identify weaknesses of design and provide the recommendations for improvements.

For PSA, it includes the requisite functions of the emergency reactor trip, engineered safety feature actuation and safety supporting systems actuation for PS, and it also includes the important function of the DAS. It does not include the main process variables control function. The accident tree model of MVCS is not integrated in PSA. So the contribution of MVCS is not considered and the safety objective can still be met.

5 Conclusion

According to the description of Sect. 4, the degree of reliability for MVCS will not bring obvious benefits for the safety of the nuclear power plant. It is reasonable and acceptable that main process variables control functions are categorized as safety category 3 and the MVCS is classified as safety class 3.

In summary, if the main process variables control functions are not credited in the safety analysis, the functions are categorized as safety category 3 and the MVCS is classified as safety class 3. Otherwise the main process variables control functions are categorized as safety category 2 and the MVCS is classified as safety class 2.

References

1. IAEA: Safety Classification of Structures, Systems and Components in Nuclear Power Plants, SSG-30 (2014)
2. IEC: Nuclear power plants - Instrumentation and control systems important to safety - Classification of instrumentation and control functions, IEC 61226, Revision 3 (2009)
3. IEC: Nuclear power plants - Instrumentation and control important to safety - General requirement for systems, IEC 61513, Revision 2 (2011)
4. IEC: Nuclear power plants - Instrumentation and control important to safety - Software aspects for computer-based systems performing category B and C functions, C 62138, Revision 1 (2004)
5. IEC: Functional safety of electrical/electronic/programmable electronic safety-related systems, IEC 61508, Edition 2.0 (2010)

Research on Pattern Recognition Method of Nuclear Power Production Data Based on Neural Network

Huan-Lin Chen(✉), Hong-Bing Tu, and He-Min Liu

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

Abstract. With the continuous development of nuclear power industry, various production data of nuclear power plant, such as reactor temperature, pressure and other data, also grow rapidly. All kinds of data are stored in the database in a structured form. This lays a data foundation for the application of big data technology in the field of nuclear power. "History is always strikingly similar". From the perspective of time series, through the comparative analysis of the historical data of temperature, pressure and other indicators, we find that there are certain similar morphological characteristics, that is, the data go out of the similar development law in two different time periods. Therefore, through the mining matching algorithm, the transient data series in the current time period are compared with the historical retention time series to identify the most similar series in history, which plays a certain early warning role for the future. This paper intends to build an artificial neural network to find the best similarity calculation algorithm through training the massive historical label data and sample data, and finally achieve the effect of intelligent classification of production data, so as to predict the development trend in the future. The experimental results show that it is feasible to build a neural network model to realize the method of production data classification.

Keywords: Time series · Pattern Recognition · Neural Network

1 Introduction

The rapid development of information technology enables people to obtain and store a large amount of data. Finding patterns, trends and anomalies in these massive data, transforming data into information, transforming information into knowledge, and presenting it to users in an easy to understand way has become a great challenge in today's information age. Big data technology based on artificial intelligence came into being. As a branch of its technical research, neural network has attracted extensive attention because of its outstanding advantages [1].

After decades of development, China's nuclear power industry has accumulated a large amount of valuable power plant data, which lays a foundation for constructing artificial neural network and mining its data value. The study of historical production

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 106–113, 2023.
https://doi.org/10.1007/978-981-99-3455-3_11

data shows that a certain type of production indicators (such as temperature, pressure, etc.) in the past period of time, the numerical trend of change will be surprisingly similar. Classifying these time series with the same change trend can form a variety of numerical change patterns with different morphological characteristics. By comparing the production data in the current time period with the classical model trend in the historical database, find out the most similar time series, and comprehensively analyze its model type, which is helpful to make a certain early warning and prediction of the future development trend of numerical value [2]. To match the most similar sequence, the key is to solve the problem of similarity measurement between two time series. After comprehensively comparing several classical calculation methods of time series similarity measurement, based on these measurement methods, this paper proposes an algorithm to identify the most similar sequence by constructing artificial neural network.

2 Research Status at Home and Abroad

The research on time series similarity measurement method is the key to solve the problem of pattern recognition such as classification and clustering. Whether the similarity measurement method is properly selected directly affects the classification effect of time series. Classification accuracy is the primary index to measure the advantages and disadvantages of similarity measurement methods. Scholars and experts at home and abroad have made a lot of exploration on the similarity measurement methods of time series. There are three mainstream:

(1) Similarity measurement method based on Euclidean distance [3]

The similarity measurement method based on Euclidean distance(ED) regards the sequence as points in multi-dimensional space, and uses the cumulative distance of these points to measure the similarity of the sequence.There are two time series with equal length $X = \{X_1, X_2..., X_n\}$ and $Y = \{Y_1, Y_2..., Y_n\}$, If they are regarded as two dimensional space points respectively, their similarity distance is defined as

$$E(X, Y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2} \tag{1}$$

Set a threshold at the same time ε, When $E(X, Y) \leq \varepsilon$, it can be considered that the sequence X and Y are similar.

(2) Similarity measurement method based on longest common subsequence [4]

Because the Euclidean distance is extremely sensitive to the time axis, if two time series have the same or similar shape in most of the time, and the violent oscillation in a short time will lead to a great difference in the Euclidean distance between the two sequences. This situation is very common in the financial field, especially in the stock market. To solve this problem,The researchers proposed the similarity measurement method based on the longest common subsequence(Longest Common Subsequence, LCS).Let the two time series be expressed as $X = \{X_1, X_2 \ldots, X_n\}$ and $Y = \{Y_1, Y_2 \ldots, Y_n\}$. If their subsequence $X' = \{X_{i_1}, X_{i_2} \ldots, X_{i_l}\}$ and $Y' = \{Y_{j_1}, Y_{j_2} \ldots, Y_{j_l}\}$ meet the following two conditions:(i) for $\forall k, 1 \leq k < l$, we have $i_k < i_{k+1}$ and

$j_k < j_{k+1}$; (ii) for $\forall k$, $1 \le k < l$, we have $x_{i_k} = y_{i_k}$. Then X' and Y' are called common subsequences with length l. The similarity of sequence X and Y is defined as

$$L(X, Y) = l_{max}/n \tag{2}$$

where, $l_{\max}$ is the maximum length of all common subsequences.

(3) Similarity measurement method based on dynamic time warping [5]

Dynamic time warping (DTW) technology was first applied in the field of speech recognition. It was introduced into the field of time series research by Berndt et al. In 1994, it solved the problem of similarity matching between unequal length sequences and supported the scaling transformation of sequences along the time axis. Since the algorithm based on improved DTW is adopted in this paper, the calculation process and related concepts of dynamic time bending distance are introduced in detail:

Given two time series $X = \{X_1, X_2 \ldots, X_m\}$ and $Y = \{Y_1, Y_2 \ldots, Y_n\}$, Tectonic cumulative distance:

$$D(i, j) = d\left(x_i, y_j\right) + min\{D(i-1, j), D(i, j-1), D(i-1, j-1)\} \tag{3}$$

For $d\left(x_i, y_j\right)$, different distance definitions can be used. In general, Manhattan distance is taken,that is $d\left(x_i, y_j\right) = |x_i - y_i|, 1 \le i \le m, 1 \le j \le n$. The initial condition is $D(1, 1) = d\left(x_i, y_j\right)$. As defined above, $D(i, j)$ Represents the minimum cumulative distance between coordinate points (x_1, y_1) to $\left(x_i, y_j\right)$. In the process of finding the best distance between X and Y, the cumulative distance between is actually the minimum distance in the matrix:

The process of finding the final measured distance between sequences X and Y is actually to find an optimal bending path W in the distance matrix B, so as to minimize the average cumulative distance. The distance matrix B is:

$$B = \begin{bmatrix} d(x_1, y_n) & \cdots & d(x_m, y_n) \\ \vdots & \ddots & \vdots \\ d(x_1, y_1) & \cdots & d(x_m, y_1) \end{bmatrix} \tag{4}$$

The bending path $W = w_1, w_2, \ldots, w_k$ is constrained, and the element $w_r = (i, j)$ indicates that the i-th point in the sequence X matches the j-th point in the sequence Y, and satisfies:

(1) Subscript boundedness, that is $max(m, n) \le k \le m + n - 1$;
(2) Boundary property: W starts from the lower left corner of distance matrix B and ends at the upper right corner of distance matrix B, that is $w_1 = (1, 1)$, $w_k = (m, n)$;
(3) Continuous monotonicity: Any two adjacent elements on W are also adjacent in the distance matrix and develop forward, that is if ,then $0 \le a_{k+1} - a_k \le 1$ and $0 \le b_{k+1} - b_k \le 1$.

The reachable range of the bending path W in the distance matrix is called the bending window, as shown in the area within the dotted line in Fig. 1. The final metric distance is defined as

$$\mathrm{DTW(X, Y)} = \min\left\{\sum\nolimits_{(\mathrm{i,j})\in \mathrm{W}} \mathrm{d}\left(\mathrm{x_i}, \mathrm{y_j}\right)/\mathrm{Q}\right\} \tag{5}$$

where, Q is the length of the bending path W.

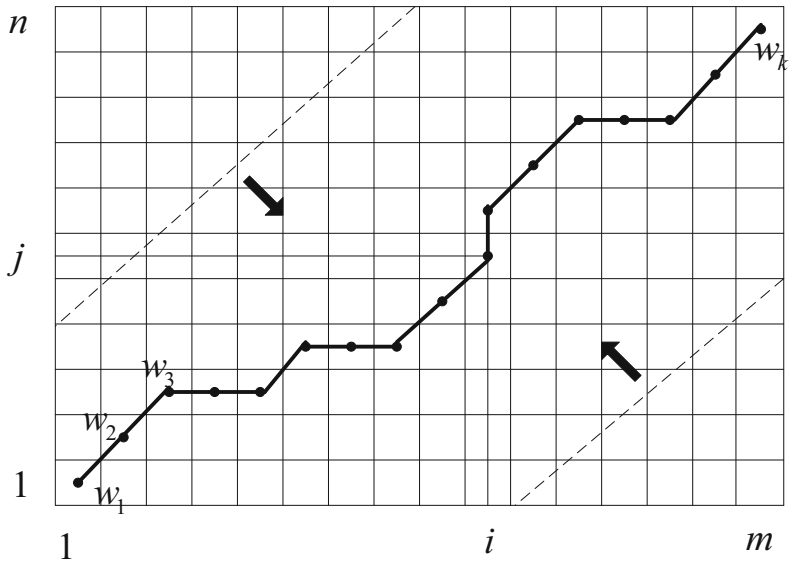


Fig. 1. Bending path and bending window

Because the above three measurement methods have their own advantages and disadvantages, selecting a measurement method for sequence matching alone will inevitably lead to the decline of accuracy. Therefore, this paper constructs a neural network, establishes the comprehensive weighting measurement formula of the three measurement methods, and selects a certain data set for training, so as to determine the weight value.

3 Pattern Matching of Nuclear Power Data Change Trend Based on Neural Network

3.1 Input Layer

The temperature of the pressure vessel is selected as the subject of the investigation data (after the pretreatment of the original data), and 24 data points are taken in each sequence (i.e. reflecting the data change trend of one day) with hour as the unit of data sampling time interval, each sequence can be represented as $X = \{x_1, x_2, \ldots, x_{24}\}$.Because each input sequence needs to be classified and matched, in order to investigate the classification accuracy when training the neural network model, the data input from the input layer must be labeled sequences, that is $X_i \in X[K_j]$, Indicating that sequence X_i belongs to class K_j(j:{1, 2, . . . , m}). In this paper, K is used to represent the pattern type.

3.2 Activation Function

After receiving the input signal from the input layer, the neuron located in the middle layer generates the output of the neuron after being processed by the activation function. In

the neural network constructed in this paper, the activation function selects the weighted values of the above three similarity measurement functions, i.e.

$$f\left(X_i, \overline{X}\right) = w_1 E\left(X_i, \overline{X}\right) + w_2 L\left(X_i, \overline{X}\right) + w_3 D\left(X_i, \overline{X}\right) \tag{6}$$

Among, X_i is the data sequence input by the input layer, $\overline{X}$ is the standard data sequence in the basic database (including all morphological types), w_1 *and* w_2 *and* w_3 are the weight coefficient, $E\left(X_i, \overline{X}\right)$ is the Euclidean distance, $L\left(X_i, \overline{X}\right)$ is the longest common subsequence distance, and $D\left(X_i, \overline{X}\right)$ is the dynamic bending distance.

3.3 Output Layer

Calculate the similarity measurement between the input sequence and all standard sequences in the standard library one by one, and find the standard sequence with the smallest measurement distance. If the minimum distance value is not greater than the threshold of the morphological type of the standard sequence (the threshold needs to be calculated in advance), the input sequence is considered to belong to the morphological type. Output its form type together in the output layer, i.e. $Y = [\overline{X}, K]$.

After the input layer, middle layer, neuron processing function and output layer are determined, the basic architecture of neural network is established, as shown in the Fig. 2 below.

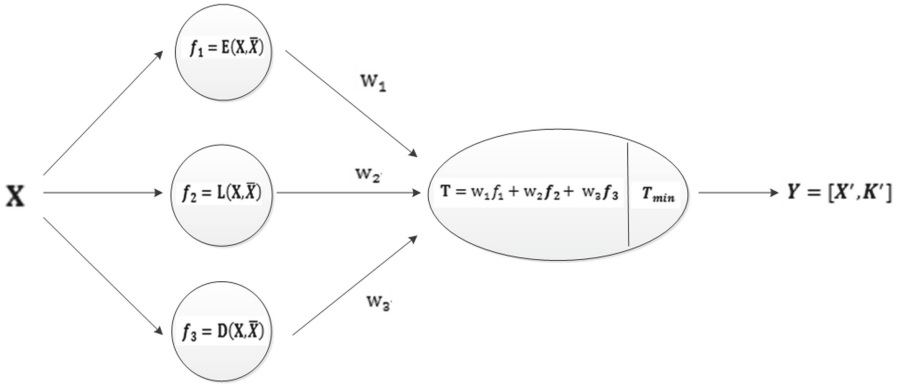


Fig. 2. Basic architecture of neural network proposed in this paper.

3.4 Training Network

In order to get the weight of each measurement function in the activation function, the neural network needs to be trained. Each morphological type K_j(j:{ 1,2, . . . ,m}) randomly selects 100 time series $\{X_{j1}, X_{j2} \ldots, X_{j99}, X_{j100}\}$ as the input layer, and then selects 100 standard sequences from each type in the standard database as the matching object to construct the training set.

In order to track the classification accuracy of the model, the objective function is set as

$$T = \sum_{i=1}^{100\ \mathrm{m}} C_i / 100\ \mathrm{m} * 100\% \tag{6}$$

*m*is the number of morphological types. C_i meets

$$C_i = \begin{cases} 1 & input\ sequence\ X_i\ can\ be\ classified\ correctly \\ 0 & input\ sequence\ X_i\ can\ not\ be\ classified\ correctly \end{cases}$$

The judgment rule of correct classification is: find out the standard sequence $\overline{X_j'}$ with the smallest similarity measurement distance with X_i. If the measurement distance value is not greater than the threshold of the morphological type to which $\overline{X}_j'$ belongs, and the morphological types of the two sequences are the same, it is considered that the input sequence X_i is classified correctly; if the above conditions are not met, it is considered that the input sequence X_i is not classified correctly.

The granularity of the weight factor is set to 0.1, and each training must meet the following conditions:

$$\begin{Bmatrix} w_1 + w_2 + w_3 = 1 \\ w_3 > 0.5 \\ w_2 > 0 \\ w_1 > 0 \end{Bmatrix} \tag{7}$$

The goal is to maximize the objective function, that is, the accuracy of sequence classification is the highest.

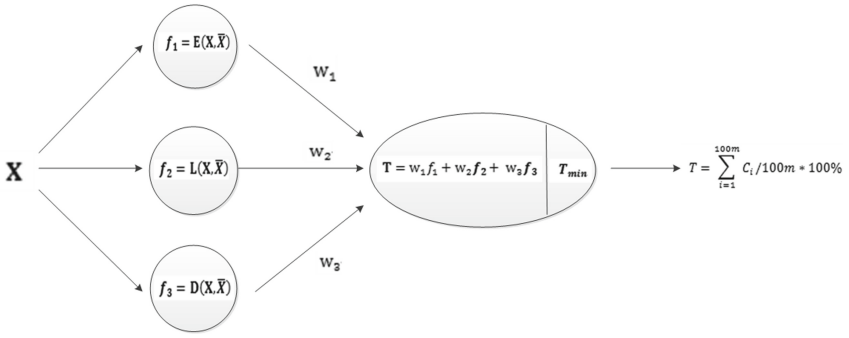


Fig. 3. Neural network training process proposed in this paper.

In this way, we have a network and a training set, and then use this training set to train the most appropriate weight value for the network, then the neural network can be built.

3.5 Test Network

The test set is divided into 5 groups of data. The first group randomly selected 100 time series $\{X_{j1}, X_{j2} \ldots, X_{j99}, X_{j100}\}$ from each morphological type $K_j(1, 2, \ldots, m)$, a total of 100 m sequence data; the second group randomly selected 200 time series $\{X_{j1}, X_{j2}..., X_{j99}, X_{j200}\}$ from each morphological type K_j(j:{ 1,2,. . . ,m}) sequence data; the third group randomly selected 300 time series $\{X_{j1}, X_{j2} \ldots, X_{j99}, X_{j300}\}$ from each morphological type K_j(j:{ 1,2,. . . ,m}), a total of 300 m sequence data; the fourth group randomly selected 500 time series $\{X_{j1}, X_{j2} \ldots, X_{j99}, X_{j500}\}$ from each morphological type K_j(j:{ 1,2,. . . ,m}), a total of 500m sequence data; the fifth group randomly selected 1000 time series $\{X_{j1}, X_{j2}..., X_{j99}, X_{j1000}\}$ from each morphological type K_j(j:{ 1,2,. . . ,m}), a total of 1000 m sequence data.

For each set of test data, the weighted distance, dynamic bending distance, longest common subsequence distance and Euclidean distance trained by the network are applied to test respectively. The experimental results are shown in the figure below. It can be seen that compared with a single distance calculation matching, the neural network model constructed in this paper still has a great improvement in classification accuracy.

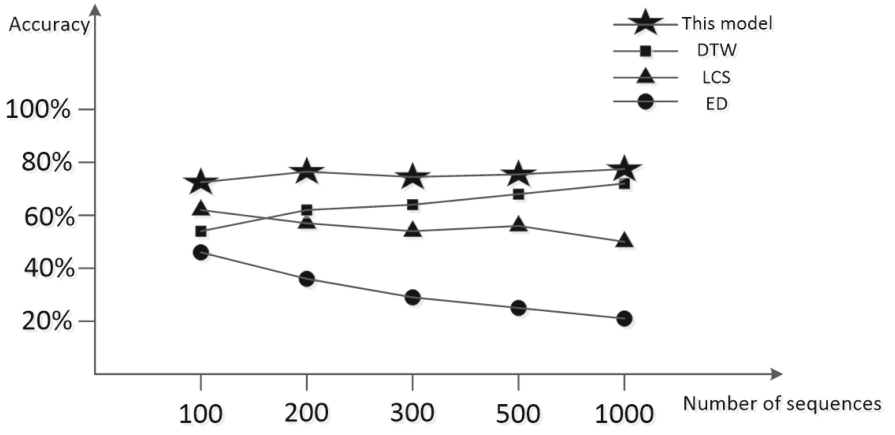


Fig. 4. Comparison of sequence matching accuracy based on each distance function

4 Summary

In order to predict the change trend of nuclear power production data, we can study its numerical characteristics from the perspective of time series, so as to accurately identify its mode, and then conduct correlation analysis on the same type of mode, which is helpful to grasp the change law and reason of actual production data. Therefore, this paper proposes a method to predict the trend by constructing neural network. In this method, the weighted values of dynamic bending distance, longest common subsequence

distance and Euclidean distance are used to measure the similarity of the two time series, and the neural network is trained through the input data to determine the weight factor. When a section of production data needs to be analyzed, it only needs to be transformed into time series, input from the input layer, and output its type after neuron processing. Compared with single distance calculation, the weighted distance formula has certain advantages in classification accuracy.

References

1. Haozhe, N.: Application of neural network algorithm in artificial intelligence recognition.Yangtze River Inf. Commun. **34**(12), 3 (2021)
2. Galbally, J., Galbally, D.: A pattern recognition approach based on DTW for automatic transientidentification in nuclear power plants. Ann. Nuclear Energy **81,** 287–300 (2011)
3. Zhang, Z., Cao, Z., Li, Y.: Research on k_means algorithm based on weighted Euclidean distance. J. Zhengzhou Univ. (1), 4 (2010)
4. Hu, J.: Algorithm research on LCs and its variants.Nanjing Forestry University (2011)
5. Li, M., Fenglan, B.: DNA sequence similarity analysis based on DTW distance. J. Biol. Math. (2), 5 (2009)

An Industrial Control System Vulnerability Analysis Method for Cyber Security in Nuclear Power Plant

Wang Xi(✉), Wei Liu, Wang-Ping Ye, and Hong-Yun Xie

China Nuclear Power Engineering Company Ltd., State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment, Shenzhen 518045, Guangdong, China
xw.dada@qq.com

Abstract. Vulnerability analysis is one of the important processes of cyber security risk assessment. With the gradual application of industrial Internet, intelligent technology, intelligent systems and equipment in the field of nuclear power, the methods of cyber attacks on nuclear power plants are gradually diversified, and the cyber security threats faced by industrial control systems are also increasing, and their cyber security vulnerabilities need to be continuously assessed. In this paper, combined with the current threat characteristics of nuclear power plant industrial control system operating environment, the cyber security vulnerability of the system is studied, and the typical vulnerability analysis items of nuclear power plant industrial control system are proposed to analyze the vulnerability characteristics of the system under different cyber security threat factors. At the same time, a vulnerability evaluation method based on functional safety impact analysis is formed, which takes the security level and consequence degree of the attacked system as the basic score, and the impact degree on the design of the defense-in-depth defense line as the weight for comprehensive scoring. Assess the vulnerability level to provide reference for the cybersecurity risk assessment and design improvement of the industrial control system of the nuclear power plant.

Keywords: Nuclear power plant · Control system · Cyber security · Vulnerability Analysis

1 Introduction

Industrial control systems such as data acquisition and monitoring systems, distributed control systems, process control systems, and programmable logic controllers are widely used in industrial fields to control the operation of production equipment [1]. Different from general systems, industrial control systems affect the entire production process, and its cyber security vulnerabilities may lead to serious industrial security and economic hidden dangers. Nuclear power plants are important industrial production facilities, and their operational safety issues may have catastrophic consequences for the social environment. In the past 20 years, nuclear power plants and energy infrastructure equipment

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 114–121, 2023.
https://doi.org/10.1007/978-981-99-3455-3_12

have been continuously attacked by cybersecurity, which has sounded the alarm for the cybersecurity of nuclear power digital I&C systems [2]. With the gradual application, the methods of cyber attacks on nuclear power plants are gradually diversified, and the cyber security threats faced by industrial control systems are also increasing, and their cyber security vulnerabilities need to be continuously assessed. Cyber security has become a key issue in the process of digital design of nuclear power plant industrial control systems, and its vulnerability assessment is an important part of the design process.

The nuclear power plant control system has proposed design concepts such as defense-in-depth, diversity, and single failure to fully cope with random and common-cause failures at the level of functional safety. With the addition of the cyber security dimension, the vulnerability of cyber security is closely related to functional safety, and the robustness of design based on functional safety needs to be re-analyzed.

2 Research on Cyber Security Vulnerability

2.1 Cyber Security Features of Industrial Control Systems

Vulnerability also becomes a weakness, which exists in the system itself. Threats always use the weakness of the system. If the system itself is strong, or when the weakness is not exploited by the threat, it will not cause damage to the system. The vulnerability of the system is hidden, and some weaknesses can only be revealed under certain conditions and environments, which is the most difficult part of vulnerability identification [3]. And, an incorrect, ineffective, or not properly implemented security measure can itself be a weakness.

Vulnerability identification is the most important link in risk assessment. It can be identified from the physical, network, system and application levels, and then corresponding to assets and threats. The basis can be international or national security standards or industry norms. Or the security requirements of the application process [4]. For the same vulnerability in different environments, the vulnerability severity is different.

Vulnerability identification can be carried out from two aspects: technology and management. Technical vulnerability involves security issues at the physical, network, system and application levels. Management vulnerability can be further divided into technical management vulnerability and organizational management vulnerability, which are related to specific technical activities and environmental management respectively [5]. Table 1 provides typical vulnerability identification content [6].

2.2 Vulnerability Levels of Industrial Control Systems

According to the degree of damage to the target system, the difficulty of technical implementation and the prevalence of the vulnerability, the severity of the identified vulnerabilities is assigned in a hierarchical manner [7]. The severity is graded, and the larger the grade value, the higher the vulnerability severity. Table 2 provides typical vulnerability severity assignments.

Table 1. Typical vulnerability items

Types	Objects	Items
Technical vulnerability	Physical environment	Fire prevention, power distribution, static electricity, grounding, lightning protection, electromagnetic, communication lines, etc. Network structure design, boundary protection, access control strategy, network equipment security configuration, etc
	Network structure	
	System software Database software Application middleware	Patches, accounts, passwords, event auditing, sharing, etc
		Access control, backup and recovery, etc
		Protocol security, data integrity, etc
	Application system	Audit mechanism, access control, data integrity, password protection, etc
Management vulnerability	Technical management	Physical domain environment security, access control, system development and maintenance, etc
	Organizational management	Security policy, organizational security, asset classification and control, personnel security, etc

Table 2. Typical vulnerability levels

Level	Means	Definition(under threat)
5	Very high	Complete damage to the target system
4	High	Major damage to the target system
3	Middle	Moderate damage to the target system
2	Low	Minor damage to the target system
1	Very low	Negligible damage to the target system

3 Cyber Security Vulnerability of Industrial System in Nuclear Power Plant

3.1 Vulnerability Analysis Items

For the cyber security design of a single system or DCS architecture, vulnerability analysis can be carried out from the following aspects of access control, linkability, system function, system equipment, monitoring and backup. Table 3 and Table 4 present a set of cybersecurity vulnerability analysis items for the control system of the nuclear power plant.

3.2 Vulnerability Assessment Method Base on Influence of Functional Safety

One of the design concepts of the industrial control system of a nuclear power plant is defense-in-depth [8]. For example, a nuclear power plant can be divided into a prevention line, a main line of defense, a diversity line of defense, a risk reduction line of defense, and a serious accident line of defense, which deal with design basis accidents of different frequencies respectively. From the perspective of functional safety, the systems of each line of defense are divided into functional safety levels (Class 1, 2, 3, and NC from high to low). Different platforms and backup disks are used to avoid common cause failures. However, due to the existence of network attacks, the original functional security line of defense will be broken. If there is no isolation and network protection design for each line of defense system existing in the same network, a network attack can penetrate all lines of defense, making defense in depth design fails. Therefore, vulnerability analysis of cybersecurity can be combined with design implications for functional safety.

Table 5 proposes a vulnerability scoring method based on functional safety impact analysis. The method is based on the analysis items in Table 5, the system function level, the level of defense line where the system is located, and the line of defense affected at the same time according to the analysis items in Table 5. The number is scored, and the calculation formula is: system damage score * the number of affected systems * the weight of the level of the defense line * the weight of the number of affected defense lines.

Table 3. Vulnerability analysis items for nuclear power plant (Part 1)

Types	Analysis items	Requirements
Access control	Logical Access Control	Device whitelist, complex password
	Physical access control	Cabinets are locked and alarmed when opened, non-essential interfaces are physically blocked
	Device authorization	Device whitelist, hardware trusted authentication
	Software Certification and Licensing	Application whitelist, file type blacklist and whitelist
	Password	Compound combination, invisible when input, cannot use factory default password
Linkability	Wireless Module/Device	Wireless device or module cannot be used
	Untrusted network	Network access authorization
	Communication integrity	Check
	Cross-domain data flow	Device whitelist
	Minimum number of access points	Keep the minimum number of access points required, no redundant vacant access points
	Communication protocol	Private protocol
	Maintenance tool	Single access path, tool authorization and authentication
Monitoring and backup	Monitoring, Auditing, Logging, Backup	System log, operation log, event type, audit system, timestamp, event/log backup system
	Malware	Antivirus software, network authorization, firewall, application whitelisting
	Abnormal detection	Detection of abnormal behavior (unauthorized attempts to access or install or modify applications, files, code, etc.), intrusion detection systems

Table 4. Vulnerability analysis items for nuclear power plant (Part 2)

Types	Analysis items	Requirements
System function	System independence	Isolated, predefined storage area
	Technical diversity	Platform diversity
	Minimum function set	System functions are kept to a minimum, and redundant functions are removed
	Predictable output	RTOS, outage avoidance operation, static resource allocation, parameter boundary protection, predefined time-based behavior, predefined communication load, predefined failsafe behavior
	Input integrity check	Validity check (length, format, range, etc.), integrity check of files and backups (hash check, etc.), preventing buffer overflow and other issues
	Resource management	Guaranteed operating load of the system
	Anti-Denial of Service	System and user data separation, access control lists, user account restrictions, anti-malware code, firewall and router filtering rules, priority design
System devices	Redundancy	Equipment, power supply, ventilation, component redundancy
	Power supply	UPS, surge protection
	Equipment and Components	Support for its latest operating system (cyber security patches), reprogrammable component management, robustness, no remote or wireless operation, support for offline updates, password protection
	Interface between systems	Hard-wired, point-to-point one-way communication (gateway, gatekeeper), high-level to low-level one-way communication, firewall, intrusion detection, physical protection

Table 5. Safety functional based vulnerability assessment method

Score	Level	Influence on system(under threat)	Influence on defense line
12	Serious	Complete damage to Class1 functional system or Complete damage to Class2 functional system	Level of defense line: 1: *1.0 2: *1.5 3: *2.0 4: *2.5 Number of effected defense lines: 1: *1.0 2: *1.5 3: *2.0 4: *2.5
10	Critical	Complete damage to Class1 functional system Major damage to Class1 functional system or Complete damage to Class2 functional system	
8	Important	General damage to Class1 functional system or major damage to Class2 functional system or complete damage to Class3 functional system	
6	Less important	Minor damage to Class1 functional system or general damage to Class2 functional system or major damage to Class3 functional system	
3	Common	Negligible damage to Class1 functional system or minor damage to Class2 functional system or general damage to Class3 functional system	
2	Low	Negligible damage to Class1/Class2 functional system or minor damage to Class3 functional system	
1	Very low	The damage to the Class1/Class2/Class3 functional system is negligible	

4 Conclusions

Combining the cyber security characteristics of the industrial control system of nuclear power plants and the characteristics of functional safety design, this paper constructs the cyber security vulnerability analysis item of the nuclear power plant control system. Based on the impact depth of defense-in-depth impact, a vulnerability analysis method based on functional safety impact analysis is proposed, which provides a reference for the testing ideas and design optimization of industrial control system cyber security.

References

1. Xi, W., Liu, W., Ye, W.P., Xie, H.Y.: A study about cyber security design basis threat for control system in nuclear power plant. In: Xu, Y., Sun, Y., Liu, Y., Gao, F., Gu, P., Liu, Z. (eds.) Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems. ISNPP 2021. LNEE, vol. 883. Springer, Singapore (2021). https://doi.org/10.1007/978-981-19-1181-1_36
2. International Electro Technical Commission: IEC 62645 Nuclear power plants - Instrumentation and control systems - Requirements for security programmes for computer-based systems, International Electro Technical Commission, Switzerland (2014)
3. Chen, J., Chu, X., et al.: Research on nuclear power plant digital instrumentation and control system cyber security. Instrumentation **24**(02, 42–44 (2017)
4. Yin, B., Ding, Y., et al.: Research on security analysis method of digital I&C system used in NPP. Nucl. Sci. Eng. **36**(03), 430–434 (2016)
5. Mao, L., Zheng, W., Zhang, S.: Cyber security system development process in nuclear power plant . Autom. Panorama **6**, 106–109 (2016)
6. Ou, H.: Overview of research on the information security of industrial control system. Process Autom. Instrum. **38**(07), 4–8 (2017)
7. Zhan, N., Qiao, Z.: The research on information security protection of industrial control system. Cybersp. Secur. **8**(12), 66–70 (2017)
8. Xi, W., Gu, P., Liu, W.: Discussions on information security test strategy for digital industrial control system in nuclear power plant. In: Xu, Y., Sun, Y., Liu, Y., Wang, Y., Gu, P., Liu, Z. (eds.) SICPNPP 2019. LNEE, vol. 595, pp. 83–89. Springer, Singapore (2020). https://doi.org/10.1007/978-981-15-1876-8_9

Study of Optimization for Calibration of Nuclear Safety Classification Pressure Transmitter

Ping Wu[1(✉)], Lin Guo[1], Qing Liu[2], Xiao-Wen Wang[2], Li Liu[1], Chang-Lei Li[1], and Qi-Meng Shen[2]

[1] China Nuclear Power Engineering Co., Ltd., Beijing 100840, China
wuping910713@163.com
[2] WECAN Precision Instruments Co.,Ltd., Chongqing401121, China

Abstract. In this paper the circuit of output current of nuclear safety classification pressure transmitter was analyzed in detail, the mathematical model of pressure transmitter was built, and the 4–20 mA output current is linear function of capacitance sensor current. The calibration process was analyzed, a non-linear duality equation group in which the two positions of potentiometers are the variables was built, and in fact the calibration process is solving the equation group. Analysis indicated that the calibration process is an iterative process, the convergence of the mathematical model was analyzed deeply, the result indicated that for proper resistance network the convergence is good, and the fact circuit meet the convergence condition. For general calibration process, a optimization method of proper excessive zero current was provided to accelerate the process, analysis and test verified that the efficiency is promoted significantly.

Keywords: Nuclear safety classification · Pressure transmitter · Current output · Capacitance sensor · Calibration

1 Introduction

In industrial automation process control, pressure transmitters are widely used. With the rapid development of control technology and network technology, high-precision intelligent instruments are more and more widely used [1–4]. However, in the field of nuclear safety applications, due to the existence of irradiation, it is necessary to consider the aging cumulative dose and accident high-dose irradiation, which has fatal damage to the widely used digital chip. At present, the research on radiation resistance of digital devices is still a hot spot [5], and application of silicon carbide devices in the future [6, 7] may solve the problem of radiation resistance of digital chips. However, pure analog circuit is the only choice in the field of nuclear safety application up to now, so the research on radiation resistance of analog devices is still very important [8–10].

The analog capacitive pressure transmitter senses the process medium pressure by the capacitive pressure sensor, as shown in Fig. 1.

The differential pressure of fluid between both sides acts on the isolation diaphragm, which leads to the deflection of the central measuring diaphragm and the differential

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 122–134, 2023.
https://doi.org/10.1007/978-981-99-3455-3_13

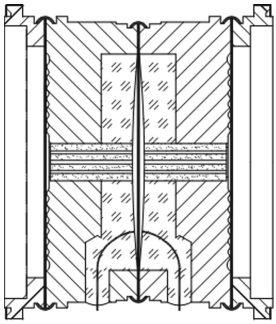


Fig. 1. Capacitance pressure sensor

change of capacitance. The excitation circuit generates AC excitation and applies it to the sensor. The demodulation circuit converts the capacitance difference into a DC current signal. This DC signal controls the output circuit to generate the corresponding 4–20 mA circulating current. The low cost and high reliability of two-wire 4–20 mA loop current is very suitable for industrial sites, which is widely used [11–13]. Therefore, the application of two-wire 4–20 mA output and pure analog circuit pressure transmitter is dominant in the field of nuclear safety application at present.

However, the calibration of the pure analog circuit pressure transmitter is completed by the zero point and range potentiometers, and the zero point and range pressures need to be applied repeatedly. The strong coupling between 4/20 mA and the positions of the two potentiometers brings complexity to the calibration. By analyzing the circuit of pure analog two-wire pressure transmitter, this paper establishes the mathematical model of sensor current and output current, takes the potentiometer position as a variable to analyze the convergence of calibration process, and then puts forward an improved method to improve calibration efficiency.

2 Current Circuit Analysis of Analog Pressure Transmitter

The sensor current and bias current can be simplified into a current source during the current circuit analysis of analog pressure transmitter, so the current circuit of pure analog pressure transmitter is simplified as shown in Fig. 2.

In the figure: V_i is the variable voltage of the positive end of the two-wire input voltage relative to the circuit ground, V_1 is the constant voltage (generated by the reference voltage), V_D is the diode voltage (slightly varying with the current), i_x is the control current (including the sensor current), i_o is the loop output current, V_2 is the control target (maintaining a constant value after the closed-loop is stable).

R_3 is a split range potentiometer. x is the position coefficient of range potentiometer and the range of x is [0,1]. Then the circuit is further transformed as shown in Fig. 3.

The output current control circuit (not shown in Fig. 3) controls the output current i_o and input voltage V_i by controlling the base of the triode, and the control target is to keep the voltage V_2 at a constant value. Using the star triangle circuit transformation, the circuit can be simplified as shown in Fig. 4.

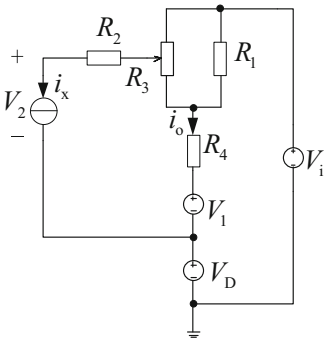


Fig. 2. Circuit of output current of transmitter

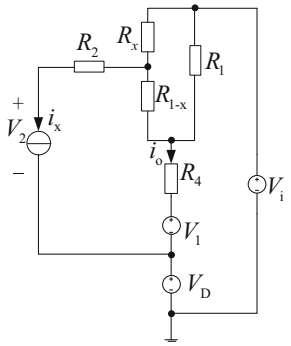


Fig. 3. Circuit of output current of transmitter about position of scale potentiometer

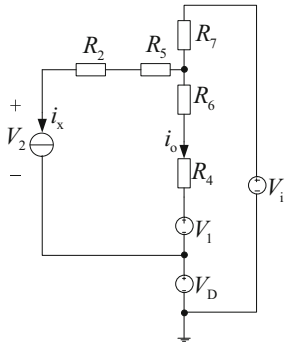


Fig. 4. Circuit of output current of transmitter after transformation

In Fig. 4, it can be calculated as follows:

$$\begin{cases} R_5 = \dfrac{R_x R_{1-x}}{R_x + R_{1-x} + R_1} = \dfrac{R_x R_{1-x}}{R_3 + R_1} \\ R_6 = \dfrac{R_{1-x} R_1}{R_3 + R_1} \\ R_7 = \dfrac{R_x R_1}{R_3 + R_1} \end{cases} \tag{1}$$

Using the star triangle circuit transformation again, the circuit can be simplified as shown in Fig. 5.

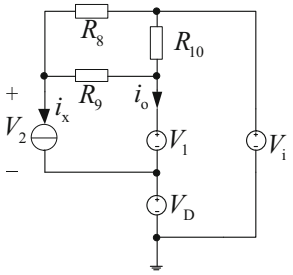


Fig. 5. Circuit of output current of transmitter after second transformation

Figure 5 meets the following equations:

$$\begin{cases} R_8 = \dfrac{(R_2 + R_5)R_7 + (R_2 + R_5)(R_4 + R_6) + (R_4 + R_6)R_7}{R_4 + R_6} \\ R_9 = \dfrac{(R_2 + R_5)R_7 + (R_2 + R_5)(R_4 + R_6) + (R_4 + R_6)R_7}{R_7} \\ R_{10} = \dfrac{(R_2 + R_5)R_7 + (R_2 + R_5)(R_4 + R_6) + (R_4 + R_6)R_7}{R_2 + R_5} \end{cases} \tag{2}$$

Thus,

$$\begin{cases} i_x = \dfrac{V_i - V_2 - V_D}{R_8} + \dfrac{V_1 - V_2}{R_9} \\ i_o = \dfrac{V_i - V_1 - V_D}{R_{10}} - \dfrac{V_1 - V_2}{R_9} \\ V_i - V_1 - V_D = R_8 i_x - \dfrac{R_8 + R_9}{R_9}(V_1 - V_2) \end{cases} \tag{3}$$

So,

$$i_o = \frac{R_8}{R_{10}} i_x - \frac{R_8 + R_9 + R_{10}}{R_9 R_{10}}(V_1 - V_2) \tag{4}$$

Since V_1 is a constant voltage and V_2 is also a constant value due to closed-loop control, it will be seen from this that the output current i_o is a primary function of current i_x.

Assuming $R_x = xR_3$ and $R_{1\text{-}x} = (1\text{-}x)R_3$, if the resistance is further substituted, the output current is further simplified as

$$i_o = \frac{(R_1R_2 + R_2R_3 + R_xR_{1\text{-}x})i_x - (R_1 + R_3)(V_1 - V_2)}{R_1R_4 + R_3R_4 + R_{1\text{-}x}R_1} \tag{5}$$

where: i_x contains three parts of current, i.e.

$$i_x = i_{sensor} + i_{zero} + I_{offset} \tag{6}$$

where: i_{sensor} is the sensor current, i_{zero} is the regulating current of zero point, I_{offset} is the bias current.

i_{zero} can be expressed as:

$$i_{zero} = (2y - 1)I_{zero} \tag{7}$$

where: I_{zero} is the maximum value of zero point current, y is the position of zero point potentiometer and the range of y is [0, 1].

Accordingly,

$$\begin{aligned} i_o &= \frac{R_2(R_1 + R_3) + R_3^2x(1 - x)}{R_1R_4 + R_3R_4 + R_3R_1(1 - x)}i_x - \frac{(R_1 + R_3)(V_1 - V_2)}{R_1R_4 + R_3R_4 + R_3R_1(1 - x)} \\ &= k_x\left[(2y - 1)I_{zero} + i_{sensor} + I_{offset}\right] + b_x \end{aligned} \tag{8}$$

where: k_x and b_x are constants related to x.

3 Analysis of Current Calibration Principle of Analog Pressure Transmitter

It can be seen from the above that the zero potentiometer regulating is to adjust y, the range potentiometer regulating is to adjust x. The transmitter calibration is to adjust these two potentiometers to realize to realize zero point output current is 4 mA and the range output current is 20 mA. The zero point and range current adjustment are coupled, that is, the zero point adjustment affects the range current, and the range adjustment also affects the zero point current. To realize 4 mA and 20 mA can correspond to the zero point and range at the same time, multiple iterations must be implemented. For this reason, the in-depth analysis of the calibration process is carried out below, and the optimized adjustment method is obtained to achieve efficient calibration.

It can be seen from Eq. (8) that the output current is a binary function, and the zero point current and range current are respectively expressed as:

$$\begin{cases} f_0(x, y) = k_x\left[(2y - 1)I_{zero} + I_{offset}\right] + b_x \\ f_1(x, y) = k_x\left[(2y - 1)I_{zero} + i_{sensor} + I_{offset}\right] + b_x \end{cases} \tag{9}$$

Then the current regulation must satisfy the nonlinear equations:

$$\begin{cases} f_0(x, y) = 0.004 \\ f_1(x, y) = 0.02 \end{cases} \tag{10}$$

Assuming that y^* and x^* are the adjusted final values, that is, the solutions of the nonlinear equations, then there is:

$$k_{x*} i_{\text{sensor}} = 0.016 \tag{11}$$

For a specific sensor, the sensor current i_{sensor} is a constant value, so k_{x*} is unique.

The derivative of k_x to x is

$$\frac{dk_x}{dx} = \frac{R_3^2(1-2x)[R_1R_4 + R_3R_4 + R_3R_1(1-x)]}{[R_1R_4 + R_3R_4 + R_3R_1(1-x)]^2} + \frac{R_3R_1\left[R_2(R_1+R_3) + R_3^2x(1-x)\right]}{[R_1R_4 + R_3R_4 + R_3R_1(1-x)]^2} \tag{12}$$

Obviously, the denominator is positive, so the sign of this derivative is determined by the numerator. After removing the positive common factor of the numerator, the sign of this derivative depends on:

$$R_3^2R_1(1-x)^2 + (R_1+R_3)[R_3R_4(1-2x) + R_1R_2] \tag{13}$$

Obviously,

$$R_3R_4(1-2x) + R_1R_2 > R_1R_2 - R_3R_4 \tag{14}$$

So actual circuit configuration meets:

$$R_1R_2 - R_3R_4 > 0 \tag{15}$$

Namely,

$$\frac{dk_x}{dx} > 0 \tag{16}$$

It is concluded that the k_x function is strictly monotonously increasing. Therefore, the uniqueness of k_{x*} determines that x^* is unique, and then y^* is also unique. That is to say, there is a unique solution to the nonlinear equations, which is the end value of calibration.

The function curve of k_x varying with x is shown in Fig. 6. It's obvious that the curve also shows its strictly monotonic property.

The current calibration process is carried out in an iterative manner.

Firstly, adjust the zero point coefficient y to make the output current as 4 mA.

Secondly, apply the range pressure and adjust the range coefficient x to make the output current as 20 mA.

Thirdly, remove the process pressure.

Then, repeat the step 1 to 3 until the output current of these two points meet the requirements. The zero point offset of a sensor need only to set different initial value instead of 0 pressure, and the principle is the same, so it is only described in terms of a zero point applying zero pressure.

The nth and (n + 1)th adjustments satisfy the equations:

$$\begin{cases} f_0(x_{n-1}, y_n) = k_{x_{n-1}}\left[(2y_n - 1)I_{zero} + I_{\text{offset}}\right] + b_{x_{n-1}} = 0.004 \\ f_1(x_n, y_n) = k_{x_n}\left[(2y_n - 1)I_{zero} + i_{\text{sensor}} + I_{\text{offset}}\right] + b_{x_n} = 0.02 \\ f_0(x_n, y_{n+1}) = k_{x_n}\left[(2y_{n+1} - 1)I_{zero} + I_{\text{offset}}\right] + b_{x_n} = 0.004 \\ f_1(x_{n+1}, y_{n+1}) = k_{x_{n+1}}\left[(2y_{n+1} - 1)I_{zero} + I_{\text{offset}}\right] + b_{x_{n+1}} = 0.004 \end{cases} \tag{17}$$

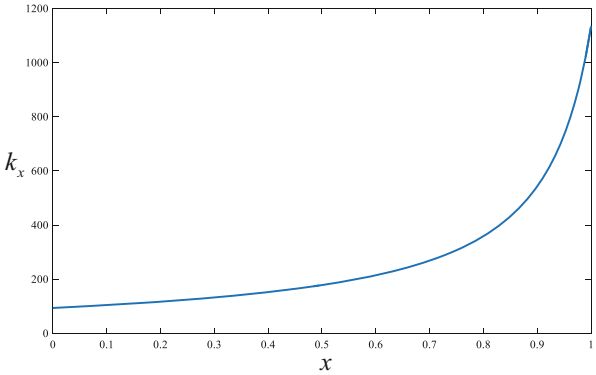


Fig. 6. k_{x} curve about x

According to the Taylor Mean Value Formula of binary function, there is:

$$\begin{cases} f_0(x_{\mathrm{n}}, y_{\mathrm{n}+1}) - f_0(x_{\mathrm{n}-1}, y_{\mathrm{n}}) \\ = \dfrac{\partial f_0(x,y)}{\partial x}\Big|_{x=\zeta_1, y=\zeta_2} (x_{\mathrm{n}} - \mathrm{x}_{\mathrm{n}-1}) \\ + \dfrac{\partial f_0(x,y)}{\partial y}\Big|_{x=\zeta_1, y=\zeta_2} (y_{\mathrm{n}+1} - y_{\mathrm{n}}) = 0 \\ f_1(x_{\mathrm{n}+1}, y_{\mathrm{n}+1}) - f_1(x_{\mathrm{n}}, y_{\mathrm{n}}) \\ = \dfrac{\partial f_1(x,y)}{\partial x}\Big|_{x=\zeta_3, y=\zeta_4} (x_{\mathrm{n}+1} - x_{\mathrm{n}}) \\ + \dfrac{\partial f_0(x,y)}{\partial y}\Big|_{x=\zeta_3, y=\zeta_4} (y_{\mathrm{n}+1} - y_{\mathrm{n}}) = 0 \end{cases} \tag{18}$$

where: ξ_1 is equal to $x_{\mathrm{n}\text{-}1} + \theta(x_{\mathrm{n}} - x_{\mathrm{n}\text{-}1})$, ξ_2 is equal to $y_{\mathrm{n}} + \theta(y_{\mathrm{n}+1} - y_{\mathrm{n}})$, ξ_3 is equal to $x_{\mathrm{n}\text{-}1} + \theta_1(x_{\mathrm{n}+1} - x_{\mathrm{n}})$, ξ_4 is equal to $y_{\mathrm{n}} + \theta_1(y_{\mathrm{n}+1} - y_{\mathrm{n}})$.That is,

$$\begin{cases} \dfrac{\partial f_0(x,y)}{\partial x}\Big|_{x=\zeta_1, y=\zeta_2} (\mathrm{x}_{\mathrm{n}} - \mathrm{x}_{\mathrm{n}-1}) \\ = -\dfrac{\partial f_0(x,y)}{\partial y}\Big|_{x=\zeta_1, y=\zeta_2} (y_{\mathrm{n}+1} - y_{\mathrm{n}}) \\ \dfrac{\partial f_1(x,y)}{\partial x}\Big|_{x=\zeta_3, y=\zeta_4} (\mathrm{x}_{\mathrm{n}+1} - \mathrm{x}_{\mathrm{n}}) \\ = -\dfrac{\partial f_0(x,y)}{\partial y}\Big|_{x=\zeta_3, y=\zeta_4} (y_{\mathrm{n}+1} - y_{\mathrm{n}}) \end{cases} \tag{19}$$

It can be seen from Eq. (9):

$$\frac{\partial f_0(x,y)}{\partial y} = \frac{\partial f_1(x,y)}{\partial y} = 2k_{\mathrm{x}} I_{zero} > 0 \tag{20}$$

The partial derivative of the output current to the position coefficient x of the range potentiometer is

$$\begin{aligned}\frac{\partial f_0(x,y)}{\partial x} &= \frac{R_3^2(1-2x)i_x[R_1R_4+R_3R_4+R_3R_1(1-x)]}{[R_1R_4+R_3R_4+R_3R_1(1-x)]^2} \\ &+\frac{R_3R_1\big[R_2(R_1+R_3)i_x+R_3^2x(1-x)i_x-(R_1+R_3)(V_1-V_2)\big]}{[R_1R_4+R_3R_4+R_3R_1(1-x)]^2}\end{aligned} \tag{21}$$

Obviously, if the denominator is positive, the sign of the partial derivative is determined by the numerator. After removing the positive common factor of the numerator, the sign of this partial derivative depends on:

$$R_3^2R_1(1-x)^2i_x+(R_1+R_3)[(R_3R_4(1-2x)+R_1R_2)i_x-R_1(V_1-V_2)] \tag{22}$$

Clearly,

$$(R_3R_4(1-2x)+R_1R_2)i_x-R_1(V_1-V_2)\geq(R_1R_2-R_3R_4)i_x-R_1(V_1-V_2) \tag{23}$$

Therefore,

$$(R_3R_4(1-2x)+R_1R_2)i_x-R_1(V_1-V_2)\geq R_1\left[\left(R_2-\frac{R_3R_4}{R_1}\right)i_x-(V_1-V_2)\right] \tag{24}$$

During the actual circuit calibration, when i_x is equal to 0.108mA, zero point output current is about 3mA, so it must meet:

$$i_x > 0.108\ \text{mA} \tag{25}$$

Use this value to get:

$$\left(R_2-\frac{R_3R_4}{R_1}\right)i_x-(V_1-V_2)=\left(17-\frac{2.2\times0.015}{0.18}\right)0.108-1.6=0.2126>0 \tag{26}$$

So,

$$\frac{\partial f_0(x,y)}{\partial x}>0 \tag{27}$$

If the range current i_x use a larger value, it also can satisfy:

$$\frac{\partial f_1(x,y)}{\partial x}>0 \tag{28}$$

Therefore, the circuit calibration always ensures that the output current increases with the increase of the two position coefficients of the zero point and range potentiometers,

that is, the partial derivative remains positive:

$$\begin{cases} \dfrac{\partial f_0(x,y)}{\partial x}\Big|_{x=\zeta_1,y=\zeta_2} > 0 \\ \dfrac{\partial f_0(x,y)}{\partial y}\Big|_{x=\zeta_1,y=\zeta_2} > 0 \\ \dfrac{\partial f_1(x,y)}{\partial x}\Big|_{x=\zeta_3,y=\zeta_4} > 0 \\ \dfrac{\partial f_0(x,y)}{\partial y}\Big|_{x=\zeta_3,y=\zeta_4} > 0 \end{cases} \tag{29}$$

Assuming x_n-$x_{n-1} < 0$ can get y_{n+1}-$y_n > 0$, and then get x_{n+1}- $x_n < 0$, continue the iteration to get y_{n+2}-$y_{n+1} > 0$, that is

$$\begin{cases} x_{n+1} < x_n < x_{n-1} \\ y_{n+2} > y_{n+1} > y_n \end{cases} \tag{30}$$

In the same way, assuming x_n-$x_{n-1} > 0$ can get y_{n+1}-$y_n < 0$, and then get x_{n+1}- $x_n > 0$, continue the iteration to get y_{n+2}-$y_{n+1} < 0$, that is

$$\begin{cases} x_{n+1} > x_n > x_{n-1} \\ y_{n+2} < y_{n+1} < y_n \end{cases} \tag{31}$$

That is to say, the potentiometer adjustment is strictly monotonic, and the uniqueness of the solution of the nonlinear equation determines that the strictly monotonic increase must have the poles, so we can get the conclusion that the calibration process must be convergent.

4 Optimization of Current Calibration Method for Analog Pressure Transmitter

The general current calibration method of analog pressure transmitter is shown in Fig. 7.

The calibration process is simulated by writing a program for solving nonlinear equations. For any initial value, this method generally needs 5 to 8 times iterations to meet the current requirements.

The analysis shows that the general method can be properly improved. If the zero point current adjustment is considered to be slightly smaller than 4mA (25% difference), the whole process converges faster. The improved calibration method is shown in Fig. 8.

After the improvement, the convergence speed is twice as fast, and the current calibration can be completed about 3 iterations, effectively improving the calibration efficiency.

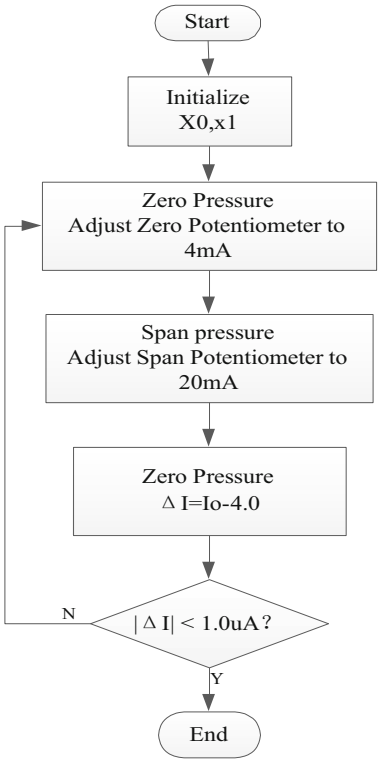


Fig. 7. Process of current calibration

5 Experimental Verification

The current calibration experiments of actual analog pressure transmitter are carried out according to the general calibration method and the improved method respectively. The actual range of this instrument is set to 180 kPa and the calibration test bench is shown in Fig. 9.

The initial potentiometer position is randomly selected for each test and tests are carried out for three times respectively. The test results are shown in Table 1.

Thus, the improved method can indeed improve the calibration efficiency.

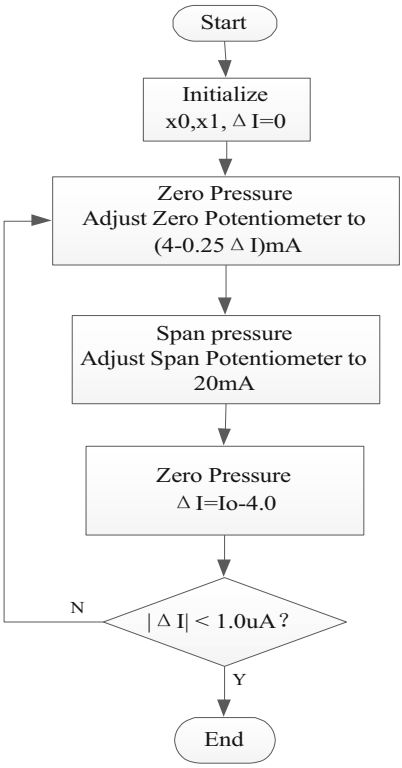


Fig. 8. Process of current calibration after optimization

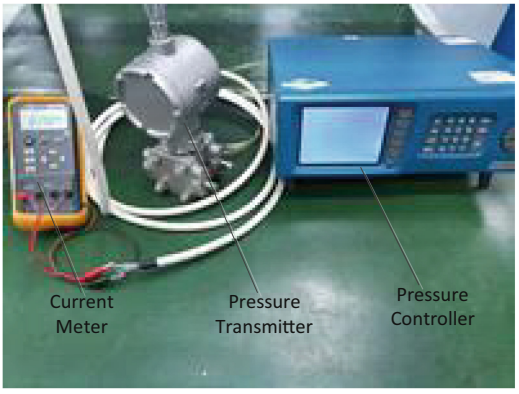


Fig. 9. Test bench of current calibration

Table 1. Test result

Test sequence	Iterations (general method)	Iterations (improved method)
1	5	2
2	8	3
3	7	3

6 Conclusion

Through the detailed analysis for the current control circuit of nuclear safety classification pressure transmitter with pure analog circuit, the mathematical model of current output pressure transmitter is established, which shows that the output current is a first-order function of the sensor current. The calibration process of zero point and range of pressure transmitter is analyzed, and the binary nonlinear equations with the positions of two potentiometers as variables are derived. The analysis shows that the actual calibration process is an iterative process to solve the equations. The convergence of the process is analyzed comprehensively and thoroughly based on the mathematical model. It shows that the process is convergent with using the appropriate resistance network and the actual circuit conforms to the convergence condition. In this paper, the usual calibration process is optimized, and an improved method with proper overshoot of zero point current is proposed. The simulation and tests both verify the correctness of the established mathematical model and the analysis conclusion and also verify that the improved method can greatly improve the calibration efficiency of safety classification pressure transmitter.

References

1. 毕监勃. : 高性能智能压力变送器的设计与实现. 化工自动化及仪表**41**(5), 4 (2014)
2. 樊岩松, 郑紫晖, 支若, 等. : 智能压力变送器多种应用及方式分析. 数字通信世界 (2), 1 (2020)
3. 钟华. : HART智能压力变送器检测方法的研究. 现代工业经济和信息化**12**(1), 3 (2022)
4. 刘培峰, 杜兴团. : 煤化工行业新型压力变送器的应用与优化. 流程工业 **4**, 4 (2022)
5. 何宝平, 周荷琴, 郭红霞, 等. 大规模集成电路浮栅ROM器件总剂量辐射效应. 半 导体学报**27**(1), 121–125 (2006)
6. 靳根, 陈法国, 杨亚鹏, 等. : 耐高温耐辐射的碳化硅半导体探测器. 核电子学与 探测技术**30**(7), 4 (2010)
7. 詹永玲, 杨银堂. : SiC器件与电路的若干关键技术. 微电子学 (4), 233–238 (2001)
8. Palkuti, L.J., Sivo, L.L., Greegor, R.B.: Process investigations of total-dose hard, Type-108 OP Amps. IEEE Trans. Nucl. Sci. **23**(6), 1756–1761 (1976)
9. Zebrev, G.I., Pavlov, D.Y., Pershenkov, V.S., et al.: Radiation response of bipolar transistors at various irradiation temperatures and electric biases: modeling and experiment. IEEE Trans. Nucl. Sci. **53**(4), 1981–1987 (2006)
10. 李骏, 王健安, 吴雪, 等.: 基区表面掺杂浓度对NPN型晶体管电离辐射效应的影 响. 现代应用物理 (2019)

11. Firth, J., Ladouceur, F., Brodzeli, Z., et al.:Liquid crystal based optical telemetry applied to 4–20 mA current loop networks. Sens. Actuat. A Phys. **260** (2017)
12. 胡秀芳, 张艾, 陈岩. : 4~20 mA压力变送器的电路设计. 中国仪器仪表 (5), 2 (2002)
13. 孙俊峰, 续艳, 刘军. : 现场压力变送器校准方法比较. 中国计量 (7), 98–100 (2012)

Modeling and Simulation of Secondary Loop Systems of a Pressurized Water Reactor Based on the 3KEYMASTER Platform

Guan-Fu Jiang, Xin-Yu Wei, and Pei-Wei Sun(✉)

School of Nuclear Science and Technology, Xi'an Jiaotong University, Xi'an 710049, China
sunpeiwei@mail.xjtu.edu.cn

Abstract. The modeling of the secondary-loop system is important to investigate its behavior. Accurate modeling and simulation under transient conditions are also necessary to verify the control system of the secondary-loop and provide basis for operation scheme. Based on the 3KEYMASTER simulation platform, a simulation model of the secondary-loop system of a pressurized water reactor was built. The model includes the main subsystems such as turbine system, reheat heating system, condensate system, feedwater system. The control system with PID controllers is also added to the model. Three steady-state working conditions are obtained at 100%, 70%, and 50% full power. Power transients, such as power step change, are simulated by changing the boundary conditions, and the system responses are recorded and investigated. The trends of key parameters are reasonable and meets the simulation experimental requirements. The secondary-loop system model follows the basic physical laws and can be used for nuclear power plant engineering simulation analysis. With reasonable simplifications and assumptions, it can be used as a control object for nuclear power plant control scheme design and verification studies. Its steady-state accuracy meets the requirements of training operators and also provides a good test environment for the design and operation of new generation nuclear power units.

Keywords: Modeling · Simulation · Secondary-Loop System · Control System

1 Introduction

As a clean energy source that can be applied on a large scale, accelerating the development of nuclear power is an inevitable way to solve the energy crisis and the environmental problems caused by fossil energy pollution. According to the China Energy Medium and Long-Term (2030–2050) Development Strategy Study, nuclear power will continue to increase its share of China's electricity, and by 2050, nuclear power generation in China will account for about 24% of total electricity generation [1]. The rapid development of nuclear power not only poses a challenge to grid peaking; at the same time, some possible events, such as turbine failure, tripping of feed pumps or other pumps in the secondary circuit, may also lead to serious accidents in nuclear power plants. Considering these two requirements, modeling studies on the secondary loop of nuclear power plants are

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 135–146, 2023.
https://doi.org/10.1007/978-981-99-3455-3_14

necessary, not only as control objects for the design and verification studies of nuclear power plant control schemes, but also to provide a good test environment for the design and operation of new generation nuclear power units.

Another code called NATDEMO was developed by Argonne National Laboratory specifically for EBR-II, including primary, feedwater and steam systems [2].

Sharma et al. simulated the BOP system of the prototype fast neutron reactor (PFBR) based on the RELAP5/MOD 3.4 code and used it to analyze some important events that can occur in the steam water system to verify the validity of the adopted procedures [3].

Somayeh Abbasi et al. [4] used RELAP5 to model the overall nuclear power unit first and second loop system and simulated the load dump transients, and the analysis showed that the reactor core pressure would increase sharply before slowly decreasing to normal operating levels.

Yang et al. developed a dual engineering simulator for the Advanced Boiling Water Reactor at Longmen (ABWR) based on RELAP5-3D with two separate RELAP5-3D modules for the reactor system and the BOP system, synchronized separately on a single platform [5].

Current nuclear power plant analysis programs focus mainly on the simulation of the first-loop model, while simplifying many of the equipment and systems in the second-loop system, and therefore have limitations in the scope of analysis. The traditional secondary-loop modeling approach uses the steam generator steam outlet and feedwater inlet as boundaries, usually giving constant pressure or constant flow boundary conditions, while all important components in the secondary-loop are ignored or greatly simplified. However, there are many operating conditions that require complete loops for analysis, such as start-up and shutdown of the reactor, bypass systems, etc., as well as for accident studies that include second loops, which also require complete models of the thermal hydraulic systems of first loop and second loop PWR nuclear power plants. Therefore, there is a great need for a complete thermal system modeling study.

Since the accuracy of the model of each part of the system will be directly related to the effectiveness of the whole plant simulation, in this paper, the 3KEYMASTER simulation platform is used as a tool to carry out the model construction of the second loop of the nuclear power plant and to test the steady state and load transients of the model. The model uses the steam generator primary side coolant inlet and outlet as the system model boundary, and this boundary can also be used as the interface to the nuclear reactor first-loop system, which can be extended to a plant-wide simulation system. With reasonable simplifications and assumptions, it can also be used for the design and verification studies of nuclear power plant control schemes.

2 A Secondary Loop Model Description

The object of this paper is the secondary-loop system of a large pressurized water reactor nuclear power plant. As shown in Fig. 1, the thermal hydraulic system of the conventional island consists of the secondary side of the steam generator (SG), the high-pressure turbine (HPT), four steam separator reheaters (MSR), three low-pressure turbines (LPT), three condensers, and three condensate extraction pumps (CEP). Twelve low-pressure heaters (two each of LPH1, LPH2, LPH3 and LPH4), deaerators, three feedwater pumps

(FP), four high-pressure heaters (two high-pressure heater No. 6 (HPH6) and two HPH7), and the corresponding valves and piping make up the plant. The 3KEYMASTER model for the secondary-loop of a nuclear power plant is based on the thermal system diagram shown in Fig. 1. The number of devices in the model matches the actual layout of the nuclear power plant, facilitating the simulation of the unlisted operation of certain devices. The modeling process simplifies the equipment operating in parallel to equipment with equivalent functions.

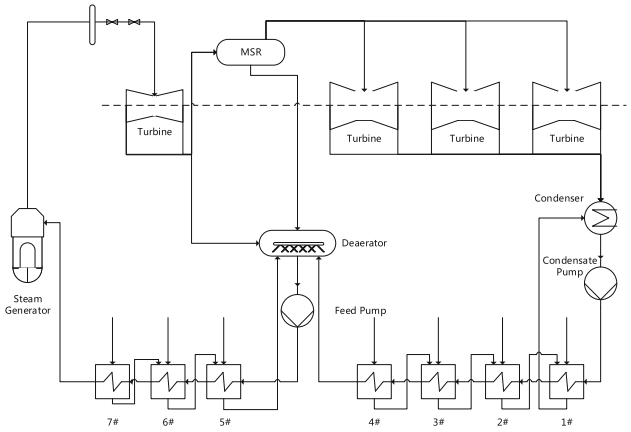


Fig. 1. Schematic diagram of the secondary-circuit thermal system of a nuclear power plant

2.1 The Steam Generator

The main function of the steam generator is to act as a heat exchange device to transfer the heat from the coolant in the first circuit to the feed water in the second circuit to produce saturated steam for supply to the steam power unit in the second circuit [6]. The model Steam generator with vertical arrangement, natural circulation and U-shaped tube type, whose structure is shown in Fig. 2. The steam generator model was modeled using the FlowBase toolbox integrated in 3KEYMASTER. The modeling process divided the steam generator into two parts according to its function and structure: the evaporation section and the steam-water separation section. A combination of heat transfer structures was used to model the heat transfer from the primary side coolant to the second loop feedwater, the evaporation section of the steam generator. The steam separation section is simulated using the fb2PhaseTank component of FlowBase, which is able to simulate the steam separation process after the feed water is heated according to its own function settings. The level control is achieved by the adjustment of the feed pump and feed valve to the steam generator model.

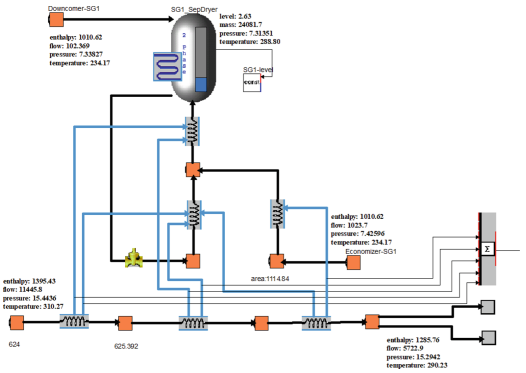


Fig. 2. The steam generator model in 3KEYMASTER

2.2 The Steam Turbine

A turbine is a device that converts the energy of high-temperature, high-pressure steam into mechanical energy [7]. In the 3KEYMASTER, modified energy, momentum and continuity equations are used for each stage. A number of stages arranged in sequence in series with equal flow rates is called a stage group, and each stage group contains stages with similar characteristics. Therefore, in the simulation modeling of turbines, the number of stages is usually modeled according to the number of stages rather than the number of stages. A coefficient is also set for the efficiency of energy conversion. In order to simulate the vapor extraction process in the turbine, vapor extraction interfaces are set in each stage group, and each interface is connected to the corresponding primary heat exchanger and high pressure heat exchanger of the MSRs to form a closed loop. As shown in Fig. 3, there is an exact model of one HPT with three stage groups. The HPT is modeled by three fbSection modules and each LPT is modeled by six fbSection modules.

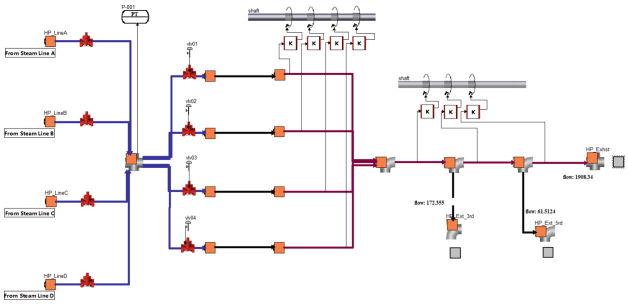


Fig. 3. The turbine model in 3KEYMASTER

2.3 The Moisture Separator Reheater

To prevent cavitation, the MSRs extract water from the turbine exhaust and reheat it [8]. Based on the operating principle of each MSR model, the model consists of a vapor separation tank as well as a two-stage reheat structure; the primary reheater is modeled with a heat transfer structure assembly with a shell for the high-pressure turbine extraction and a secondary reheater with a new steam interface on the side of the shell (Fig. 4).

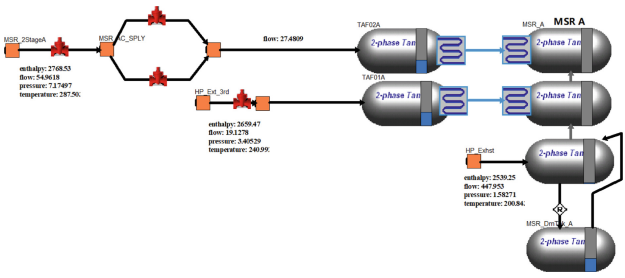


Fig. 4. The MSR model in 3KEYMASTER

2.4 The Condensate System

The condensers provide an economic back pressure for the turbine generator and allow the unit to operate safely and reliably within the specified cooling water temperature range and operating conditions. The condensers are modeled using the same fb2PhaseTank components and heat transfer structure, with three condensers corresponding to the discharge connections of three LPTs. The circulating water system is used as the cooling source for the condenser equipment. The condenser outlet is arranged with three condensate pumps, which are modeled by the pump assembly. Two feedwater booster pumps were also simulated in the model along with three feedwater pumps. In order to accurately simulate these eight pumps, their respective geometric parameters and characteristic curves (flow and head curves) are set, and the control of feedwater flow and feedwater pressure can be achieved under the action of the control system.

2.5 The Feedwater Heater System

Feedwater heater system can not only improve the efficiency of the plant by pumping steam to heat the feedwater, while heating the feedwater also reduces the temperature difference between the primary and secondary sides of the steam generator, making the equipment less thermal stress. For the No. 6 and No. 7 high-pressure heaters, the overall level of hydrophobic, such as the No. 7 high-pressure heater to the No. 6 high-pressure heater hydrophobic, No. 6 high-pressure heater to the deaerator hydrophobic; low-pressure feedwater heater system also includes low-pressure heaters and its hydrophobic system.

There are three rows of low-pressure heaters in the model, and each row includes LPH No. 1, No. 2, No. 3 and No. 4. Unlike the HPH, the LPH basically have no superheated steam cooling zone due to the low pumping superheat of the LPH, and the shell side of the LPH mainly consists of the main condensing section and the hydrophobic cooling section. LPH hydrophobic using the pressure difference between the heaters step by step self-flow, and finally from the first stage of LPH evacuation pipe into the condenser. The water level of each heater in the feedwater heater system is controlled by a valve on the downstream piping to avoid high hydrophobic water level flooding the tube bundle and resulting in reduced condensation area on the shell side, causing a drop in heat transfer (Fig. 5).

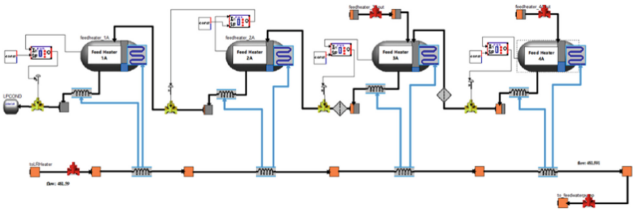


Fig. 5. The LPH model in 3KEYMASTER

2.6 The Deaerator

Because dissolved oxygen in feedwater can have a corrosive effect on thermal equipment and piping, a deaerator is required to deaerate and heat the feedwater. The deaerator used in this system is also built from the fb2PhaseTank module, which acts as both a deaerator and a feedwater storage tank. The deaerator pressure is maintained by extracting steam from the turbine to ensure that the feedwater pressure is sufficient to meet the net positive suction pressure head required by the feedwater pumps. The deaerator model receives preheat sources from the MSR, No. 6 HPH and HPT, which are mixed with condensate in the stubs and then pressurized by the feedwater pump and sent to the high pressure heater. The actual model does not contain oxygen and other non-condensable gases in the two-loop flowing mass, so the deaerating link is simplified to model the mixing and heating process (Fig. 6).

The power variation of the nuclear reactor is simulated by modifying the enthalpy of the inlet coolant on the primary side of the steam generator. Steady-state points at 100%, 70%, and 50% power levels were preset in the model. In addition to the steady-state operating points, transient simulations of the turbine load from 100% power level to 50% low power were also simulated. Figure 7 shows the secondary loop model HMI.

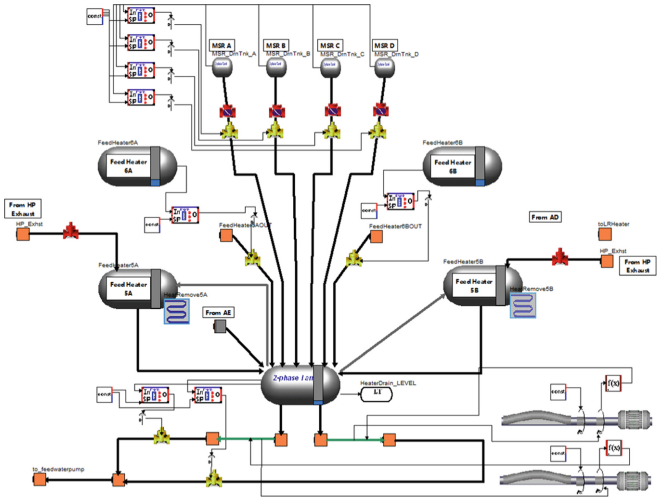


Fig. 6. The deaerator model in 3KEYMASTER

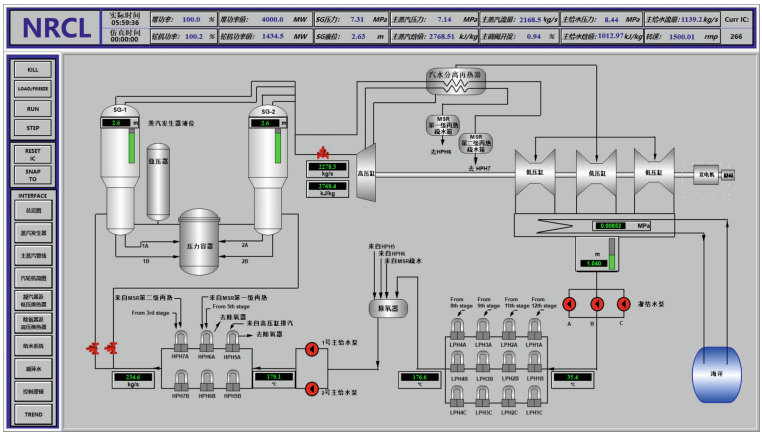


Fig. 7. Secondary loop model HMI

3 Simulation and Discussion

The model testing and validation are divided into two parts: steady-state validation and transient validation. The simulation parameters of 100%FP, 70%FP and 50%FP steady-state operating points are selected for comparison with the design parameters in the steady-state verification to verify the correctness and reliability of the model. The error between them is less than 3% and the error of key parameters is no more than 1%. The results of the 100% FP working condition are shown in Table 1.

The transient verification is achieved by modifying the model boundary conditions. The automatic control system in the conventional operating condition of the two-loop model can regulate the power of the turbine generator set to maintain the power generated in the second loop near the set value. The pressure control mode and load control mode were tested separately in the model. In the pressure control mode, the main steam header pressure is regulated at a constant value to keep the turbine-generator power matching the reactor power, and the controller input is the deviation between the main steam header pressure setting value and the measured value, and the PI controller output valve opening is used to control the main steam header pressure to reach the setting value. In the load control mode, the load deviation is used as the controller input, and the valve opening is output by the PI controller to control the steam flow into the high pressure cylinder.

The change in the first-loop coolant temperature of the nuclear reactor during the transient process is simulated by changing the movable boundary of the primary side inlet of the steam generator. The change in boundary was introduced after 60 s of stable operation of the system to simulate power reduction at a rate of 1% FP/s: the initial value of the primary side inlet boundary flow rate of the steam generator was the initial value of enthalpy as shown in the following table (Table 2).

Table 1. Validation of steady-state parameters.

Parameter	Calculation value	Nominal value	Error
Main steam flow /kg/s	2253.0	2253.0	0.00%
Main steam pressure /MPa	7.1	7.1	0.00%
Main steam temperature /°C	287.2	287.2	0.00%
Turbine power /MW	1409.0	1400.0	0.71%
Low pressure heater outlet condensate temperature /°C	152.0	150.5	0.99%
Low pressure heater outlet condensate pressure /MPa	176.6	173.7	1.67%
Deaerator outlet feedwater temperature /°C	200.1	194.3	2.98%
Deaerator outlet feedwater pressure /MPa	3.3	3.3	0.60%
High pressure heater outlet feed water temperature /°C	234.1	231.3	1.21%
High pressure heater outlet feed water pressure /MPa	8.61	8.6	0.00%
Feedwater pump outlet pressure /MPa	9.3	9.3	0.53%
Feed water temperature /°C	234.6	231.4	1.38%

Table 2. Model boundary setting values for transient conditions

Power Percentage	Parameter	Value
100%	SG Inlet Flow Rate(kg/s)	10747
	SG Inlet Enthalpy(kJ/kg)	1469.59
	SG outlet enthalpy(kJ/kg)	1283.6
	SG Outlet Pressure(MPa)	15.5
90%	SG Inlet Flow Rate(kg/s)	10747
	SG Inlet Enthalpy(kJ/kg)	1451.0
	SG Outlet Enthalpy(kJ/kg)	1281.1
	SG outlet pressure(MPa)	15.5

The model runs steadily at 100% FP level for 60s and then reactor power drops to 90% FP at 1% FP/s, 90% FP steady state reached at 350 s, end of simulation at 600 s. This simulation uses the turbine pressure control mode, and the MSRs, condenser, deaerator, LPHs and HPHs use regulating valves arranged on the downstream piping to control the liquid level stable near the set value. And there is a feed pump speed control system for adjusting the speed of the steam feed pump, so that the differential pressure between the feed pump inlet and outlet is close to a constant, and keep the differential pressure between the main steam line and the main feedwater line to the specified programmed differential pressure. At the same time by the three impulse (feed water flow, steam flow and steam generator water level) regulator control two feedwater regulating valves to maintain the stability of the steam generator level.

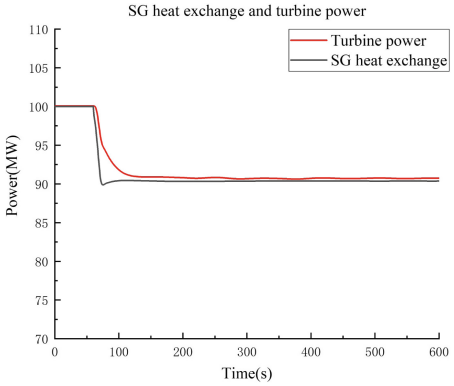


Fig. 8. The turbine power under power reduction condition.

Figure 8 shows the variation of turbine power. And Fig. 9 shows the variation curve of steam flow rate and feedwater flow rate. Figure 10 shows the variation of the liquid level of the two steam generators. The temperatures of the Steam generator outlet steam,

HPT inlet, HPT exhaust steam, LPT inlet, LPH outlet, deaerator outlet and feedwater are shown in Fig. 11. The steam and feedwater pressure variation curves are shown in Fig. 12.

Because of the adoption of the constant main steam pressure scheme, the decrease in SG primary side inlet coolant temperature will lead to a decrease in SG secondary side steam production, which will affect the steam outlet pressure to reduce it, then the main steam header pressure is lower than the pressure setting, and the main regulator valve opening is reduced to keep the pressure in front of the valve near the setting value. According to Fig. 8, it can be seen that the reduction of steam inlet flow to the turbine leads to the reduction of the turbine power. The steam generator level first drops and then returns to the set value because the feed water flow is greater than the steam flow.

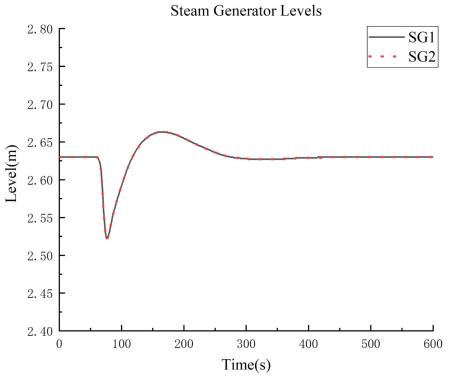


Fig. 10. The liquid level of the two steam generators under power reduction condition.

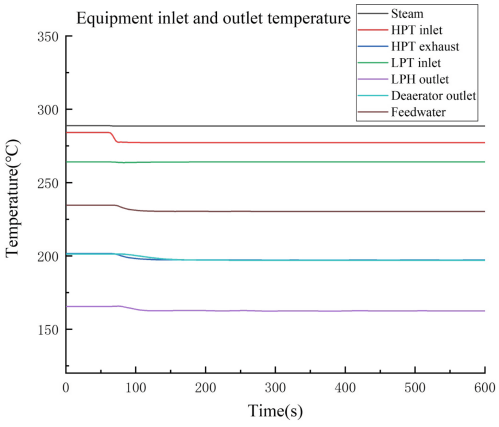


Fig. 11. The Temperature of SG outlet, HPT inlet, HPT exhaust, LPT inlet, LPH outlet, deaerator outlet and feedwater under power reduction condition.

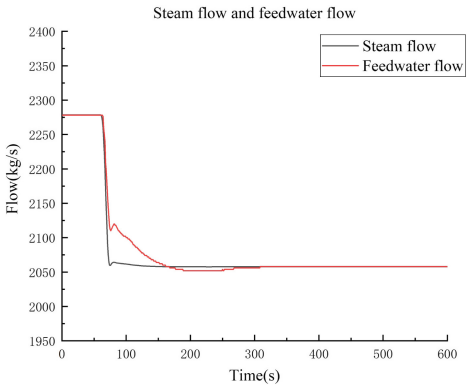


Fig. 9. The steam flow rate and feedwater flow rate under power reduction condition.

In Fig. 11, as the main regulating valve maintains a constant pressure in front of the valve, the valve opening decreases, resulting in a decrease in the pressure behind the valve and thus a decrease in the turbine inlet temperature; at the same time, the turbine's pumping capacity to the heater decreases as the power decreases, and the water temperature at the outlet of the heaters and deaerators at all levels also decreases. As can be seen in Fig. 12, the main steam pressure decreases due to the main regulating valve and then returns to 7.145 MPa under the action of the control system; the mismatch of steam and water flow caused by the power change will cause the feedwater regulating valve opening to decrease, and the feedwater pressure will rise first, and then the feedwater pressure will be slightly lower than the initial value because the set value of the pressure difference between the steam bus and the feedwater pump outlet bus will decrease with the power reduction.

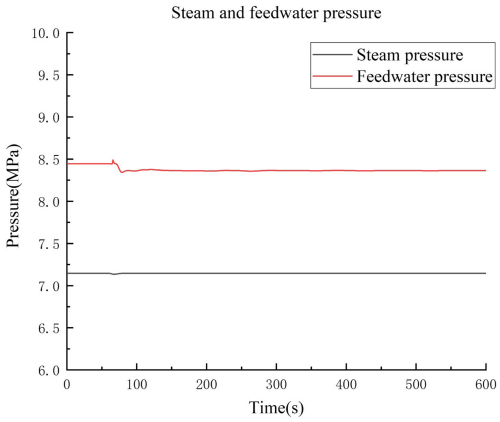


Fig. 12. The steam and feedwater pressure under power reduction condition.

4 Conclusions

Based on 3KEYMASTER simulation platform, a secondary-loop model of a PWR was built. And the separate steady state of the load from 100% to 50% is realized. The parameter verification shows that the error between the calculated value of the model steady state and the actual design value meets the simulation requirements, and the error of the main parameters is less than 3%, which is acceptable. The control logic of each system is also set, the model can correctly and effectively reflect the dynamic characteristics in the range of normal operating conditions during the transient process of power lifting and lowering, and the changes of each parameter are in accordance with the actual physical process. The model can be used as a reference for further research on the simulation of dynamic characteristics and the design or improvement of control systems in the full operating range of the second loop of nuclear power plants.

References

1. Chinese Academy of Engineering Project Team: Study on China's Medium and Long-Term Energy Development Strategy (2030–2050). Science Press, Beijing (2011)
2. Planchon, H.P., Singer, R.M., Mohr, D., Feldman, E.E., Chang, L.K., Betten, P.R.: The experimental breeder reactor II inherent shutdown and heat removal tests—results and analysis. Nucl. Eng. Des. **91**(3), 287–296 (1986)
3. Sharma, P., Natesan, K., Selvaraj, P., Balasubramaniyan, V., Chellapandi, P.: Dynamic modeling of steam water system of prototype fast breeder reactor using RELAP code. Ann. Nucl. Energy **68**, 209–219 (2014)
4. Abbasi, S., Hadad, K.: Analysis of the loss of heat sink transients in the secondary circuit of a VVER-1000 using RELAP5/MOD3.2. Ann. Nucl. Energy **47**(none), 28–37 (2012)
5. Yang, C.-Y., Liang, T.K.S., Pei, B.S., Shih, C.K., Chiang, S.C., Wang, L.C.: Development and application of a dual RELAP5-3D-based engineering simulator for ABWR. Nucl. Eng. Des. **239**(10), 1847–1856 (2009)
6. Xiong, J., Fu, L.: Modeling and Simulation of nuclear steam generator. Nucl. Sci. Eng. **01,** 20–33 + 5 (1989)
7. Dulau, M., Bica, D.: Mathematical modelling and simulation of the behaviour of the steam turbine. Procedia Technol. **12**, 723–729 (2014)
8. Elliott, T.C., Chen, K., Swanekamp, R.: Standard Handbook of Powerplant Engineering, 2nd edn. McGraw-Hill, New York (1997)

Treatment and Analysis of SG Level Control Problems in Nuclear Power Plant Startup and Low Power Stage

Fei Song[1(✉)], Hang Liu[1], Jian-Feng Qiao[1], and Peng Liu[1,2]

[1] China Nuclear Power Engineering Co., Ltd., Shenzhen 518172, Guangdong, People's Republic of China
thomashust@163.com

[2] College of Mechatronics and Control Engineering, Shenzhen University, Shenzhen 518000, Guangdong, People's Republic of China

Abstract. Steam generator level is the key and difficult point of nuclear power plant control. Improving the automation level of Steam generator level control can reduce the workload of nuclear power operators, reduce human errors and improve the work efficiency of operators. In the start-up and shutdown stage and low power stage of a GEN-II nuclear power plant, Steam generator is supplied with water by ASG system and operators manually operated control SG level. In a GEN-III nuclear power plant, Steam generator is supplied with water by AAD system in the start-up/shutdown stage, and SG level is automatically controlled by ARE Start-up control valve, thus it has realized the automatic control of SG level under all working conditions of the nuclear power plants and improved the intelligent level for the nuclear power plants. In the start-up and shutdown stage and low power stage of the nuclear power plants, the steam flow and feed water flow are extremely small, the measurement is inaccurate, and the conventional cascade control of SG level and feed water flow cannot be adopted. This paper mainly introduces the principle, test validation and optimization, problems and solutions of SG level automatic control in the start-up and shutdown stage of the GEN-III power plants.

Keywords: SG level · ARE start-up control valve · Coupling · Flow characteristic correction · Differential pressure control

1 Introduction

During the start-up/shutdown phase of GEN-II nuclear power plants, the Steam generator is supplied by emergency water supply system (hereinafter referred to as ASG system) and passes through SG liquid level in manually operated, Regulating valve, manually operated, as shown in Fig. 1. However, the ASG system in the GEN-III nuclear power plant has only safety function, but no operation function. It is only used in water supply accidents with loss of APA system(Main feed water pump system) and AAD system(Start up and shut down feed water system) and take out the waste heat of the core, so that the

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 147–157, 2023.
https://doi.org/10.1007/978-981-99-3455-3_15

power station can reach and maintain a safe shutdown state. The GEN-III nuclear power plant is supplied with water by the AAD system during the start-up/shutdown phase, and the SG level is automatically controlled by ARE Start-up control valve(hereinafter referred to as SCV), as shown in Fig. 2. This paper mainly introduces the principle, test validation and optimization, problems and solutions of SG level automatic control in the start-up and shutdown stage of the GEN-III power plants.

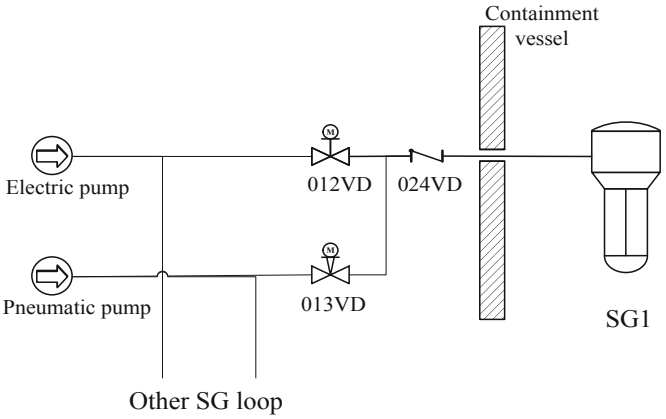


Fig. 1. SG level control flow diagram in the start-up stage of GEN-II nuclear power plants

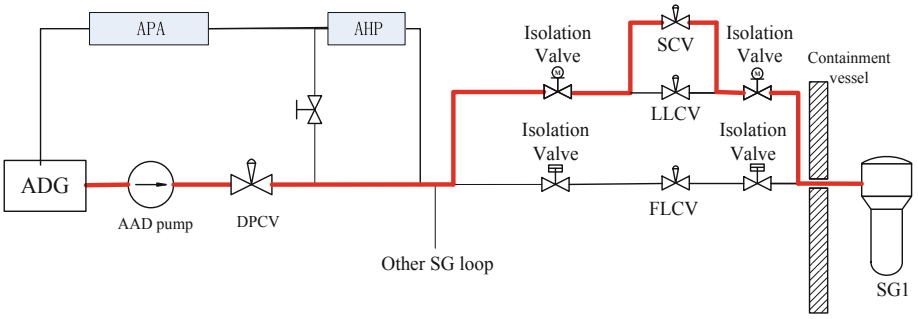


Fig. 2. SG level control diagram in start-up stage of a GEN-III nuclear power plant

2 SG Level Control Principle of ARE Start-Up Control Valve

2.1 Stage Division of SG Level Control in the GEN-III Nuclear Power Plants

SG level control in the GEN-III nuclear power plants is divided into three stages. ARE SCV valve is used to control SG level under start-up shutdown and hot standby conditions, ARE low load control valve (hereinafter referred to as LLCV) is used to control SG level when the nuclear power is 2%–20%, and ARE full load control valve (hereinafter

referred to as FLCV) is used to control SG level when the nuclear power is 20%–100%, see Table 1 for details. The division of SG level control in the last two stages in the GEN-III nuclear power plant is similar to that in the GEN-II nuclear power plant, but the control realization in the GEN-III nuclear power plant is quite different from that in the GEN-II nuclear power plant. This paper mainly introduces the problem of SCV SG level control.

Table 1. Three stages of SG level control of the GEN-III nuclear power plants

Nuclear power	SCV opening	LLCV opening	FLCV opening	SG Water Supply System
0 ~ 2%	0 ~ 100%	0	0	AAD
2 ~ 20%	0	0 ~ 100%	0	APA
20 ~ 100%	0	100%	0 ~ full power opening	APA

2.2 Principle of SG Level Control by SCV

Different from SG level cascade control in power operation stage, SCV SG level control adopts single-loop PID control, only Level controllers, not Flow controllers. The measurement range of flow in feed water pipeline is about 500 t/h (narrow range) and 2400 t/h (wide range), while the working condition of ARE SCV is the start up/shut down and hot standby stage of the plant. Under this condition, the feed water flow is extremely small, about 2 t/h–50 t/h, which cannot be accurately measured. The Flow gauges error range of Venturi pipe is extremely large, so it is inappropriate to adopt ARE flow and SG level cascade control which is used in the power operation stage.

Above Fig. 3 is a diagram of ARE SCV SG level control. The deviation between SG level setpoint and SG level measured value is calculated by PI Controller to obtain the required feed water flow. Feed water flow, differential pressure of ARE SCV upstream and downstream, and feed water temperature are calculated by formula to get CV value as output. Then, according to the corresponding relationship between valve CV and opening, the SCV opening instruction is finally output to control SG level to return to the setpoint. Under the working condition of SCV, the steam flow rate and feed water flow rate are extremely small. If the setpoint of SG level is less than the measured value of SG level, and the deviation is large, The output feedwater flow of PID Controller will become very small, even zero, resulting in feed water interruption. The flow limiting module in the figure prevents feed water interruption when SG level is automatically controlled, limiting the minimum flow rate and avoiding cold and hot shock caused by intermittent feed water in SG nozzle and ARE pipeline.

2.3 Correction of Flow Characteristic Calculation

Compared with SG level control of GEN-II nuclear power plants in power operation stage, CV calculation logic of ARE SCV is an innovation for SG level control. Because

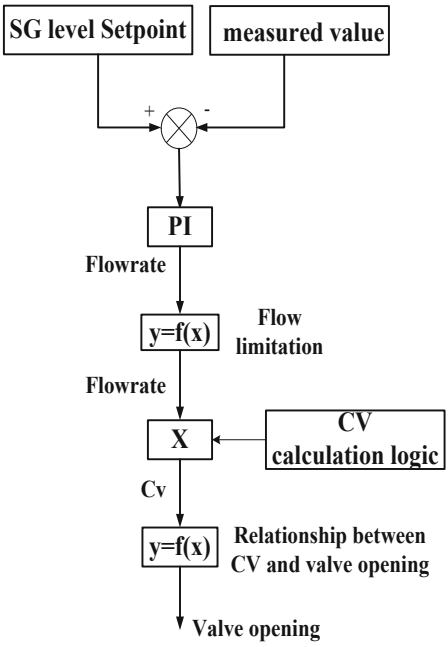


Fig. 3. ARE SCV SG Level Control Diagram

the feed water flow can not be accurately measured during the start-up shutdown and hot standby conditions which is the working condition of ARE SCV, CV calculation logic can make the valve opening output more accurate, so as to improve the control capability of SG level.

According to the definition of Sect. 4.6.2 of national standard GB/T 17213.1–2015 "Industrial process control valves-Part 1: Control valve terminology and general considerations", the flow coefficient Cv is a control valve flow coefficient in non-national standard system of units, which can be expressed numerically as the number of US gallons of water flowing through the valve at a temperature of 40 F–100 F in 1 min under the condition of 1 psi in Pressure drop. Under other conditions, it can be calculated by the following formula:

$$C_V = Q\sqrt{\left(\frac{\triangle p_{cv}}{\triangle p}\right)\left(\frac{\rho}{\rho_w}\right)} \tag{1}$$

Where:

Q —Volume flow of control valve fluid in American gallons per minute (1 American gallon per minute = $6.039 \times 10^{-5} m^3/s$),

ρ_w— 40°F ~ 100°F(4°C-38°C) The density of water in Pound per cubic foot (1b/ft3 = $16.018 kg/m^3$),

ρ —Density of fluid passing through the control valve in Pound per cubic foot,

Δp—Static pressure loss at both ends of the control valve in Pound per square inch (psi), (1 psi = 6894.8 Pa);

$\Delta p_{cv} = 1psi$;

By transforming the above formula, the CV calculation logic shown in the red dotted box in the following figure can be obtained. The unit of feed water temperature is °C, the unit of differential pressure of ARE SCV upstream and downstream is bar, and the unit of density in the temperature-density correspondence function in the following figure is kg/m^3.

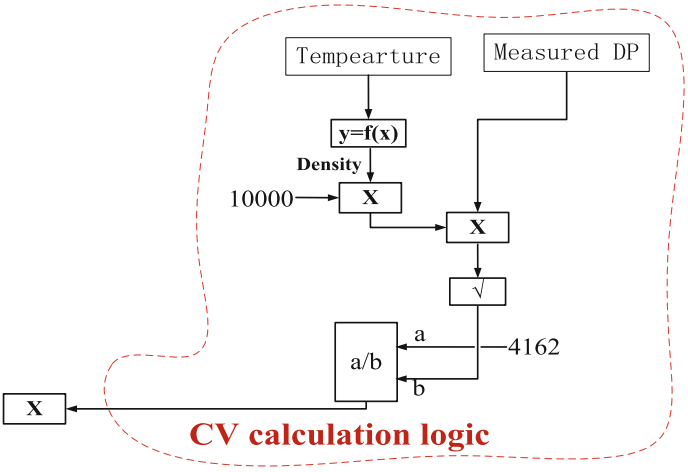


Fig. 4. CV calculation logic of ARE SCV SG level control

The coefficient 4162 in CV calculation logic of Fig. 4 is obtained by dimensional change, and the detailed process is as follows:

$$\begin{aligned} Cv &= Q\sqrt{\left(\frac{\Delta p_{ev}}{\Delta p}\right)\left(\frac{\rho}{\rho_w}\right)} \\ &= \frac{q \div \rho}{6.309 \times 10^{-5}} \times \sqrt{\left(\frac{6894.8}{\Delta P \times 10^6}\right)\left(\frac{\rho}{1000}\right)} \\ &= q \times \sqrt{\frac{1}{10000\rho\Delta P}} \times \frac{\sqrt{6894.8 \times 10^5}}{6.309} \\ &= q \times 4162 \times \sqrt{\frac{1}{10000\rho\Delta P}} \end{aligned} \tag{2}$$

where: Q is mass flow and its unit is kg/s; P is the differential pressure of ARE SCV upstream and downstream, and the unit is MPa; Density in kg/m^3.

3 Test Validation and Optimization

Although accurate CV value can be calculated by CV calculation logic, but the final output of the ARE SCV PID controller is the valve opening instruction. In order to make the ARE SCV opening instruction output accurately, the accurate corresponding relationship between the SCV CV value and its opening is needed.

Because the CV curves provided by valve manufacturers are quite different from the measured CV curves, and the CV curves of valves with the same functional position code of different units in the same manufacturer are also quite different, the ARE SCV CV value calculation test was added during the first start-up of the GEN-III nuclear power plants. Through this test, the CV values corresponding to different opening of ARE SCV are calculated, and the corresponding relationship between CV values and ARE SCV opening is obtained. The corresponding relationship between CV values and opening shown in Fig. 4 is updated in logic configuration to improve the SG level control capability of the plant in the start-up stage.

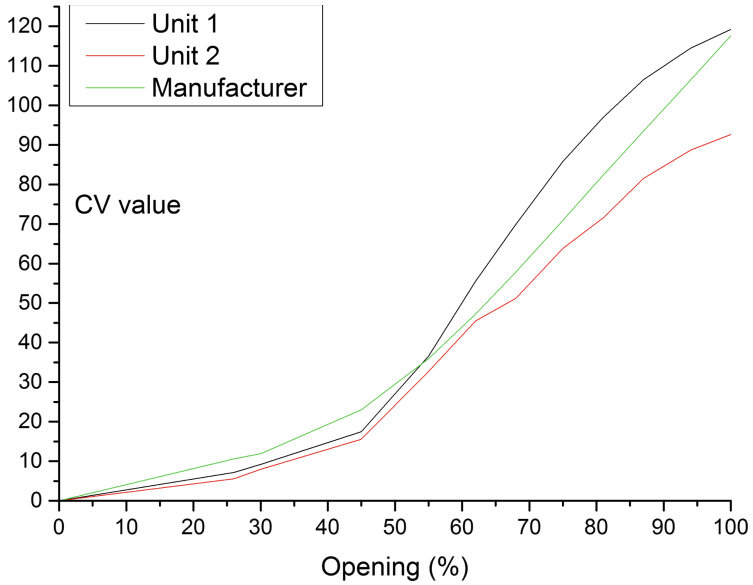


Fig. 5. Corresponding relationship between ARE SCV valve opening and CV value

The Fig. 5 shows the comparison of CV curve provided by ARE SCV manufacturer of a GEN-III nuclear power plant, measured CV curve of unit 1 and measured CV curve of unit 2. Because the comparison of flow coefficient CV is not intuitive, it is converted into the corresponding relationship between flow and opening for comparison. The following are the parameters under normal working conditions of ARE SCV: feed water temperature is 110 °C, differential pressure of ARE SCV upstream and downstream is 3.5 bar, and feed water pressure is 8 MPa. According to the corresponding relationship curve between flow coefficient CV and opening in Fig. 5, it is transformed into the

corresponding relationship between flow rate and valve opening under normal working conditions of ARE SCV. Under normal working conditions, the flow deviation between data provided by valve manufacturers and data measured in unit 1, data provided by valve manufacturers and data measured in unit 2, and the flow deviation between data measured in unit 1 and data measured in unit 2 under different valve opening are shown in the following figure.

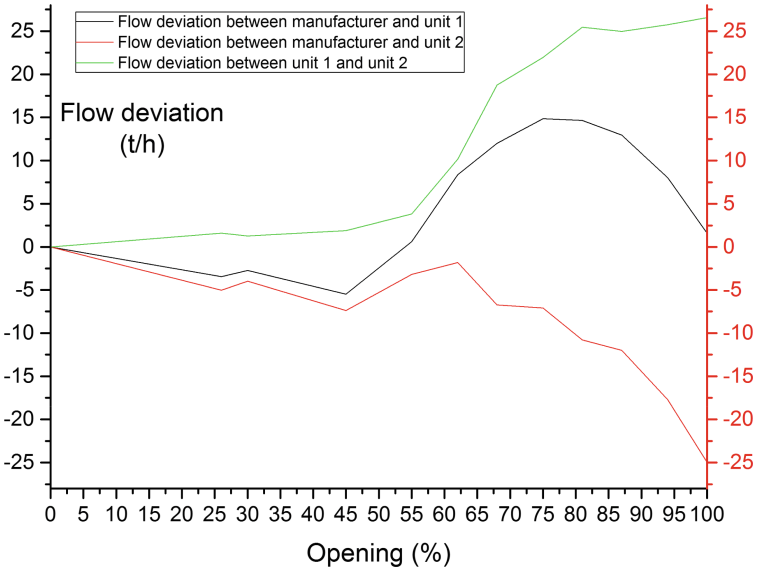


Fig. 6. Flow deviation of ARE SCV with the same opening of a GEN-III nuclear power plant

It can be seen from the Fig. 6 that in the normal working condition of ARE SCV, the maximum flow deviation between the measured data of unit 1 and the manufacturer data at the same opening is 12 t/h, and the average deviation is 5 t/h; Under the same opening, the maximum flow deviation between the measured data of unit 2 and the manufacturer data is −24 t/h, and the average deviation is −8.4 t/h; Under the same opening, the maximum flow deviation between data of unit 1 and data of unit 2 is 26t/h, and the average flow deviation is 13 t/h. During the normal working condition of ARE SCV, the feed water flow rate is about 1 t/h–20 t/h. The flow deviation showed above will leads to the capability difference of SG level control response. So if the corresponding relationship between CV value and opening shown in Fig. 4 is not updated, There will be a big deviation as mentioned above between the required flow rate of PID output and the actual flow rate corresponding to the valve opening, which will result in abnormal SG level control and slow response.

Table 2. Flow deviation under the same opening

Flow deviation	Manufacturer and unit 1	Manufacturer and unit 2	Unit 1 and unit2
Maximum	12 t/h	−24 t/h	26 t/h
Average	5 t/h	−8.4 t/h	13 t/h

4 Control Coupling Problem

From formula (1) and formula (2), it can be seen that the differential pressure of ARE SCV upstream and downstream has a great influence on the flow rate under the same valve opening. And under the same flow rate, the valve opening of different differential pressure is also different. The control principle of AAD differential pressure control valve is shown in the following figure. The differential pressure setpoint of ARE SCV upstream and downstream is given by the main steam pressure according to the corresponding relationship function.

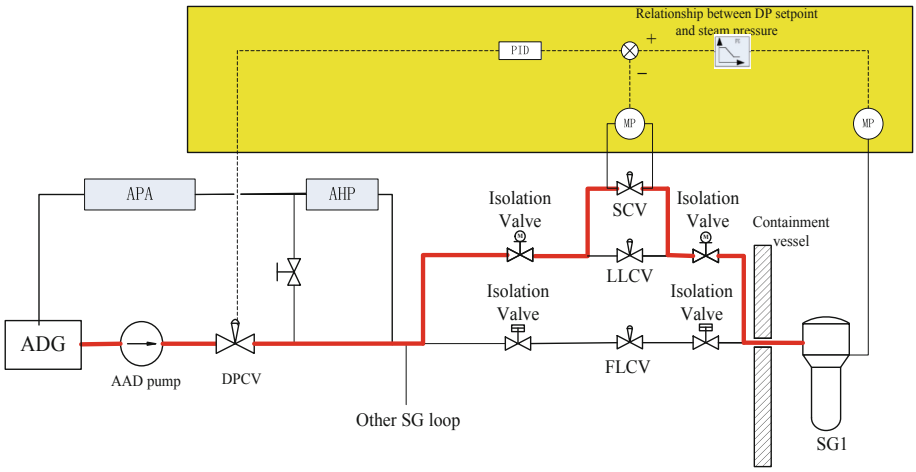


Fig. 7. ARE SCV differential pressure control

As shown in Fig. 7, the differential pressure of ARE SCV upstream and downstream is controlled by control valve located downstream of AAD pump outlet(hereinafter referred to as AAD DPCV). The change of ARE SCV opening will lead to the change of differential pressure △P of ARE SCV upstream and downstream, and then lead to the change of AAD DPCV opening. In the start-up/shutdown stage of the GEN-III nuclear power plant, when the AAD DPCV and the secondary loop of the plant are disturbed, the opening of ARE SCV and AAD DPCV may fluctuate at the same time, but the SG level remains stable around the setpoint during the whole valve fluctuation process. The following figure shows the coupling oscillation curve of AAD DPCV and ARE SCV. The maximum and minimum values of AAD DPCV's opening, ARE SCV's opening, AAD flow rate and SG level during oscillation are shown in Table 3 below.

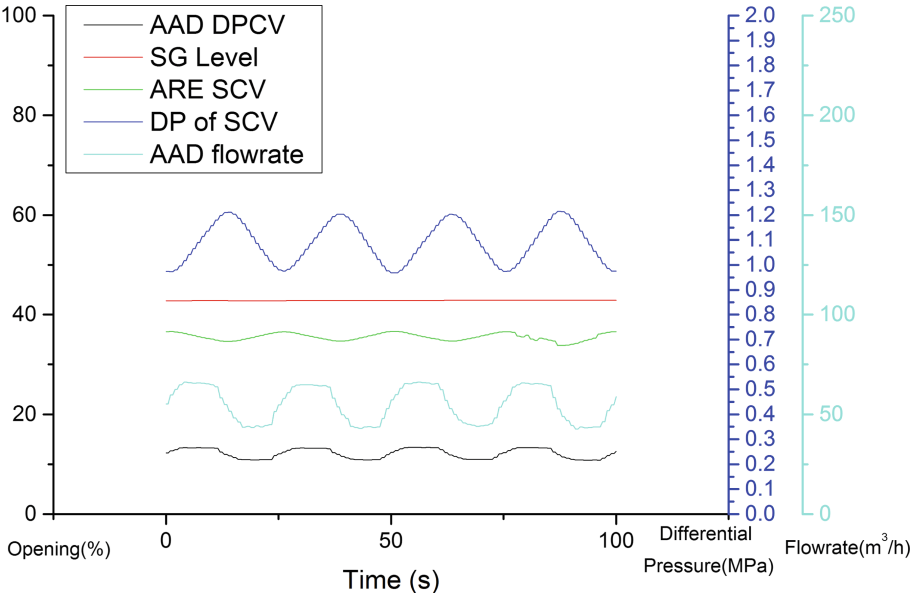


Fig. 8. ARE SCV and AAD DPCV Oscillation

Table 3. Maximum and minimum values of ARE SCV and AAD DPCV oscillation process

Extreme value in coupling process	Opening of AAD DPCV	Opening of ARE SCV	SG level deviation between setpoint and actual value	AAD flowrate	Differential pressure
Maximum	13.39%	36.64%	0.006 m	66.2 m^3/h	1.215 MPa
Minimum	10.81%	33.82%	−0.001 m	42.6 m^3/h	0.968 MPa

It can be seen from the above Table 3 that during the whole oscillation process, SG level is always maintained at its setpoint. So according to Fig. 3 ARE SCV SG Level Control Diagram, we can deduce that the output of ARE SCV PID remains unchanged, and the opening change command of ARE SCV is mainly generated by CV correction logic. The change of ARE SCV opening leads to the change of differential pressure of ARE SCV upstream and downstream, and the change of differential pressure of ARE SCV upstream and downstream makes the output of opening command of ARE SCV change by CV correction logic. However, differential pressure control lag in the partial opening area of AAD DPCV, it is unable to quickly maintain the differential pressure at the setpoint, resulting in oscillation.

5 Solutions

The root cause of ARE SCV and AAD DPCV oscillation is that the opening command of ARE SCV is too sensitive to differential pressure changes, while AAD DPCV PID control lags behind. The solution is to reduce the sensitivity of ARE SCV to differential pressure change, or to improve the response speed of AAD DPCV differential pressure control. According to the above solutions, there are three schemes.

5.1 Change the Correction Logic

The first scheme is that differential pressure, who participates in CV calculation logic as showed in Fig. 4, uses differential pressure setpoint of ARE SCV upstream and downstream, instead of actual measured value of differential pressure. The differential pressure setpoint of ARE SCV upstream and downstream, are only related to the main steam pressure, regardless of nuclear power plants in steady state or transient state can achieve better correction effect.This scheme has a large amount of logical changes, and has higher requirements for AAD DPCV control capability (Fig. 9).

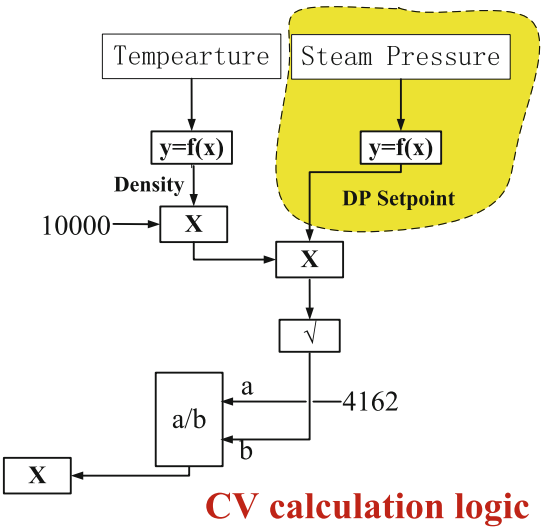


Fig. 9. Change the correction logic

5.2 Improve the Response Speed of Differential Pressure Control

The third scheme is to improve the response speed of AAD DPCV control. AAD DPCV Controller belongs to AAD system. Differential pressure measuring instruments belong to ARE system.The two systems are distributed at different control stations. The maximum transmission delay of DCS network is about 2 s, which causes a large delay to

AAD DPCV control response in differential pressure measurement. So ARE measuring instruments are hardwired to AAD system, instead of network transmission. On the other hand, the first-order filter module is added to the CV calculation logic of ARE SCV control, which makes the response speed of AAD DPCV control faster than that of ARE SCV, thus avoiding the coupled oscillation between ARE SCV and AAD DPCV. However, this scheme will affect the response capability of SG level control.

5.3 Final Solution

Since ARE SCV and AAD DPCV control mostly perform well, and coupling is only an occasional phenomenon. It is solved by temporarily setting ARE SCV from automatic to manual operation, and re-setting ARE SCV to automatic quickly. In the process of reactor start-up, even if there is short-term coupling, the response capability of SG level control is excellent. Considering the cost and benefit comprehensively, the GEN-III nuclear power plant did not adopt the above scheme except differential pressure signals are transmitted by hard wiring, and finally adopted the ARE SCV to be cut into manually operation for a short time to solve the coupling shock problem.

6 Summary

This paper mainly studies the SG level automatic control in the start-up process of the GEN-III nuclear power plants, focusing on the principle and realization method of flow characteristic correction, introducing the experimental Validation and optimization of SG level in the commissioning stage, the coupling problem between ARE SCV and AAD DPCV, the solution idea and scheme of the coupling problem. The ARE SCV and AAD DPCV control scheme can be further optimized.

The capability of automatic control of SG level in the start-up process of the GEN-III nuclear power plant has achieved validation, which has realized the automatic control of SG liquid level in the whole process of start-up and power operation, and improved the intelligent level of nuclear power plants.

References

1. Liu, P., Liu, Y., Luan, Z., Wu, G., Song, F., et al. Improvement and research about the steam generator level control system of a GEN-III Nuclear Power Plant. In: 2019 Chinese Automation Congress (CAC) (2019)
2. Li, F.-Y., Lu, C.-B., Zhang, L.-F.: Improved double PI control for nuclear steam generator water level. Atomic Energy Sci. Technol. (2010)
3. Qian, H., Ye, J.-H., Qian, F.: Transient thermal- hydraulic characteristics analysis software for PWR nuclear power systems. Nucl. Power Eng. (2010)
4. Jizhou, Z., Jianqiang, S., Bin, Z.: Operation of Pressurized Water Reactor Nuclear Power Plant. Atomic Energy Press, Beijing (2008)
5. Guozhen, M., Jisheng, Q.: Commissioning and Start-Up. Atomic Energy Press, Beijing (2000)
6. Ma, Z.-C., Zheng, G.-M., Fang. Z.: Fuzzy control of water level in NPP steam generators at low power. Nuclear Safety (2005)
7. Harris, T.J.: Assessment of control loop performance. Can. J. Chem. Eng. **67**, 856–861 (1989)
8. Yang, Z.-W., et al.: Application of nuclear power plant simulation technology in reactor control system debugging. Nucl. Power Eng. **30**(6), Supplement (2009)

Weakness Analysis and Improvement on the Technical Galleries and Gutters Fire in CPR1000 Nuclear Power Plant

Dan-Dan Sun(✉) and Xu-Tao Bai

Suzhou Nuclear Power Research Institute, Suzhou 215004, Jiangsu, China
baixutao@cgnpc.com.cn

Abstract. This paper firstly analyses the characteristics of fire in the technical galleries and gutters of nuclear power plant, and based on the current situation of some nuclear power plant of China, it introduces the design features of technical galleries and gutters equipment layout, fire prevention zoning, fire detection, fire extinguishing facilities and smoke control and exhaust system. It then analyses the problems and insufficiency of these aspects of the fire protection system of technical galleries and gutters of nuclear power plant, and gives the relevant improvement suggestions.

Keywords: technical galleries and gutters · fire zone setting; fire fighting capacity · fire protection system

1 Introduction

The safe and reliable operation of nuclear power plant is an important prerequisite for the sustainable development of nuclear power industry in China. The comprehensive technical pipe gallery of nuclear power plant is a special tunnel for communication, power, water supply, drainage, steam and other lines and pipelines. It is the nerve and blood vessel of nuclear power plant and is very important to ensure the safe and reliable operation of nuclear power plant. However, there are no specific standards or codes for the fire protection design of the comprehensive technical pipe gallery of nuclear power plant.

The comprehensive technical pipe gallery is located below the ground and connects various plants in the area. The building structure is complex, and the personnel are not familiar with the internal environment and structural trend. It has the disadvantages of coexistence of multiple pipelines, large amount of combustibles, wide connection area and difficult fire fighting. Once a fire occurs, it is extremely easy to spread, which will lead to the expansion of the fire scope, and then have a wide range of impact, and even threaten the safe and stable operation of nuclear power units. Next, the author mainly analyzes the weak links of fire protection in CPR1000 Nuclear Power Plant comprehensive technical pipe gallery, and puts forward corresponding improvement measures and suggestions according to the analysis results.

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 158–167, 2023.
https://doi.org/10.1007/978-981-99-3455-3_16

2 Fire Characteristics of Comprehensive Technical Pipe Gallery

Under the normal operation of the unit, the combustible materials in the comprehensive technical pipe gallery are mainly power cables, control cables and pipeline insulation materials, specifically: Line filler, line insulation layer and protective layer, insulation filler, and solid fire loads such as lighting, fire fighting, security system operation equipment in the pipe gallery. In special cases, there may be gas fire loads such as combustible gas released from drainage pipeline or leaked from hydrogen generation station [2].

According to the characteristics of fire load and operating equipment in the comprehensive technical pipe gallery, the main causes of fire in the comprehensive technical pipe gallery are as follows:

(1) Equipment short circuit: electrical equipment or power cable of lighting system, fire fighting system and security system in the pipe gallery has short circuit fault, resulting in electric spark and causing fire [3];
(2) Line overload, overheating: power cable overload, resulting in line overheating, easy to cause fire;
(3) Fire operation: when fire operation is involved in the maintenance and transformation of the pipe gallery, if the protection measures for fire operation are not in place, it is easy to cause fire;
(4) Smoldering of fallen leaves and sundries: the terrain in the pipe gallery is complex, and there are few people passing through in some areas. After falling and accumulating from the ventilation shaft, fallen leaves and sundries are prone to smoldering and fire in summer.

The function of the comprehensive technical pipe gallery is to provide the laying place for the required process pipes and cables for most buildings (structures) in the plant area. At the same time, it is required to facilitate the inspection and maintenance of the laid pipes and cables. Because of its long laying distance, many types of equipment, large number of branches and complex structure, the comprehensive technical pipe gallery has high fire risk; moreover, once a fire occurs, it is very difficult to put out and evacuate.

Taking the underground comprehensive technical pipe gallery of a nuclear power plant in China as an example, its total length is about 3,400 m, connecting 34 plants including steam turbine plant, electrical plant, hydrogen generation station, switch station and comprehensive office building. The specific layout of the underground utility tunnel is shown in Fig. 1.

The comprehensive technical pipe gallery of CPR1000 Nuclear Power Plant is a network structure, including ring structure and multi branch structure in some parts. The overall structure has many branches and the layout is complex, which puts forward higher requirements for the sensitivity of fire detection system, the effectiveness of fire separation and the completeness of fire extinguishing system [4].

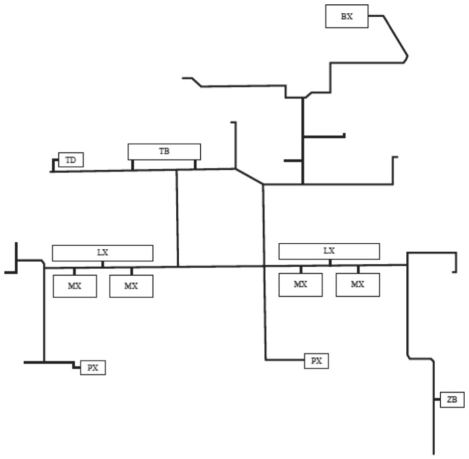


Fig. 1. Layout of Underground Comprehensive Technical Pipe Gallery of a CPR1000 NPP

3 Fire Design Status of Comprehensive Technical Pipe

3.1 Cable Tray and Pipeline Layout

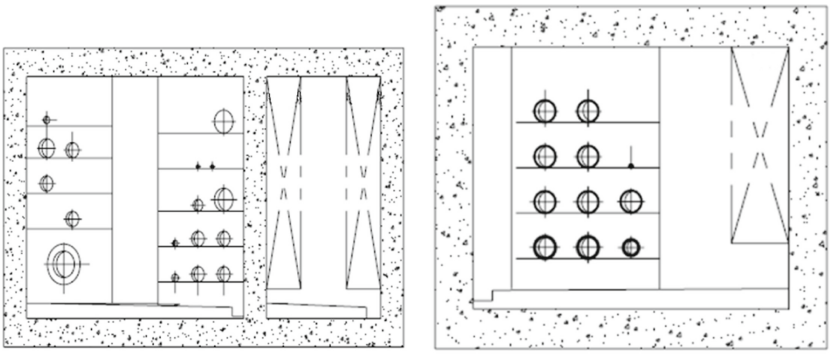
The layout of cable tray and pipeline in the integrated technical pipe gallery of nuclear power plant is mainly divided into the following types,As shown in Fig. 2.

Figure 2. Layout of cable tray and pipeline in integrated technology pipe gallery.

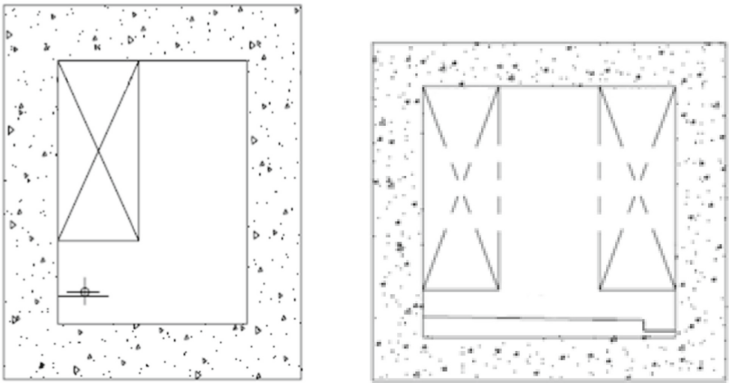
(1) When the number of cable tray is large, the cable tray and process pipe are laid in a separate pipe gallery, with partition wall in the middle, or in the same Gallery, the cable tray is laid above or on the side of the pipe;
(2) The process pipeline is arranged on one side of the corridor, the cable tray is arranged on the other side, and 0.8 m pedestrian passage is reserved in the middle;
(3) The pipeline and cable tray in the corridor are arranged on the same side, and the pipeline is arranged below the cable tray;
(4) Pure cable gallery, only cable tray is arranged in the gallery.

3.2 Fire Compartment and Zoning

Crosslinked polyethylene cable insulated and low smoke halogen-free flame retardant polyolefin sheathed cables are used in the underground corridor; The power cable and control cable are arranged in layers; Due to space limitation, the power cable and control cable are laid on the same layer of tray, and the partition board is set to separate them; Each building expansion joint in the corridor (with a spacing of about 20 m) is provided with an independent fire wall, and the entrance to the ground building is provided with a fire wall to prevent the spread of fire [5].



a) Partition layout b) Bilateral layout



c) One side mixed layout d) Cable tray layout only

Fig. 2. layout of cable tray and pipeline in integrated technology pipe gallery

In the design of comprehensive technical pipe gallery of nuclear power plant, according to the code for fire protection design of buildings, the underground gallery is divided into fire zones according to the units, and the fire extinguishing system is set up uniformly. For example, there are four units in a nuclear power plant, and the underground comprehensive technical gallery is mainly used for the connection of auxiliary buildings, which is divided into a fire compartment as a whole [6].

3.3 Fire Detection Mode

The fire detection in the underground corridor is mainly based on the early detection of cable fire. In the comprehensive technical pipe gallery with cables, the fire detection method of combining the point type photoelectric smoke detector with the cable type linear temperature sensing cable is adopted; in the pipe gallery with only pipelines inside, the fire detection device is not set. Among them, the point type photoelectric smoke detector is installed in the middle of the ceiling, and the protection radius is less than 6 m; the cable type linear temperature sensing cable is laid close to the cable surface

in the form of sine wave according to the number of layers of cable laying. All detection equipment in each comprehensive technical pipe gallery is designed according to the same fire compartment.

3.4 Fire Fighting Facilities

In the comprehensive technical pipe gallery, mobile fire extinguisher is the main fire extinguishing facility, and fixed fire extinguishing device is not set. MF/ABC8 type fire extinguisher shall be equipped at the position where hydrogen pipeline passes according to class C fire serious danger level, and the protection spacing shall be less than 18 m; MF/ABC3 type fire extinguisher shall be equipped at other positions according to the protection spacing less than 30 m.

3.5 Smoke Control and Lighting System

A certain number of installation holes are set in the comprehensive technical pipe gallery. After the installation, ventilation shutters are made on both sides of the mounting holes exposed to the ground, the smoke control and exhaust is mainly natural ventilation, and the active smoke control and exhaust system and smoke retaining wall are not set.

The comprehensive technical pipe gallery is a technical workshop, which is equipped with normal lighting and emergency lighting. The normal illumination is required to be 100 lx. One emergency lighting lamp is set in every three lamps. The emergency lighting is powered by the corresponding emergency lighting distribution box, and the lamps are equipped with batteries. When both normal lighting and emergency lighting fail, the batteries of the emergency lamps can provide the necessary lighting for one hour, so as to ensure the safe evacuation of operators. Sealed industrial single tube fluorescent lamp is selected for normal lighting and emergency lighting.

4 Analysis of Weak Links in Fire Fighting

4.1 Unreasonable Division of Fire Compartment

According to the requirements of code for fire protection design of conventional island of nuclear power plant, the length of each fire compartment in cable trench, cable tunnel and complex corridor containing oil pipeline or cable shall not be more than 200 m. At present, the design of underground corridor fire compartment is different from the requirements of code for fire protection design of conventional island of nuclear power plant [7]. There is no physical partition between the whole underground corridors. In case of fire, the fire wall only set between the bridges will not be able to effectively prevent the spread of fire.

4.2 Single Type of Fire Detection

At present, the comprehensive technical pipe gallery of domestic nuclear power plant only monitors the automatic fire alarm system in the area where cables are laid. Some

nuclear power plants use the combination of point type photoelectric smoke detector and cable type linear temperature sensing cable or temperature sensing optical fiber for monitoring, and some nuclear power plants use cable type linear temperature sensing cable or temperature sensing optical fiber for single detection. For areas without cables, no fire detection device is provided. Therefore, there is a blind area for monitoring. Once there is a fire in the auxiliary equipment or oil-bearing and hydrogen containing pipeline in this area, it is difficult to find and respond in time. In addition, there is no combustible gas detection device in the connection section with the combustible gas production plant; The lighting, ventilation and other equipment in the pipe gallery are non explosion proof devices. Once the combustible gas enters the pipe gallery, it is easy to deflagration.

4.3 Insufficient Fire-Fighting Facilities and Single Form

In the comprehensive technical pipe gallery, the fire-fighting facilities are only equipped with mobile fire extinguisher, which can not meet the fire fighting demand in the comprehensive technical pipe gallery. Due to the complexity of the layout of the comprehensive technical pipe gallery, it is difficult for the fire brigade to reach the fire site at the first time to put out the fire after the fire, which is likely to spread in a large area. When a fire occurs, the portable fire extinguisher can not meet the needs of fire fighting.

4.4 Insufficient Smoke Control Facilities

Lack of smoke control facilities, natural ventilation measures can not meet the fire requirements. There are no smoke control facilities in the corridor, only ventilation shutters are installed on both sides of the installation holes on the corridor.

5 Suggestions for Improvement Measures

5.1 Optimize the Fire Zone Setting

Taking a comprehensive technical pipe gallery of a CPR1000 Nuclear Power Plant as an example, its total length is about 3,400 M. according to the requirements of the code for fire protection design of conventional island of nuclear power plant, combined with the actual functions and building structure of the comprehensive technical pipe gallery, the following rules are used for division:

(1) Fire wall shall be set at the interface between corridor and workshop (or trench) to prevent the interaction between the workshop and the comprehensive technical pipe gallery in case of fire;
(2) When the cable gallery is above or at the side of the pipeline corridor, the cable gallery shall be divided into fire prevention zones according to the requirements of the code for fire protection design of conventional island of nuclear power plant. Only the isolation walls are set at both ends of the corridor at the pipeline side, and the pipeline corridor and cable gallery shall be physically separated to avoid the fire interaction;

(3) When the pipes and cables are in the same corridor, fire protection zones shall be carried out according to the requirements of the specification.

According to the above rules, the comprehensive technical pipe gallery can be divided into 20 fire zones [8]. The fire protection zones are physically isolated by fire barriers, which limit the fire to the fire zone, isolate the potential fire, minimize the risk of fire spread and the consequent pollution caused by corrosive gases, fire extinguishing agents, smoke and other pollution.

Concrete solid block wall is added at the connection between corridor and each sub item to meet the fire isolation requirements. According to the different status of the connection between the sub items and the corridor, the following different ways are adopted:

(1) The corridor and sub items are connected in the form of shallow ditch. When there is no need and feasibility for people to pass, the wall can be completely blocked in proper position;
(2) When there is a need for personnel passing through the corridor and sub item connection, the wall can be built on one side of the sub building, and the door hole for personnel passing through the wall shall be reserved, and fire doors meeting the fire resistance limit requirements shall be installed; if the masonry wall on one side of the sub item building cannot be realized, it can be blocked on the corridor side. That is, according to the actual pipeline layout on site, fire isolation is carried out in the place near the connection and less bridge is convenient for masonry wall. Meanwhile, personnel passageway is reserved and fire door meeting fire resistance limit requirements is installed.

Since the wall is built after various pipe bridges are installed in place, the openings where the objects passing through the wall cannot be accurately positioned in the design stage, so the construction unit shall cooperate closely with the construction site according to the pipeline layout. Moreover, the holes in the wall need to be sealed to meet the fire protection requirements of the wall.

5.2 Optimize Fire Detection Methods

Because the active ventilation system is not set in the comprehensive technical pipe gallery and the drainage of some sections is not smooth, the water in the pipe gallery in rainy season is serious. Fire detector is in high humidity environment for a long time, and the failure rate in summer is high, which brings some hidden danger to fire monitoring. It is suggested that while strengthening ventilation and dehumidification and reducing environmental humidity, we should select detection devices (such as infrared flame detector, infrared smoke detector, etc.) with large detection range and high humidity resistance to supplement the existing detection methods.

There is a situation where hydrogen pipeline and cable share in some sections of underground corridor. Combustible gas detection device is not set in this section. If the pipeline leaks, the leakage can not be found by existing fire detection methods. Therefore, combustible gas detection device should be added in the section where hydrogen pipeline is laid and controlled in linkage with hydrogen production equipment.

5.3 Improve Fire Fighting Capacity

The main equipment of the comprehensive technical pipe gallery is mobile fire extinguisher, and no fixed fire extinguishing system is set. This kind of setting of underground corridor fire extinguishing system can only meet the requirements of the norms and regulatory departments under the conditions at that time. In the face of increasingly severe fire situation and constantly improving fire fighting standards, it can not meet the requirements. The water spray/dry powder extinguishing device in the cable tunnel is also stipulated in the code for fire protection design of the conventional island of the nuclear power plant. Therefore, fire extinguishing system should be added according to the actual situation of corridor. Combined with the relevant specifications at home and abroad, the fixed fire extinguishing systems that can be used in the integrated gallery and cable corridor include the following: automatic sprinkler system, water spray fire extinguishing system, gas fire extinguishing system, high pressure water mist, and ultrafine dry powder.

(1) Automatic sprinkler system. Water spray system can be used for cable gallery and cable layer specified in code for fire protection design of nuclear power plant. The corresponding fire protection transformation has been completed at Dayawan Nuclear Power Station and Lingao phase I nuclear power plant in China, and no adverse feedback has been made at present. If such fire extinguishing facilities are set, the cables in the underground comprehensive pipe gallery shall be cut off in time after the fire to avoid electric shock and fire drainage.
(2) water spray fire extinguishing system. In domestic related industrial standards, water spray fire extinguishing system is recommended for cable tunnels. Water spray fire extinguishing system uses water spray nozzle to smash water powder into fine water droplets, then spray onto the surface of the burning substance, and extinguish the fire by surface cooling, asphyxiation, emulsification and dilution. Water spray fire extinguishing system is widely used in electrical fires due to its electrical insulation characteristics. However, combined with the characteristics of underground integrated pipe corridors, there are the following problems in water spray: the distance between the electrical corridors and the integrated corridors of nuclear power plants is longer, and the water spray system is an open system. In order to control the fire water volume, it needs to be divided into multiple fire zones, and a sprinkling valve room near the fire prevention sub zone is set up. This will cause too many deluge valves, complex system, and difficult to reconstruct in the nuclear power plant [9].
(3) Gas fire extinguishing system. The fire extinguishing mechanism of gas fire extinguishing system is mainly suffocation, isolation and chemical suppression. The fire extinguishing agent is carbon dioxide and heptafluoropropane, etc. to extinguish the fire in the way of full submergence. The underground comprehensive technical pipe gallery is a large space. If gas fire extinguishing system is set, it needs to be divided into several protection areas, with large gas cylinder volume and complex system setting; in addition, the requirements for sealing and pressure relief port cannot be realized. Therefore, gas fire extinguishing system is not suitable for underground integrated technology pipe gallery.
(4) Automatic fire extinguishing device for dry powder. At present, the hanging dry powder automatic fire extinguishing device is widely used in cable layer and cable

tunnel, which has the characteristics of small volume, convenient installation and quick alarm. It can extinguish local or large space type A, B, C, e and f fires, which need to be replaced once in 5–10 years. The dry powder automatic fire extinguishing device has no pipe network, normal pressure, no daily maintenance, simple design and convenient installation. Compared with the water spray fire extinguishing system, there is no need for the rain valve room, there is no complicated pipe network and valves, and the initial project investment is relatively small. In recent years, the well-known ultra-fine dry powder fire extinguishing system has the characteristics of less consumption, good effect, anti burning, moisture failure and long life (up to 10 years).

In conclusion, considering the advantages and disadvantages of the above fire extinguishing methods, combined with the space restriction of the comprehensive pipe gallery and the experience of corridor fire fighting transformation in the nuclear power plant, it is suggested to adopt water spray or ultra fine dry powder fire extinguishing system for the fire fighting transformation of the comprehensive pipe gallery in the nuclear power plant; meanwhile, due to the limited site, the system setting can be simplified appropriately.

5.4 Add Active Smoke Control System

At present, the ventilation of underground gallery mainly adopts preset ventilation holes and shutters to ventilate and smoke in normal and accident conditions. In case of fire, these vents and shutters can not effectively prevent the spread of toxic smoke. In order to improve the corridor environment, reduce the failure rate of fire system, ensure that smoke can be effectively prevented during fire and prevent the spread of fire, active ventilation system should be added in sections. During normal operation, according to the change of temperature and humidity, the environment in the comprehensive technical pipe gallery shall be adjusted to prevent a large number of alarms caused by excessive humidity and affect fire monitoring; in case of accident, the fire area shall be isolated in time to prevent the spread of smoke and gas and timely discharge the smoke and gas out of the corridor.

6 Conclusion

By analyzing the characteristics of the fire protection design of the comprehensive technical pipe gallery, combined with the layout, fire load and fire characteristics of the comprehensive technical pipe gallery of the nuclear power plant.Some suggestions for fire protection design improvement are put forward, such as optimizing the setting of fire compartment, strengthening fire detection means, improving fire extinguishing capacity and adding active smoke control system.These promotion means can effectively enhance the fire prevention and control capacity of the integrated technical pipe gallery and provide basic guarantee for the safe and stable operation of the nuclear power plant.

References

1. Zheng, Y.: Analysis of fire protection characteristic of thermal power plant and effective solution. Mod. Archit. Electric **2**, 35–37 (2011)

2. Yun, Z., Hua, W., Yanping, Z.: Further discussion on fire protection design of underground utility tunnel. Water Wastewater Eng. **43**, 117–119 (2017)
3. Rongzhou, D., Jun, H., Bingkui, Y.: The fire extinguishing system design and analysis on comprehensive pipe rack. Shanxi Archit. **23**, 23–25 (2018)
4. Wei-jun, S., Jie, W.: Discussion on fire monitoring and alarm technology for comprehensive pipeline. Fire Sci. Technol. **42**, 120–122 (2016)
5. Yinhui, Y., Wei, S.: Wang chuang study and application of PWR fire vulnerability analysis. Nuclear Saf. **13**, 57–60 (2014)
6. Lizhong, Y., Kai, Y.: A review of research on fire safety codes and fire science in urban utility tunnels. China Saf. Sci. J. **31**, 132–138 (2021)
7. Yanyun, G., Fengnian, A., Xuefeng, Q.: Discussion on fire protection design of utility tunnel. Municipal Eng. Technol. **39**, 109–114 (2021)
8. Weiguang, A., Tao, W., Kai, L.: Numerical simulation on cable fire in T-shaped underground pipe gallery. Fire Sci. Technol. **39**, 1120–1123 (2020)
9. Hongfu, M., Yaling, L., Wenjing, Y.: Research on optimization control mode of smoke for cable fire in utility tunnel based on FDS. J. Saf. Sci. Technol. **16**, 100–105 (2020)

Response Time Analysis Method of Safety-Level DCS in Nuclear Power Plant Based on Probability Theory

Jing Wen(✉), Xian-Jian He, Zhao Chen, Zi-Yuan Wan, and Zhi-Qiang Wu

Science and Technology on Reactor System Design Technology Laboratory, Nuclear Power Institute of China, Chengdu 610000, China
960989410@qq.com

Abstract. Aiming at the incompleteness and inadequacy of the response time analysis method of the current nuclear power plant safety-level digital-control system (DCS), this paper proposes an analysis method based on probability theory for the response time of nuclear power plant safety-level DCS. Firstly, according to the structure and characteristics of the safety-level DCS, the probability model of the response time of the safety-level DCS is established, and the calculation method of the probability distribution of the response time is obtained. Then, according to the obtained calculation method and the parameters of the engineering example, the rang of the response time and the probability density function are calculated, and the response time of the engineering example is simulated, and the simulated response time rang, frequency and probability density function fitting curve are obtained. Finally, the response time of the engineering example is tested by the response time automatic test device, a large amount of data with statistical significance is obtained. After the data is processed, the range, frequency and probability density fitting curve of the response time are obtained. By comparing the theoretical calculation results, simulation results and test results of engineering examples. The correctness and feasibility of the analysis method are verified.

Keywords: nuclear power plant · Safety-level DCS · response time · probability theory · analysis method

1 Introduction

As the "central nervous system" of the nuclear power plant, the safety-level digital control system (DCS) of the nuclear power plant mainly realizes the emergency shutdown function and the driving function of the special safety facilities, and is an important system to ensure the safe and reliable operation of the nuclear power plant [1]. The shutdown response time and the drive response time of the special safety facility are its key performance indicators, and strict analysis and verification are required to confirm whether the design requirements are met.

At present, the response time analysis method of DCS system is to calculate the maximum time of the whole signal transmission link. Firstly, analyze the signal transmission

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 168–178, 2023.
https://doi.org/10.1007/978-981-99-3455-3_17

path and identify each module or device passing through the signal transmission path, then obtain the maximum response time of each module according to the performance parameters of each module or device, and finally add the maximum response time of each module or device to obtain the maximum response time of the whole link [2]. This method has limitations. Due to the randomness of DCS system response time, only analyzing the maximum response time of the system can not fully reflect the characteristics of system response time. Therefore, a response time analysis method based on probability theory is proposed in this paper, and the correctness of this method is verified by calculation, simulation and experiment.

2 Response Time Analysis

The overall idea is to identify the modules or devices passing through the signal transmission link in DCS, analyze the characteristics of each module and device, so as to obtain their respective response time probability distribution law, and finally analyze the relationship between each module and device to obtain the response time probability model of the whole path.

2.1 Response Time Analysis Example

Taking an engineering simulation based on the advanced safety-level DCS platform (NASPIC) independently developed by China Nuclear Power Research and Design Institute as an example, its structure is shown in Fig. 1, in which the equipment in the gray area is the engineering simulation, and the rest are for coordination test equipment. The response time of a specially designed drive function in the simulation is selected for analysis. The trigger signal of this function is injected by the signal conditioning cabinet (PIPS), and after logical operations in the protection group processing cabinet (RPC) and the special processing cabinet (ESFAC), the control optimization is performed. The Priority Logic Selection Module (PLM) in the drive cabinet outputs commands.

2.2 Response Time Signal Path Analysis

The selected special response time signal path is shown in Fig. 2. In the RPC, the on-site sensor signal is conditioned and distributed through the signal conditioning module (PA), collected by the analog input module (AI), logically calculated by the main control module (MPU), and then passed through point-to-point the communication is sent to the ESFAC for operation, and the PLM output is controlled by the switch output module (DO) after the ESFAC operation.

The above process is decomposed into each physical module according to the asynchronous characteristics among the modules, as shown in Fig. 3.

According to the above decomposition results, the response time (T_{ES}) of the driving function of special safety facilities is:

$$T_{ES} = T_{RPC} + T_{ESFAC} \tag{1}$$

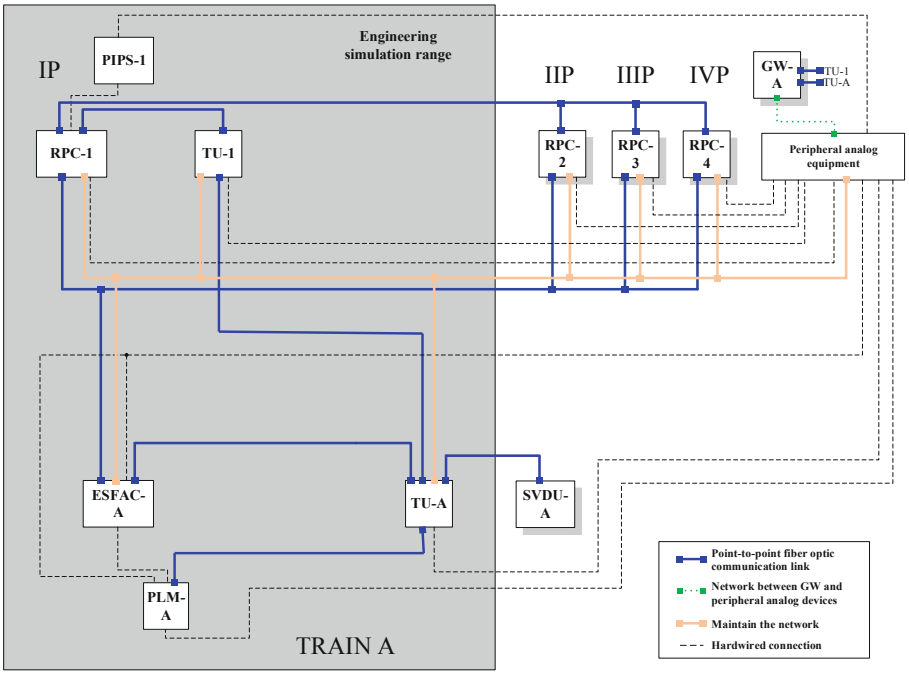


Fig. 1. Schematic diagram of analysis example

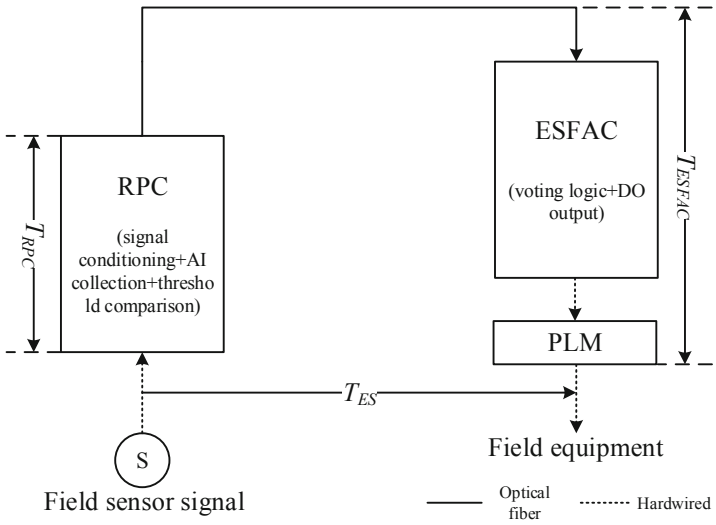


Fig. 2. Schematic diagram of response time path of driving signal of special safety facilities

$$T_{RPC} = T_{IS} + T_{AI} + T_{MPU-I} + T_{COM-I} \tag{2}$$

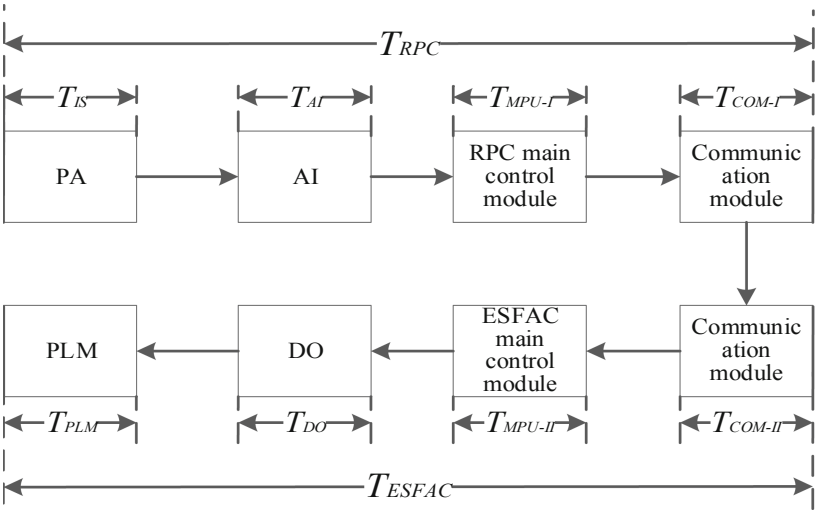


Fig. 3. Response time decomposition diagram of module

$$T_{ESFAC} = T_{COM-II} + T_{MPU-II} + T_{DO} + T_{PLM} \tag{3}$$

According to the characteristics of naspic platform module, T_{IS} and T_{PLM} can be considered as fixed time, and T_{AI}, $T_{COM\text{-}I}$, $T_{COM\text{-}II}$, $T_{MPU\text{-}I}$, $T_{MPU\text{-}II}$ and T_{DO} are random variables varying in a certain range. Therefore, according to the comprehensive formulas (1), (2) and (3), TEs can be simplified as:

$$T_{ES} = T_{AI} + T_{MPU-I} + T_{COM-I} + T_{COM-II} + T_{MPU-II} + T_{DO} + C \tag{4}$$

where C is a constant whose value is equal to the sum of T_{IS} and T_{PLM}.

2.3 Probability Distribution of $T_{MPU\text{-}I}$, $T_{MPU\text{-}II}$

The main control module (MPU) adopts fixed cycle operation processing, and its CPU cycle (t_{CPU}) is composed of CPU processing time (t_P) and idle time (t_I). $t_P$divided by t_{CPU} is CPU load (l_{CPU}), and the relationship is:

$$t_{CPU} = t_P + t_I \tag{5}$$

$$l_{CPU} = \frac{t_P}{t_{CPU}} \tag{6}$$

As shown in Fig. 4, when the signal reaches the MPU, the response time T_{MPU} range is:$t_{CPU} \times l_{CPU} \sim t_{CPU} \times (1 + l_{CPU})$. Due to the randomness of signal arrival time, the probability density function of T_{MPU} satisfies uniform distribution, that is, $T_{MPU} \sim U($ $t_{CPU} \times l_{CPU}, t_{CPU} + t_{CPU} \times l_{CPU})$. The probability density function is:

$$f_{MPU}(x) = \begin{cases} \frac{1}{t_{CPU}}, & t_{CPU} \times l_{CPU} \le x \le t_{CPU} \times (1 + l_{CPU}) \\ 0, & other \end{cases} \tag{7}$$

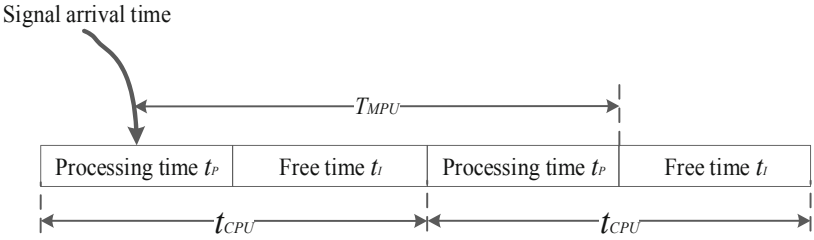


Fig. 4. Range analysis diagram of "T_{MPU}"

2.4 Probability Distribution of T_{AI}, T_{DO}, $T_{COM\text{-}I}$, $T_{COM\text{-}II}$

The analog input module (AI) operates according to a certain period (t_{SAI}), as shown in Fig. 5. The response time T_{AI} range is: $t_{SAI} \sim 2t_{SAI}$. Due to the randomness of signal arrival time, the probability density function of T_{AI} satisfies uniform distribution, that is, $T_{AI} \sim U(t_{SAI}, 2t_{SAI})$. The probability density function is:

$$f_{AI}(x) = \begin{cases} \frac{1}{t_{SAI}}, & t_{SAI} \le x \le 2t_{SAI} \\ 0, & other \end{cases} \tag{8}$$

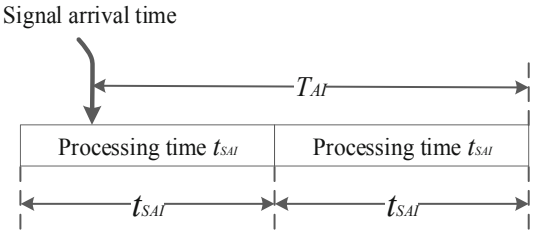


Fig. 5. Range analysis diagram of "T_{AI}"

Similarly, the switching value output module (DO) and communication module (COM) operate according to a certain cyclet_{SDO} and t_{SCOM} respectively, so the response time T_{DO} range is: $t_{SDO} \sim 2t_{SDO}$ and T_{COM} range is: $t_{SCOM} \sim 2t_{SCOM}$. Due to the randomness of signal arrival time, the probability density functions of T_{DO} and T_{COM} meet uniform distribution, that is,$T_{DO} \sim U(t_{SDO}, 2t_{SDO})$ and $T_{COM} \sim U(t_{SCOM}, 2t_{SCOM})$. The probability density functions are:

$$f_{DO}(x) = \begin{cases} \frac{1}{t_{SDO}}, & t_{SDO} \le x \le 2t_{SDO} \\ 0, & other \end{cases} \tag{9}$$

$$f_{COM}(x) = \begin{cases} \frac{1}{t_{SCOM}}, & t_{SCOM} \le x \le 2t_{SCOM} \\ 0, & other \end{cases} \tag{10}$$

2.5 Probability Distribution of T_{ES}

It can be seen from the above analysis that T_{ES} is obtained by adding T_{AI}, $T_{MPU\text{-}I}$, $T_{COM\text{-}I}$, $T_{COM\text{-}II}$, $T_{MPU\text{-}II}$ and T_{DO} six independent random variables that satisfy uniform distribution and the constant C. Assuming that the probability density functions of T_{AI}, $T_{MPU\text{-}I}$, $T_{COM\text{-}I}$, $T_{COM\text{-}II}$, $T_{MPU\text{-}II}$ and T_{DO} are $f_{AI}(x)$, $f_{MPU\text{-}I}(y)$, $f_{COM\text{-}I}(z)$, $f_{COM\text{-}II}(u)$, $f_{MPU\text{-}II}(v)$ and $f_{DO}(w)$, respectively, the probability distribution function $M(t)$ and probability density function $m(t)$ of T_{ES} are respectively as shown in formulas (12) and (13) [3]:

$$n(x, y, z, u, v, w) = f_{AI}(x) \cdot f_{MPU-I}(y) \cdot f_{COM-I}(z) \cdot f_{COM-II}(u) \cdot f_{MPU-II}(v) \cdot f_{DO}(w) \tag{11}$$

$$M(t) = \int_{x+y+z+u+v+w \le t-C} n(x, y, z, u, v, w)dxdydzdudvdw \tag{12}$$

$$m(t) = (f_{AI} * f_{MPU-I} * f_{COM-I} * f_{COM-II} * f_{MPU-II} * f_{DO})(t - C) \tag{13}$$

3 Response Time Calculation and Simulation

3.1 Response Time Calculation

The engineer station reads the values of the configuration cycle (TCPU) and main control load (LCPU) of the main control module in RPC and ESFAC, so as to obtain the probability density functions of $T_{MPU\text{-}I}$ and $T_{MPU\text{-}II}$. According to the response time performance parameters of PA, AI, DO, COM and PLM (the parameters are not listed here because of business secret), the probability density functions of T_{AI}, $T_{COM\text{-}I}$, $T_{COM\text{-}II}$ and T_{DO} and the value of constant C are obtained, and then the probability density function $m(t)$ of T_{ES} is calculated by Eq. (13). The function expression is shown in Eq. (14), and the function image is shown in Fig. 6. The maximum value, minimum value and average value are 150.4 ms, 40.2 ms and 95.3 ms respectively.

From Eq. (14), it can be seen that the probability density function is a polynomial piecewise function, which has good characteristics: continuity, monotonicity, symmetry and differentiability, which is very similar to the probability density of normal distribution. Since the value range of $T_{MPU\text{-}I}$ and $T_{MPU\text{-}II}$ is much larger than that of T_{AI}, $T_{COM\text{-}I}$, $T_{COM\text{-}II}$ and T_{DO}, $T_{MPU\text{-}I}$ and $T_{MPU\text{-}II}$ have a great influence on the probability density of T_{ES}. Therefore, the probability density function image of T_{ES} shown in Fig. 6 is similar to a triangular distribution. If the value ranges of the random variables (T_{AI}, $T_{MPU\text{-}I}$, $T_{COM\text{-}I}$, $T_{COM\text{-}II}$, $T_{MPU\text{-}II}$, T_{DO}) that make up T_{ES} are not much different, then the normal distribution probability density can be used for a good approximation [4].

$$
m(t)=\frac{1}{1093500}\times\begin{cases}
0 & (t<40.2)\\
\frac{1}{120}(t-40.2)^5 & (40.2\le t<43.2)\\
\frac{1}{8}(t-43.2)^4+\frac{3}{4}(t-43.2)^3+\frac{9}{4}(t-43.2)^2+\frac{27}{8}(t-43.2)+\frac{81}{40} & (43.2\le t<45.2)\\
-\frac{1}{60}(t-45.2)^5+\frac{1}{8}(t-45.2)^4+\frac{7}{4}(t-45.2)^3+\frac{39}{4}(t-45.2)^2+\frac{203}{8}(t-45.2)+\frac{1031}{40} & (45.2\le t<47.4)\\
-\frac{1}{40}(t-47.4)^5-\frac{7}{120}(t-47.4)^4+\frac{613}{300}(t-47.4)^3+\frac{34733}{1500}(t-47.4)^2+\frac{1455853}{15000}(t-47.4)+\frac{56059973}{375000} & (47.4\le t<48.2)\\
-\frac{1}{120}(t-48.2)^5-\frac{19}{120}(t-48.2)^4+\frac{509}{300}(t-48.2)^3+\frac{41561}{1500}(t-48.2)^2+\frac{2067869}{15000}(t-48.2)+\frac{91114601}{375000} & (48.2\le t<50.2)\\
-\frac{29}{120}(t-50.2)^4+\frac{29}{300}(t-50.2)^3+\frac{50131}{1500}(t-50.2)^2+\frac{3949709}{15000}(t-50.2)+\frac{240109051}{375000} & (50.2\le t<50.4)\\
\frac{1}{120}(t-50.4)^5-\frac{29}{120}(t-50.4)^4-\frac{29}{300}(t-50.4)^3+\frac{50131}{1500}(t-50.4)^2+\frac{4150291}{15000}(t-50.4)+\frac{260359051}{375000} & (50.4\le t<52.4)\\
\frac{1}{40}(t-52.4)^5-\frac{19}{120}(t-52.4)^4-\frac{509}{300}(t-52.4)^3+\frac{41561}{1500}(t-52.4)^2+\frac{6032131}{15000}(t-52.4)+\frac{516364601}{375000} & (52.4\le t<53.2)\\
\frac{1}{60}(t-53.2)^5-\frac{7}{120}(t-53.2)^4-\frac{613}{300}(t-53.2)^3+\frac{34733}{1500}(t-53.2)^2+\frac{6644147}{15000}(t-53.2)+\frac{643309973}{375000} & (53.2\le t<55.4)\\
\frac{1}{8}(t-55.4)^4-\frac{7}{4}(t-55.4)^3+\frac{39}{4}(t-55.4)^2+\frac{4117}{8}(t-55.4)+\frac{111191}{40} & (55.4\le t<57.4)\\
-\frac{1}{120}(t-57.4)^5+\frac{1}{8}(t-57.4)^4-\frac{3}{4}(t-57.4)^3+\frac{9}{4}(t-57.4)^2+\frac{4293}{8}(t-57.4)+\frac{153441}{40} & (57.4\le t<60.4)\\
540(t-60.4)+5454 & (60.4\le t<85.2)\\
-\frac{1}{60}(t-85.2)^5+540(t-85.2)+18846 & (85.2\le t<88.2)\\
-\frac{1}{4}(t-88.2)^4-\frac{3}{2}(t-88.2)^3-\frac{9}{2}(t-88.2)^2+\frac{2133}{4}(t-88.2)+\frac{409239}{20} & (88.2\le t<90.2)\\
\frac{1}{30}(t-90.2)^5-\frac{1}{4}(t-90.2)^4-\frac{7}{2}(t-90.2)^3-\frac{39}{2}(t-90.2)^2+\frac{1957}{4}(t-90.2)+\frac{429889}{20} & (90.2\le t<92.4)\\
\frac{1}{20}(t-92.4)^5+\frac{7}{60}(t-92.4)^4-\frac{613}{150}(t-92.4)^3-\frac{34733}{750}(t-92.4)^2+\frac{2594147}{7500}(t-92.4)+\frac{4206565027}{187500} & (92.4\le t<93.2)\\
\frac{1}{60}[(t-92.4)^5+(t-95.2)^5-(t-98.2)^5]-\frac{25}{6}[(t-92.4)^3+(t-95.2)^3-2(t-93.2)^3]-90(t-93.2)^2+373(t-93.2)+\frac{677919}{30} & (93.2\le t<95.2)\\
\frac{1}{60}[(t-92.4)^5-(t-98.2)^5]+\frac{25}{3}[(t-93.2)^3-(t-97.4)^3]-90[(t-93.2)^2+(t-97.4)^2]+\frac{707961}{30} & (95.2\le t\le 95.4)\\
\frac{1}{60}[(98.2-t)^5+(95.4-t)^5-(92.4-t)^5]-\frac{25}{6}[(98.2-t)^3+(95.4-t)^3-2(97.4-t)^3]-90(97.4-t)^2+373(97.4-t)+\frac{677919}{30} & (95.4<t\le 97.4)\\
\frac{1}{20}(98.2-t)^5+\frac{7}{60}(98.2-t)^4-\frac{613}{150}(98.2-t)^3-\frac{34733}{750}(98.2-t)^2+\frac{2594147}{7500}(98.2-t)+\frac{4206565027}{187500} & (97.4<t\le 98.2)\\
\frac{1}{30}(100.4-t)^5-\frac{1}{4}(100.4-t)^4-\frac{7}{2}(100.4-t)^3-\frac{39}{2}(100.4-t)^2+\frac{1957}{4}(100.4-t)+\frac{429889}{20} & (98.2<t\le 100.4)\\
-\frac{1}{4}(102.4-t)^4-\frac{3}{2}(102.4-t)^3-\frac{9}{2}(102.4-t)^2+\frac{2133}{4}(102.4-t)+\frac{409239}{20} & (100.4<t\le 102.4)\\
-\frac{1}{60}(105.4-t)^5+540(105.4-t)+18846 & (102.4<t\le 105.4)\\
540(130.2-t)+5454 & (105.4<t\le 130.2)\\
-\frac{1}{120}(133.2-t)^5+\frac{1}{8}(133.2-t)^4-\frac{3}{4}(133.2-t)^3+\frac{9}{4}(133.2-t)^2+\frac{4293}{8}(133.2-t)+\frac{153441}{40} & (130.2<t\le 133.2)\\
\frac{1}{8}(135.2-t)^4-\frac{7}{4}(135.2-t)^3+\frac{39}{4}(135.2-t)^2+\frac{4117}{8}(135.2-t)+\frac{111191}{40} & (133.2<t\le 135.2)\\
\frac{1}{60}(137.4-t)^5-\frac{7}{120}(137.4-t)^4-\frac{613}{300}(137.4-t)^3+\frac{34733}{1500}(137.4-t)^2+\frac{6644147}{15000}(137.4-t)+\frac{643309973}{375000} & (135.2<t\le 137.4)\\
\frac{1}{40}(138.2-t)^5-\frac{19}{120}(138.2-t)^4-\frac{509}{300}(138.2-t)^3+\frac{41561}{1500}(138.2-t)^2+\frac{6032131}{15000}(138.2-t)+\frac{516364601}{375000} & (137.4<t\le 138.2)\\
\frac{1}{120}(140.2-t)^5-\frac{29}{120}(140.2-t)^4-\frac{29}{300}(140.2-t)^3+\frac{50131}{1500}(140.2-t)^2+\frac{4150291}{15000}(140.2-t)+\frac{260359051}{375000} & (138.2<t\le 140.2)\\
-\frac{29}{120}(140.4-t)^4+\frac{29}{300}(140.4-t)^3+\frac{50131}{1500}(140.4-t)^2+\frac{3949709}{15000}(140.4-t)+\frac{240109051}{375000} & (140.2<t\le 140.4)\\
-\frac{1}{120}(142.4-t)^5-\frac{19}{120}(142.4-t)^4+\frac{509}{300}(142.4-t)^3+\frac{41561}{1500}(142.4-t)^2+\frac{2067869}{15000}(142.4-t)+\frac{91114601}{375000} & (140.4<t\le 142.4)\\
-\frac{1}{40}(143.2-t)^5-\frac{7}{120}(143.2-t)^4+\frac{613}{300}(143.2-t)^3+\frac{34733}{1500}(143.2-t)^2+\frac{1455853}{15000}(143.2-t)+\frac{56059973}{375000} & (142.4<t\le 143.2)\\
-\frac{1}{60}(145.4-t)^5+\frac{1}{8}(145.4-t)^4+\frac{7}{4}(145.4-t)^3+\frac{39}{4}(145.4-t)^2+\frac{203}{8}(145.4-t)+\frac{1031}{40} & (143.2<t\le 145.4)\\
\frac{1}{8}(147.4-t)^4+\frac{3}{4}(147.4-t)^3+\frac{9}{4}(147.4-t)^2+\frac{27}{8}(147.4-t)+\frac{81}{40} & (145.4<t\le 147.4)\\
\frac{1}{120}(150.4-t)^5 & (147.4<t\le 150.4)\\
0 & (t>150.4)
\end{cases}
\tag{14}
$$

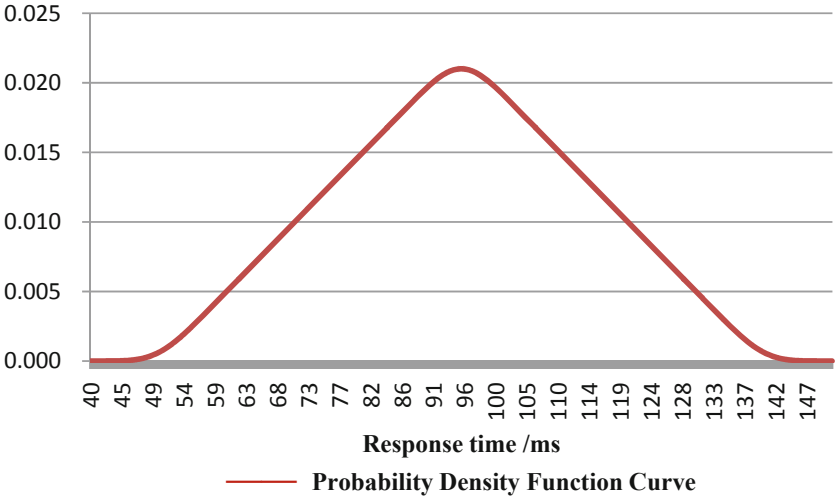


Fig. 6. Probability density function graph

3.2 Response Time Simulation

According to Eqs. (7)~(10), the values of T_{AI},$T_{MPU\text{-}I}$,$T_{COM\text{-}I}$,$T_{COM\text{-}II}$,$T_{MPU\text{-}II}$ and T_{DO} can be expressed in the form of "$RAND(0, 1) \times k + b$". According to the parameters of each module, the configured cycle and load of the main control module, the value of "C" and the corresponding values of "k" and "b" are obtained, and the simulation is carried out according to Eq. (4) to generate 1 million simulation data. After sorting the data, the frequency distribution and probability density fitting curve shown in Fig. 7 are obtained. In the results, the maximum value, minimum value and average value are 148.3ms, 43.7ms and 95.3ms respectively, which are in line with the theoretical calculation results. Comparing the simulation results in Fig. 7 with the theoretical calculation results in Fig. 6, it can be seen that the simulation results are consistent with the theoretical calculation results.

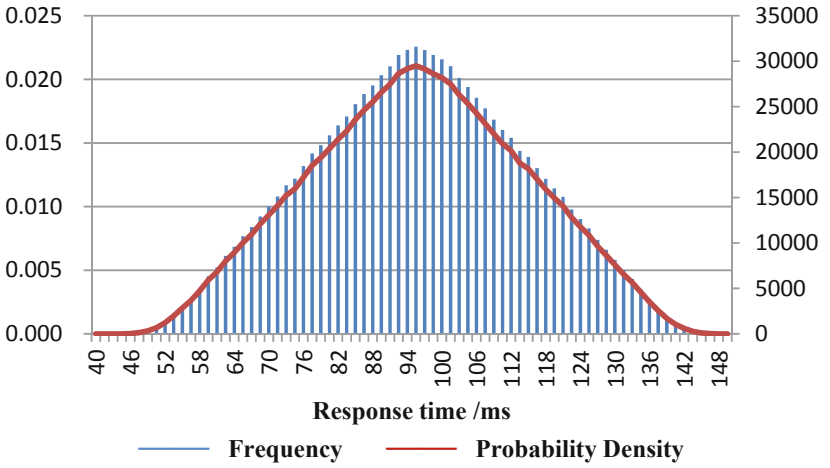


Fig. 7. Simulation data frequency distribution and probability density fitting curve

4 Calculation and Simulation Results Verification

4.1 Testing Environment

The test environment is shown in Fig. 8, which mainly includes the tested DCS system and the multifunctional response time test device.

1) DCS system under test
   Including signal Conditioning Cabinet (PIPS), Protection Group Processing Cabinet (RPC), Special Security Facility Drive Cabinet (ESFAC) and Preferred Drive Cabinet. The DCS system under test collects the analog signal of the working condition, performs isolation, distribution, and logical operation on it, and then outputs the operation result to the optimal drive cabinet to issue a special drive signal.
2) Multifunctional response time test device
   The device can realize the functions of signal generation, signal acquisition, automatic calculation of response time, test data storage and so on. Compared with the traditional method of using oscilloscope combined with signal generator, the device has the advantages of high efficiency and less labor demand, and can realize the calculation and storage of a large number of response time test data. During the test, the device automatically injects the working condition simulation signal into the tested DCS system according to the test case, collects the driving signal of the special Security facilities output by the tested DCS system, records the change time of the working condition simulation signal (marked as *T0*) and the change time of the driving signal of the special Security facilities output by the tested DCS system (marked as *T1*), and automatically calculates the response time (that is, the value of "*T1-T0*").

4.2 Test Method

The test method is as follows:

1) Check the tested DCS system and confirm that there is no abnormality or state affecting the test;
2) Connect the working condition analog signal input terminal and special drive signal output terminal of the tested DCS system to the corresponding signal terminal of the multifunctional response time test device with the test cable;
3) The test case is imported into the test device and executed in the test cycle.

4.3 Test Results

Execute 1 million test cases and sort out the data to obtain the frequency distribution and probability density fitting curve as shown in Fig. 9. In the results, the maximum value, minimum value and average value are 147.0ms, 45.0ms and 95.5ms respectively, which are in line with the theoretical calculation and simulation results. Comparing the test results in Fig. 5, the simulation results in Fig. 7 and the theoretical calculation results in Fig. 6, it can be seen that the test results are consistent with the theoretical calculation and simulation results. To sum up, the response time meets the requirements and the probability analysis method is correct.

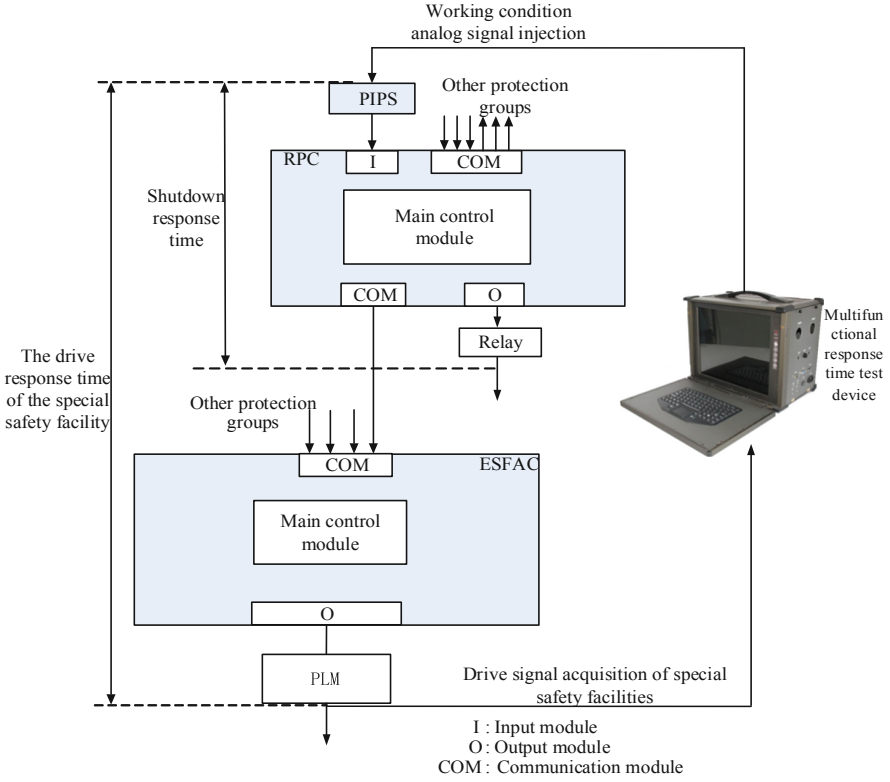


Fig. 8. Response time test environment

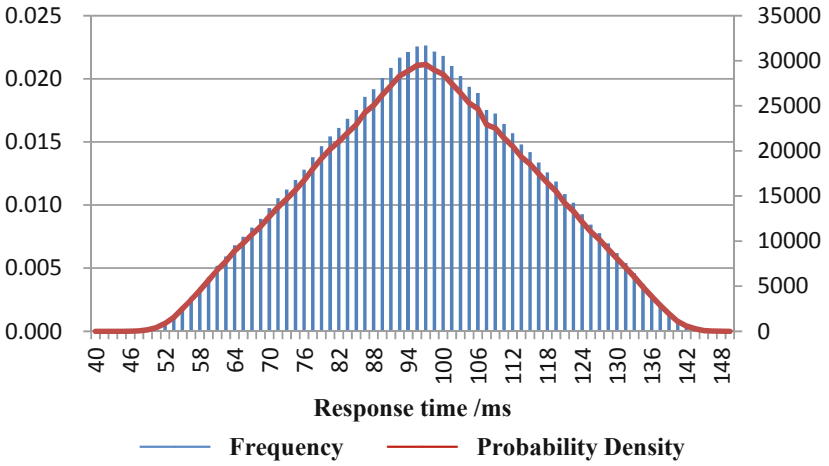


Fig. 9. Test data frequency distribution and probability density fitting curve

5 Summary

This paper proposes a response time analysis method of safety-level DCS based on probability theory. The method is used to analyze engineering examples, and then the feasibility and correctness of the analysis method are verified through calculation, simulation and testing of engineering examples. Compared with the current response time analysis method, this method has obvious advantages, and can reflect the characteristics and laws of the response time more comprehensively and fully. Through further research and expansion of this method, it can provide reference for the design, testing and judgment of system abnormality of safety-level DCS.

References

1. Wei, L., Hongchun, L., Jixiang, Z.: et al.: Design of longteng safety-level DCS platform. In: Progress Report on China's Nuclear Science and Technology (Volume 4)—Proceedings of the 2015 Annual Conference of the Chinese Nuclear Society, Vol. 2, pp. 221–226 (2015)
2. Jining, W., Aiping, Z., Yongxue, X., Yuan, Z.: Analysis and test of emergency shutdown response time of nuclear power plant reactor protection system. Nuclear Power Eng. **33**(02), 5–10 (2012)
3. Sheng, J.: Probability Theory and Mathematical Statistics. Higher Education Press, Beijing (2018)
4. Yong, D.: The properties of the sum of independent and uniformly distributed random variables. Stat. Decis. Making **37**(17), 71–74 (2021)

Rational Argument of the Closed Loop of the Reactor Spent Fuel

Jia-Kang Zheng(✉)

Nuclear and Radiation Safety Center, Beijing 102401, China
zhlc135@sina.com

Abstract. With the rapid development of nuclear power and the accelerated progress of decommissioning and treatment of corresponding nuclear facilities, it is inevitable to build a large number of nuclear fuel cycle facilities, so as to complete the production of nuclear fuel elements required by nuclear power plants and the recovery and treatment of spent fuel and corresponding three wastes (wastewater, waste gas and solid waste) generated by nuclear power plants. According to the nuclear power medium and long term development plan (2005–2020), China's nuclear power industry follows the path of closed nuclear fuel cycle [1]. Based on this, this paper makes a preliminary analysis and demonstration of the rationality of the reactor closed nuclear fuel cycle.

Keywords: nuclear fuel cycle facility · closed nuclear fuel cycle · disposal of spent fuel

1 Concept of Closed Nuclear Fuel Cycle

The cycle must turn a circle, end to end. But in the nuclear fuel cycle, there are two ways: closed nuclear fuel cycle and once through nuclear fuel cycle. The once through cycle includes the production, use, and reprocessing of nuclear fuel; the closed cycle is that the reprocessing product reused to make nuclear fuel.

The closed nuclear fuel cycle (see Fig. 1) is the process of chemically treating spent fuel to recover about 96% of the Uranium and about 1% of the Plutonium and to recycle it to its full potential. Only about 3% of the total long lived fission product and minor actinides (Neptunium, Americium, Curium, etc.) are glass-solidified as high level waste for final geological disposal.

2 Process Method and Case of International Advanced

2.1 Process Method

There are three types of disposal of spent fuel in nuclear weapon states: First, be sent to reprocessing facility to recover the Uranium and Plutonium contained in the waste; second, be stored in intermediate storage facility, and the third, be placed in geological repository for final disposal.

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 179–185, 2023.
https://doi.org/10.1007/978-981-99-3455-3_18

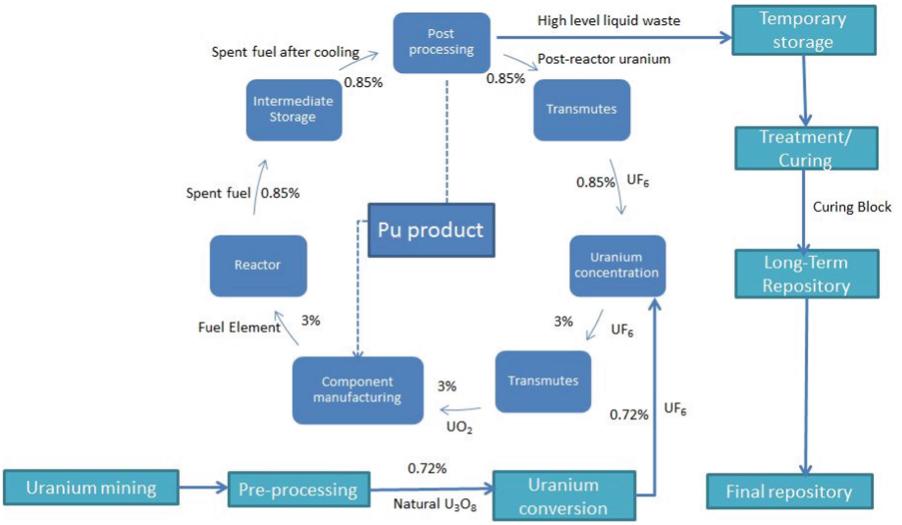


Fig. 1. The closed nuclear fuel cycle

At present, most of the world's spent fuel is stored in nuclear power plants in its place of origin. Depending on the disposal route selected, the final repository may therefore receive untreated spent fuel, or general waste, or both. The repository is an underground facility for the disposal of nuclear materials such as spent fuel, usually hundreds of metres below the surface, in stable geological formations that ensure long term isolation of the radionuclide from the biosphere.

Now, the international nuclear fuel cycle is divided into closed nuclear fuel cycle and once through nuclear fuel cycle. Closed nuclear fuel cycle means that the recovery of fissile materials such as Uranium and Plutonium from spent fuel, as well as materials such as Minor actinide that can be used, and the reprocessing of fissile materials into nuclear fuel assemblies, other radionuclide are disposed of as waste; once through nuclear fuel cycle is the direct final disposal of spent fuel as radioactive waste.

2.2 Hand Cases

Recently, the countries that choose closed nuclear fuel cycle in the world mainly include France, Britain, Russia, Japan and India. The United States also officially announced the adoption of closed nuclear fuel cycle in 2006 [3].

As early as the 1950s, the United States developed the PUREX process for spent fuel reprocessing, and built the world's first military spent fuel reprocessing plant using the PUREX process. Subsequently, the United States greatly promoted the commercial reprocessing of spent fuel in nuclear power plants, and successively built three civilian reprocessing plants, as shown in Table 1.

While, France has the largest, most mature and most advanced commercial spent fuel reprocessing and recycling industry in the world. Argyle spent fuel reprocessing plant [4] is one. If it is operated at full capacity, it can undertake the spent fuel reprocessing

Table 1. Civilian reprocessing plants

No	Name	Capacity	Closed time	Closed reason
1	West Valley, NY	300 T/year	1978	Increased safety regulatory requirements
2	Morris Reprocessing Plant, IL	300 T/year	1974	New process failed
3	Barnwell reprocessing plant, South Carolina	1500 T/year	Closed before debug	Policy shift

task produced by 90–100 million KW nuclear power units per year. After 40 years of development, Argyle spent fuel reprocessing plant has become the largest, most advanced and most mature commercial light water reactor spent fuel reprocessing base in the world. It not only handles spent fuel in France, but also imports spent fuel for Germany, Japan, Italy and other countries. No major accident has occurred in the operation of the plant so far.

Argyle spent fuel reprocessing plant has two reprocessing workshops, namely UP2–800 and UP3, both of which use mature PUREX Process. UP2 started construction in 1962 and was put into operation in January 1967, with a processing capacity of 400 T/year, but after transformation, it can process more than 800 T/year, and was renamed as UP2–800; UP3 was jointly funded by foreign customers from seven countries (excluding France), and was put into commercial operation in 1990 with a rated processing capacity of 800 T/year. The total processing capacity of the two workshops is about 1700 T/year. If they are operated at full load, they can undertake the post processing task of spent fuel produced by 90–100 million KW nuclear power plants per year. At present, the global spent fuel reprocessing capacity of light water reactors is about 3000 T/year, and Argyle spent fuel reprocessing plant accounts for more than half of it.

Figure 2 shows the annual treatment capacity of the two reprocessing plants in Argyle spent fuel reprocessing plant in 30 years. In recent years, its annual processing capacity has been maintained at about 1000 tons, about 60% of the design capacity.

According to data monitored over many years at the Argyle spent fuel reprocessing plant, the average radiation dose to the public near the industrial park was 30 micro Sieverts (uSv) per year. As an example, the natural background radiation dose we receive in daily life is about 3.1 mSv (1 mSv = 1,000 uSv), which is 100 times that of the nuclear fuel cycle plant in Argyle.

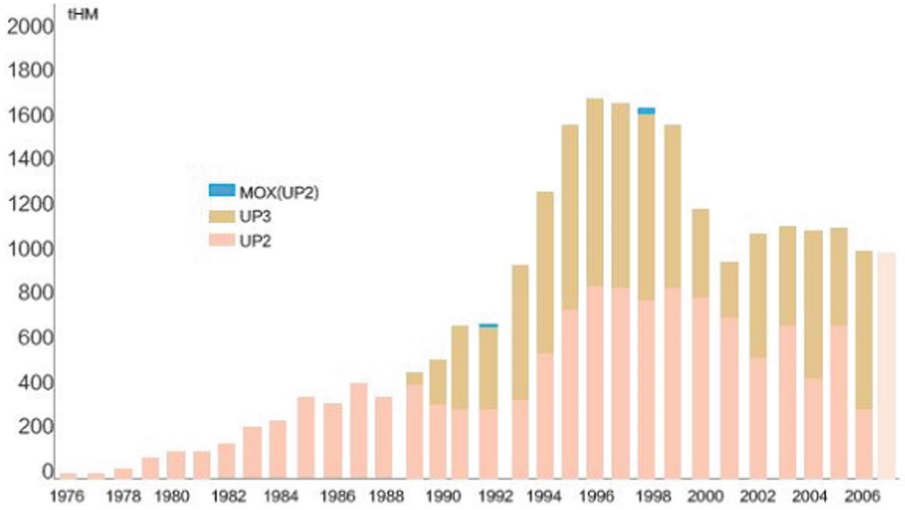


Fig. 2. Operation rate of UP2 and UP3 reprocessing plants in France in the past 30 years

3 National Policy Orientation

Uranium resources are characterized by high difficulty in development and smelting and low total amount. As early as the beginning of the development of nuclear power plants in the early 1980s, China established the national policy of closed nuclear fuel cycle and formulated the strategy of nuclear energy "three steps" (pressurized water reactor, fast reactor, and fusion reactor). Post treatment must be developed for the development of nuclear power. The closed nuclear cycle spent fuel management policy has been reiterated in all national implementation reports of the convention on nuclear safety. This policy is reflected in the corresponding national plans, such as the medium and long term development plan of nuclear power (2005–2020), the 11th five year development plan of the nuclear industry, the white paper of China's energy policy (2012), the action plan for energy development (2014–2020), the 13th five year development plan of the nuclear industry, and the action plan for energy technology revolution and innovation (2016–2030), etc. [1, 5–9].

The three-step strategy of nuclear energy is a scientific choice made from the actual situation of China's resources and environment, and it is also the fundamental direction of the development of China's nuclear energy science and technology. The implementation of the closed nuclear cycle of spent fuel is an integral part of the "three-step" strategy of nuclear energy and the basis for the sustainable development of nuclear energy. Through the development of spent fuel reprocessing technology in nuclear power plants, the coordinated development of thermal reactors and fast reactors in China can greatly improve the utilization efficiency of Uranium resources and ensure national energy security.

In 2017, the State Council officially approved the "13th five-year plan for nuclear safety and radioactive contamination prevention and control" and the long term goal for

2025 [10]. On March 23, the Ministry of Environmental Protection held a press conference, it is interpreted as follows: China has attached importance to nuclear power plant spent fuel safety, in order to make full use of fissile material resources, the establishment of spent fuel reprocessing closed nuclear fuel cycle policy. To this end, China has set up a special fund for spent fuel, to protect spent fuel reprocessing funds, and actively promote spent fuel reprocessing technology research and development. The Ministry of Environmental Protection (NNSA) has put forward strict technical requirements for the construction of spent fuel reprocessing plants and implemented an approval system. Safety and environmental requirements are kept at the same level as nuclear power plants.

4 Current Situation, Successful Experience and Benefit in China

4.1 Domestic Situation

Now, the majority of nuclear power plants in operation in China are light water hydrothermal neutron reactors. One of its characteristics is that the fuel does not burn completely in the reactor, the remaining primary and secondary (regenerative) nuclear fuel can be returned to the reactor after corresponding reprocessing. According to the nuclear energy development strategy, the main task of the radiochemical industry at present is to treat the fuel of thermal neutron power reactors. Economic Calculation shows that the optimum production capacity of spent nuclear power plant is 1200–1800 TU per year. This would allow the plant to process the offloaded fuel from a nuclear power plant with a total power capacity of 40–50 GW, and would be economical.

With the development of nuclear power, China's post processing industry has developed rapidly. After years of practice and exploration, China has fully mastered the post-treatment process and manufacturing technology of key equipment, and built an intermediate test plant for spent fuel post-treatment in power reactors. The thermal commissioning was completed in December 2010, the spent fuel pool has been receiving spent fuel from the Daya Bay nuclear power plant since 2003 and has been operating successfully for 12 years, as a platform for post-treatment experiments and research and development of actinides, it has laid a solid foundation for the construction of scientific research capacity in China.

4.2 Successful Practice

At present, the total nuclear power in China is about 30–50 GW, and the annual power output can reach 150–250 billion KWH. The reprocessing and recycling of spent fuel is the weakest link in China's nuclear fuel cycle, and temporary storage is the main solution. The 404 pilot plant, the first and only intermediate test plant for spent nuclear fuel reprocessing, has an annual capacity of about 50 tons per year, which is far from meeting the demand of spent nuclear fuel reprocessing in China.

According to the national requirement of nuclear power development and international experience, it is feasible to build nuclear fuel reprocessing plant with small production capacity (400-800TU/year). Therefore, two major development cooperation

projects have been implemented: 1. Longteng 2020 Project: 200 tons of large scale commercial spent fuel reprocessing project with China's own intellectual property rights, to start construction in 2020; 2. China-France nuclear cycle project: 800 tons of spent fuel reprocessing plant to be commissioned by 2030.

Finally, high level radioactive waste generated by closed nuclear fuel cycle is an indispensable, and sometimes the only, source of radionuclide in some areas of science and technology. With the progress of science and technology, the fission products of Technetium (99Tc), Iodine (129I) and minor actinides separated in the post-treatment process can be transformed into short lived or stable nuclides by transmutation technology in the future, thus greatly reduces the radiation to the environment the harm, causes the nuclear energy utilization to be cleaner.

4.3 Benefits

First, post-treatment can make full use of Uranium resources to ensure the sustainable development of nuclear power plants. The development of post-treatment industry is an important link to ensure the sustainable development of nuclear power. The Uranium-235 content of spent PWR fuel is 0.8% to 1.3%, which is higher than the 0.71% content of natural Uranium. And then there's the new fissile Plutonium-239. After post-treatment, useful Uranium and Plutonium can be recovered from the spent fuel, and then made into UO2 or MOX fuel to be returned to the heat reactor or fast reactor for use, thus greatly improving the Utilization rate of Uranium resources. According to experts' calculations, about 30% of natural Uranium can be saved by returning the Uranium and Plutonium from reprocessing to pressurized water reactors. If a closed nuclear fuel cycle of fast reactors and reprocessing can be achieved, the Utilization rate can be increased by about 60 times, which means that natural Uranium, which could have been used for only 50–60 years, could be used for more than 3,000 years.

Second, post-treatment can reduce the volume and toxicity of radioactive waste. The amount of high level radioactive waste (HLW) is about 2M3/TU, if the spent fuel discharged from the power reactor is disposed of in a "once through nuclear fuel cycle" way. At the current international level of reprocessing plants, the amount of HLW waste produced from reprocessing of spent fuel is about 0.5 M3/TU, which is only 1/4 of the former. At the current post-treatment technology level, the recovery rate of Uranium and Plutonium could reach 99.75%, reducing the radioactive toxicity of the final disposal waste by more than one order of magnitude.

5 Conclusions

The closed nuclear fuel cycle is the ultimate choice of China, and the main starting point for the implementation of the closed nuclear fuel cycle is the sustainable development of the nuclear power plants and the enhancement of the overall strength of the nuclear industry. The implementation of the closed nuclear fuel cycle technology route should be based on state action. Specifically:

1. Formulate technology policies, development plans and implementation plans.

2. Provide financing channels, including research and development of key technologies and construction of major projects.
3. Examine, approve and supervise major construction projects.

References

1. National Development and Reform Commission. Medium and long term development plan of nuclear power (2005–2020) (2007)
2. Hua, L.: Overview of spent fuel reprocessing abroad. Chem. Eng. Equip. (2012)
3. USA. Integrated process for reprocessing spent nuclear fuel. A7665209 DE93 002017
4. Polaris power network. Current situation of world spent fuel reprocessing industry, May 2013
5. Commission of science, technology and industry for national defense. The 11th Five Year Plan for the development of nuclear industry (2006)
6. Information Office of the State Council. White paper on China's energy policy (2012) (2012)
7. General Office of the State Council. Strategic action plan for energy development (2014–2020) (2014)
8. State Administration of science, technology and industry for national defense. 13th five year plan for nuclear industry development (2017)
9. National Development and Reform Commission, national energy administration Notice on printing and distributing the action plan for energy technology revolution and innovation (2016–2030) (fgny [2016] No. 513) (2016)
10. Ministry of environmental protection, national development and Reform Commission, Ministry of finance, national energy administration, national defense science and Industry Bureau The 13th five year plan for nuclear safety and prevention of radioactive pollution and the long-term goal of 2025 (2017)

Pressurizer Control Optimization with Deep Learning-Based Predictions

Jing-Ke She[1(✉)], Wei-qi Li[1], Yi-fei Ma[1], Yi-fan Zhang[2], and Liang Liu[3]

[1] College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, Hunan, China
shejingke@hnu.edu.cn

[2] College of Information and Intelligence, Hunan Agricultural University, Changsha 410128, Hunan, China

[3] Hunan University of Arts and Science, Changde 415000, Hunan, China

Abstract. With a consideration of alleviating the unstable control responses in traditional pressurizer control, this work adopts the cutting-edge deep learning method to optimize the PID control performance. A Long Short-Term Memory (LSTM) model is trained by data from a traditional PID control simulation and is then used to provide predictions to the PID controller such that the newly constructed intelligent controller can produce control signals for real time working conditions. The verification experiments conducted for both functionality and complex inputs successfully proved the advantages of the intelligent controller, showing up to 80.7% overshoot reduction and up to 60.73 s decrease in the control time for a steady state. Although its performance varies in different control cases, it does provide a deep learning-based control option for the pressurizer control in nuclear power plants.

Keywords: Pressurizer Control · PID · Deep Learning · LSTM

1 Introduction

As the pressure and water-level control equipment in nuclear power plants (NPPs), pressurizer plays an important role in keeping stable pressure in the Primary Heat Transfer (PHT) loop and preventing the coolant from boiling inside the reactor [1]. Its current control method relies on traditional PID controller with a consideration of safety and maturity. The PID controller has the advantages of clear structure, legible implementation, and proved robustness. However, the parameters of the pressurizer vary with time and the working condition, making it a nonlinear, time-variant, and inertial system that is hard for the control strategy design and optimization [2].

Current method for PID optimization can be mainly divided into three categories.

1) Regular PID parameter adjusting, including using transient characteristics [3] and the Ziegler-Nichols frequency domain response [4]. PID parameters (k_p, k_i, and k_d) are adjusted based on the responses from the controlled object, which is simple, effective, but lacks theoretical support and can only be applied to certain scenarios.

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 186–199, 2023.
https://doi.org/10.1007/978-981-99-3455-3_19

2) Intelligent PID parameter adjusting uses cutting-edge theories such as Quantum-behaved Particle Swarm Optimization (QPSO) [5] and ant colony algorithm [6]. The optimized PID parameters can be determined according to the system characteristics.
3) Self-adaption PID parameter adjusting, such as single-neuron PID based on Hebb rule [7], self-adaption PID based on fuzzy control theory [8], immunity-PID [9], etc. Constrains in these methods are realized by pre-defined rules in order to optimize the PID control outputs. It provides a solution with more universality than the above two.

The above parameter-adjusting methods are all constructed and implemented based on the physical principles of the pressurizer itself. However, building an accurate model for the precise PID control is difficult due to the nonlinearity and time-variance of the pressurizer system, i.e., using the "White-Box" strategy is facing harsh challenges. With the rapid development of the Artificial Intelligence (AI) methods, as well as the enormous industry data produced and stored during past decades, applying deep learning to the control strategy becomes feasible. The potential and advantages proved by deep learning methods in feature extraction and model fitting have been successfully applied to control optimization [10]. The deep learning model trained by plenty of industry data can predict the system behavior using data-driven method, avoiding building the complex system models. Such "Black-Box" strategy allows the system behavior to be described using the "past behavior" and can generate predicted system behavior to compensate the system delay causing control errors. LSTM model has been proved to be an option for the prediction of the operation condition and parameters in NPPs [11]. Furthermore, the LSTM used in [12] demonstrates its excellent prediction performance in data processing for long time series data generated during the Steam Generator (SG) level control process.

This work is inspired by the previous successful LSTM control applications and aims at optimizing the PID control with LSTM-based predictions. The main idea is using an LSTM model trained by historic pressurizer operating data to compensate the delay between the sensor and the PID controller, such that the PID controller can obtain a "real-time" perception of the actual working conditions and produce corresponding control signals. The exploration is conducted within a simulation platform built with MATLAB Simulink such that the pressurizer control loop, the LSTM model, and the expected intelligent control strategy can be fully tested through simulations.

This paper starts with an introduction in Sect. 1, followed by the construction of an intelligent PID control platform in Sect. 2. After the verification experiments and results shown in Sect. 3, this work is than concluded in Sect. 4.

2 The Pressurizer Pressure Control Model

2.1 Theoretical Basis of the Pressure Control

A pressurizer pressure control simulation model is firstly constructed in this work using MATLAB Simulink platform. It provides an object to study the system behaviors, especially complex time-variant behaviors, of the pressurizer. Since the system dynamic performance evaluation is normally based on the system response under step function [13], the control simulation model is built according to the step response curve [14].

For a 2nd order step response, such as the pressurizer pressure control, its transfer function can be represented as,

$$G(s) = \frac{K}{(T_a s + 1)(T_b s + 1)}, T_a \geq T_b \tag{1}$$

where K, T_a, and T_b are coefficients to be determined from its step responses. K stands for the process amplification or the amplification coefficient, while T_a, and T_b are time constant. K can be derived through an estimation of the stable value $y(\infty)$ of the controlled object,

$$K = \frac{y(\infty) - y(0)}{r} \tag{2}$$

where $y(\infty)$ and $y(0)$ are new and original stable values, respectively; r is the step signal amplitude.

T_a and T_b are obtained through a "two-point method" shown in Fig. 1.

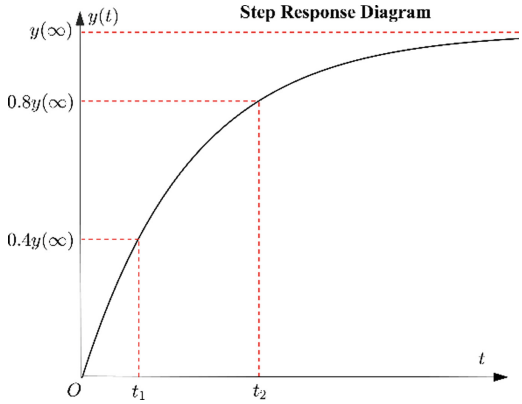


Fig. 1. Step Response Curve of the 2nd order System

The "two-point method" uses an approximate formula from [15],

$$T_a + T_b \approx \frac{t_1 + t_2}{2.16} \tag{3}$$

$$\frac{T_a T_b}{(T_a + T_b)^2} \approx 1.74\frac{t_1}{t_2} - 0.55 \tag{4}$$

The transfer functions of the pressurizer pressure control, which is a 2nd order step response system, is then presented as following according to [14] and [16].

$$G(s) = \frac{0.004838}{(3400s + 1)(100s + 1)} \tag{5}$$

$$G(s) = \frac{1.776}{3300s^2 + 450s + 1.34} \tag{6}$$

(2–5) stands for the step response function when a single group of heaters (case 1) is running, while (2–6) illustrates the step response when all the four groups of heaters (case 4) are turned on for pressure control.

2.2 Pressure Control Loop in Simulink

The traditional pressurizer pressure control loop is implemented first with dataset generation and performance validation purposes. It consists of the major components belong to a traditional PID control system, such as the threshold input, error calculation, PID controller, actuator, feedback loop, etc. The classic structure and its Simulink representation is provided in Fig. 2 and Fig. 3.

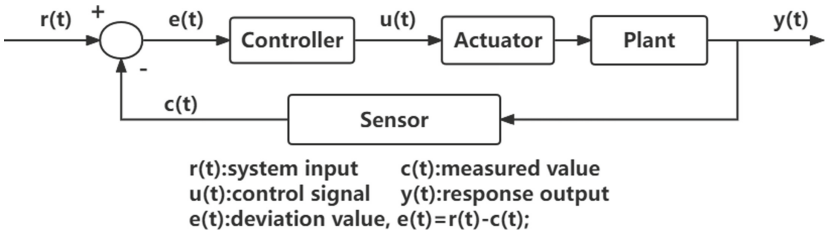


Fig. 2. Traditional PID-based Pressure Control

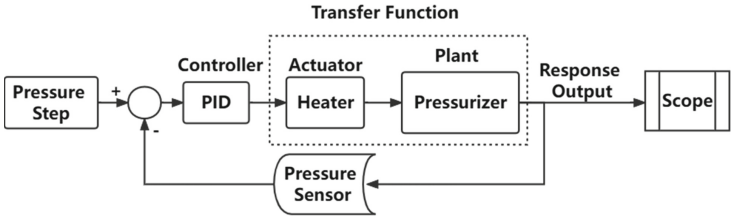


Fig. 3. Simulink Implementation of the Traditional PID Controller

2.2.1 Calculation Unit

The calculation unit is composed by the error calculation unit and the control calculation unit.

The error calculation unit, implemented using SUM function, is used to calculate the error between the control threshold provided by a step function and the actual pressure measured by sensors.

The control calculation unit is built by configuring a PID module with parameters needed for the pressurizer pressure control process, as shown in Fig. 4. It is used to control the water level of the pressurizer according to the calculated error. k_p, k_i, and k_d are set by 10, 0.3, and 50, respectively.

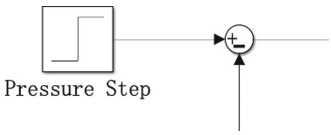


Fig. 4. Error Calculation Unit

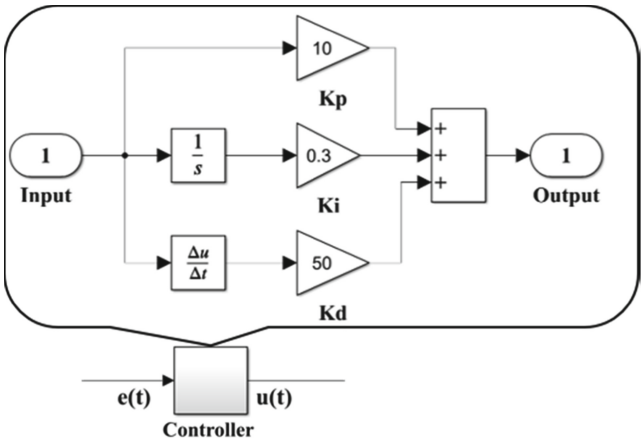


Fig. 5. Control Calculation Unit

2.2.2 Actuator Unit

The actuator unit is realized simply using an amplifier from the Simulink, as shown in Fig. 5. Since the operating condition with different heater effect is considered in the transfer function construction, the amplification coefficient is set to 1 (Fig. 6).

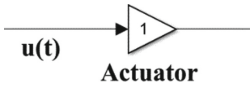


Fig. 6. Actuator

2.2.3 Feedback Unit

The feedback unit captures the current level and passes the measured value to the error calculation unit. Its physical device is an industrial pressure transmitter, which is simulated here using a scale 1 amplification unit (Fig. 7).

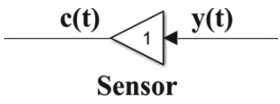


Fig. 7. Feedback Unit

2.2.4 Simulation of the Traditional Pressure Control

Using the components introduced above, a Simulink-based pressure control platform is established. The pressure control simulation is then carried out for case 1 and case 4. In Fig. 8 that illustrates a case 4 simulation, t_r, t_p, and t_s represent 1) the time when the pressure reaches the threshold for the first time; 2) the time when the pressure reaches the peak value of entire control process; and 3) the time when the pressure reaches the stable condition where its variation is within ± 5% of the threshold, respectively.

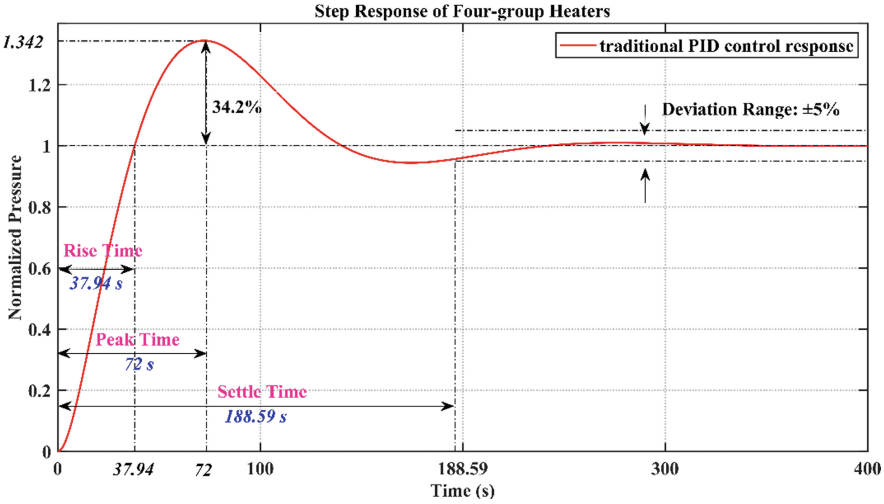


Fig. 8. Simulation of the Traditional Pressure Control

It can be summarized from Fig. 8 that,

1) the traditional PID control is not sensitive to the step input since it has a long response with $t_r = 37.94$ s and $t_p = 73.52$ s.
2) the traditional PID control cannot offer a timely control process since it takes a long t_s (196.2 s) to reach the stable condition.
3) the traditional PID control cannot keep the control process smooth since the overshoot measurement δ is a large value 34.2%.

The above challenges must be confronted when the optimization and improvement need to be brought to the pressure control of the pressurizer. Basically, these challenges are caused by the delay during the sensor value feedback and the PID calculation of the control signals. That's to say, the control signal generated at time t_n is according to the pressure/level value measured at t_{n-x}, which is not a timely reflection of current

pressure/level condition at t_n. The idea of using deep learning methods then comes out with an envisage that a prediction for t_n based on parameters measured at t_{n-x} can compensate the control loop delay and offer the PID controller most current system parameter values, offering a real-time control in which control signals are generated for the actual system situation.

3 The Intelligent Control Using Deep Learning Method

The controlled process is nonlinear and time-variant, resulting in control challenges listed in previous section when a single control method is applied. A combination of deep learning and PID control is investigated in this section as a solution in which the delay issues are dealt with using the predictions from a deep learning model.

3.1 The Structure of the Intelligent Control Model

From the model structure perspective, the intelligent control model is built by adding a deep learning module between the error calculation unit and the PID unit. The deep learning module, which is an LSTM model, is trained using the dataset obtained from traditional PID control simulation in Sect. 2. The control delay x between t_n and t_{n-x} is also estimated using such dataset. When the error calculated based on sensor value at moment t_{n-x} reaches the LSTM model, a prediction value for current moment t_n is calculated and fed into the PID controller. By this means, the PID controller sees the real time system situation and, consequently, can produce an appropriate control signal (Fig. 9).

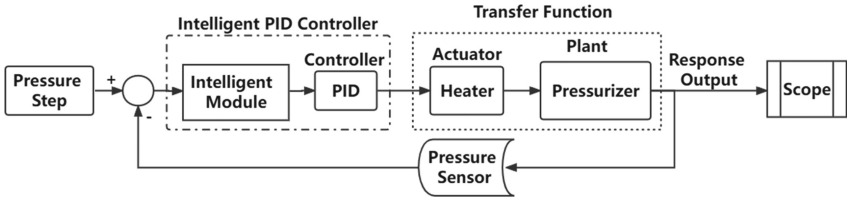


Fig. 9. Main Structure of the Intelligent Control Model

3.2 Training and Implementation of the Intelligent Control Model

LSTM is chosen as the deep learning method due to its prediction performance and fast convergence demonstrated in [11] and [12]. Its training process adopts the dataset generated from simulations in Sect. 2, where LSTM model learns the performance of the traditional control loop. Adam optimizer is used as the model training optimizer due to its excellent performance in the trainings of RNN related models. The configuration of the LSTM model used in this work is presented in Table 1.

Table 1. Parameters of the LSTM Model

Model parameters	Value
Epoch	250
Batch Size	1000
FC_2 Cells	1
Learning Rate	0.01
LSTM Cells	8

In order to evaluate the prediction accuracy, Mean Square Error (MSE) is selected as the regression analysis method, which is defined as,

$$MSE = \frac{1}{n}\sum_{i=1}^{n}\left(y_i^* - y_i\right)^2 \tag{7}$$

The Simulink implementation for both traditional control and intelligent control is shown in Fig. 10 (case 1) and Fig. 11 (case 4). Their model parameters are listed in Table 2.

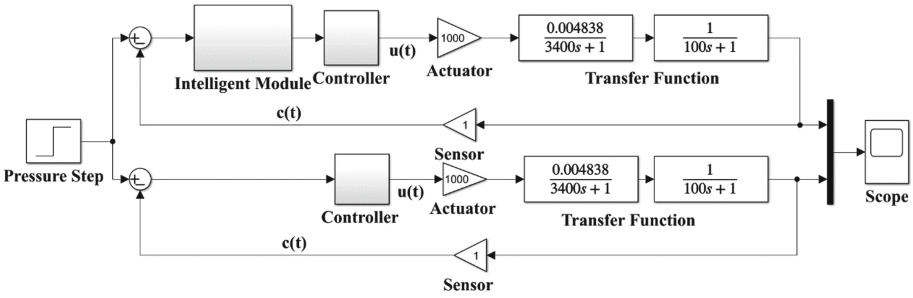


Fig. 10. Simulink Implementation for Case 1

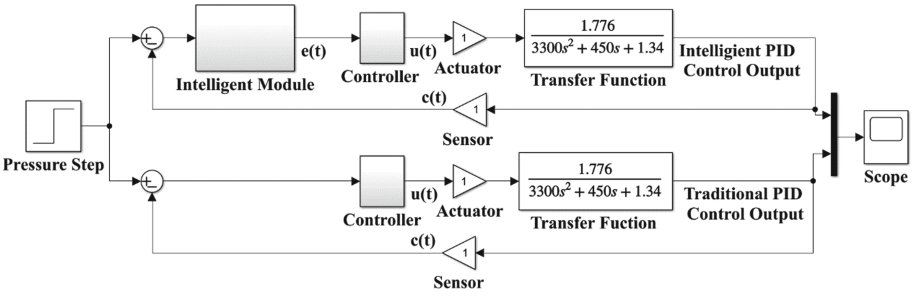


Fig. 11. Simulink Implementation for Case 4

Table 2. Parameters of the Simulink Implementation

Model parameters	Case 1	Case 4
K_p	63.8	10
K_i	0.385	0.3
K_d	1000	50
Actuator	1000	1
Sensor	1	1

3.3 Experiments and Results Analysis

The verification experiments are designed to provide a comparison between the traditional PID control and the intelligent control under the same operating conditions. Two test cases, single group of heaters (case 1) and four groups of heaters (case 4) as mentioned in Sect. 2.2.4, are implemented in Simulink. The experimental platform contains two loops in which the traditional PID control and the intelligent control are both implemented.

For each test case, there are two experiments to be conducted. The first one is a regular functionality test in which a simple step input comes into the system as a control request. Both control loops must respond to the input by adjusting the pressure to the threshold indicated in the step function, such that their capability to control the pressurizer pressure is demonstrated. Another test is a scenario where several step functions are fed into the system in a periodically order, imitating a complex operating scenario. During this test, the control performance of two control loops is analyzed not only for the functionality, but also for the control stability and robustness.

3.3.1 Functionality Experiments

The step input for the functionality experiment is from 0 to 1, i.e., a control request of increasing the pressure from 0 to a normalized 100% pressure. The functionality performance for both case 1 and case 4 are plotted in Fig. 12 and 13 below. Detailed comparisons between performance parameters are listed in Table 3 (case 1) and Table 4 (case 4), respectively.

Figure 10 describes the performance difference between the two loops. Comparing to the traditional PID control, the proposed intelligent control has only one overshoot which is much lower than that of PID (80.7% decrease in case 1 and 28.57% decrease in case 4). Meanwhile, the control response from the intelligent model reaches the stable status much faster than the traditional one, e.g., intelligent t_s is 55.7% shorter than the traditional t_s in case 1, and 60.73% in case 4).

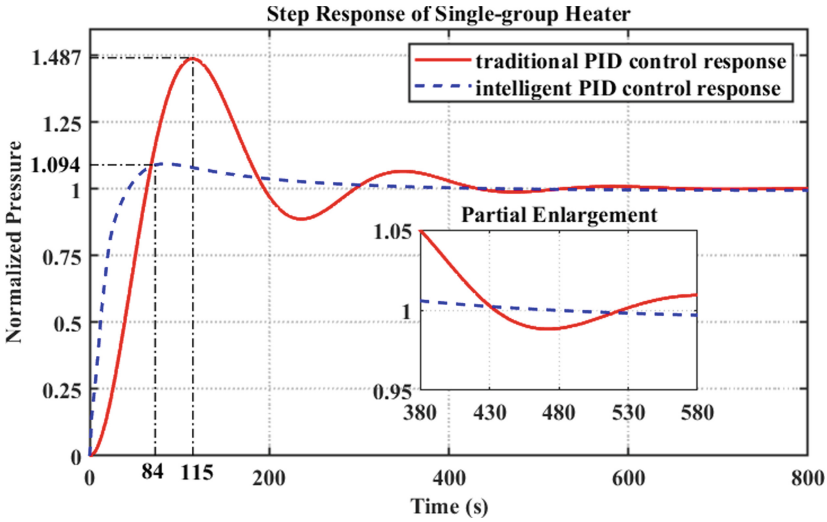


Fig. 12. Functionality Test Results for Case 1

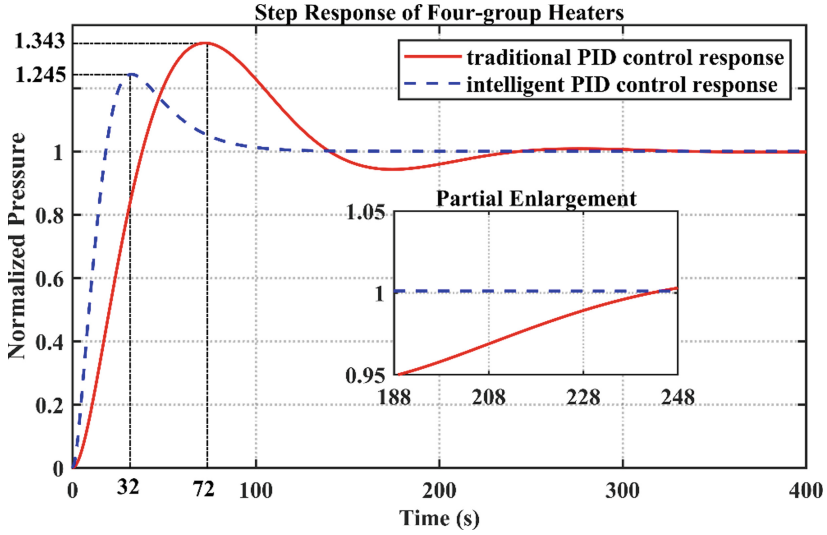


Fig. 13. Functionality Test Results for Case 4

Table 3. Performance Comparison for Case 1

Parameters	PID	LSTM	Optimization
$\mathbf{t_r}$(s)	63.7	43.25	32.10%
$\mathbf{t_p}$(s)	115	84	26.96%
$\mathbf{t_s}$(s)	384.01	170.11	55.70%
Overshoot	0.487	0.094	80.70%

Table 4. Performance Comparison for Case 4

Parameters	PID	LSTM	Optimization
$\mathbf{t_r}$(s)	37.94	18.2	52.03%
$\mathbf{t_p}$(s)	72	32	55.56%
$\mathbf{t_s}$(s)	188.59	74.05	60.73%
Overshoot	0.343	0.245	28.57%

3.3.2 Multiple Step-Inputs Experiments

During the multiple step-inputs experiments, both case 1 and case 4 are experiencing several step inputs that come to the input in a periodical order. The control loops are tested in this way to verify if they are able to produce accurate and stable control during a complex operating condition.

The first step input is the same as the functionality test, i.e., from 0 to 100% pressure. When both control loops reach the steady state, a new control request (decreasing the pressure from 1 to 0.3) is introduced with a new step function input, etc. Such consecutive input variations represent frequent control demands and require the control to be stable, reliable, and robust.

The results plotted in Fig. 14 and 15 show the performance comparison during such complex operating condition. It is noticed that the traditional PID produces several overshoots before reach its steady state after a relative long period. The control response of the intelligent controller, on the contrary, convergent much faster to the steady state with only one much lower overshoot for all the three presented step inputs.

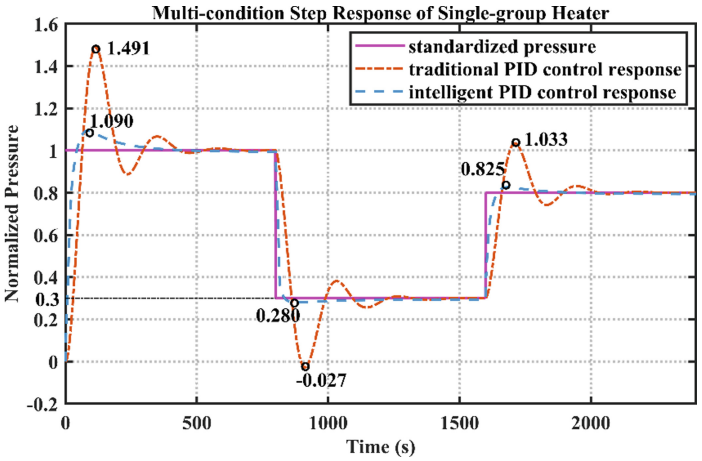


Fig. 14. Multiple Step-Inputs Test Results for Case 1

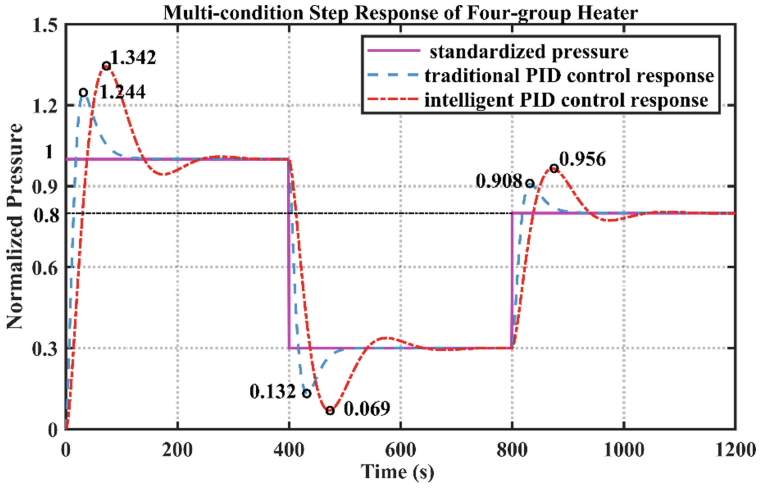


Fig. 15. Multiple Step-Inputs Test Results for Case 4

4 Conclusion

A deep learning-based control optimization method is proposed in this work, which uses the predictions from an LSTM model to compensate the signal delay such that the PID controller can produce a control signal for the real time working conditions. The LSTM model is trained using dataset from a traditional PID simulation to ensure proper predictions for a specific PID controller. It is inserted to the traditional PID control loop right between the error calculation unit and the PID controller. During the verification experiments for both functionality test and complex condition test, the optimized controller demonstrates its performance advantages over the traditional one.

The control overshoot is reduced as much as 80.7% in the best performance case and the time reaching steady state is reduced to 40 ~ 45% of the traditional controller. It can then be concluded that the intelligent controller offers a deep learning-based solution to optimize the traditional PID control algorithm.

However, the control performance of the intelligent controller varies for different operation cases. Its overshoot in case 1 is obviously lower than that of case 4, reflecting the fact that it becomes more difficult to control multiple groups of heaters for this method. During the multiple step-input experiment, its performance parameters (t_r, t_p, and t_s) cannot stay steady when the inputs keep varying, which implies further improvement for this controller to adapt more complex operation conditions.

Acknowledgement. The authors would like to thank the financial and technical support kindly provided from the following research projects and institutions, including but not limited to:

1. National Key Research and Development Project, 2020YFB1713400, 2020;
2. the Industrial Internet Innovation and Development Project of China, TC19084DY, 2019;
3. the State Power Investment Co. Ltd.;
4. China Guangdong Nuclear Research Institution Co. Ltd.;
5. Hunan Xiangjiang Artificial Intelligence Academy.

References

1. Zang, X.N.: Nuclear Power Plant Systems and Equipment, 2nd edn. Tsinghua University Press, Beijing (2010)
2. Zhang, G.D., Yang, X.H., Xu, X., Lu, D.Q.: Simulation of pressure control system for pressurized water reactor nuclear power plant. Comput. Simul. **30**(01), 193–196 (2013)
3. Strm, K.J., Hagglund, T.: PID Controllers: Theory, Design, and Tuning, 2nd edn. Instrument Society of America, North Carolina (1995)
4. Zigler, J.G., Nichols, N.B.: Optimum settings for automatic controllers. Trans. ASME **64**, 759–768 (1942)
5. Wudhichai, A., Chrissanthi, A., Jirapun, P.: Proportional-integral-derivative parametric autotuning by novel stable particle swarm optimization (NSPSO). IEEE Access **10**, 40818–40828 (2022)
6. Zhang, X.L., Zhang, Q.: Optimization of PID parameters based on ant colony algorithm. In: 2021 International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS), pp. 850–853. IEEE (2021)
7. He, L., Cheng F.Q., Wang D.Q., Xu J.T.: Adaptive control of steam generator feed-water system based on improved single neuron self-adaptive control. In: 2016 International Conference on Cybernetics, Robotics and Control (CRC), pp.18–21. IEEE (2016)
8. Chen, D., Liao, K.J., Qian, K., Liu, C.: Research on steering gear electric loading System based on fuzzy Adaptive PID algorithm. In: 2021 IEEE 5th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), pp. 1701–1705. IEEE (2021)
9. Mustapha, S., Mohammed, S., Mohamed, F.K.: An artificial immune optimization approach in tuning nonlinear PID controllers. In: 2014 Second World Conference on Complex Systems (WCCS), pp. 425–430. IEEE (2014)
10. Duan, Y.J., Lv, Y.S., Zhang, J., Zhao, X.L., Wang, F.Y.: Deep learning research status and prospect in the field of control. Acta Automatica Sinica **42**(5), 643–654 (2016)

11. She, J.K., Xue, S.Y., Sun, P.W., Cao, H.S.: The application of LSTM model to the prediction of abnormal condition in nuclear power plants. In: Xu, Y., Sun, Y., Liu, Y., Wang, Y., Gu, P., Liu, Z. (eds.) SICPNPP 2019. LNEE, vol. 595, pp. 463–476. Springer, Singapore (2020)
12. She, J.-K., Wang, J.-N., Yang, S.-Y., Xue, S.-Y.: The design and implementation of an LSTM-based steam generator level prediction model. In: Xu, Y., Sun, Y., Liu, Y., Gao, F., Gu, P., Liu, Z. (eds.) SICPNPP 2020. LNEE, vol. 779, pp. 505–517. Springer, Singapore (2021). https://doi.org/10.1007/978-981-16-3456-7_49
13. Song, J.M.: Principle of Automatic Control, 1st edn. Beijing Institute of Technology Press, Beijing (2020)
14. Zhang, G.D.: Research on Pressurized Water Reactor Regulator Control System Based on Intelligent Control Theory. Shanghai Electric Power College, Shanghai (2013)
15. Wang, Z.L., Guo, Y.K.: Process Control and Simulink Application. Electronic Industry Press, Beijing (2006)
16. Lin, J.: Research on the Pressurizer Control System of Nuclear Power Plant Based on Auto-disturbance rejection. Shanghai Electric Power Institute, Shanghai (2014)

Research and Application of Endogenous Security Active Defense Technology for Domestic Nuclear Safety-Level Gateway Equipment

Yong Li(✉), Ming-Xing Liu, Hao Peng, Rong-Bin Hou, Quan Ma, Ru-Qiao Wang, and Gen-Hua Liang

Science and Technology on Reactor System Design Technology Laboratory Nuclear Power Institute of China, Chengdu 610213, China
18856301679@163.com

Abstract. Gateway is a protective equipment at the boundary of the nuclear safety-level I&C system. Aiming at the unknown threat across the boundary of information physical space, this paper studies several key technologies of active defense, and constructs the gateway deep secure architecture that can resist multi-level and multi-dimensional complex attacks. Firstly, the systematic control mechanism of the gateway is constructed, which mechanism includes access control for data flow, IP whitelist at network layer, function code whitelist at application layer, IP/MAC binding and the isolation mechanism of chip's external ports. Secondly, based on the domestic trust root, the trusted chain from bootloader to the upper-layer application is built to guarantee the secure startup of the embedded system, and the key application processes are measured periodically and verified dynamically during the running process. Based on the above, from building equipment embedded trusted system environment to its security functions, a set of active security defense mechanisms of the gateway equipment sare formed, which enhances the security of the system and improves the information security protection n capability of the equipment.

Keywords: Gateway · Trusted computing · Access control

1 Research Background

In recent years, cyber security incidents have occurred frequently around the world. Especially in the power industry, cyber-attacks against critical information infrastructure are becoming more intense and intelligent, such as the US nuclear power plant was attacked in 2017, the large hydropower station in Venezuela suffered a cyber attack in 2019, the European energy giant EDP suffered a ransomware attack in 2020, and the Iranian nuclear facility suffered an unknown cyber attack in 2021, etc.

Due to the severity of the information security situation of the industrial control environment, China has promulgated the "Cryptography Law", "Data Security Law", "Classified Protection 2.0", "Regulation on Security of Critical Information Infrastructure " and other policy documents, and has carried out a series of work on information

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 200–211, 2023.
https://doi.org/10.1007/978-981-99-3455-3_20

security protection of critical information infrastructures in terms of regulations and policies, standards and specifications, inspection and evaluation, etc. The nuclear industry has also successively implemented policies such as "Cyber Security Technology and Policy for Nuclear Power Plants" and "HAD102/10", which have made complete information security protection requirements for critical control systems. Nuclear safety-level I&C system is an important part of national critical energy projects and critical information infrastructure in the modern nuclear field, and is a key target of cyber attacks, so all countries regard it as the focus of cyber security prevention and raise it to the height of national security. Considering the requirements of real-time and functional safety, information security should not adversely affect the performance, effectiveness, reliability or operation of safety-important functions, while the system logical architecture should be as simple as possible, so boundary protection is one of the key prevention research objectives for nuclear safety level instrumentation and control systems facing external information security threats. Taking into account the requirements of real-time and functional safety, information security must not adversely affect the operation of safety-critical functions such as performance, availability, reliability, etc. At the same time, the logical architecture of the system should be as simple as possible. Therefore, boundary protection is one of the key research objectives of nuclear safety-level I&C systems facing external information security threats.

2 Information Security Requirements Analysis

Gateway equipment is the boundary connection equipment between the safety level and non-safety level of the nuclear power plant I&C system. It performs protocol conversion, data transmission and information security protection functions. The protection capability of the gateway device directly affects the capability of the security-level I&C system to resist external attack threats in the field environment. Referring to the requirements of relevant domestic and foreign standards, the nuclear safety-level I&C system requirements for gateway equipment in the boundary of the security area are shown in Table 1. However, in the face of large-scale network attacks or advanced persistent threats, Gateway equipment rely on traditional passive protection methods such as defense and blocking, which cannot be effectively defended. Especially new network attacks, which can be attacked through the vulnerabilities of the attacked system itself. More precisely, establishing an active immune mechanism on the basis of the original system, to implement the system according to predetermined steps, and prevent unauthorized changes and operations is one of the effective methods for key network communication equipment to solve these kinds of problems.

Therefore, considering that the basic protection capability of gateway equipment is weak, especially in the application software, operating system, and communication protocols of embedded equipment, there are known and unknown vulnerabilities. This paper aims to combine the constraint rule strategy of traditional multi-dimensional access control, study the key technologies of active defense of gateway equipment endogenous security, refer to the coordination solution of functional safety and information security [1–12], and establish a set of active defense system of gateway equipment to ensure the reliability, availability and security of the safety level I&C system throughout the whole life cycle.

Table 1. Gateway equipment information security protection requirements

System requirements	Measures category
Border Protection	Access and data flow for controlled interface communication
	Network behavior checking/restrictions
Access control	Access Control Rule Minimization
	Check source address, destination address, source port, destination port and protocol
	Provide access based on session status information
	Data flow in and out of the network to achieve access control based on application protocols and application content
	Security mechanism failure alerts
Intrusion Prevention	Internal/external network attack behavior protection
	Advanced Persistent Threat behavior analysis and defense
	Attack behavior logging, alarm
Security Audit	User behavior and security event auditing
	Audit records are tamper-proof, deletion and overwriting
Trust Computing	Trust Computing for border equipment

3 Gateway Equipment Information Security Protection Design

The data flow of the gateway equipment is shown in Fig. 1. The security side receives data from the security level I&C system in one direction, and the non-security side sends the data to the non-security level system after taking out and encapsulating it into a standard protocol format, such as modbus-tcp. This paper aims to protect the concealed malicious behavior in the operation of the I&C system, studies the multi-dimensional fine-grained access control technology and the lightweight trusted verification technology based on domestic passwords, and builds a system-level endogenous security active defense system for gateway equipment.

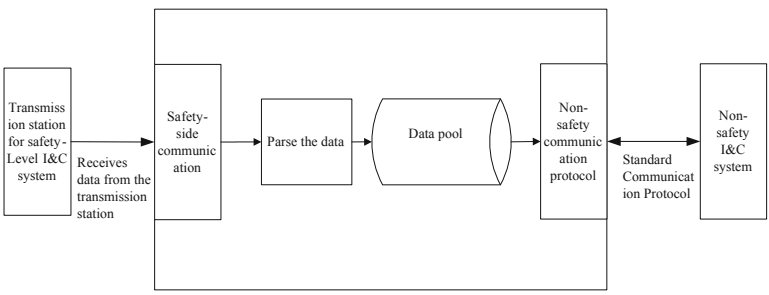


Fig. 1. Gateway Data Flow

3.1 Multi-dimensional Fine-Grained Access Control

The non-safety side of the gateway uses domestic switching chips. In terms of the traditional protection of the gateway, Firstly, the author systematically analyzes and quantifies the boundary threat of the system. Secondly, from three aspects of the communication protocol, including internal solidification, access control, and application command whitelist, to achieve IP/MAC address binding, protocol read and write command whitelist, IP address whitelist, security event log audit, illegal data and command isolation, port security isolation, denial of service protection, protocol layer security control strategy and other functional design, to construct a "white environment" based on the application layer of the operating system and the communication protocolstack (Fig. 2).

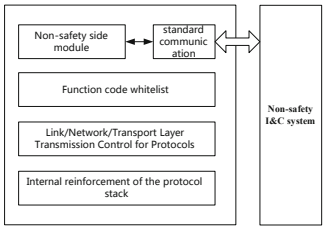


Fig. 2. Multi-dimensional access control

1) Protocol command whitelist, IP address whitelist, IP/MAC address binding
   The engineering station configures the gateway through the configuration data interface. After the gateway completes the initialization of the peripheral interface and function module, it waits for the configuration information to be issued. After the gateway successfully obtains the information configuration, it initializes the communication protocol, completes the whitelist writing of IP and corresponding MAC addresses, and the whitelist writing of protocol commands (modbus function codes).
2) Protocol layer access control
   Through the configuration of the engineering station, the non-security side implements part or all of the access control policy, including the source IP address, destination IP address, source port, destination port, and MAC address of the communication protocol land external port isolation.
3) Security Log Audit
   The gateway has the functions of recording and alarming protocol layer access control logs, configuration management operation logs, security event logs, equipment function logs, etc., and can export and view log files on the engineering station.

3.2 Trusted Calculation Design

Design Framework for Trusted Computing The Trust Computing Group (TCG) defines trustas [13]: If an entity is credible, then it always behaves in the expected

manner toward the desired goal. Therefore, the basic idea of trusted computing can be summarized as starting from the trusted root, measuring and passing trust step by step, and finally realizing the trust of the whole target system.

In this paper, the trusted computing design refers to the trusted computing 3.0 architecture and standards, and takes the national cryptographic algorithm as the basis for the design of information security. The support relationship between the national cryptographic algorithm to the gateway trusted computing and the system is shown in Fig. 3.

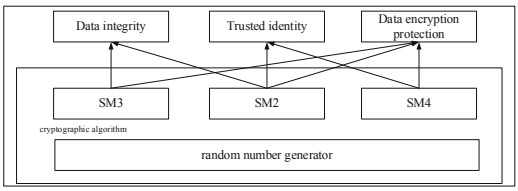


Fig. 3. Use of cryptographic algorithm

Trusted computing is the core technology for the gateway equipment to implement active immunity. The root of trust is established by implanting the hardware trusted cryptographic module. Under the premise of trusting the current execution link, the reliability and security of the next link are measured in the link, and the next step of the system is determined according to the measurement results. In this way, the system trust chain is established, the trust scope of the system is gradually expanded, and the system is trusted without tampering.

When the system is running, the Trusted Module actively performs integrity metrics on critical configuration information and data on the system, whitelist control of critical security behaviors in the system, and system trusted log storage and alerts. At the same time, At the same time, according to the pre-determined trusted policy of the equipment downloaded by the engineer station, the judgment mechanism of the equipment trusted system determines the authorization and rejection of the behavior of the functional system.

The gateway embedded trusted computing architecture is shown in Fig. 4.

The functions and design of each level are listed in Table 2.

The Trust Cryptography Module (TCM for short) is the basis for building a trusted verification mechanism, and can establish an independent and protected safe operating environment by itself. Hardware components include executor CPU, cryptographic modules (SM2, SM3, SM4), true random number generator, volatile/non-volatile storage space, and I/O interface. The firmware includes an operation management program, a function command program, and an interface for interacting with the gateway function main program.

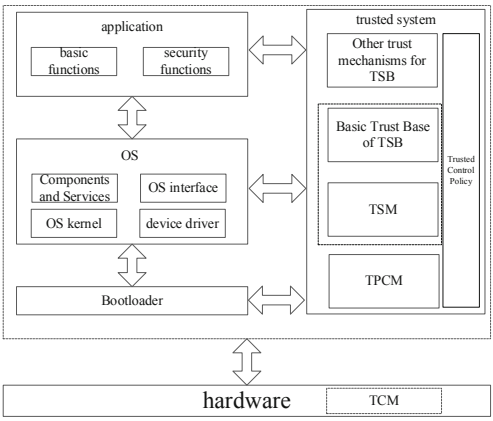


Fig. 4. Gateway Trusted Computing Design Architecture

Table 2. Design Points for Trustworthy Computing Functions

Function Point	Specific functions
TCM	provide cryptographic operation support for trusted computing
TPCM	After the controller is powered on, the TCM chip is called to measure the credibility of the PMON. After the verification is passed, the motherboard is powered on to control the hardware to start and boot
TSM	Encapsulate TCM resource management and functional commands into an interface that conforms to the standardized trusted computing support platform interface specification, providing trusted metrics and other cryptographic services to applications
TSB	Undertake trusted trust chain delivery and trusted verification of application layer code segments

```
//The underlying data structure of the signature：
typedef struct tdTCM_CERTIFY_INFO{
        TCM_STRUCT_VER version;/* version*/
        TCM_KEY_USAGE keyUsage;/* keyUsage*/
        TCM_KEY_FLAGS keyFlags;/* keyFlags*/
        TCM_AUTH_DATA_USAGE authDataUsage;/* authDataUsage*/
        TCM_KEY_PARMS algorithmParms;/* algorithmParms*/
        TCM_DIGEST_ PUBKEYdlGEST;/* PUBKEYdlGEST*/
        TCM_NONCE_ data;/* Anti-replay attack parameters*/
        BOOL parentPCRStatus;/* Whether the parent key is bound to the PCR or not*/
        UINT32 PCRInfoSize;/* PCR length*/
        [size_is(pcrInfoSize)]BYTE* PCRInfo;/* PCR information*/
}TCM_CERTIFY_INFO;{


//The underlying data structure of PCR information：
typedef struct tdTCM_PCR_INFO{
        TCM_STRUCTURE_TAG tag;
        TCM_LOCALITY_SELECTION localityAtCreation;/* locality information when creating a data block*/
        TCM_LOCALITY_SELECTION localitAtRelease;/* locality information when unpacking data or using a key*/
        TCM_PCR_SELECTION creationPCRSelection;/* PCR selection information when creating a data block*/
        TCM_PCR_SELECTION releasePCRSelection;/*CR selection information when unpacking data or using a key*/
        TCM_COMPOSITE_HASH digestAtCreation;/* Digest value of the selected PCR values when the data block was created*/
        TCM_COMPOSITE_HASH digestAtRelease;/* Digest value of PCR value selected when unpacking data bound to platform
configuration information or using a key bound to platform configuration information*/
}TCM_PCR_INFO;
```

The design of the trusted computing framework is based on the Trust Cryptography Module (TCM), and provides trusted metrics, trusted reports, and trusted storage service mechanisms through the Trust Software Base (TSB).

1) Trust Measurement

Based on the root of trust, the integrity measurement value of the gateway system is calculated, and the system trust chain is established to complete the entire integrity trust chain process including the trust measurement root core, BOOT, OS kernel measurement and repair, and system application layer protection.

```
// The underlying interaction interface of the decision
mechanism：
int tsb_estimate
(
    TSBContext *context,/*  TSBContext*/
    const char *estimate_name,/* estimate_name*/
    const char* action/* action*/
);
//The underlying interactive interface of the measurement
mechanism：
int tsb_measure
(
    TSBContext *context,/* TSBContext*/
    const char *measure_name,/* measure_name*/
    const char* action_name/* action_name*/
);
//The underlying data structure of the measurement results：
typedef struct tsb_measure_result
{
    int result;/* Measurement results*/
    int length;/* The length of Measurement results */
    const char value[0];/*The data of Measurement results*/
}TSBMeasureResult;
```

2) Credible Report

Identify the credibility of the gateway platform's identity, with uniqueness, based on the trusted report root, to realize the system's identity certification and integrity report.

```
//Low-level data interface used to create platform identity and certificate requests
TSM_RESULT Tsip_TCM_CollateIdentityRequest
(
    TSM_HTCM hTCM,/* TCM object handle*/
    TSM_HKEY hKeySMK,/* SMK object handle*/
    TSM_HKEY hCAPubKey,/* The handle to the key object containing the trusted party's public key information*/
    unsigned int uIIdentityLabelLength,/* LabelLength*/
    unsigned char* rgbIdentityLabeData,/* points to a string representing the platform identity set by the user*/
    TSM_HKEY hIdentityKey,/* IdentityKey*/
    TSM_ALGORITHM_ID algID,/* Symmetric Cipher Algorithm Type*/
     unsigned int* pulTCMIdentityReqLength,/* Output*/
     unsigned char** prgbTCMIdentityReq/* Input*/
);
```

3) Trusted Storage

Based on the trusted storage root, it implements key management and platform data security protection functions, and provides corresponding cryptographic computing services. All metrics, entity information values are stored in the root of trust.

```
//Platform Data Protection Operations
TSM_RESULT Tcsip_Seal
(
   TCS_CONTEXT_HANDLE hContext,/* HANDLE Context*/
   TCS_KEY_HANDLE keyHandle,/* keyHandle*/
   TCM_ENCAUTH encAuth,/* Encrypted authorization data*/
   unsigned int pcrInfoSize,/*pcrInfoSize*/
   unsigned char* PcrInfo,/* PCR information*/
   unsigned int inDataSize,/* Length of data to be encapsulated*/
   unsigned char* inData,/* encapsulated data*/
   TCM_AUTH* pAuth,/* The authorization data verification code for executing the encapsulation operation key is
also the output authorization data verification code*/
   unsigned int* SealedDataSize,/* SealedDataSize*/
   unsigned char** SealedData,/* SealedData*/
);
//Platform identity key management, creating key and certificate information
TSM_RESULT Tsip_TCM_MakeIdentity
(
   TCS_CONTEXT_HANDLE hContext,/* TCS_CONTEXT_HANDLE*/
   TCM_ENCAUTH identityAuth,/* identityAuth*/
   TCM_CHOSENID_HASH IDLable_PrivCAHash,/* Summary of platform identity, trusted party public key
(TCM_PUBKEY structure data)*/
   unsigned int idIdentityKeyInfoSize,/* idIdentityKeyInfoSize*/
   unsigned char* idIdentityKeyInfo,/* Parameters for generating PIK.*/
   TCM_AUTH* pSmkAuth,/* SMKAuthorization session verification information*/
   TCM_AUTH* pOwnerAuth,/* OwnerAuthorization session verification information*/
   unsigned int* idIdentityKeySize,/* PIK length*/
   unsigned char** idIdentityKey,/* idIdentityKey*/
   unsigned int* pcIdentityBindingSize,/* prgbIdentityBinding length*/
   unsigned char** prgbIdentityBinding,/* Digitally sign the result with the PIK private key*/
   unsigned int* pcEndorsementCreadentialSize,/* EK certificate data length*/
   unsigned char** prgbEndorsementCreadential,/* EK certificate data*/
);
```

Integrity Measurement Mode

The nuclear safety level I&C system belongs to the critical information infrastructure of nuclear power plants. The trusted measurement mode of the gateway equipment adopts the adjudication measurement mode. The design process is shown in Fig. 5.

The integrity measurement mainly uses the cryptographic hash algorithm (SM3) to calculate the hash value of the measured object, and the integrity check can be performed by comparing the ordered aggregate value of the integrity measurement with the integrity reference value. The process of gateway integrity measurement and storage is shown in Fig. 6. By calculating the measurement value of the measurement object, the event is

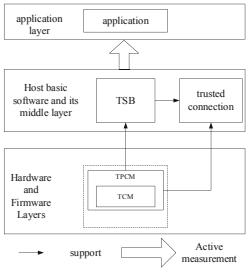


Fig. 5. Adjudication Measurement Model

recorded in the event log, and the measurement value is recorded in the platform configuration register(PCR)within the trusted cryptographic module, implement the integrity report provided by the platform to the verifier.

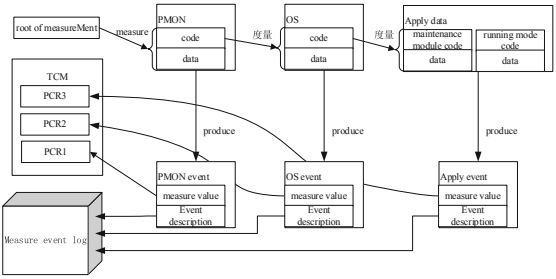


Fig. 6. Integrity Measurement and Storage Processes

In the integrity measurement and storage process, the integrity measurement value of the same component (that is, the hash value Hash(C) of the signature file content C) is stored in the same PCR. From the first one, the integrity measurement value is hashed with the existing stored value, and the operation value is updated and stored in the PCR.

$$\mathrm{PCR}_{new} = \mathrm{Hash}_{256}(\mathrm{PCR}_{old} || \mathrm{Hash(C)})$$

Static Trusted Measurement

Loongson 2k1000 is a processor compatible with MIPS instruction system, using PMON as the bootloader. The PMON startup is divided into three stages. The first stage is the assembly code part to complete the configuration of the processor operating environment, the initialization of the memory controller and the setting of the related stacks. The second stage is part C, which completes the initialization of data structures, system environment variables and related equipment; the third stage completes the operation of loading the OS kernel file. The trusted integrity measurement mode is constructed by using the characteristics of the Hash Algorithm (SM3), and the measurement values, logs and other related feature descriptions are stored in the TCM. The design process is shown in Fig. 7.

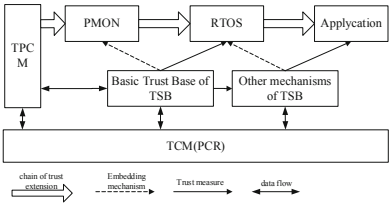


Fig. 7. Static Measurement

In the first step, the root of trust is responsible for the initial trust chain construction, and according to the measurement mechanism, checks the three stages of the boot program, system configuration, kernel image, etc. Further, verify the credibility of the bootloader, and extend the trusted scope to the bootloader.

The second step is to measure the integrity of the core part of the RTOS (including attestation service, kernel, etc.) and other mechanisms (active monitoring mechanism, trusted baseline policy library, etc.) of TSB by embedding the basic trust base of TSB into the bootloader;

In the third step, TSB's active monitoring mechanism uses the pre-installed t trusted baseline policy library to measure the integrity of the application program (mainly including protocol conversion, fault handling, maintenance communication, status self-checking, and configuration management).

Application Process Dynamic Measurement After the OS is trusted to start, in order to ensure that it has not been tampered with during the entire life cycle of the system, and considering that it does not affect the communication processing capability of the gateway and other access control measures, only the key data of the system and the application tasks of communication with non-security are considered to perform dynamic integrity measurements. The design process is shown in Fig. 8.

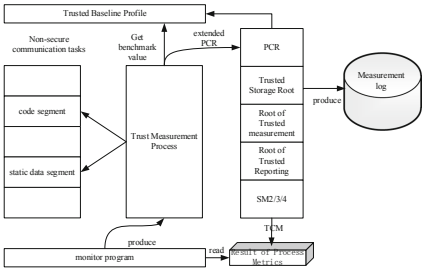


Fig. 8. Dynamic Measurement

The monitoring program creates trusted measurement processes for processes that are scheduled to be measured. The trusted measurement process can run, suspend, and restart the running process. Through the real-time dynamic measurement process, the dynamic measurement results are compared with the reference values of the measurement results. Finally, after the monitoring program periodically reads the comparison

results, the results are processed according to the processing method pre-configured from the engineering station.

4 Conclusions

This paperanalyzes the information security protection requirements at the boundary of the nuclear safety-level I&C system, referring to the coordination scheme of functional safety and information security, and combining with the actual software and hardware design environment, studies the traditional multi-dimensional and multi-type key protection technologies. On the OS application layer and the communication protocol layer, the gateway "network white environment" and "application white business" are constructed. The gateway of "network white environment" and "application white behavior" are constructed on the operating system application layer and communication protocol layer.At the same time, for the endogenous security protection of the gateway, we have studied the trusted computing technology, designed a dual-system full life cycle trusted computing protection architecture, proposed key software interfaces, and built a trusted execution environment for applications. Based on the above two points, the active defense function of endogenous security of the gateway device is systematically realized, and its information security protection capability is comprehensively improved.

References

1. U.S. NRC. Cyber security programs for nuclear facilities: RG 5.71–2010[S]. Washington, DC: NRC, pp. 4–20 (2010)
2. International Electrotechnical Commission. Nuclear power plants Instrumentation and control systems Requirements for coordinating safety and cybersecurity:IEC 62859-2016. International Electrotechnical Commission, Geneva, pp. 18-20 (2016)
3. AVENT. A unified framework for risk and vulnerability analysis covering both safety and security. Reliab. Eng. Syst. Saf. **92**(6), 745–54 (2007)
4. IECTR 63069–2019 Industrial-process measurement, control and automation Framework for functional safety and security
5. Miller, C Dr., Valasek, C.: Remote exploitation of an unaltered passenger vehicle, August 2015
6. IEC 62859, Nuclear power plants Instrumentation and control systems Requirements for coordinating safety and cybersecurity
7. IEC 62443-3-3, Industrial communication networks - Network and system security
8. IEC62645, Nuclear power plants instrumentation and control systems requirements for security programmes for computer-based systems
9. IEC 61508-3, Functional safety of electrical/electronic/programmable electronic safety-related systems Part 3
10. International electro technical commission. Failure Modes and Effects Analysis (FMEA and FMECA) : IEC 60812–2018. International electro technical commission, Geneva, vol. 20 (2018)
11. International Electro technical Commission. Functional safety of electrical/electronic/programmable electronic safety related systems-Part 1: General requirements: IEC 61508-1-2010. International Electro technical Commission, Geneva, vol. 55–56 (2010)

12. International electro technical commission. Functional safety of electrical/electronic/programmable electronic safety related systems- Part 2: Requirements for electrical/electronic/programmable electronic safety related systems: IEC 61508-2-2010. International Electro technical Commission, Geneva, pp. 15-40 (2010)
13. TCG. https://www.trustedcomputinggroup.org. [EB/OL]

I&C Design for Heat Supply Retrofit in Nuclear Power Plant

Guo -Bin Xu(✉), Jian-Wei Li, and Bing- Zhuo Zhang

Shandong Nuclear Power Company, Haiyang 265100, Shandong, China
bin5301@163.com

Abstract. Digital Instrument and Control System (I&C) is called the "Nerve Center" of nuclear power plant (NPP), which plays an extremely important role in ensuring the safe and reliable operation of nuclear power plant units. Therefore, the optimal control strategy and design scheme must be adopted for I&C in the design stage of combined heat and power retrofit projects in nuclear power plants. This paper introduces I&C design process and related technical evaluation for cogeneration retrofit of AP1000 NPP Units. It provides the key points of the renovation design of the I&C and also gives some suggestions. Because this project is the first I&C retrofit for combined heat and power among domestic nuclear power plants, it has great reference significance for the subsequent similar projects aiming at supplying district heat by nuclear power plants.

Keywords: Heat Supply · I&C · Retrofit · Nuclear Power Plant

1 Introduction

In recent years, the central heating system supplied by co-generation plants (i.e. CHP-Combined Heat and Power) or boilers which are coal-fired has been widely adopted in northern cities of China [1]. The emission of harmful substances produced by coal combustion is huge, which is a major contributor of environmental air pollution and haze weather. Therefore it is urgent to seek new clean alternative energy and improve people's living environment. As one of the clean energy resources, nuclear energy heating technology which has solved the safety problem, can become an important heating resource with great economic and social benefits in the future [2]. Units 1 and 2 of Shandong Haiyang Nuclear Power Plant are 2 × 1250MW AP1000 pressurized water reactor nuclear power units, which have been put into commercial operation in October 2018 and January 2019, respectively. The first phase of Haiyang Extraction Steam Heat Supply, NuanheOne,was officially put into operation in November 2019, using the existing auxiliary steam margin of the plant to achieve clean heating for 700,000 square meters of residential buildings in the surrounding area. According to the calculation, the project can save 23,200 tons of standard coal, reduce 382 tons of sulfur dioxide and 60,000 tons of carbon dioxide [3, 4], with significant environmental benefits.

In order to implement the national "14th Five-Year Plan" requirement of "carrying out demonstration of comprehensive utilization of nuclear energy in Haiyang, Shandong

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 212–223, 2023.
https://doi.org/10.1007/978-981-99-3455-3_21

Province" [5], Haiyang NPP, after completing the first commercial heat supply project for nuclear power plants in China, has launched the phase II heat supply project of NuanheOne, which has put into operation in November 2021. Covering the entire city of Haiyang with clean heating, replacing 12 local coal-fired boilers [6] and supplying an area of nearly 5 million square meters, Phase II heat supply project made Haiyang NPP Unit 1 the world's largest combined heat and power NPP unit [7]. In the first heating season, the heat supply was stable for 143 days, reducing the consumption of raw coal by about 180,000 tons [8]. The project achieves heat supply by extracting steam from the High-pressure cylinder of the turbine of Unit 1. This paper will introduce the design principles, scheme and impact assessment of the I&C retrofit regarding cogeneration heating system in detail.

2 Transformation of Mechanical System

The steam of phase II heat supply project of NuanheOne is extracted from the cold section of the high-pressure cylinder of Unit 1 turbine, which has a maximum capacity of 346t/h. The mechanical structure of the turbine body can meet the steam supply demand without changing. As shown in Fig. 1, each steam extraction pipe is connected respectively from the two cold section steam discharge pipes of the high-pressure cylinder and these two pipes converge to a steam main pipe where a manual isolation valve, a pneumatic check valve and a Hydraulic-operated fast-closing control valve are installed to prevent the turbine from water ingress and overspeeding, and to isolate the extraction steam during the non-heating season. In the following process, the main pipe is divided into two branches to connect respectively two separate heaters, and after heat exchange, the condensed steam returns to the condenser of turbine. The relevant equipment is arranged in the newly constructed house called Adjoining House which is adjacent to the steam turbine building. In addition, $4 \times 25\%$ variable frequency circulation pumps are set up to supply the pressurized and heated circulating water to the secondary heat station of heat network outside of the NPP. The pressure maintaining and water supplemental system will automatically track the system pressure for constant pressure water replenishment, and the related equipment are installed in the First Heating Station (FHS) located at the Balance of Plant (BOP) area of the NPP physical protection area (also called physical security) [9].

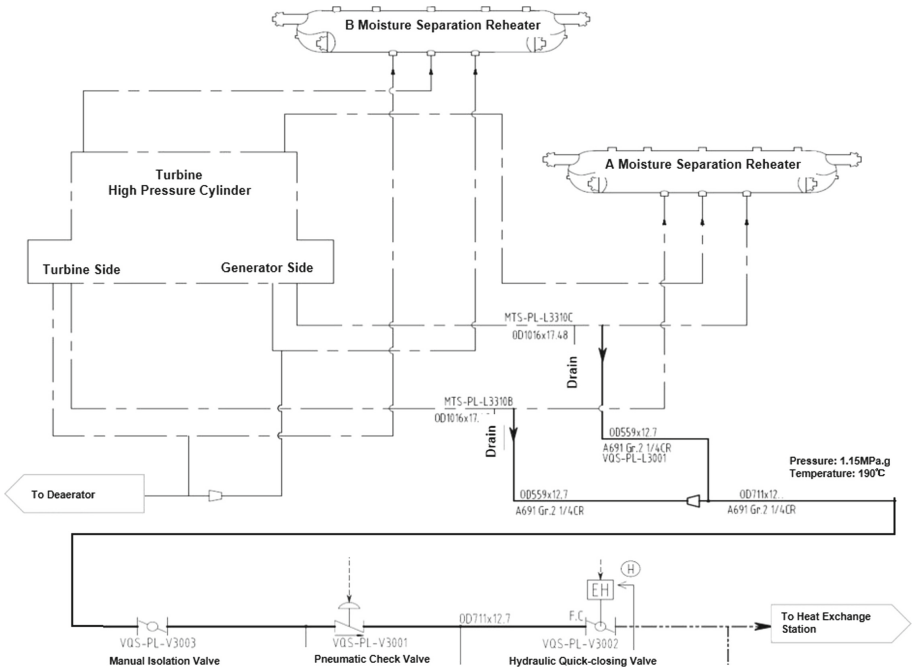


Fig. 1. Extraction Steam Process Diagram

3 I&C Retrofit Design

3.1 Main Design Principles

Several main principles and key points are considered in the I&C retrofit design scheme for combined heat and power of NPP units:

1) The design scheme should be fully evaluated and must not negatively affect the existing I&C system of the NPP units (including both software and hardware).
2) Information and network security is a key aspect to consider in the design, and the design must meet the requirements of relevant current regulations, standards and codes.
3) Important protection and control signals shall consider redundant configuration and the hard-wired signal transmission is preferred [10].
4) The design solution must fully consider the implementability of site construction, installation and commissioning.
5) The I&C retrofit scheme must take into account the requirements from the department of operation and management (e.g. different operation groups may have different requirements for the monitoring of new equipment).

3.2 I&C Overall Design Plan

The I&C retrofit for combined heat and power purpose mainly includes the modification of PLS (Plant Control System, the non-safety I&C system for NPP units) located in the turbine building as well as the PLC (Programmable Logic Controller) in the FHS. The PLS is implemented via Ovation platform supplied by Westinghouse, which is used to control and monitor the heating equipment located in the Adjoining House, while the PLC (Siemens S7–400 series) in the FHS is mainly to complete the monitoring of the new Frequency converter and circulating pumps as well as other equipment arranged in FHS. According to the design principles in Sect. 3.1 and the requirements of the operators, the following overall design requirements was formed.

1) Monitoring requirements

The monitoring and control of the equipment in the Adjoining House (e.g. steam pipes, heaters and related valves) is incorporated into the Main Control Room (MCR) of the NPP units and monitored by the units operators, and the control is implemented by PLS; the monitoring and control of the equipment within the scope of the FHS is incorporated into the BOP Central Control Room and monitored by the BOP operators, and the control is performed by the PLC controller located in the FHS.

2) Scope of PLS transformation

Considering the implementability of the transformation, a pair of Ovation-based upgrade OCR controllers with an additional cabinet are added, which are more powerful than the existing controller and can be perfectly interfaced with the existing PLS system through proper configuration. With the new control cabinet, the equipment under the control of the PLS can be monitored and operated from the MCR of the unit, including all controlled equipment and measurement points on the extraction steam pipes, such as Quick-closing control valves, extraction steam check valves, drain valves, extraction steam pressure, temperature and flow measurement points, etc.. It also includes equipment and measure points on the heaters in the Adjoining House, such as steam inlet valves, drain valves, temperature measurement, circulating water inlet valve and outlet valve, heater tank level, etc.

Considering the important parameters on the circulating water side at FHS (e.g.circulating pump operation status, water supply flow, etc.) are closely related to the heater operation in the Adjoining House and need the attention of the operator at MCR, this part of information shall also be directed to the new PLS cabinet through the remote PLC I/O (input and output) cabinet for remote monitoring of the operator at MCR (shown in Fig. 2). The new PLS cabinet is connected to the switch in computer room through fiber optic cable to realize the combination with the existing PLS platform.

1) Modification scope of BOP monitoring and control

The scope of BOP monitoring and control mainly includes the equipment at the FHS, such as circulating water pumps, frequency converters, water make-up devices, etc. Other information that needs to be monitored includes the status of circulating water inlet and outlet valves of heaters and extraction steam flow at Adjoining House next to turbine building.

As the phase II heat supply project of NuanheOne added circulating pumps, frequency converters, and other equipment in the FHS, the capacity of the original PLC controller could not meet the needs of the new equipment, so the corresponding I/O modules were added on the basis of the original PLC configuration. The original S7–300 series PLC was also upgraded to the more powerful S7–400 series controller. In addition, a new PLC remote I/O cabinet was added, responsible for the signal exchange between the new PLS cabinet and the PLC at FHS. The signals from the PLC remote I/O cabinet is hard-wired to the new PLS cabinet, while the signals exchange between the remote I/O cabinet and the PLC controller at FHS are via fiber optic cable. Despite a local operator station is installed at the FHS, another operator station is also set up at the centralized control room of BOP to realize the remote monitoring and control of the heating system at FHS.

2) Cyber security considerations

From the definition and classification of I&C system, PLS in turbine building and PLC at FHS both belong to the category of Industrial Control System (ICS) [11], they are classified together in Control Zone (also called Safety Zone I) in nuclear power plants and defined as level 3 [12]. According to the requirements, the communication between different safety zones or subsystems within the same safety zone or industrial control system, which are divided according to different operational characteristics, should be technically isolated [11, 12]. Therefore, taking into account the amount of signals exchanged between the PLS and FHS PLC as well as the cost of deploying equipment for information security protection, this project adds a new PLC remote I/O cabinet and uses hard-wired access to achieve conservative and secure information transfer.

3) Design of important protection and control signals

Important protection and control signals mainly refer to those signals that implement protection and control function which may have a great impact on the safe operation of NPP units in case of signal failure, such as discrete signals, e.g.Turbine Trip, load Run Back (RB), turbine Overspeed Protection Control (OPC), Generator Circuit Break (GCB) open, etc., and analog signals, e.g. MW Signal, Turbine first stage pressure, Turbine exhaust pressure signal, etc.. These signals are involved in the interlocking and protection logic of heating extraction Quick-closing valves, check valves and other important equipment for heating (described in Sect. 3.3) and need to be hard-wired into the systemto ensure the safe operation of the NPP units and the heating system [13].

As shown in Fig. 2, important control and protection signals are sent from the PLS Drop 21/26/31 control cabinets to Drop 37 (the new PLS cabinet for heating) through hard-wiring, while non-important signals for display, alarm and operation are communicated from Drop 37 to the DDS (data display and processing system) through optical fiber to realize the monitoring and operation of heating equipment at Adjoining House from MCR. It is worth mentioning that the OPC signal design is relatively difficult. On the one hand, it has a response time requirement, which requires fast cut-off of heating steam when the OPC is in operation (the whole processing cycle is less than 1s) in order to prevent the turbine from overspeeding and water ingress. On the other hand, it is not advisable to take the signal directly from the Relay cabinet of the Turbine Protection

System, which will increase the difficulty of implementation and may introduce risks to the Turbine protection system.These two requirements are contradictory. After studying, the retrofit team creatively proposed the solution of collecting three signals from Drop 31 (turbine auxiliary system control cabinet) and at the same time reducing the processing cycle in Drop 37, which not only solved risks of relay circuit expansion in the protection cabinet but also resolved the issue of fast response.

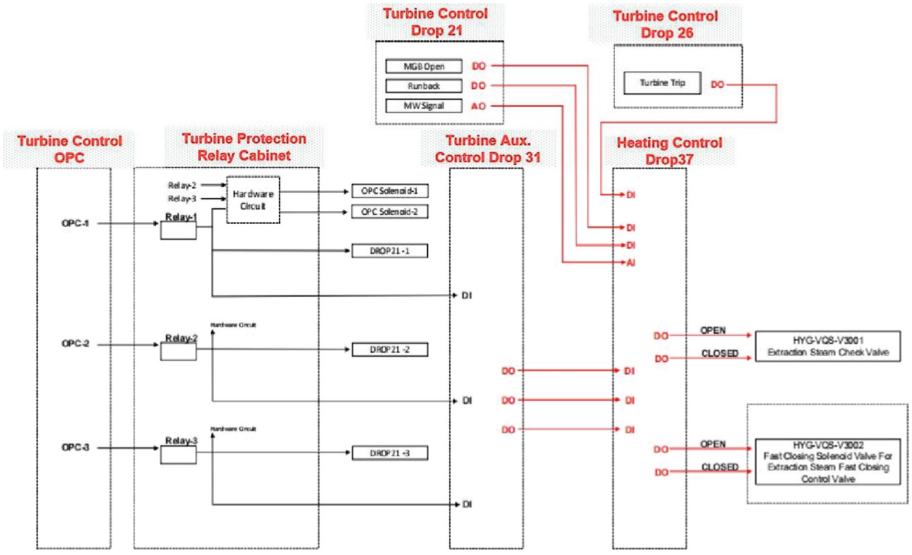


Fig. 2. Signal Exchange Diagram

3.3 I&C Control Logic Scheme

1) Control Logic Design Principle

I&C control logic design is an important part of the digital I&C system application software, and its design quality will influence the safe and stable operation of the NPP units. The design of control logic mainly observes the following principles:

a. The control logic design must be subject to a strict functional design process, including the mutual submission of information from different majors (mechanical, electrical, I&C, etc.) within the design institute as well as the information submission between the design institutes and I&C system supplier.

b. The design of the I&C control logic for heat supply must have relative independence and can be separated from the existing I&C platform, so that the independent test and verification of the main functions can be carried out. The relatively independent design is not only conducive to shortening the design and development cycle of the software, but also conducive to the quick and efficient completion of most of the field commissioning and verification work before the overhaul, to minimize the retrofit work during the overhaul (the overhaul leaves only 1–2 weeks

for the modification of the I&C system), which is an important principle to be considered at the beginning of the design.

c. Carry out the impact assessment of the retrofit project on the existing I&C system regarding both hardware and software, which is an important work that must be considered before the modification of digital Instrumentation and Control system. The purpose of the evaluation is to ensure that the impact of the software and hardware changes from the project on the performance of the existing I&C platform is acceptable.

2) Heat supply system IN/OUT logic

a. Extraction steam IN: When the NPP unit load is $\geq 50\%$ of the rated load, the local hydraulic oil station(for Quick-closing valve) is ready, the operation of the steam extraction is allowed to be put into operation.

b. Fast cut-off of the extraction steam: When any of the following conditions is met, it leads to Fast cut-off of the heat supply system:
   ① Turbine trip
   ② MGB Open
   ③ OPC Action
   ④ Pressure Ratio (exhaust steam pressure /first stage pressure of high pressure cylinder)

   After the Fast cut-off occurs, it directly leads to the fast-close of the extraction steam Quick-closing control valve (speed at 400%/s), check valve and electrical shut-off valve, and the heat supply system will exit operation in about 1s.

c. Slow cut-off of the extraction steam: Satisfying any of the following conditions will result in Slow cut-off of the heating system:
   ① NPP unit load $< 50\%$ of rated load
   ② Unit RB (Run Back)
   ③ Heater level high 3
   ④ Heat load removal (all circulating water pumps stop)
   ⑤ Manual exit

   When the Slow cut-off occurs, the Quick-closing control valve on extraction steam line closes slowly (speed at 1.667%/s), the valve position of the check valve and electrical shut-off remain unchanged, and heat supply system will be out of operation after about 1 min.

3) Control Logic of the Quick-closing Control Valve

The Quick-closing control valve is a hydraulic-driven valve used for controlling extraction steam flow. On site the valve is equipped with a set of independent hydraulic oil station as well as a set of PLC controller for the control of the oil station equipment and the local operation of the Quick-closing valve, but also for the interface of the remote PLS command drive signal. According to the design requirements, considering the large heat capacity in the heating system, there is no need to adjust the valve frequently. Therefore, the Quick-closing control valve is designed to realize the adjustment of heat supply by manual operation. The relevant control functions are as follows:

a. Normal Operation: If the Extraction Steam IN exists and there is no signal of Pressure Ratio, the a.Quick-closing control valve is allowed to open. If the signal

of Pressure Ratio is present during the opening process, the valve will be blocked to open further.

b. Abnormal Operation: When the fast closing command, e.g. Turbine trip, MGB Open, OPC Action and Pressure Ratio exists, the Quick-closing control valve closes quickly.
c. Command Tracking: at local control mode, the valve will be in tracking state and the tracking value is the actual valve position feedback. While at Fast cut-off mode, the valve closes at a rate of 400%/s and the valve closes at a rate of 1.667%/s at Slow cut-off mode.
d. Remote/Local Control: the local PLC is equipped with a remote/local changeover switch. When the remote control is selected, the valve position control command from PLS sends a 4-20mA signal to the valve proportional valve via local PLC to control the linear operation of the valve; when the local control is selected, the manual button on the control panel of the local control cabinet can realize the slow opening, slow closing and fast closing functions of the valve.

4) Design transients and Related Logic

During heat supply operation, the main design transients and responses are as follows:

a. When the electrical power is below 50% of the rated power, the extraction steam check valve and the Quick-closing control valve are automatically closed after a delay of 1 min to remove the heat supply.
b. when RB occurs, after a 3s-delay it automatically closes the extraction steam check valve and the Quick-closing control valve to remove the heat supply.
c. When the water level of both heaters are up to high 3, extraction steam check valve and the Quick-closing control valve will automatically close.
d. When the generator is off the grid, it needs to quickly close the check valve as well as the Quick-closing control valve to remove the heat supply.
e. When turbine trip occurs, check valve and the Quick-closing control valve shall be quickly closed to prevent turbine from entering water and overspeeding [14]. At the same time, the turbine trip signal also automatically opens drain valves on the extraction steam pipes.
f. When OPC operates, it quickly closes the check valve and the Quick-closing control valve to remove the extraction steam.
g. When the Pressure Ratio reaches low alarm, the Quick-closing control valve is automatically restricted from continuing to open; when the pressure ratio reaches low-low, both check valve and Quick-closing control valve are quickly closed to cut off the heat supply.

5) Pressure Ratio Protection Logic

The steam extraction capacity of "Nuanheone" Phase II project is 346t/h, and the steam flow can ensure flow adjustment in full range without the involvement of ICV (turbine low pressure cylinder inlet regulating valve) to maintain extraction steam pressure. However, in order to be sure of the safe turbine operation and avoid damage to the last stage blades of high-pressure cylinder [15], a Pressure Ratio logic has still been set up, and a low Pressure Patio alarm (0.171) will automatically restrict the Quick-closing control valve from continuing to open wide (the valve can be closed

at a rate of 1%/s), and a low-low Pressure Ratio (0.165) is used to quickly cut off the extraction steam to prevent the pressure ratio from continuing to deteriorate.

6) Function of Reactor-Turbine Power Matching

AP1000 nuclear reactor and turbine representing the first and second loop respectively are in the reactor-following mode during normal operation of NPP, which is achieved by the reactor tracking the turbine first stage pressure (representing turbine load). The turbine load signal is derived from measurement of the turbine first stage pressure, and it is calculated from turbine first stage pressure using the polynomial: PTU = A0 + A1 (TP) + A2 (TP^2). (PTU is turbine load; TP is turbine first stage pressure; A0, A1, and A2 are empirically determined coefficients which is 0.036%, 22.56%/MPa guage and -0.44%/MPa guage respectively.)

However, the current implementation uses a function generator with the data points in the curve (Fig. 3). The reactor power control loop converts the first stage pressure of turbine into the reactor thermal power according to the curve shown in Fig. 3, and then generates the reference average temperature (Tref), and finally regulates the reactor power by adjusting the control rods.

The first-stage pressure relationship curve will produce a certain deviation (less than 0.43%) during heat supply operation than that in non-heat supply condition and the impact after evaluation on the nuclear island related control system is small and acceptable. The reactor control loop can retain the exiting curve and the corresponding control logic does not need to be modified.

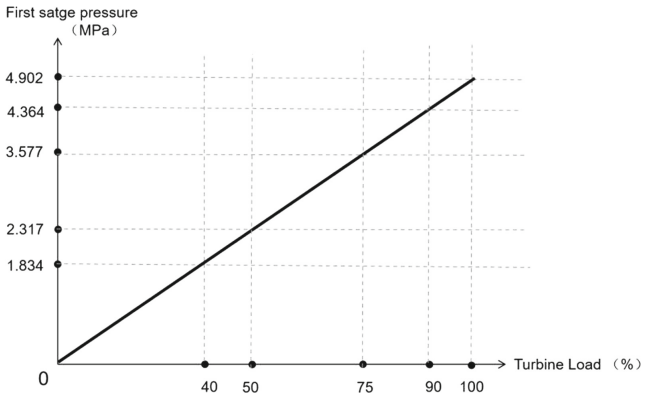


Fig. 3. Turbine first stage pressure versus turbine load curve

4 Evaluation of Existing I&C System

The increase of I/O points in PLS system of this heat supply renovation is about 210 points which is not large scale, and the complexity of the control logic change is average, but considering that the total number of points in the Ovation platform of the existing PLS system is close to 200,000 points capacity limit and the number of DDB (Dynamic

Data Blocks) of Ovation platform has reached 2804 (maximum allowed value 3072), the impact on the overall performance of the existing system is not clear. Therefore, it is necessary to conduct an overall evaluation for the existing PLS system, including evaluation of the number of DDBs, network load and controller performance, etc. to ensure that the impact on the overall performance of the I&C platform after the heat supply renovation is acceptable.

4.1 DDB Impact Assessment

Each type of points of Ovation system contains Dynamic Data, which are broadcasted periodically to the Ethernet in the form of Ethernet frames (SNAP subnet access protocol) with DDB as carrier to realize real-time data exchange. Since the length of LD/LA/RM/LP/LC types is 20/24/28/12 bytes respectively, the length of each point is about 18 bytes by weighted average calculation, and the maximum length of DDB according to Ovation user manual is 1400 bytes for Ethernet (4044 bytes for FDDI/CDDI network), so this modification generates a total of 1822 Internal points, about 24 DDBs, compared with 2804 before the modification, the increase is only 0.85%, the impact is very small.

4.2 Network Load Assessment

The calculation of network load is mainly determined based on DDB and network bandwidth. Since each DDB occupies 1400Byte, i.e. 1400*8 = 11200 bits, and the bandwidth of this system is 100Mbps, so the occupied bandwidth of each DDB is 11200/100000000 = 0.0112%, and the number of original DDB is 2804, then it occupies 2804*0.0112% = 31.4%. Considering that 256 reserved DDB occupies 0.52% bandwidth and the original total capacity is 31.93%. Therefore, with 24 new DDBs, the network bandwidth rises to 32.2%, but it is still lower than the design requirement value of 40%.

4.3 Controller Performance Evaluation

As mentioned earlier, a pair of upgrade Ovation controllers was added to this retrofit, and the controllers were tested in simulated environment during the factory test to evaluate the potential impact on the database as well as the newly added logical applications. The results showed that the average cycle time and worst cycle time of the new processor were significantly lower than those of existing processors, and the performance of the new controllers was improved. Because new application function logic newly added in this project is all performed in the new Drop controller and the other related Drops are only responsible for sending out a small amount of signals involved in functional logic, there is almost no impact on its own controller performance.

By evaluating the technical parameters that mainly affect the performance of the I&C system platform, the results show that the I&C modification regarding heat supply retrofit has no adverse impact on the performance of the existing Ovation platform.

5 Conclusion

The I&C system plays a key role in the safe and stable operation of the NPP units and must be carefully modified. This paper introduces the technical strategy, evaluation and design process of the I&C retrofit for the first domestic nuclear power plant heat supply renovation project, and puts forward many innovative design ideas in the absence of reference, which not only solves the many difficulties of the project in terms of technical difficulty, time constraint and implementability requirements, but also ensures the safety and reliability of the overall I&C platform. Through factory testing, on-site commissioning and one district-heating season operation, the relevant I&C design has been fully validated, providing a strong guarantee for safe and reliable long-term operation of the NPP unit during the heating season. Due to some constraints, the design and evaluation of this project still have certain shortcomings, further optimization and improvement can be carried out in the subsequent "Nuanheone" Phase III 900MW heat supply project. The design and recommendations of the I&C modification presented in this paper can provide reference for the similar heat supply projects of the nuclear power units.

References

1. International Atomic Energy Agency (IAEA): Guidance on nuclear energy cogeneration. IAEA nuclear energy series No. NP-T-1.7, Printed by the IAEA in Austria (2019)
2. Li, X.B., Zhang, H.N., Qu, K.Y., Li, F.C.: Analysis of the superiority of nuclear energy centralized heating system. Huadian Technol. **42**(11), 69–82 (2020)
3. https://www.world-energy.org/article/14011.html. Accessed 31 July 2022
4. https://www.neimagazine.com/news/newschinas-nuclear-heating-project-begins-operation-7527361. Accessed 31 July 2022
5. Xinhua News Agency: Outline of the Fourteenth Five-Year Plan for National Economic and Social Development of the People's Republic of China and the Vision 2035 (2021)
6. https://www.nucnet.org/news/city-of-haiyang-first-in-country-to-have-district-heating-system-powered-by-nuclear-11-5-2021. Accessed 31 July 2022
7. https://global.chinadaily.com.cn/a/202111/09/WS618a4332a310cdd39bc744c8.html.Accessed 31 July 2022
8. People's Daily: State Power Investment Corporation-Warming Thousands of Households and Guarding the Blue Sea and Blue Sky.10 May 2022
9. Xu, G.B., Zhang, B.Z., Li, J.W.: Introduction of network architecture for real-time information management system in nuclear power plant. In: Xu, Y., Sun, Y., Liu, Y., Gao, F., Gu, P., Liu, Z. (eds) The Sixth International Symposium on Software Reliability, Industrial Safety, Cyber Security and Physical Protection of Nuclear Power Plant (ISNPP), Lecture Notes in Electrical Engineering, vol. 883, 34–41. Springer, Heidelberg (2022). https://doi.org/10.1007/978-981-19-1181-1_4
10. International Electrotechnical Commission: Nuclear power plants - Instrumentation, control and electrical power systems important to safety - Categorization of functions and classification of systems, IEC Std.61226–2020 (2020)
11. Standardization Administration, China: Information Security Technology - Baseline for Classified Protection of Cyber Security, GB/T 22239–2019 (2019)
12. National Energy Administration: Notice on the Issuance of Security Protection Schemes and Evaluation Specifications for Security Protection of Power Monitoring Systems (2015)

13. Standardization Administration, China: Code for the design of conventional islands of nuclear power plants, GB/T 50958–2013 (2013)
14. Lian, H., Li, B.Z.: Analysis of the implementation of heat supply and coordination control logic for supercritical condensing heating units. Energy Environ. **06**, 12–16 (2016)
15. Liu, B., Gai, D.F.: Analysis of control system design in heating renovation for pure condensing units of thermal power plants. Huadian Technol. **38**(1), 22–24 (2016)

Research and Application of Current Following Electrical Fire Monitoring Technology

Xu-tao Bai(✉) and Bao-cheng Sun

Suzhou Nuclear Power Research Institute, Suzhou 215004, Jiangsu, China
baixutao@cgnpc.com.cn

Abstract. This paper briefly introduces the frequent occurrence of electrical fires in China, analyzes in detail five failure modes in electrical fires, such as short circuit, poor heat dissipation, poor contact, overload and leakage, and analyzes the current main domestic electrical fire monitoring methods according to the failure modes. By studying the serious problem of false alarm in the process of residual current monitoring, the current follow-up technology is creatively developed, which effectively avoids the "false alarm" problem of electrical fire monitoring caused by the change of inherent leakage current.

Keywords: Residual current · Electrical fire · Current follow-up

1 Introduction

In recent years, electrical fires have occurred frequently in China, with casualties and major property losses occurring from time to time. From 2015 to 2019, there were 1.452 million fires in China, with 7,723 deaths and 4,927 injuries, and direct property losses of 19.87 billion yuan. Among them, there were more than 498000 electrical fires, causing a total of 2,795 deaths and 1,809 injuries, with a direct economic loss of 8.89 billion yuan. The four indexes of electrical fire accounted for 34.3%, 36.2%, 36.7% and 44.7% of the total fire statistics in China respectively. From 2015 to 2019, there were 408 major fires nationwide, of which 234 were caused by electrical reasons, accounting for 57.4% [1]. In the first half of 2020, there were more than 30 major fires, including 18 electrical fires, accounting for 60%.

The electrical safety risk is still at a high level, and the fundamental characteristics of electrical fires affecting the fire trend have not changed. In addition to the nuclear reactor, the nuclear power plant also has power generation, transmission, distribution and control. In order to ensure the safety of nuclear power generation, it is necessary to monitor the operation status of electrical equipment through electrical fire monitoring equipment to avoid electrical fire.

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 224–232, 2023.
https://doi.org/10.1007/978-981-99-3455-3_22

2 Electrical Fire Electrical Fault Analysis

2.1 Short-Circuit

Once a short-circuit occurs in the circuit, the current in the circuit will increase sharply. According to the heat theorem, the heat generated is proportional to the square of the current, so the heat generated is huge, which makes the temperature of the circuit rise sharply in a very short time, quickly exceeding the rated current of the circuit and instantly exceeding the allowable range of the current. The resulting high temperature will reach or even exceed the ignition point of surrounding combustibles, thus igniting adjacent objects and causing electrical fires. In addition to the influence of temperature, another influence caused by short-circuit is the high-temperature metal particles splashed everywhere. These splashed metal particles can easily ignite combustibles with their own ultra-high temperature, which leads to electrical fires.

Metal short-circuit and arc short-circuit are two different forms of short-circuit fault. Metallic short-circuit refers to the melting and welding of conductors at the short-circuit point. In addition to the large short-circuit current, it will also produce abnormal high temperature, which will ignite the insulated conductor. The characteristic of arc short-circuit is that the conductors at the short-circuit point are not connected together when the short-circuit fault occurs, but the short-circuit point will produce spark arc with ultra-high temperature, which can even reach more than 2,000 °C. Under this high temperature condition, fire is easy to happen. Because the arc impedance is very large, it limits the short-circuit current when the arc occurs, so generally, the overcurrent protection device will not act and cannot cut off the power supply. As the power supply is still in arcing short-circuit, it will continue to maintain, which is very likely to cause fire [2].

2.2 Poor Heat Dissipation

Electrical equipment will inevitably generate heat during use. The unreasonable design of the heat dissipation system of the electrical equipment itself or the improper selection of materials will cause the electrical equipment to not get timely and effective heat dissipation, which will always be maintained at a relatively high temperature level, and the combustibles around the equipment will be ignited due to the high temperature.

The main causes of electrical fire caused by poor heat dissipation include: the degradation of heat dissipation capacity of electrical equipment with long operation time; The design of the equipment is irrational or the materials have quality problems. These factors can make the equipment unable to dissipate heat effectively. In addition, failure to operate according to regulations or untimely cooling of equipment will also lead to poor cooling.

2.3 Poor Contact

Various conductive circuits are composed of multiple conductive elements. Among them, the two pieces are in conductive contact with each other through mechanical connection to achieve conductivity, which is called electrical contact. Poor contact mainly occurs in the connection between wires and electrical connectors, the connection between wires

and electrical appliances, and the connection of electrical switches themselves. Poor contact is mainly manifested in excessive contact resistance and contact vibration or looseness. Therefore, there are three main reasons for fire caused by poor contact:

(1) Bad contact will cause excessive contact resistance and overheating, which will ignite surrounding combustibles and cause fire.
(2) Short-circuit and fire caused by poor contact develop rapidly.
(3) It is caused by loose switch and poor contact, causing arc or fire.

2.4 Overload

Circuit overload is another important factor causing fire. Overload will not directly cause fire, but in the long-term overload line, it will cause the thermal conductor to increase the temperature rise, accelerate the aging of wire insulation, and reduce the insulation strength, which is easy to cause insulation breakdown and short-circuit. Under severe overload conditions, the heat generated can ignite the surrounding combustibles and cause a fire. Therefore, overload often leads to short-circuit, poor contact, leakage and other faults.

2.5 Leakage

Affected by external forces and the environment, as well as the natural loss of insulation aging, the leakage current from the flowing line of the building abroad, the infrastructure attached to the low insulation material line of an object, in order to generate high-temperature two-way flow, electric arc and electric spark caused the fire of combustible combustion, which is called electric leakage fire.

The leakage fire caused by the live line low-voltage line is one of the more specific and difficult to prevent. It is usually caused by short-circuit, overload and fire hazards. Line leakage causes fire. Phase line and neutral line can occur between phase line and land, but the most common is line to ground [3].

3 Main Monitoring Means

3.1 Residual Current

Residual current is one of the main causes of electrical fire. Residual current electrical fire monitoring system can prevent the failure of distribution circuit by monitoring the change of residual current value of the protected line. Residual current electrical fire monitoring system is composed of residual current sensor and signal processing unit, which can monitor the leakage current of the whole distribution circuit, and the alarm value of the detector is set between 20 ~ 1,000mA,. It is usually arranged in the primary or secondary distribution system, and can also be arranged in the tertiary distribution system, so as to more accurately locate the fault location and provide convenience for the troubleshooting of grounding faults [4].

3.2 Equipment and Ambient Temperature

Temperature measuring electrical fire detectors are mainly used to prevent and control overheating faults. The commonly used temperature measuring electrical fire detectors can be divided into point based temperature detectors (such as thermocouples and platinum resistors), wire based temperature detectors (such as optical fiber temperature sensing and temperature sensing cables) and surface based temperature detectors (such as infrared thermal imagers) according to their detection areas. These detectors generate alarm signals by monitoring the temperature change of a certain distribution device or electrical equipment (distribution cabinet, distribution box, connection part of distribution line, electrical equipment, etc.) in the distribution system, so as to achieve the purpose of preventing electrical fire. Its characteristic is that it is only effective for a certain point or local range of the monitoring object.

3.3 Fault Arc

Short-circuit and poor contact are the main causes of electrical fire. Most short-circuit faults can be solved by the function of power distribution system, and some short-circuit faults show that short-circuit produces fault arc. At this stage, there is still a certain blind area in the distribution system, which can not effectively monitor and protect such faults. The main reason is that the short-circuit contact surface or the line impedance that generates fault arc limits the size of short-circuit current, which often makes the circuit breaker unable to reach the action conditions. This kind of fault is very harmful, causing the insulation of the distribution line to carbonize and catch fire quickly, or the flammable substances around the fault point are ignited by local high temperature, resulting in electrical fire. The fault arc type electrical fire monitoring detector is an electrical fire detection device that can identify the fault arc. It is convenient to access the existing electrical fire monitoring system, and can monitor the voltage, current and fault arc data of the monitored line or equipment in real time. It can send an alarm signal immediately after the fault arc monitoring value exceeds the alarm threshold. This technology can effectively make up for the shortcomings of the existing electrical fire detection technology, and effectively reduce the electrical fire caused by the fault arc by early warning or cutting off the fault power supply [4].

3.4 Pyrolysis Particles

Pyrolysis particles refer to the smallest particles that exist in a free state when a substance is heated. Pyrolytic particle detector refers to a detection device that uses advanced detection means to detect pyrolytic particles emitted by insulating materials heated in the air. Due to the use of a variety of composite detection means and advanced software design, it can improve the sensitivity and accuracy of detection. It is a new type of electrical fire detection device. Pyrolytic particle type electrical fire monitoring detectors are generally configured in the primary or secondary low-voltage distribution cabinets, network cabinets in large data centers, important communication equipment cabinets in communication base stations, etc. by detecting the concentration of pyrolytic particles emitted by the insulation sheath of wires when various equipment and wires are overheated, fire

alarm prediction is carried out. It fills the gap in the monitoring of distribution equipment and helps to realize the early warning of electrical fire in distribution equipment.

4 Residual Current Test Principle

By comparison, the residual current electrical fire monitoring system has the advantages of wide monitoring range, wide application range and long pre tightening period. At present, the method of measuring residual current is that three phase lines and N lines pass through the residual current transformer at the same time [5].

According to vector analysis, under normal conditions, when the three-phase currents are basically the same, the vectors of the three-phase currents differ by 120° respectively. It should be noted that assuming that the alarm value is set to $S_{alarm} = 300\,mA$, the following analysis is made to see what the difference is between the abnormal currents of each phase in this case.

Assuming that the current of each phase is basically balanced under normal conditions, the residual current amplitude after synthesis is $S_n = 30\,mA$, the included angle with phase A is $\alpha = 30°$,The abnormal residual current of each phase is SFa、SFb、SFc, which is calculated as follows.

$$\begin{cases} SFa = \sqrt{S_{alarm}^2 - S_n^2 Sin^2\alpha} - SnCos\alpha \\ SFb = \sqrt{S_{alarm}^2 - S_n^2 Sin^2(60° + \alpha)} + SnCos(60° + \alpha) \\ SFc = \sqrt{S_{alarm}^2 + S_n^2 - 2SnS_{alarm}Cos(120° + \alpha)^2} \end{cases} \tag{1}$$

Put $S_{alarm} = 300\,mA$, $S_n = 30\,mA$, $\alpha = 30°$ can be obtained by substituting into formula (1): $SFa = 273.6\,mA$、$SFb = 298.5\,mA$、$SFc = 326.3\,mA$, The maximum difference between the sensitivity of each phase is $SF_{max} = |SFa - SFc| = |273.6 - 326.3| = 52.7\,mA$.

In fact, due to the poor balance between the residual currents of each phase, if the residual current amplitude after synthesis reaches 80\,mA, the included angle with the standard phase A $\alpha = 30°$. When the alarm value is still 300\, mA, $S_n = 80\,mA$, $\alpha = 30°$, Substitute formula (1) to obtain: $SFa = 280.0\,mA$、$SFb = 289.1\,mA$、$SFc = 371.4\,mA$, The maximum difference between the sensitivity of each phase is $SF_{max} = 143.4\,mA$.

This shows that if the system alarm value is preset to 300\, mA, the abnormal residual current value required becomes smaller, that is, the alarm sensitivity becomes higher. When phase a reaches 228\, ma or phase B reaches 289\, ma, it may alarm. In fact, this is also a false alarm [6].

5 Residual Current Follow-Up Threshold Alarm Technology

Through the test, it is found that in the current power system, switching power supply, thyristor voltage regulation and frequency conversion equipment are widely used, so a large number of harmonics are generated, of which the third harmonic of power frequency is generally the most influential. At the same time, when the power cable transmits

power, the existence of distributed capacitance and distributed inductance between the conductors in the cable forms the leakage current caused by the distributed capacitance to the alternating current, which is the so-called "inherent leakage" current.

$$\text{Residual current value} = \text{inherent leakage current value} + \text{fault leakage current value} \quad (2)$$

Through the research, it is found that the inherent leakage current changes with the number of electrical equipment. The more electrical equipment is turned on, the greater the inherent leakage. The leakage current value is concentrated in the range of 10−500 mA, and some can exceed 1000 mA. The inherent leakage problem cannot be solved, and there are a lot of "false alarm" problems in the application of residual current electrical fire monitoring detectors.

According to the two-year follow-up survey of dozens of users of electrical fire monitoring systems in major cities across the country, it is found that the magnitude of all residual currents is constantly changing and changing regularly. However, the alarm threshold of the electrical fire monitoring detector is preset, which leads to different alarm sensitivity, sometimes high and sometimes low, resulting in a high false alarm rate. Figure 1 shows the residual current curve of an actual test.

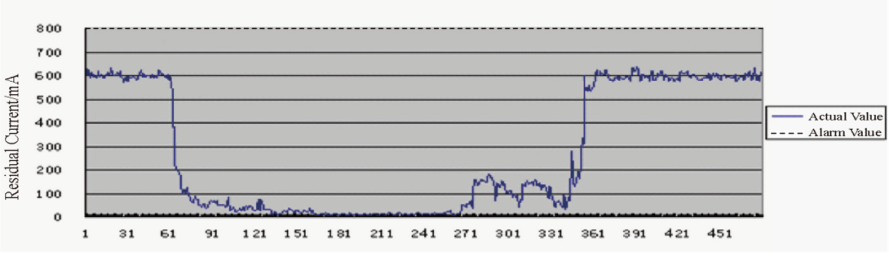


Fig. 1. Inherent leakage current curve of actual test

For convenience of explanation, Fig. 1 is simplified to Fig. 2.

It can be seen from Fig. 2 that the inherent leakage current is relatively large during a and C. at this time, as long as there is residual current superposition, it is easy to exceed the alarm threshold and alarm occurs. At this time, the alarm sensitivity is very high; During period B, the inherent leakage current value is low, and even if there is a large fault leakage current, the alarm may not be given. At this time, the alarm sensitivity is very low. According to statistics, the false alarm rate of the current electrical fire alarm system is 75−90%, which is the main obstacle to the popularization and application of the electrical fire alarm system.

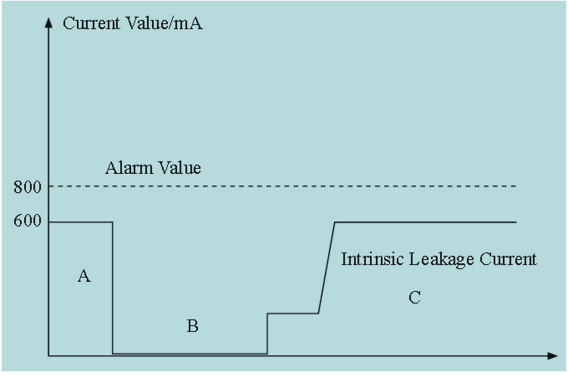


Fig. 2. Simplified inherent leakage current curve

The data of three-phase working current, leakage current and three-phase voltage in the distribution room have been measured and recorded continuously for one year. In the analysis of its data, the magnitude of the inherent leakage current changes with the number of electrical equipment. When most of the electrical equipment stops working, the value of the inherent leakage current is very small, even negligible (generally less than 10mA), but when most of the electrical equipment starts working, the value of the inherent leakage current also increases. This feature is common in all electrical units, as shown in Fig. 3.

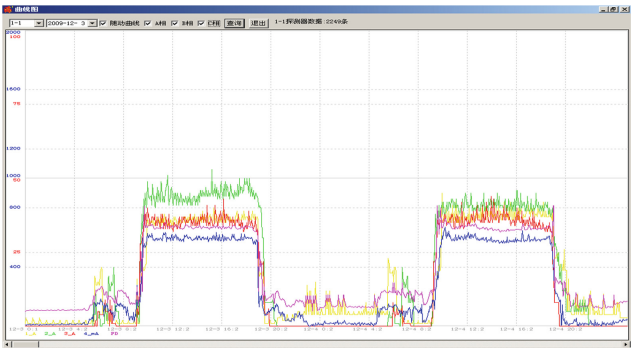


Fig. 3. Phase current and inherent leakage current monitoring

In Fig. 3, blue is the actual leakage curve. It can be seen from the figure that the inherent leakage current is closely related to the working current. As long as the working current increases, the inherent leakage current must increase at the same time. This shows that when the electrical equipment is not working, the inherent leakage current is small, and when the electrical equipment is working, the inherent leakage current becomes larger. There is a clear correlation between the leakage current and the working current, which is the theoretical basis of the follow-up alarm system.

The basic design of the follow-up threshold alarm system is that the setting of the alarm value is no longer a fixed straight line, but a curve that follows the change of the leakage current. The alarm value is formed according to the change law of working current in a week. The leakage current curve will not always follow the current curve. As long as there is a sudden fault with a large residual current, the residual current will exceed the alarm value curve and generate an alarm by superimposing the inherent leakage current; In addition, the leakage current cannot be allowed to increase indefinitely, and the alarm value also increases arbitrarily. A fixed high limit alarm value is also set. As long as the residual current is higher than this fixed alarm value, the detector will send an alarm.

If the follow-up alarm threshold keeps following the inherent leakage current, it will never alarm. In fact, it must alarm in the following two cases: one is the sudden leakage current, which is when someone connects the temporary electrical equipment in the distribution line. It happens that the equipment has a large leakage, and the leakage current instantly exceeds the follow-up alarm threshold, and the leakage alarm will occur; There is also a gradually increasing leakage current. For example, when the insulation of the conductor is aging gradually, the leakage current will gradually increase. When the insulation resistance is suddenly broken down, the leakage current will suddenly increase greatly. At this time, the follow-up threshold alarm system will also give an alarm, so the follow-up threshold alarm system will not form a situation of never giving an alarm. Generally, the difference value of follow-up is set at 100−200 mA. The specific follow-up threshold is shown in the pink curve in Fig. 3.

In fact, the follow-up alarm technology also has the last “line of defense”. After setting the follow-up alarm threshold, a relatively high fixed alarm value is also set, which is generally set at about 900−1000 mA. No matter how the fixed leakage value changes, as long as it is greater than the last line of defense, the detector will also send.

6 Conclusion

After statistics, compared with the ordinary fixed threshold alarm detector, the false alarm rate is 1.5%, which is significantly lower than the original 50–60% false alarm rate after using the “follow-up threshold alarm” technology. The test shows that the false alarm rate of the detector with follow-up threshold alarm technology is 98% less than that of the residual current detector without follow-up technology, and the effect is remarkable.

References

1. Guo-xin, X.I.N.G., Hai-long, Z.H.A.O., Zhi-qiang, W.U.: Application of pyrolytic particle electric fire detector in subway. Fire Sci. Technol. **40**(11), 1695–1698 (2021)
2. Yu, B., Lü, H., Zhang, X.: Discussion on the characteristics of electric equipment fire accident and fire extinguishing system. Electric Safety Technol. **22**(8), 33–37 (2020)
3. Zan, H., Wang, X.: Intelligent fire prevention and control for substation electrical fire prevention and control. Shandong Electric Power **47**(5), 51–55 (2020)
4. Li, Y.: Research on Key Technologies of Electrical Fire Detection System Based on Data Fusion Technology. Hunan University of Technology, 18–20 June (2021)

5. Zhao, Y., Guo, X.: Research on electrical fire warning algorithm based on multi-source data collaborative sensing. J. Taiyuan Univ. Technol. **52**(6) 907–912
6. Huang, B., Han, J., Zhou, T.: Research on residual current electric fire monitoring system. Chin. Comput. Commun. **24**(12), 86–91 (2019)

Prediction of Electromagnetic Shielding Effectiveness of DCS Cabinet Based on Neural Network

Xu Zhang[1(✉)], You-wei Yang[1], Jing-hua Yang[2], and Jun Li[1]

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

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

Abstract. The shielding effectiveness (SE) of structural components is one of the important indicators of electromagnetic compatibility (EMC) performance, and it is related to the size, material, frequency and test points position in the structure. The measurement of SE is governed by a variety of factors. SE of structural components is affected by the measuring antenna size which is adopted to different frequencies and the testability of certain observation points. To address this issue, this paper introduces an example of the SE of DCS cabinet of nuclear power plant control system, where the neural network algorithm was used to build the relationship between spatial location and SE in the cabinet at specified frequency, so that the SE of unknown points could be predicted by the SE of known points. Besides, the model parameters were optimized by training with a large amount of data, the HPR1000 safety-class DCS cabinet was adopted for the verification, and high prediction accuracy was obtained.

Keywords: Neural network · Electromagnetic shielding effectiveness · Prediction · DCS cabinet

1 Introduction

Electromagnetic shielding, commonly referred to as shielding, reduces or ideally prevents the coupling of unwanted electromagnetic energy from the outside environment into an electronic device, and it also reduces the transmission of undesirable emission from the device to affect the outside environment. Generally, shielding can be achieved by using a suitable conducting or metallic screen as barrier between two regions. But it may be noted that the perfect shielding of a device is impractical because of many intentional discontinuities of the barrier walls, which are required as the input and output accesses of the device.

The question of how to determine the protective properties of a shield against electromagnetic disturbance is difficult one to be addressed, even in frequency domain. According to conventional standard measurement procedures (IEEE Standard 299–1997), only the electric or magnetic SE of the empty shield is measured and the SE is doomed to

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 233–240, 2023.
https://doi.org/10.1007/978-981-99-3455-3_23

vary with positions. And since the shield usually forms a cavity resonator with internal resonances, the shielding effectiveness (SE) breaks down at the cavity's characteristic resonance frequencies. In addition, it becomes a function of frequency.

In engineering project, SE measurement is limited by the number and space arrangement of sensors, and sensors are not able to be set at an ideal site. In addition, due to design flaws or limited test condition, not all spatial location can be effectively measured. Therefore, taking neural network (NN) algorithm to predict the cabinet electromagnetic SE, and taking some measurable sites to predict other measurable or non-measurable sites, can effectively predict and calculate the SE of some key points in the cabinet.

2 SE Calculation

Shielding can be specified in terms of the reduction in magnetic and/or electric field strength caused by the shield. It is convenient to express this SE in units of decibels (dB) [1]. Use of decibels permits that several shieldings produced by various effects can be simply added to obtain the total shielding. SE is defined for electric fields as:

$$SE = 20 \log \frac{E_0}{E_1} \tag{1}$$

and SE can be also defined for magnetic fields as:

$$SE = 20 \log \frac{H_0}{H_1} \tag{2}$$

In the equations above, $E_0(H_0)$ is the incident field strength, and $E_1(H_1)$ is the field strength of the transmitted wave from the shield. In the design of a shielded enclosure, there are two primary considerations: (1) the SE attributed to shield material itself. (2) the SE attributed to discontinuities and apertures of shield.

This equation can be adjusted into a form which corresponds better to the physical mechanisms of the shielding effect. This adjustment is described in publications [2] and [3].

$$SE = R + A + M$$

where the individual characters indicates are:

R –attenuation by reflection.

A –attenuation by absorbent.

M –attenuation by multiple reflection.

In the near field, the electric and magnetic fields must be considered separately, because the ratio of them is not constant. In the far field, however, they combine to form a plane wave which having an impedance of 377 Ω. Therefore, when plane waves are discussed, they are assumed to be in the far field.

For any electromagnetic wave, the wave impedance is defined by

$$Z_0 = \sqrt{\frac{j\omega\mu}{\sigma + j\omega\varepsilon}} \tag{3}$$

For plane wave in the far field, Z_0 is also equal to the wave impedance. For free space, Z_0 equals 377 Ω.

3 Algorithm Implementation

3.1 Design of BP NN Algorithm

At the specified frequency, the SE is in accordance with a nonlinear logical relationship to the spatial coordinates. The BP NN is capable of fitting this nonlinear relationship by training with large data.

The basic principle of BP NN is to propagate the error from back layer to front layer, and calculate the hidden layer error. Based on the least squares and gradient search methods, the difference between actual value and desired value of the output can be minimized. A BP NN consists of input nodes, output nodes, and one or more hidden layers nodes, with the input and output nodes respectively corresponding to the independent and dependent variables of the regression model. Models of input-output relationships can be used to describe the nonlinear relationships between them, and to describe relationship of discrete data or complicated expressions. The BP NN model can not only approximate the input-output relationship between the discrete data points, but also describe the relationship between other data points of the discrete points.

Based on the analysis above, the following BP NN model can be achieved. A model consists of three-input and single-output was designed,where three inputs correspond to three spatial locations and output corresponds to shielding effectiveness. The neuron nodes in an intermediate layer receive the input signals from the previous layer, then combine their weights, and compare the total input value with the threshold value of neuron, whose output is to be processed by activation function. Assume that the weight between node i and node j is w_{ij}, and the threshold of node j is b_j. Input value is x_i, and output S_j can be expressed as

$$\mathrm{S}_j = \sum_{i=0}^{m-1} w_{ij} x_i + b_j \tag{4}$$

The Sigmoid function is chosen for the activation function, and is as shown in Eq. (5).

$$\mathrm{f(x)} = \mathrm{sigmoid}(x) = \frac{1}{1 + e^{-x}} \tag{5}$$

3.2 SE Prediction Model Based on BP NN Algorithm

The input data should be normalized before substituted into the model, and then the final output should be denormalized.

The algorithm implementation flow is shown in Fig. 1.

(1) Model Training

The relationship between input and output should to be mined and trained with a large amount of data. After training with a large amount of labeled data, the weight

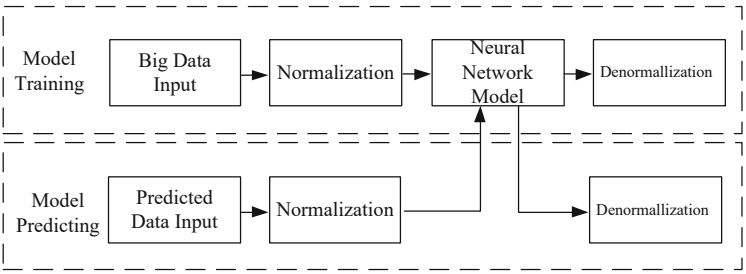


Fig. 1. Algorithm implementation flow

matrix and bias array of the NN are gradually updated to reach the final state of the model.

(2) Model Simulation

After the training of the model, the coordinates of the position to be predicted are taken into the well trained model, and then the predicted value of SE at a specified frequency can be obtained by the NN.

(3) Model Preservation

In order to take the model to be used repeatedly, the key parameters of the network model should be saved, so that the NN can be quickly reconstructed in an appointed unknown applications. The key parameters to be saved include the number of layers, the number of neurons for each layer, the learning rate, the weight matrix, the bias array, and the maximum and minimum values of each variable.

4 Case Study

4.1 Analysis Subjects

In this research, a typical DCS product produced by NPIC (Nuclear Power Institute of China) is selected, which has been used in HPR-1000 nuclear power plant in China. In some applications, shielded cabinets are necessary, because the electromagnetic environment at the intended operational condition could be too severe for the electronic units inside the cabinet. This may also be true because the external electromagnetic environment needs to be protected from the electromagnetic emissions from the electrical or electronic units inside the cabinet. Cabinet shielding requires metal cabinets or plastic cabinets with highly conductive metal-coated surfaces (plastic with conductive fillers is very difficult to use effectively). Very careful attention should be paid to detail design and assembly, to insure that the shielding provided in the cabinet is not be ruined. Shielded cabinets with shielded windows and ventilation with excellent EMC performance can be gotten from a number of manufactures. But they may be easily ruined completely by apertures for doors, drilling holes, poor filter, poor cable shielding or shield bonding, or open doors.

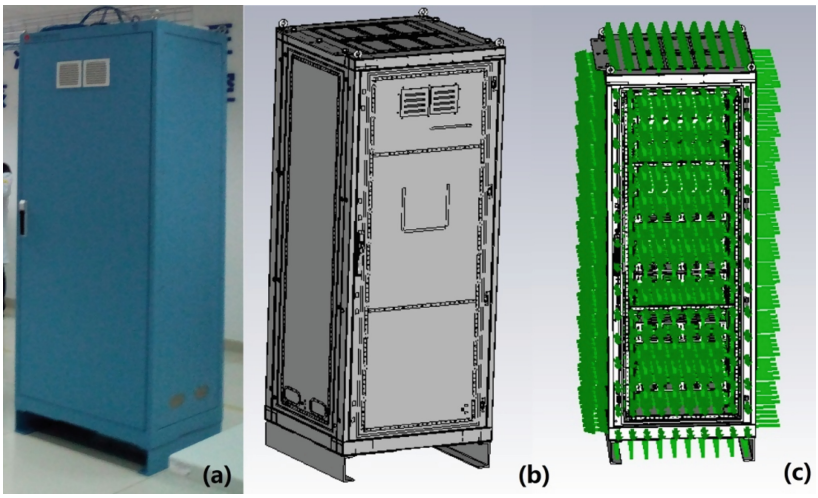


Fig. 2. (a) typical DCS cabinet, (b) SE geometry model, (c) probe distribution.

Typical power plant should be thought as a series of nested boxes, with outer architectural shell as the outer box, the control room as the second smaller box, the equipment rack in the control room as the third smaller box, and the chassis in the rack as the lowest level box in the nest. The shielding (and grounding) should be considered from the lowest level, where the sensitive electronic system is ultimately located, outward to potential EMI (electromagnetic interference) aggressors at each nesting level [4]. In case of an operating power plant, a few of these boxes will be provided with complete electromagnetic shielding, but the others will be provided with some specific form of EMI protection [5].

In the existing general electromagnetic compliance test, the SE of the cabinet is not a testing item, and it will not be taken into consideration until the radiation emission or radiation susceptibility test fails [6]. In this paper, a cabinet of the safety-related DCS is modeled and the SE of the cabinet is studied. The cabinet is 0.8 m length, 0.8 m weight and 2.2 m high. Most locations exist in the cabinet and the SE differs from each other, while a proportion of the locations are difficult to measure. As the results of the random nature of signals, real systems also demonstrate statistical behaviors in their parameters and responses, including their EMC performance. So, the EMC evolutions of the locations should also be predicted. Figure 2 shows the real product picture and model of a DCS cabinet, and massive number of probes in the model can be seen. In the simulation model, the incident plane is in front of the cabinet and it is invisible.

4.2 Construction of BP NN Model

The NN is designed with 3 layers, where the number of input and output layers coincide with the number of input and output variables, and the numbers of neurons are 3 and 1 respectively. The number of neurons in the hidden layer can be obtained by experimental debugging. The comparison of the effect of different number of neurons in the hidden layer is shown in Fig. 3.

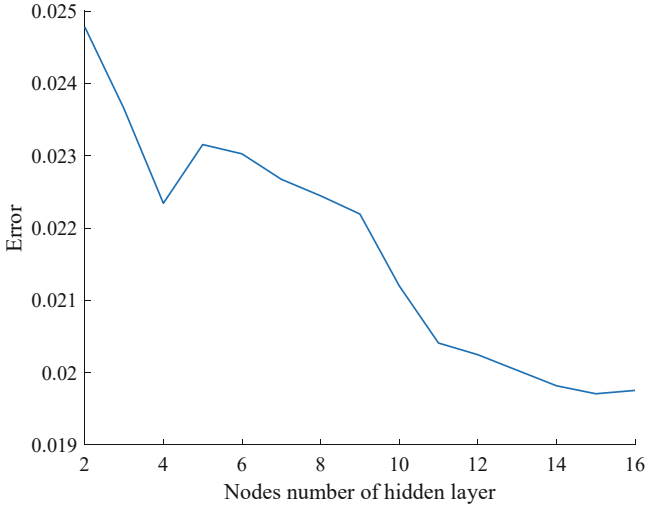


Fig. 3. Node number in hidden layer and training error.

Therefore, the NN was finally designed with three layers which consist of 3, 15 and 1 neurons respectively. The NN model for SE prediction is shown in Fig. 4.

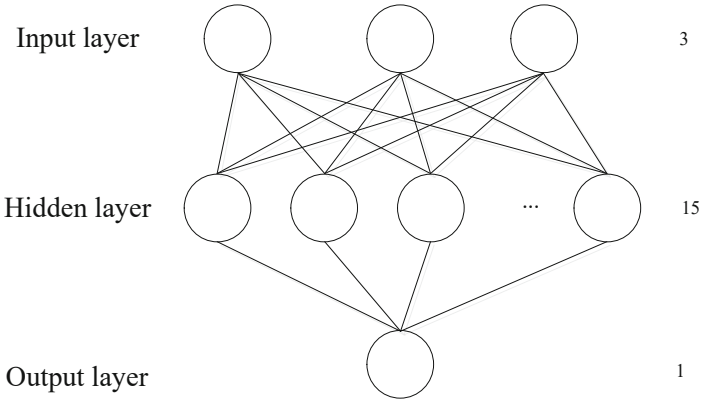


Fig. 4. NN model for SE prediction

The learning rate was set to 0.2 and trained 1000 times to avoid overfitting or overlearning. The error in the training process is shown in Fig. 5.

It is obviously shown in the figure that the training process could effectively reduce the error and improve the fitting effect.

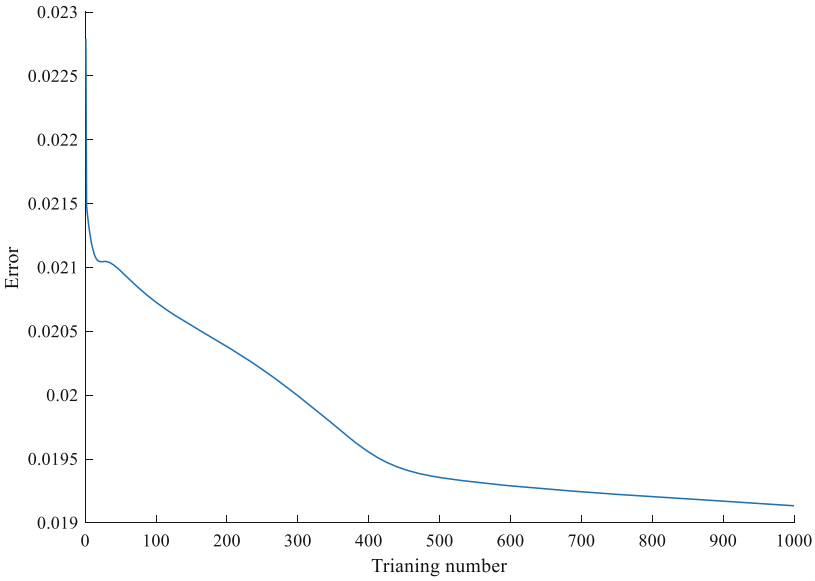


Fig. 5. Error of training process.

4.3 Analysis of Experimental Results

NN model was obtained after training, and predicted SE value could be obtained by applying the appointed coordinate data into the model. The prediction and actual SE value was compared to get the evaluation (Table 1).

Table 1. Comparison of predicted results and SE at operating frequencies.

Point number	Coordinate X	Coordinate Y	Coordinate Z	measured SE	predicted SE
1	2.00	5.58	7.5	95.11	101.44
2	2.00	9.17	13	77.20	95.82
3	2.00	13.65	6.71	85.33	92.39
.	…	…	…	…	……
30	6.57	14.55	2.00	86.38	90.45
.	…	…	…	…	……

Root Mean Square Error (RMSE) could be used to aggregate errors in various prediction values, and is commonly used in the evaluation of predictors. The RMSE is defined as shown in Eq. (6).

$$\mathrm{RMSE} = \sqrt{\frac{\sum_{i=1}^{n} (X_{obs,i} - X_{\mathrm{mod}\ el,i})^2}{n}} \tag{6}$$

where $X_{obs,i}$ denotes the predicted value, $X_{model,i}$ denotes the measured value, and n denotes the number of points.

Based on the experimental results, RMSE was calculated as 0.1110, according to Eq. 6. It could be seen that DCS cabinet electromagnetic SE prediction based on NN method had a high prediction accuracy.

5 Conclusion

Based on BP NN algorithm, the model of electromagnetic SE for DCS cabinet can be constructed by mining the relationship between location and the SE at specified operating frequency. This paper shows that the model used to predict SE of cabinet can be well fitted, and is important for the predicting and evaluating the SE where no sensors are arranged in a cabinet.

The project was funded by Sichuan Provincial Science and Technology Fund for Distinguished Young Scholars (2020JDJQ0068).

References

1. Ott, H.W.: Noise Reduction Techniques in Electronics Systems, 2nd edn. Wiley, New York (1988)
2. Paul, C.R.: Introduction to Electromagnetic Compatibility. Wiley, New York (1992)
3. Kodali, V.P.: Engineering Electromagnetic Compatibility. IEEE Press, New York (1996)
4. Guidelines for Electromagnetic Interference Testing in Power Plants, Revision 3 to EPRI TR-102323, TR-1003697, Electric Power Research Institute, Palo Alto, CA (2004)
5. Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems, Regulatory Guide (R.G.) 1.180, U. S. Nuclear Regulatory Commission (1996)
6. Minimizing the Risk of Electromagnetic Interference in Modifying Power Plants and Mixed Control Equipment: Increasing Preparedness for Modern EMI Problems and Achieving EMC for Changing Plants. EPRI, Palo Alto, CA, 1016729 (2008)

Design and Implementation of DCS Design List Automatic Generation and Check System Based on LabVIEW

Xiao-Jun Deng(✉), Xu Zhang, Shi-Man Feng, Hao Peng, and Ying-Fan Yao

Science and Technology on Reactor System Design Technology Laboratory, Nuclear Power Institute of China, Chengdu, China
jxlgdx123@163.com

Abstract. The DCS configuration design process involves a large number of variables and multiple lists, and designers need to spend more time on the preparation, checking and maintenance of the lists. Manual compilation of files is a lot of work, and prone to human error. In this process, the use of automatic software to assist in the design can effectively improve efficiency. Based on the practical requirements of safety-class DCS design project of a nuclear power plant unit 1 and 2, this paper designs and implements a set of automatic generating and checking system of accounting list, which implements the automatic generation and typesetting of list files, and obtains good application effect.

Keywords: LabVIEW · DCS · Listing report · Automatically generate

1 Introduction

The process of designing and manufacturing DCS (Digital Control System) involves a large number of list files, including IO lists, set value lists, network signal lists, etc. Due to large quantity of control stations and variables in each station, the list is usually long and error-prone, so automatic software needs to be designed, to improve the efficiency of design and reduce errors. Some lists need to follow the relevant specifications and is prone to errors, so integrated checking methods and tools are particularly important [1].The automatic software can be developed with traditional languages such as C and C + +. But for non-professional developers, the visual graphical programming software is simpler and easier to be understood, such as LabVIEW, and is more convenient for processing tabular data [2]. The flexibility and functional integrity of LabVIEW is very powerful, which makes it ideal for developing human-machine interface programs.

LabVIEW is developed by NI (National Instruments), whose advanced and convenient graphical development method is widely used today [4].With the help of the file development interface in LabVIEW, an automatically generating and checking software can be developed by reading the data exported from maintenance engineer station (MTS) and generating or checking DCS design list according to the specified file format.

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 241–256, 2023.
https://doi.org/10.1007/978-981-99-3455-3_24

2 Functional Requirements Analysis

The design process includes system design, software design and hardware design. When system design is completed, the software design and hardware design can be carried out. Software design and hardware design are related, and it is necessary to ensure consistency between them. Moreove, the number of these documents is large, and manual checking of their relevance is prone to error. In addition, a standard format of software design is also necessary, which takes much time to design manually. The detailed requirements are analyzed.

2.1 IO Variable Configuration Check Function

The software configuration determines the quantity and content of IO variables, specifically signal variable name, unit, cabinet number, chassis number, signal description, etc. The hardware wiring diagram includes slot and channel, from which IO distribution list can be obtained [5]. And then, the software configuration designers complement the configuration location of the variables in the MTS. Content should be consistent between software design and hardware design. However, human error will be caused in the interaction, especially when the hardware and software design is upgraded.

2.2 Set Value List Generation Function

Set value list should be generated by information such as variable name, data type, initial value, unit, station number, upper limit, lower limit, description, function diagram page number, remarks, and version based on the parameter variables, which can be got from MTS.

2.3 Network Signal List Generation Function

Network signal list includes variable name, data type, device type, input network variable, station number, cabinet, chassis, slot number, channel, source network variable, source network variable station number, opposite end routing, description, function diagram page number, remarks, version, etc. Network signal list should be gathered to form a file.

3 Solution

3.1 IO Variable Configuration Check Function Design Implementation

The IO list shows the variable settings of the DCS and the location assignment of the variables in IOmodule. The IO list is the interactive part between the software design and the hardware design. Parameter configuration is usually completed by software configuration designer, and then the hardware designer supplements the location allocation information of the variable in the card. Therefore, the variables of the list should be consistent.In engineering practice, due to the large workload, the variables may be duplicated or reduced due to human error. The comparison of the software design with the hardware design enables the above error checking. Automaticcheck is shown in the following flow chart (Fig. 1 and 2).

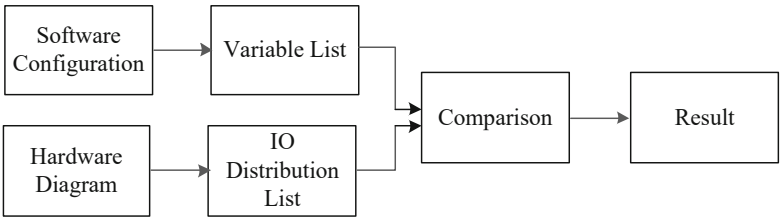


Fig. 1. Flowchart of the IO list check

3.1.1 Human-Machine Interface and Event Branch Design

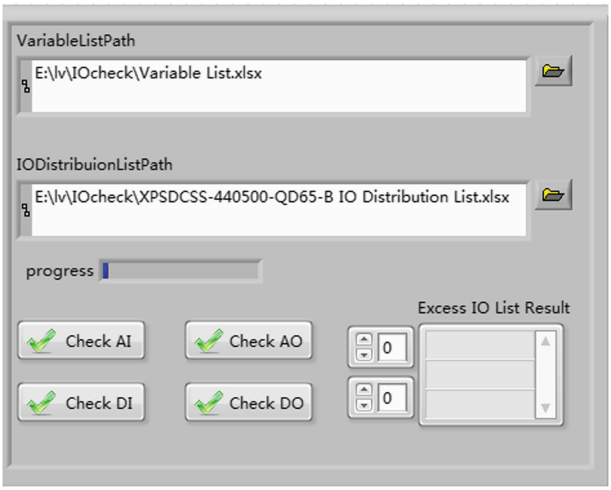


Fig. 2. Main interface

The main program is designed with user event processor framework, which is mainly divided into 6 events processing branches, as shown in Fig. 3.

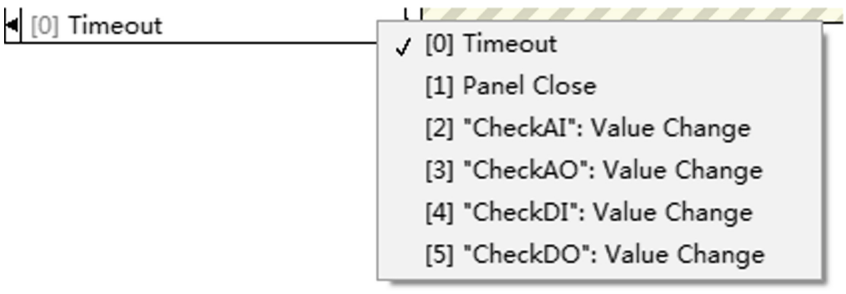


Fig. 3. Event processing branch

Timeout event does not perform any operation and the program waits for user input, and the front panel close event signify that the program exits when the user closes the program. Several other events handle variables such as AI, AO, etc., separately.

3.1.2 Function Implementation

The check functions of various variables are implemented similarly. Take AI as an example, the program design is shown in Fig. 4.

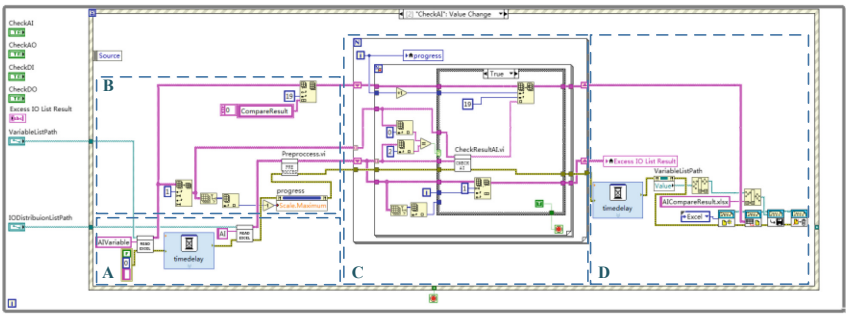


Fig. 4. Main program design

The procedure processing flow is as follows.

Step 1, read the IO variables list and get all the IO variables properties, stored in array 1;

Step 2, read the IO distribution list, get the IO channel distribution and other information of the hardware design, delete the spare channels and table headers, get the hardware IO distribution list, and store it in array 2;

Step 3, the loop body, traverse the variables of array 1, and find each variable in array 2. If the same variable is found, enter the comparison program module, and get the comparison result, mark the comparison result to record (stored in array 1), then delete the variable of the line of array 2. Otherwise, the current variable is marked as "not found", and the loop ends after comparing all variables in array 1;

Step 4, save array 1 as the comparison result and save array 2 as the ungrouped IO variable list.

According to the logical structure, the program can be divided into several parts: A file reading module, B pre-processing module, C inspection module, and D result output module.

3.1.2.1 File Reading Module

The structure of the variables is shown in Fig. 5.

variable name	datatype	unit	site number	class	cabinet number	chassis number	board number	channel number	up limit	low limit	description	alg page
H10JEV30CF001	analog	mA	51	AI	520	1	7(5)	1	20	4	cooling air flow 10JEV30BR025	JEVS003A

Fig. 5. Variable list structure

The structure of the IO distribution list is shown in Fig. 6.

order	variable name	datatype	unit	site number	class	cabinet number	chassis number	board number	channel number	up limit	low limit	description	signal input										signal source
													module type	connect module type	terminal number	terminal (+)	terminal (-)	power supply	alg page	schematic page	source variable name		
1	H10JEV30CF001	analog	m³/h	51	AI	10CRC20	GH401	7	1	2500	0	cooling air flow 10JEV30BR025	SAAI21	SAST21	GF127	A1	B1	SBO*	JEVS003A	500	10JEV30CF001	LOCAL	

Fig. 6. IO distribution list structure

The file reading module uses ActiveX to read Excel, which is implemented in Fig. 7.

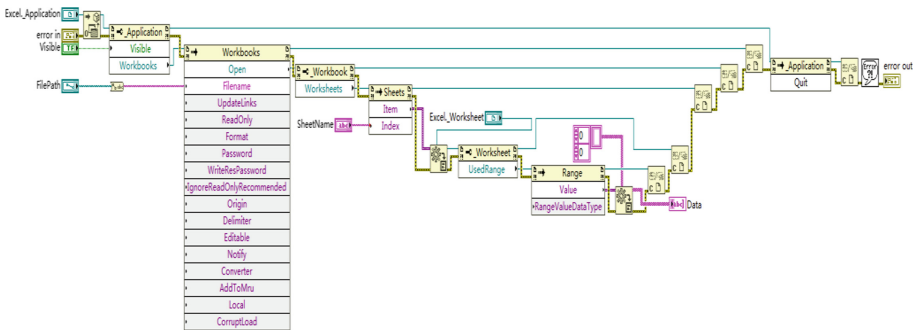


Fig. 7. File reading module

3.1.2.2 Pre-processing Module

The table headers and backup channel in IO distribution list data are deleted, and only the variable data with channels already distributed are retained, as shown in Fig. 8.

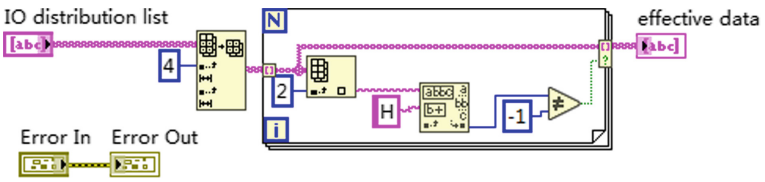


Fig. 8. Pre-processing module

3.1.2.3 Inspection Module

There are four comparison modules, namely AI, AO, DI and DO variable attribute comparison module.

Take the comparison of AI variables as an example, the comparison items include unit, station number, cabinet number, chassis number, slot number, channel number, etc.. The "cabinet number" checking uses a conditional structure to characterize the one-to-one mapping between the software IO list and the hardware IO distribution list of "cabinet numbers" (Fig. 9).

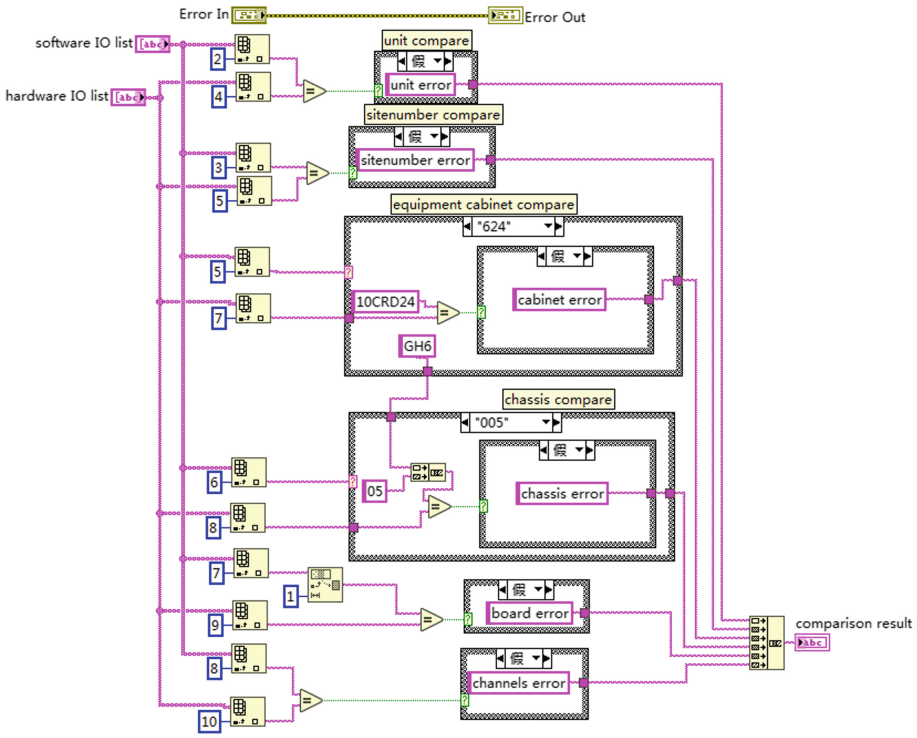


Fig. 9. Comparison of IO variable properties

3.1.2.4 Result Output Module

The output is represented in a table, with the first few columns describing the details of the signal and the last column listing the comparison error. The output result table is shown in Fig. 10.

3.2 Set Value List Generation Function Design Implementation

3.2.1 Human-Machine Interface and Event Branch Design

QMH (Queued Message Handler) framework, also often called producer/consumer design pattern, is the most basic design pattern in multi-threaded programming. This

variable name	datatype	unit	site number	class	cabinet number	chassis number	board number	channel number	up limit	low limit	description	alg page	check result
H10JEV30CF001	analog	mA	51	AI	520	1	7(5)	1	20	4	cooling air flow 10JEV30BR025	JEVS003A	description error

Fig. 10. Structure of the output result table

example consists of 2 main loops, one with an event structure to handle human-machine interaction and the other loop responsible for analyzing and processing data, whose source is the data inserted into the queue from the previous cycle.

3.2.1.1 Set Value List Front Panel

The front panel mainly has inputs such as site number, site name, project name, project code, document name, document number, body generation button, cover generation button, etc. The main interface is shown in Fig. 11.

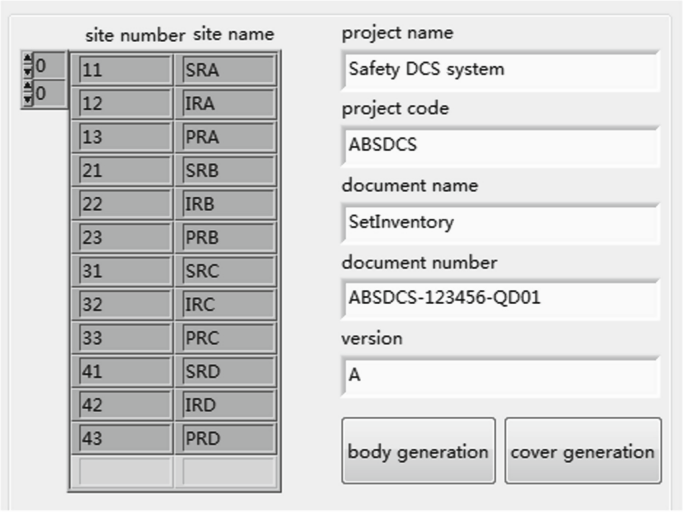


Fig. 11. Main HMI of the set value list

3.2.1.2 Program Block Diagram of Set Value List

The program block diagram of set value list is mainly divided into two loops and queues and other operations, as shown in Fig. 12.

A: The main function is to queue user events, there are 4 events.

Event 1: Timeout, waiting for user input, no action performed.

Event2: The front panel closes, captures the user command to exit the program, and inserts the message "Quit" into the queue when the user closes the program (Figs. 13 and 14).

Event 3: "Cover generation": the value changes and the front panel input (station number, project name, project code, document name, document number) and the message "Cover generation" is inserted into the queue.

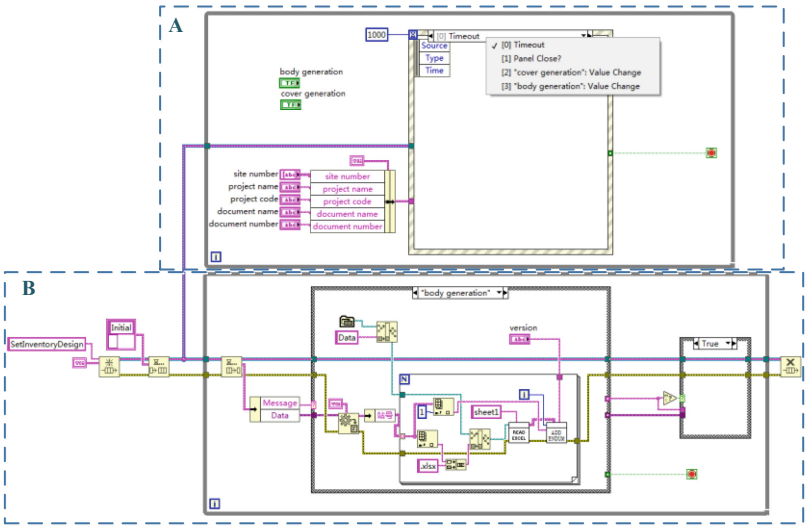


Fig. 12. Program block diagram of set value list

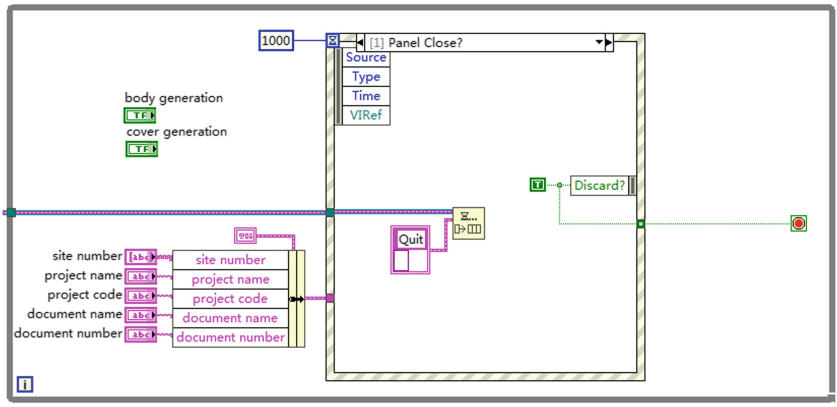


Fig. 13. Sub-pannelof Event 2 (A in Fig. 12)

Event 4, "Body Generation": value change, inserting the front panel input (station number, project name, project code, document name, document number) and the message "Body Generation" into the queue (Fig. 15).

B: Manage the queue. The queue is createdfrom left to right, the control instruction "Initial" is inserted into the queue, the loop body, and the queue is released. Among them, the loop body will mainly be the elements of the queue out of the queue operation, and according to the queue of messages to perform different procedures, message content processing a total of five branches, as shown in Fig. 16.

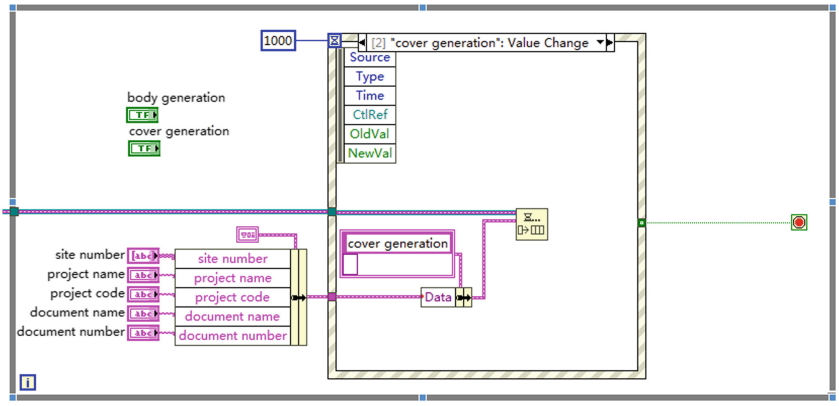


Fig. 14. Sub-pannelof Event 3 (A in Fig. 12)

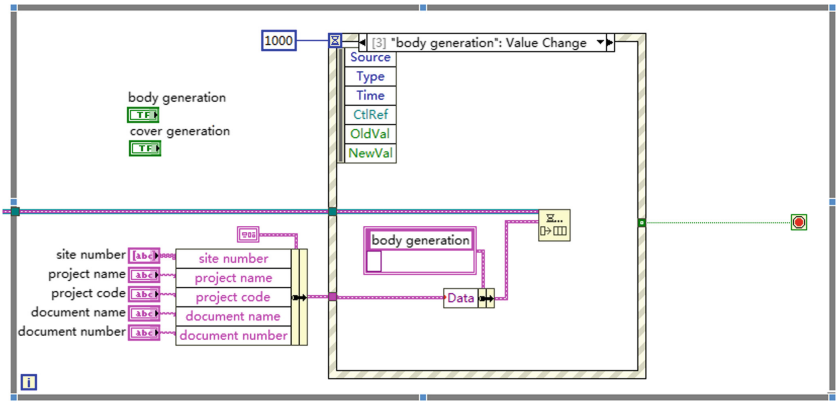


Fig. 15. Sub-pannelof Event 4(A in Fig. 12)

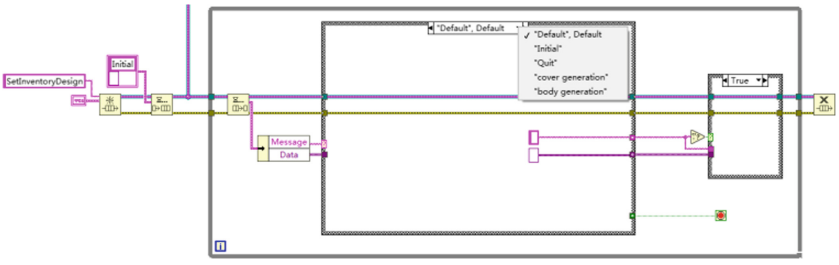


Fig. 16. Block diagram of set value list program

Branch 1: "Default ", default. The default operation, execute this branch on an empty message and reinsert the message "" into the queue, keeping the queue empty for the operation, as shown in Fig. 17.

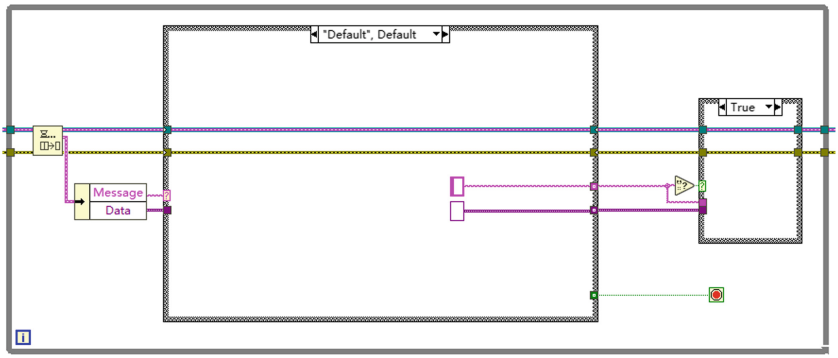


Fig. 17. Program block diagram of branch 1(B in Fig. 12)

Branch 2: “Initial”. Perform the initialization to check the existence of Data folder, and if not, create the folder to store the variable table as shown in Fig. 18.

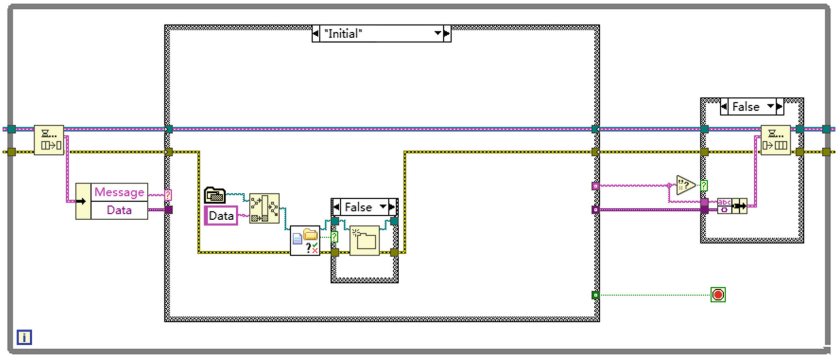


Fig. 18. Program block diagram of branch 2(B in Fig. 12)

Branch 3: “Quit”. Perform the operation of emptying the queue as shown in Fig. 19.

Branch 4: “Cover generation”, executes the procedure for setting the cover of the list, and then the contents of the queue “Item Name”, “Item Code”, “Document Name” and “Document Number” are passed to “ SetInventoryCover.vi”, as shown in Fig. 20.

The content of “SetInventoryCover.vi”is detailed in Sect. 4.2.

Branch 5: “Body generation”. Execute the procedure for generating the body of the set value list, as described in detail in Sect. 4.3 and summarized in Fig. 21.

The main purpose of branch 5 is to read the parameter variables of the Excel file according to the station number and pass them to the sub-VI “SetInventoryCover.vi” for processing, whose processing procedure is detailed in Sect. 4.3.

3.2.1.3 Execution Flow of Set Value List Program

The program is designed using the QMH framework, where part A is to collect and insert user instructions into the queue; part B is to execute the corresponding program according to the message content of the queue.

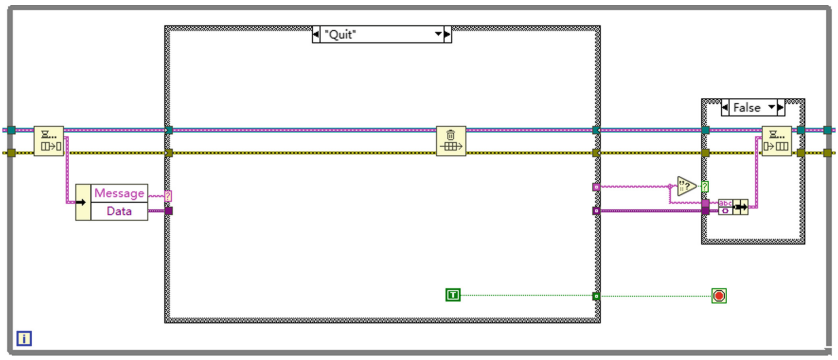


Fig. 19. Program block diagram of branch 3 (B in Fig. 12)

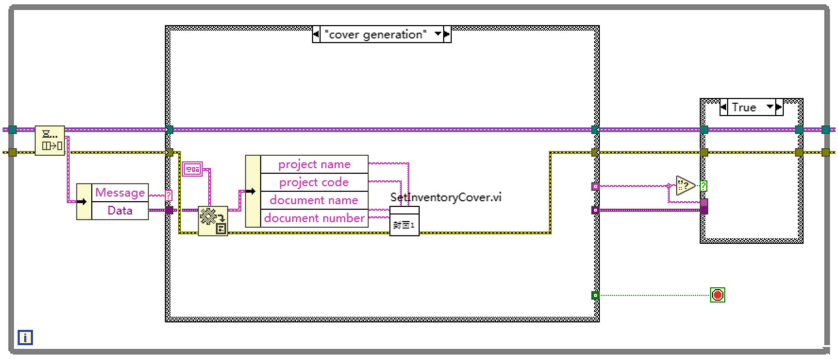


Fig. 20. Program block diagram of branch 4 (B in Fig. 12)

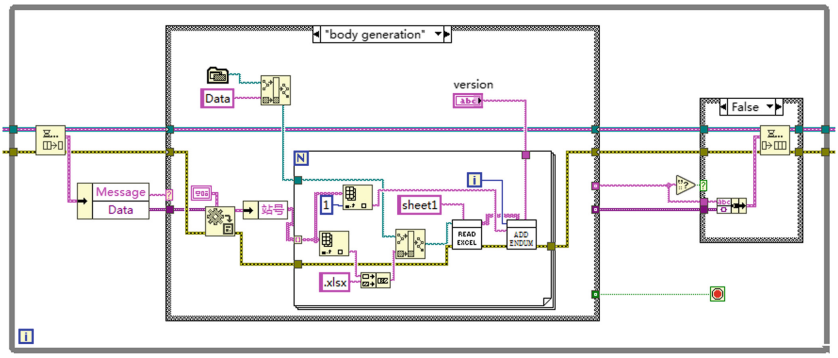


Fig. 21. Block diagram of branch 5 program (B in Fig. 12)

In practical applications, the specific procedure execution steps are as follows.

1. Run the program, which will create a new Data folder in installation directory.
2. Use MTS to export all variable table files to..\Data folder.

3. Fill in the front panel with information such as station number, station name, project name, project code, document name, document number, etc., and press the "Generate Text" button.
4. Part A program inserts the message "body generated" into the queue.
5. Part B "body generation" the queue messages out of the queue and executes the procedure in branch 5.
6. Press the cover generation button and the Part A program inserts the message "cover generation" into the queue.
7. Part B "cover generation" the queue messages out of the queue and executes the procedure in branch 4.
8. Close the program, part A inserts the message "Quit" into the queue, part B takes the message out of the queue, empties the queue and exits the loop.
9. Combine the document cover and the document body into a complete document.

3.2.2 Design of Document Cover

The design of the document cover is mainly implemented by the sub-VI "SetInventoryCover.vi". According to the template bookmark positioning, write the document number, document name, document content, etc., to form a new document (Figs. 22 and 23).

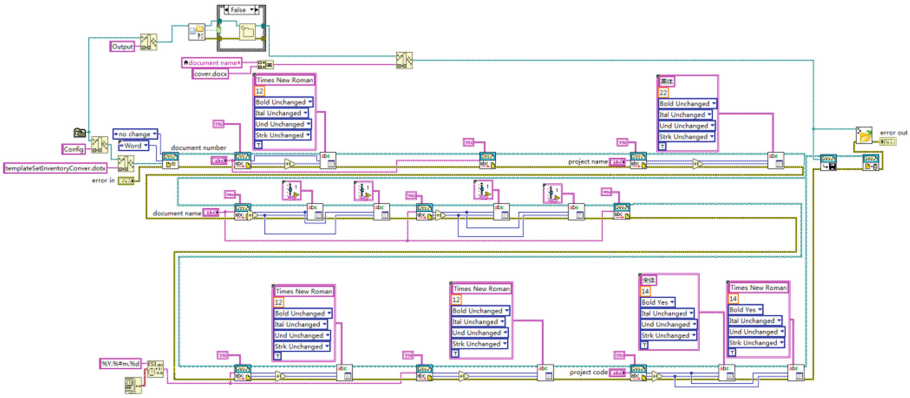


Fig. 22. Block diagram of the sub-VI "SetInventoryCover.vi"

3.2.3 Design of Document Body

The design of the document body is mainly based on the data obtained from the variables table in the format given by the template to form a document that meets the formatting requirements. The content is mainly implemented by "SetInventoryaddendum.vi".

The contents of the set value variable array are inserted into serial number on the left, and notes and versions on the right, and then stored in the format of the template.

Using the report tool, write the properties of the set value variables for each station into the appropriate report template and write schedule 1 in table header.

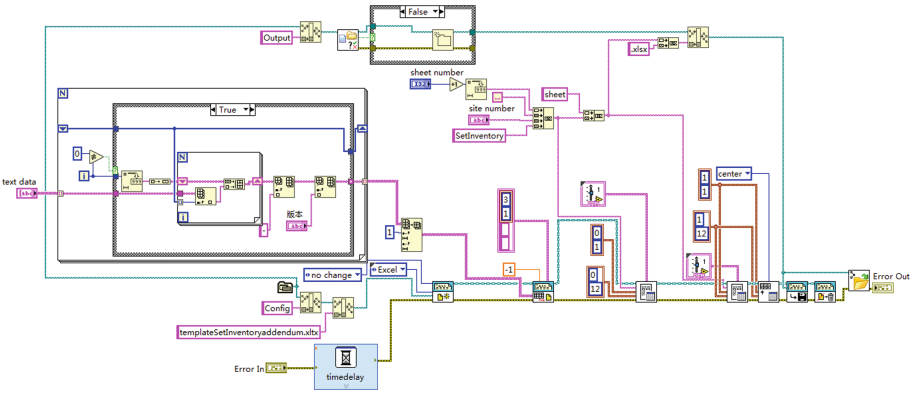


Fig. 23. Block diagram of the sub-VI "SetInventoryaddendum.vi"

3.3 Network Signal List Generation Function Design Implementation

3.3.1 Human-Machine Interface and Event Branch Design

The interface is designed with QMH framework, similar to the set value list, and the main interface is shown in Fig. 24.

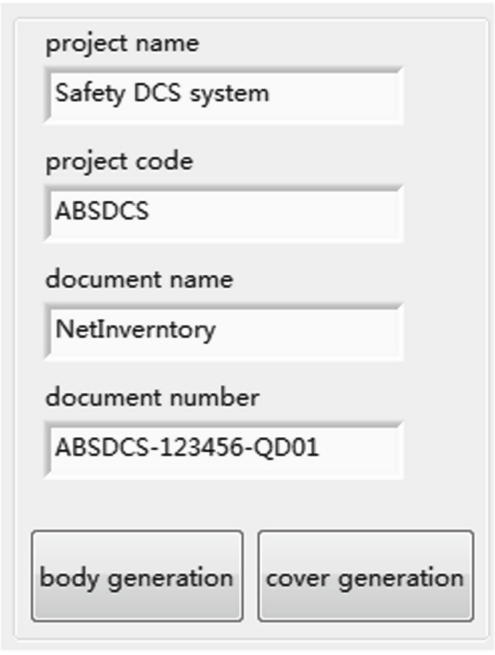


Fig. 24. Network signal list main interface

The program block diagram is similar to the set value list, the difference is that the two event branches are handled differently, which is as shown in Fig. 25.

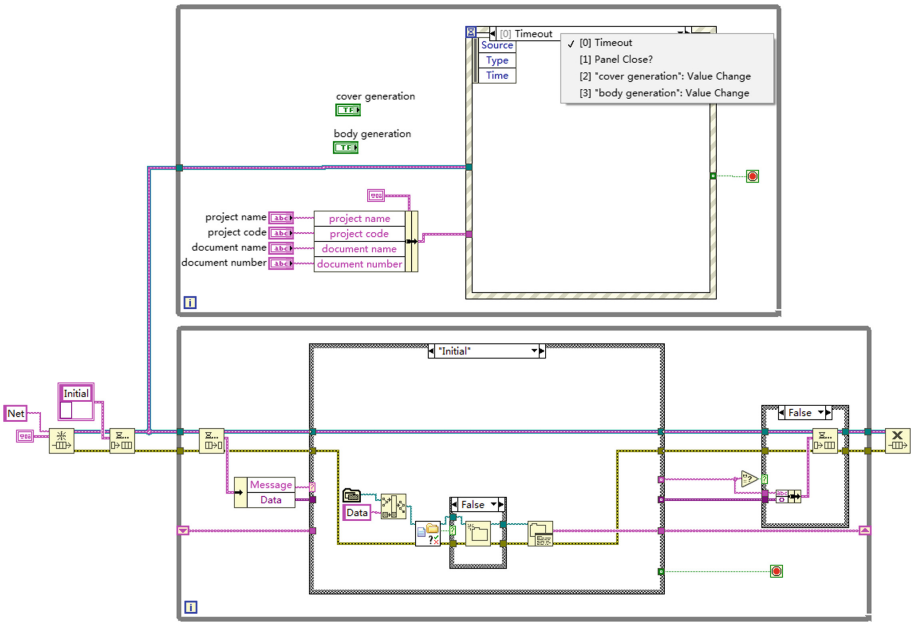


Fig. 25. Network signal list program block diagram "Initial" branch

This branch uses the enumerate folder function to enumerate the variable files in the Data folder and stores all the station file names in the shift registers, pending the use of the "body generation" branch (Fig. 26).

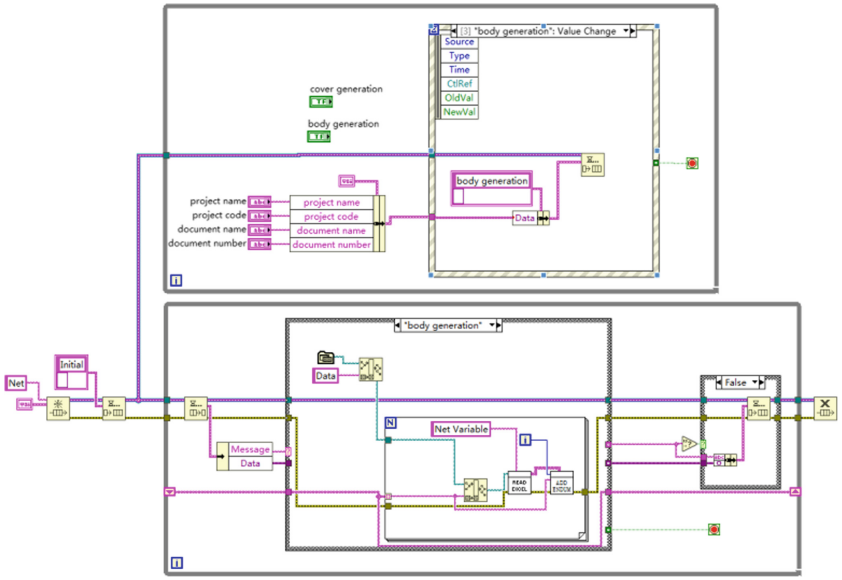


Fig. 26. Network signal list program block diagram "Body generation" branch

3.3.2 Design of Document Cover

The design of the document cover is mainly implemented by the sub-VI "NetInventoryCover.vi". According to the MS Word template bookmark (bookmark) positioning, write the file number, file name, file content, etc., respectively, to form a new document. The program block diagram is similar to the sub-VI "SetInventoryCover.vi" in Sect. 4.2 above.

3.3.3 Design of Document Body

The design of the body of the file is mainly based on the data obtained from the variables table in the format given by the template to form a file that meets the formatting requirements. Its content is mainly realized by the sub-VI "NetInventoryaddendum.vi" (Fig. 27).

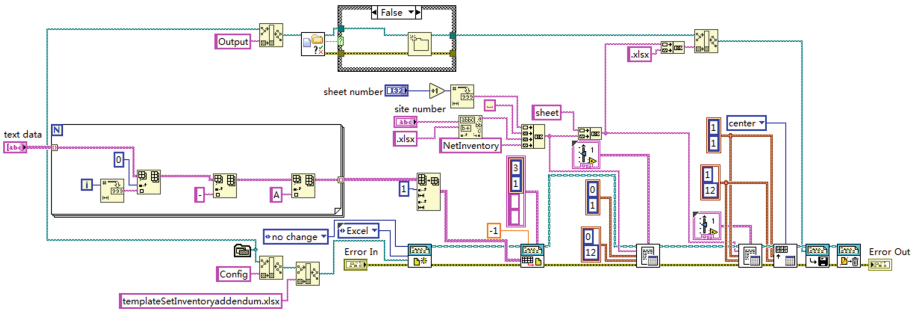


Fig. 27. Block diagram of the sub VI "NetInventoryaddendum.vi"

4 Result

The check tool realized the consistency check of the IO distribution list of software code design and hardware design, whose accuracy rate reached 99.99%. More than 1000 files were processed in practical application, and 500 errors were found. The generation tool described above produced 500editions of 36 documents, reducing the manual effort.

5 Conclusion

In this paper, a software based on LabVIEW is designed to realize the automatic checking and generation of files and lists in DCS design process. This system has been applied to the design process of a nuclear power plant safety-class DCS project, which improves efficiency and reducing human error.

The project was funded by Sichuan Provincial Science and Technology Fund for Distinguished Young Scholars (2020JDJQ0068) and Science and Technology on Reactor System Design Technology Laboratory Operating Scholars(Research and development of translation type virtual nuclear safety-class DCS).

References

1. Zhang, X., Guan, Y.: Defects of DCS configuration project and research on the IO List standardization problems. East Chin. Electric Power **38**(03), 424–428 (2010)
2. Wang, D.: Data recording and storage based on LabVIEW. Ind. Control Comput. **31**(06), 119–120 (2018)
3. Deng, X., Zhu, J., Zhang,X., et al.: DCS network variable automatic generation system based on LabVIEW. Mod. Comput. **27**(24): 144–148+153 (2021)
4. Zhang, X., Yao, Z., Li, J.: Design and implementation of Eplan automatic inspection system. Ind. Control Comput. **33**(12), 1–3 (2020)

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

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

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

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

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

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

1 Introduction

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

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

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

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

2 Research Object and Research Status

2.1 Research Analysis

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

2.2 Structural Analysis

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

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

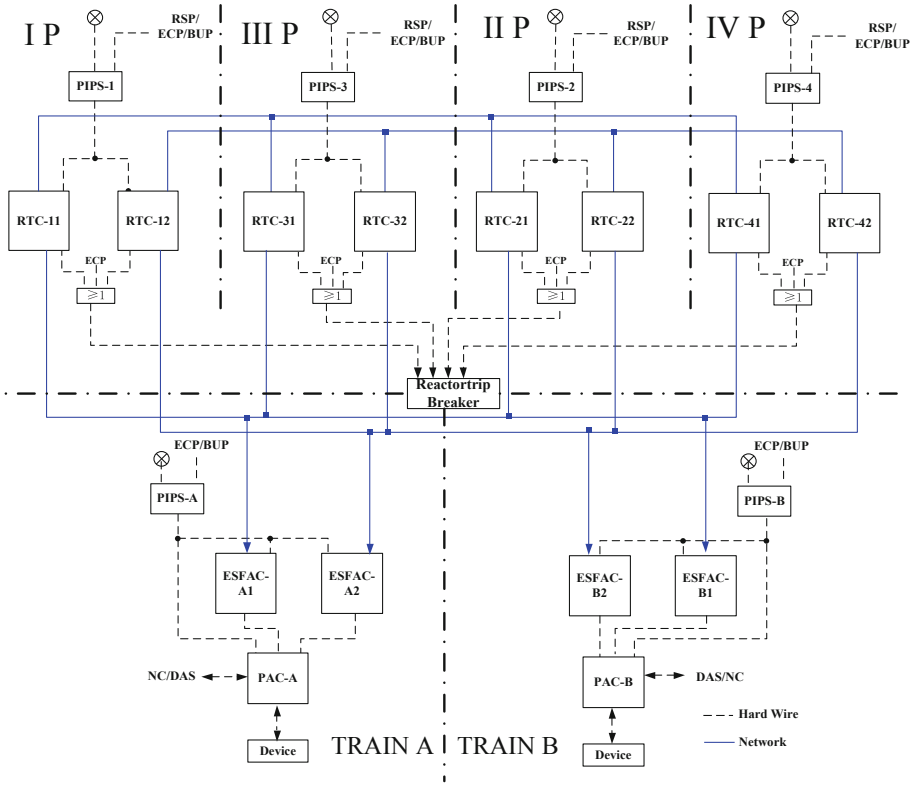


Fig. 1. Schematic Diagram of Safety-class DCS

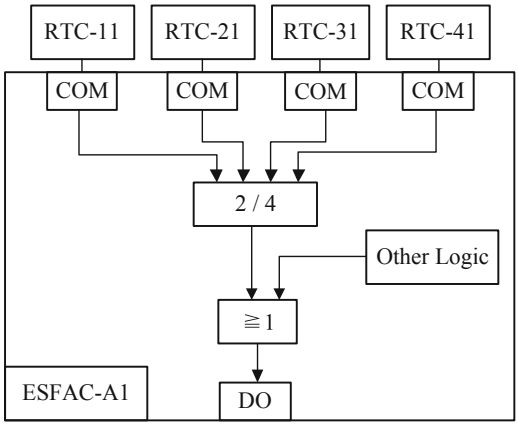


Fig. 2. Logic Diagram of TFM031VL Close Driver Command

3 ESFAS System Reliably Model

3.1 FTA Method

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

3.2 Reliably Parameters Calculation Method

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

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

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

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

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

3.3 FT Model

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

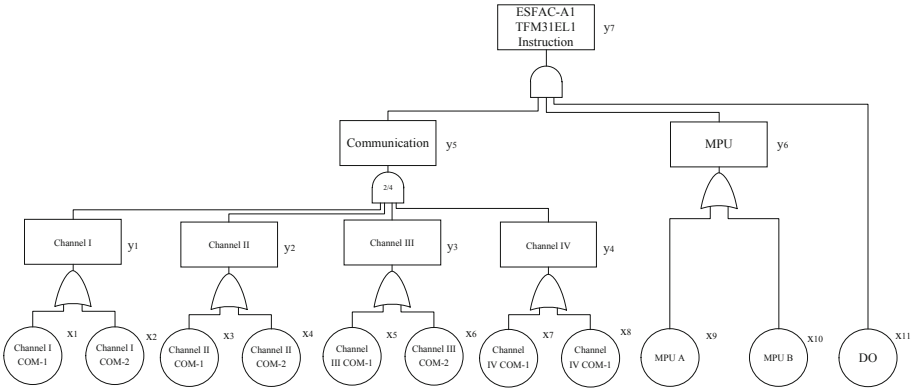


Fig. 3. Logic Diagram of TFM031EL1 Instruction in ESFAC-A1

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

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

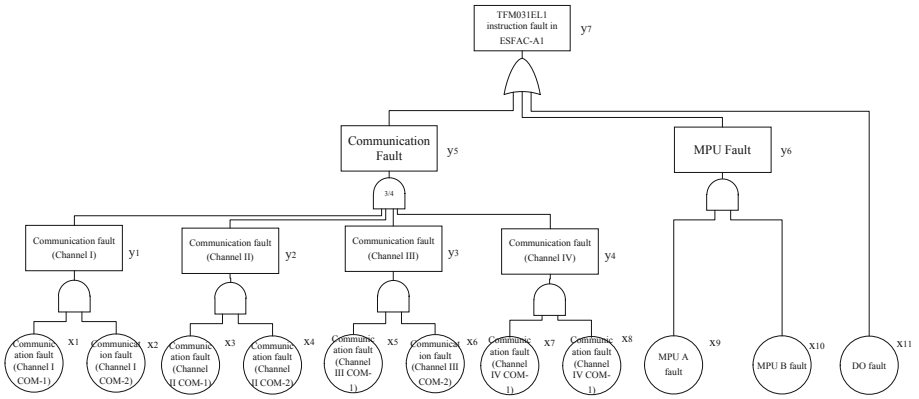


Fig. 4. FT Model of TFM031EL1 Instruction Fault in ESFAC-A1

4 Simulation Experiment

4.1 Reliability Parameter Calculation

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

Table 1. Equipment Model and failure rate (λ)

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

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

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

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

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

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

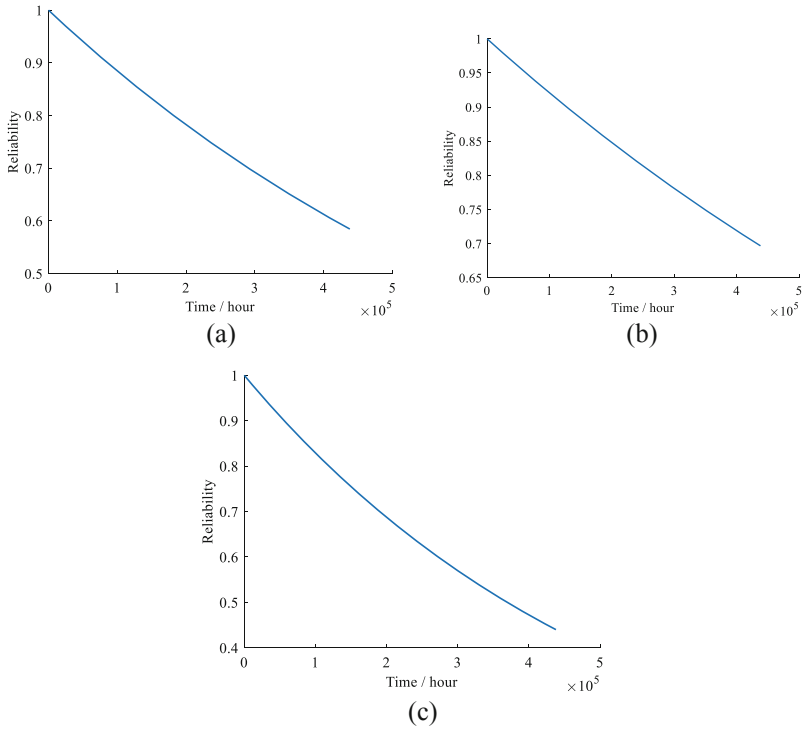


Fig. 5. Simulation Results of Equipment Reliability

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

4.2 Sub-system and System Reliability Simulation Analysis

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

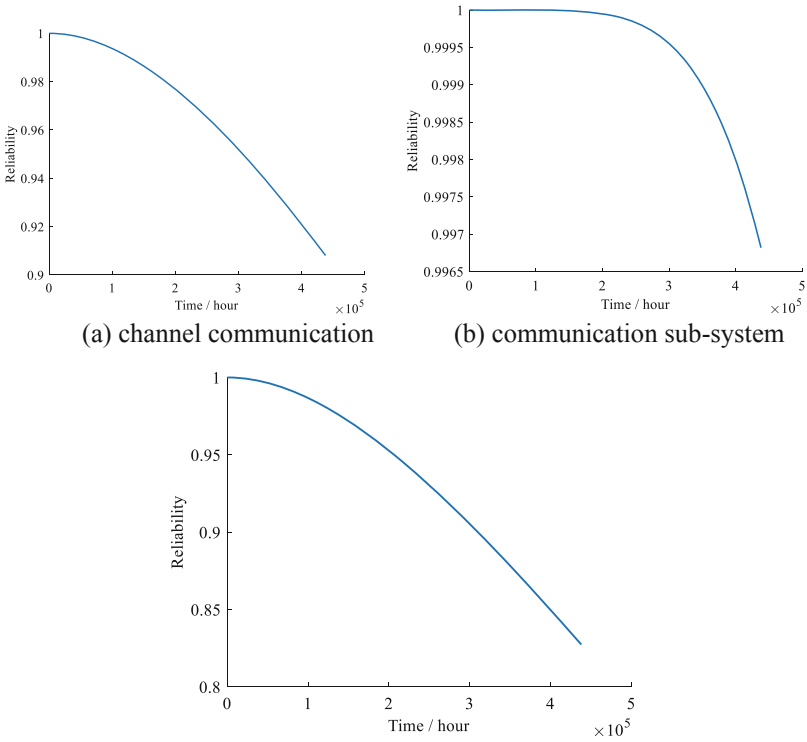


Fig. 6. Simulation Results of Sub-system Reliability

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

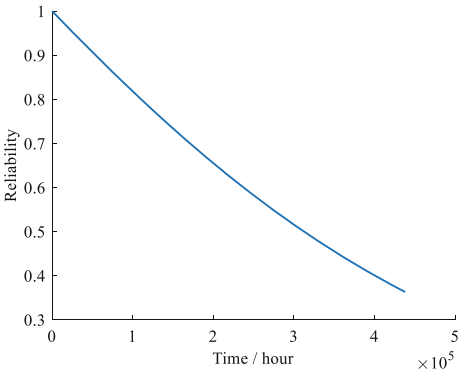


Fig. 7. Simulation Results of Single Control Station Reliability

Table 2. Deterioration of Reliability

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

4.3 Minimum Cut Set and Importance Analysis

4.3.1 Minimum Cut Set Analysis

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

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

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

Table 3. Minimum Cut Set and Probability

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

4.3.2 Minimum Cut Set Analysis

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

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

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

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

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

Table 4. Minimum Cut Set and Probability

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

4.3.3 Failure Probability Calculation

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

Table 5. Minimum Cut Set and Probability

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

4.4 Control Station Redundancy Design

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

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

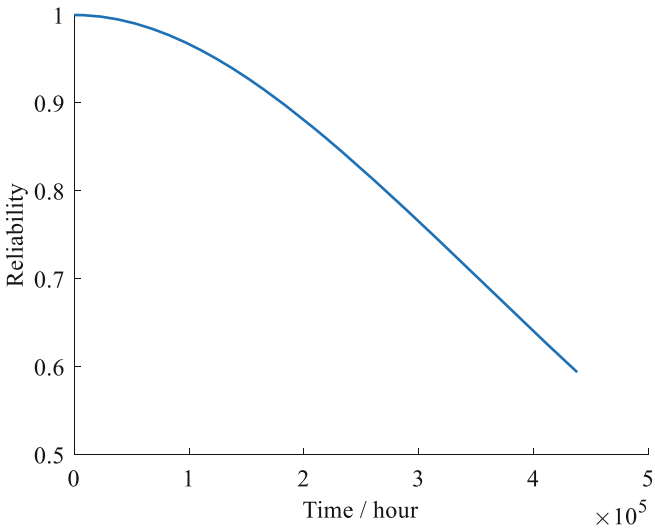


Fig. 8. Control Station Reliability

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

Table 6. Deterioration of Reliability

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

4.5 Maintenance Scheme Optimization

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

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

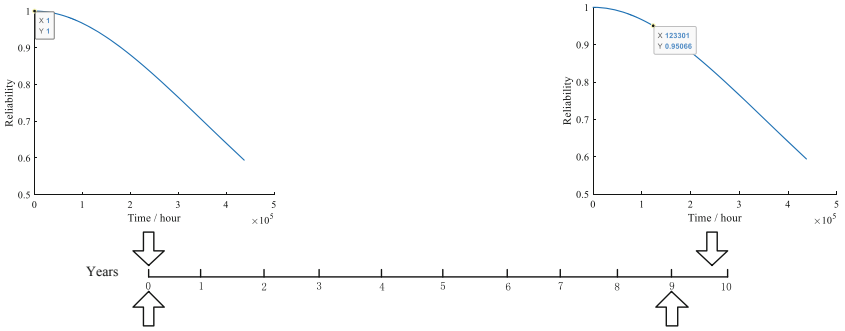


Fig. 9. Schematic Diagram of System Maintenance Scheme Optimization

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

5 Conclusion

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

References

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

Research on Forward Design Process of Network Security Protection Design for Instrument and Control System in Nuclear Power Plant

Chu-Hao Xi[1,2], Yan-Feng Zhao[1,2], Long-Qiang Zhang[1,2], and Jing-bin Liu[3(✉)]

[1] China Nuclear Power Engineering Company LTD., Shenzhen 518045, Guangdong, China
[2] State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment, China Nuclear Power Engineering Co., Ltd., Shenzhen 518172, Guangdong, China
[3] China Nuclear and Radiation Safety Center, Taiyuan 100082, China
Liujingbinjob@163.com

Abstract. Network security protection design for instrument and control (I&C) system in nuclear power plant is an important measure to ensure safe and stable operation of instrument and control system in nuclear power plant. Relevant national departments have put forward a number of regulatory requirements for network security design of instrument and control system, including the general principles of safety protection of power monitoring system proposed by Energy Bureau, Guidelines for grading of classified protection of cyber security by Ministry of Public Security and the technical policy requirements of network security of nuclear power plant proposed by China Nuclear and Radiation Safety Center. How to coordinate network security protection measures to meet multiple regulatory requirements is an important issue in the design of nuclear power plant network security protection. This paper introduces a forward design process of network security that coordinates and considers the above regulatory requirements, and analyzes and explains the design elements and reference standard for the design process, such as zoning and domain design, grading of classified protection, and critical digital asset classification protection.

Keywords: Network security protection design · instrument and control system · nuclear power plant

1 Introduction

The I&C system of nuclear power plant undertake the important responsibility of ensuring the safety and normal operation of nuclear power plant, and belongs to the national key information infrastructure. The network security design of the I&C system of nuclear power plant should meet the requirements of the Network Security Law of the People's Republic of China. In order to implement the Cyber Security Law, the Ministry of Public Security issued Guidelines for grading of classified protection of cyber security. Then, the Energy Bureau promulgated the "Overall Plan for Safety Protection of Power Monitoring System", which requires the implementation of the overall principles of safety

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 269–273, 2023.
https://doi.org/10.1007/978-981-99-3455-3_26

protection of power monitoring system, such as “safety zoning, network dedicated, horizontal isolation and vertical certification”. And, China Nuclear and Radiation Safety Center released the technical policy requirements of network security of nuclear power plant. Many regulations have brought difficulties and challenges to the network security protection design of nuclear power plants, so it is necessary to plan a reasonable forward design process, that is, to implement the requirements of different regulators step by step, and at the same time, to coordinate and unify the protection measures among different regulatory requirements.

2 The Route Map of the Forward Design Process

According to the practical experience of nuclear power plants, this paper proposes the following design process to coordinate and deal with the regulatory design requirements of various departments, as shown in Fig. 1.

Step1. Implement zoning protection in nuclear power plants according to the regulatory requirements of the Energy Bureau, and further divide network security zones into domain(sub-zone) in order to facilitate the Guidelines for grading of classified protection of cyber security (abbreviation to grading protection) in Step 2. See the third part of this paper for detailed design instructions.

Step2. According to the regulatory requirements of the Security Bureau, determine the grading of protection class for each security domain, and then determine the requirements of network security protection measures for the corresponding security domain according to standard GB/T 22239. See the fourth part of this paper for detailed design instructions.

Step3. According to the regulatory requirements of the Safety Audit Center, identify critical digital assets (CDA) according to the correlation degree with nuclear safety, security and nuclear emergency, and implement protection measure by asset type for CDA. See the fifth part of this paper for detailed design instructions.

Step4. After completing the design of asset protection measures, it is necessary to analyze whether the requirements of grading protection are met from the perspective requirement of security domain in step 2. In terms of the situation that the technical control means can not meet, it is necessary to properly adjust the division of security domain or the design of system network. In terms of the situation that the security domain or system network design cannot be modified, it is necessary to carry out Arguments and replace technical control means equivalently through necessary management means.

Through the above four steps, the network security protection design can form a forward design process which considering multi-party regulatory requirements, and form a design closed loop, so that the design scheme can be iteratively optimized continuously.

3 The Network Security Zone and Domain

Based on the requirements of the Energy Bureau, nuclear power plants can be easily divided into control zones (zone I), non-control zones (zone II), production management zones (zone III), office intranet zones (zone IV) and office extranet zones (zone V). However, if the safety zone of nuclear power plant is directly taken as the object for

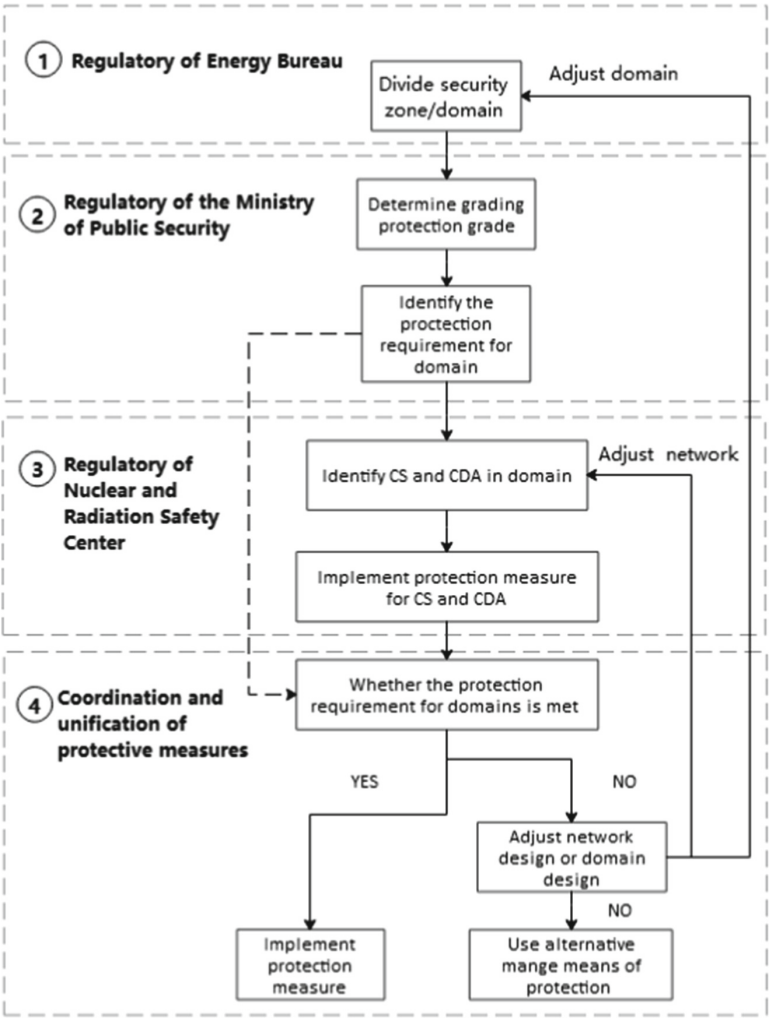


Fig. 1. Forward design process

grading protection, the protection requirements of some systems will be too high due to the large control particles, resulting in waste of protection resources. Therefore, in order to reasonably implement the requirements of grading protection, it is necessary to further split the above zones to form a network security domain, and then take the network security domain as the grading object to complete the grading protection.

Network security domain is a logical zone, which merges I&C systems with similar importance (such as security class, security class, power station capability requirements, etc.) for network security management and protection.

According to IEC 62645, besides importance, the factors considered in the design of network security domain can include organizational responsibility, layout location, overall network structure and technical characteristics of the plant, etc.

1) The security domain should conform with the Defence in Depth strategy of nuclear power plant network architecture, that is, it is not appropriate to classify information or instrument control systems of different and Defence in Depth into one safety domain;
2) The boundary of network security domain should not cross the boundary of security zones;
3) Systems with similar functions and performance requirements should be merged into the same network security domain;
4) Different safety divisions of the same system should be divided into the same network security domain;
5) Multiple systems that share the same network or have multiple network communication between systems should be merged into the same network security domain;
6) The system in the same security domain should have similar nuclear safety class, and physical security class.

4 Grading Protection for Security Domain

According to GB/T 22240, the grade of grading protection is mainly determined by two elements, namely, the intruded object and the damage degree of intruded object. The intruded object needs to consider two aspects of damage, including business information security and system service security. The grade of grading protection of intruded objects is determined by the higher grade of business information security protection and system service security protection. For specific protective measures, please refer to GB/T 22239.

5 Identification and Protection for CDA

According to the regulatory requirements of China Nuclear and Radiation Safety Center, critical systems in the security domain and critical assets in the system should be identified, and system/assets performing the following functions should be identified as critical systems (CS) or critical digital assets (CDA):

1) Systems or assets that implement or support functions for nuclear safety, physical security and emergency response;
2) Systems or assets that affect nuclear safety, physical protection and emergency response functions or that affect the performance of related functions by CS or CDA;
3) A system that provides a path for the above-mentioned CS or CDA to be attacked by cyber attacks, and the path provided by the system may lead to damage and degradation of nuclear safety, physical protection and emergency response;
4) Systems or assets supporting the above-mentioned CS or CDA;

5) Systems or assets that protect such CS or CDA from cyber attacks.

It should be noted that for support systems or equipment that are not directly related to nuclear safety, physical protection and emergency response functions, the operating unit should conduct correlation analysis, and if the analysis shows that it will cause adverse effects, it should also be CS or CDA.

CS or CDA also implement protection by asset type, and the requirement for each asset type please refer to NEI 13–10.

6 Conclusion

This paper introduces a forward design process of network security with closed design loop that coordinates and considers the multiple regulatory requirements, and analyzes and explains the design elements and reference standard for the design process. It is help for the design practise for network security design of nuclear power plant,and it is already used in the design of commercial nuclear power plant which is iteratively optimized continuously.

References

1. Cyber Security Law of the People's Republic of China (Order No.53 of the President of the People's Republic of China)
2. Regulations on the Protection of Key Information Infrastructure (Order No.745 of the State Council)
3. "Nuclear Power Plant Network Security Technology Policy" (China Nuclear [2020] No. 298)
4. Regulations on Safety Protection of Power Monitoring System (China Energy Order No.14 [2014] of the National Development and Reform Commission)
5. "Overall Plan for Safety Protection of Power Monitoring System" (China Energy Security [2015] No. 36)
6. GB/T 32919–2016 Information Security Technology Industrial Control System Security Control Application Guide
7. RG 5.71–2010 Cyber Security Programs for Nuclear Facilities
8. NEI 13–10–2017 Cyber Security Control Assesses
9. IEC 62645–2014 Requirements for security programmes for computer-based systems
10. GB/T 22239–2019 Information security technology-Baseline for classified protection of cybersecurity
11. GB/T 22240–2020 Information security technology- Classification guide for classified protection of information system

Application of Optocoupler Isolation in Rotation Speed Measuring Circuit of Maglev Blower

RuiNan Wu, Kai Zhang, Yang Xu(✉), and MingSheng Zhou

Tsinghua University, Beijing 100084, China
wrn22@mails.tsinghua.edu.cn

Abstract. The main helium fan of a high-temperature gas-cooled reactor uses a magnetic bearing as a shaft bearing, whose pulse signal of rotation speed could be easily disturbed by a high-power variable-frequency drive. There are also problems such as strong electromagnetic interference, potential safety hazards, and different potential distribution between strong and weak electric circuits. Moreover, analog signals require step-down to match digital signals when using AD conversion to transmit signals. This study uses optocoupler isolation to match voltage and improve the transmission quality of rotation speed signal without changing the circuit. Tests and verification have been done on the test maglev blower. The results show that under the same conditions, compared with no isolation, the application of optocoupler isolation is reliable and effective. The application of this technique provides a reference for voltage regularization and enhances the anti-interference ability of analog signal transmission in a complex electromagnetic environment, like maglev blowers.

Keywords: Optocoupler isolation · Voltage matching · Anti-electromagnetic interference · Electromagnetic compatibility

1 Introduction

The main helium fan of a high-temperature gas-cooled reactor uses a magnetic bearing as a shaft bearing, which solves the problems like mechanical wear and high energy consumption of traditional blowers [1]. It has the advantages of energy saving [2] and high efficiency [3]. However, problems such as strong electromagnetic interference and different potential distribution due to high-power variable-frequency drive [4] impact the transmission and stability of rotation speed pulse signal.

Besides, AD conversion is usually adopted to transfer the analog signal into a digital signal to enhance the anti-interference ability and reduce the attenuation of the signal. During the process, the low-voltage rotation speed measurement circuit integrated by the motor is in common ground with the high-voltage circuit. The high-voltage is possible to surge into the low-voltage device, resulting in potential safety hazards. Meanwhile, the output rotation speed pulse signal may not match the voltage of the converter module, which requires an analog signal step-down.

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 274–280, 2023.
https://doi.org/10.1007/978-981-99-3455-3_27

The problems above can be solved by separating the rotation speed measuring circuit from the signal transmission circuit. There is transformer coupling, optocoupling, relay isolation, and other electrical isolation types. Considering the small size, strong electromagnetic signal interference, low transmission rate requirements of rotation speed measuring circuit, and cost, using an optocoupler to separate the circuit can well meet the requirements of matching voltage, protecting the circuit, and suppressing interference for the maglev blower.

2 Optocoupler

2.1 Characteristics of the Optocoupler

The optocoupler is an integrated device, whose infrared light emitting and receiving device and signal processing circuit are encapsulated in the same tube seat. It has the advantages of small volume, long working life, [5] insulation between input and output, and strong anti-interference ability [6].

Common optocouplers can be divided into many types according to the different photosensitive elements, such as photoelectric triode type, high rotation speed type, Darlington type and photo-controlled thyristor type. Common optocoupler devices have very low (less than 1 kΩ) input impedance, large (greater than 10^8 kΩ) insulation resistance [7], and good electrical isolation, which can effectively suppress system noise and improve the device performance. Thus, the optocoupler is a wise choice for industrial automation control, power monitoring, and other occasions that need electrical isolation. [8].

In this article, a high-rotation speed optocoupler is used in a magnetic test machine, as shown in Fig. 1.

Fig. 1. Schematic Diagram of High-Rotation speed Optocoupler

The component is an NPN-type device with a maximum response frequency of 72 kHz, sufficient to transmit rotation speed. The input (signal source) circuit and output (signal transmission) circuit are separated by the different ground at both ends of the device.

2.2 Operating Principle

In the test maglev blower, the integrated measuring circuit outputs a speed pulse signal of 0–15 V, while the signal voltage received by the AD transformation module is 0–5 V.

So the optocoupler isolation device is required to reduce the pressure. Current limiting resistors and other devices used are shown in Fig. 2.

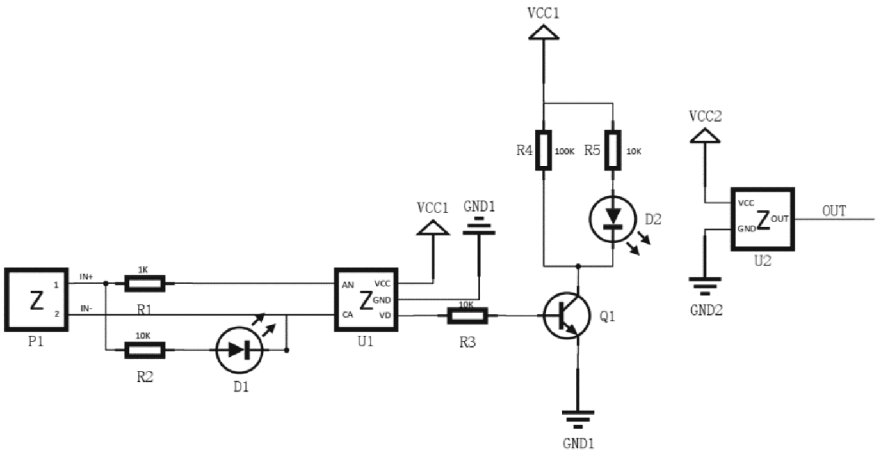


Fig. 2. Optocoupler Circuit Diagram

Following is the brief working principle of the circuit. An electrical signal is inputted to drive LED D1 to emit light. Meanwhile, the signal is amplified by the processor (considered as an operational amplifier) U1 to drive D2, powered by VCC1 (24V), to glow. After the electrical signal converts into an optical signal, the optical signal is converted by the integrated device U2 to the electrical signal, which is processed by the operational amplifier to output. If the input is a low signal, the left light-emitting diode and the triode are equivalent to a cut-off light-emitting triode. D2 does not light and there is no signal on the corresponding output.

The circuits have ground and power respectively and transmit the signal by photoelectricity. Therefore, the signal is transmitted through a linear isolation method.

2.3 Voltage Regularization

In the optocoupler, the input signal is not directly output but used to stimulate LED D1, therefore making the light-emitting circuit conducting and LED D2 luminescing. The output electrical level comes from VCC2 and is controlled by an optical signal. This shows the input and output signals of the optocoupler are not related, so the output voltage can be adjusted with appropriate power supply and resistance values.

The optocoupler can not only realize voltage matching adjustment but also save other information of pulse signal, including period, duty cycle, rise and fall edge, etc. The highest response frequency of the high-speed optocoupler is 72 kHz, and the response time of U2 output is less than 1μs. At the high-frequency speed of 400 Hz, for a pulse cycle, the response delay of the optocoupler is less than 1%, that is, the period, duty cycle, rising and falling edge and other information can be almost nondestructive.

2.4 Suppression Interference

In the new circuit with optical coupling isolation, an electromagnetic interference is equivalent to increasing an interference voltage source series interference resistance in the circuit. The internal resistance of the interference source is generally large (MΩ magnitude), while the input resistance of the optocoupler is small (10^2 Ω magnitude). So even for high voltage transient, the partial pressure of the optocoupler is also small. The partial pressure of the optocoupler is simply calculated as follows:

$$U_{opto} = U_d \times R_{opto-in}/(R_d + R_{opto-in}) \sim 1 \times 10^{-4} U_d \quad (1)$$

This shows the partial voltage of electromagnetic interference on the photocoupling device is small, and the corresponding current input to the photodiode is also small. Thus, generally, electromagnetic interference cannot reach the current required to change the light-emitting state of the light-emitting diode. Therefore, the interference signals existing in the original circuit are mostly blocked on the input side under the optocoupler isolation, realizing interference suppression [9].

2.5 Circuit Safety

Optocouplers can isolate the electrical and magnetic connection of the circuit at both ends and improve the safety of the system [10].

In the original circuit without electrical isolation, the measuring circuit of low voltage is directly connected to the motor circuit of high voltage. In this case, high voltage can easily surge into devices of low voltage, which may lead to an accident.

With the optocoupler connecting the two ends of the circuit by the light signal, the two circuits have respective ground and power. This can prevent the high voltage transient from surging into other circuits, therefore avoiding circuit interference and damage.

3 Application of Optocoupler Isolation in Measuring Circuit

Given the requirements of non-destructive voltage regulation, anti-interference, and circuit safety of the speed measuring circuit of the maglev blower, the author designs an isolation scheme in the optocoupler and then sets up a test machine. The speed sensor outputs the original speed pulse signal of 0–15 V and 0–200 Hz, and the tachometer receives the signal of 0–5 V and carries out AD conversion.

Without isolation, the input and output voltage regulation needs resistance for voltage division. The speed-measuring circuit without electrical isolation is shown in Fig. 3.

The circuit is simple, but the impedance is introduced while the voltage is divided, which affects the period of the signal. The direct connection of the tachometer has no shielding effect on signal interference, but the potential safety hazard of voltage surging into low-voltage devices.

Given the disadvantages of the circuit without electrical isolation, the optocoupler isolation device mentioned above is added to the test machine as shown in Fig. 4. This application is also widely used in PLC external modules and other places to improve these shortcomings. [11].

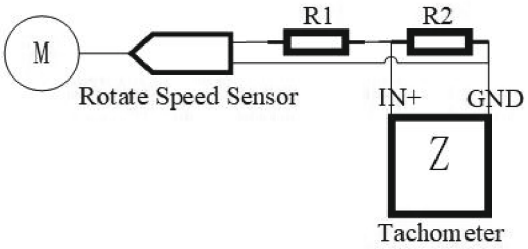


Fig. 3. Speed Signal Circuit without Electrical Isolation

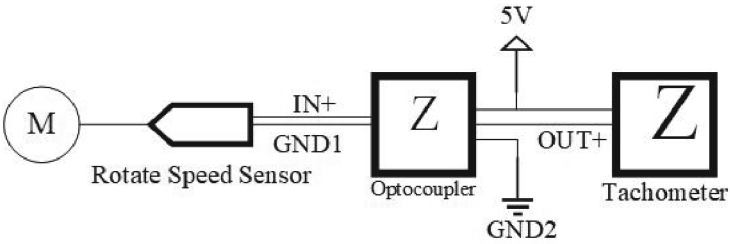


Fig. 4. Speed Signal Circuit with Electrical Isolation

3.1 Voltage Regularization

The main purpose of the optocoupler is to adjust the voltage of the pulse signal nondestructively, retaining the signal characteristics at the same time. On the test machine, the original pulse signal of the speed-measuring circuit is shown in Fig. 5.

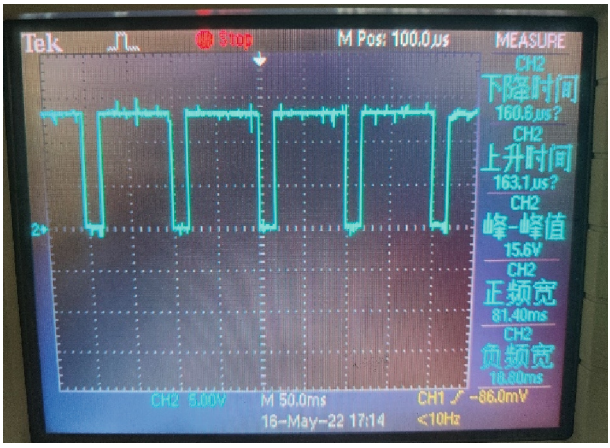


Fig. 5. Output of Circuit without Isolation

For the circuit with optocoupler isolation, the measurement output is shown in Fig. 6.

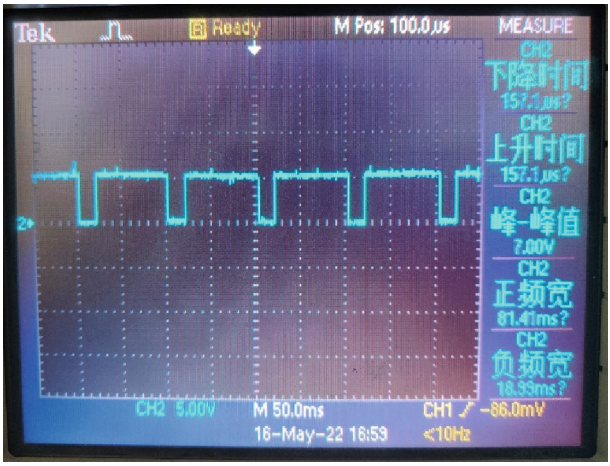


Fig. 6. Output of Circuit with Isolation

The optocoupler converts the 0–15 V signal at the input end into the 0–5 V signal output, realizing the function of voltage matching. The rotation speed signal is still effective, as the frequency is still 10 Hz and the duty cycle is 81.4%.

3.2 Suppression Interference

Electromagnetic interference caused by high-power variable-frequency drive often appears as the occasional voltage transient of rotation speed signal. Although it will turn normal soon, the voltage transient, which needs to be suppressed, may exceed the warning threshold and lead to shaft failure.

In optocoupler devices, the internal resistance of the interference source is generally large, and the input resistance of the optocoupler itself is very small. Even if the interference voltage is large, the partial voltage of the optocoupler is still small, which has little impact on the voltage of the light-emitting diode. Generally, the interference does not affect the luminescence of the light-emitting diode. Therefore, the interference signals existing in the original circuit are mostly blocked on the input side under the optical coupling isolation.

On the test machine with the optocoupler isolation, it is observed that the rotational speed is stable without transient for a long time. The optocoupler effectively inhibits electromagnetic interference.

3.3 Circuit Protection

The circuit with a motor is of high voltage, whose direct connection with the signal transmission circuit has potential safety hazards. In the circuit without isolation, the surge caused by the quick disconnection of the power supply will be directly fed back to the tachometer, which instantly shows overflow.

With the optocoupler isolation, the circuit at both ends is connected by an optical signal, and the voltage surge cannot flow into each other. The quick closure of the power supply will not interfere with the tachometer, and the voltage will not exceed the limit.

The test machine with the optocoupler has passed the speed assessment and can work stably in long term.

4 Conclusion

In this article, a simple, low cost and implementable optocoupler isolation scheme is designed on the rotation speed signal measuring circuit of the maglev blower. Experimental verification shows that the optocoupler is reliable and effective in voltage regulation, interference suppression and circuit protection by comparing the speed pulse signal without isolation under the same conditions. The application of this technique provides a reference for voltage matching and enhancing the anti-interference ability of signal transmission in a similar complex electromagnetic environment.

References

1. Li, H.: Electromagnetic loss analysis of driving motor of main helium fan under inverter power supply, no. 5. Harbin University of Science and Technology, MA thesis 2014(5)
2. Oner, Y., Altintas, A.: Two dimentional static magnetic analysis of radial magnetic bearing systems with different structures. Pamukkale Univ. J. Eng. Sci. **11**(3), 351–356 (2005)
3. Jiarui, H.: Application analysis of maglev blower. Gen. Mach. **12**, 60–61 (2019)
4. Guo, F.: Study on electromagnetic compatibility in DCS system and frequency converter. Xi'an Technological University, MA thesis 2013(7)
5. Briggs, R.D., Armendariz, M.G., Choquette, K.D., Geib, K.M., Serkland, D.K.: Fabrication, packaging, and performance of VCSELs and photodetectors for space applications. In: Vertical-Cavity Surface-Emitting Lasers III, Conference 1999, LNCS, vol. 3627, pp. 40–46. SPIE (1999)
6. Svilainis, L., Chaziachmetovas, A.: Electroluminescence-based isolated high voltage bus DC current sensor. In: Measurement, Conference 2020, LNCS, vol. 151, no. 107203, pp. 1–4 (2020)
7. Quansen, L., Jun, L., Hong, B.: The application of optocoupler in intelligent measurement and control system. Mach. Electron. **02**, 53–56 (2008)
8. Zhang, L., Li, Y., Liu, Y., Jiang, C., Chen, L., Ou, Y.: High voltage isolation and high linearity photoelectric coupler. Semicond. Optoelectr. **2004**(04), 264–267 (2004)
9. Pettersen, F.J., Hogetveit, J.O.: Optically isolated current source. J. Electr. Bioimp. **6**(1), 18–21 (2015)
10. Xueying, L.: Research on baseband transmission of optical coupling isolation in monitoring and monitoring system. Coal Mine Autom. **04**, 15–19 (1996)
11. Januarto, E., Supratno, S.: Plcmikro Sebagai Solusi Otomatisasi Industri. In: Jurnal Kajian Teknologi, Conference 2011, LNCS, vol. 13, no. 2, pp. 16–23 (2011)

Research and Practice on Hardware Failure Verification of Nuclear Instrument Control Platform

Shuang -Cheng Chen(✉), Lei Fu, Zhan Xu, Yuan Zhang, Chao-li Li, and Ke Zhang

CNNC China Nuclear Control System Engineering Co., Ltd, Beijing 102401, China
chenshuangcheng@cncs.bj.cn

Abstract. The digital I&C system of nuclear power plants integrates a number of technologies such as computer, communication, control and display, optimizes the monitoring and operation of nuclear power plants, provides more advanced control and management means, and is the brain and command center of nuclear power plants. Hardware equipment is the basic component of the digital I&C system of nuclear power plants, and its reliability level directly determines whether the system can operate safely, reliably and stably. Reliability analysis of the hardware is carried out, and the failure mode and failure mechanism of the hardware are studied to improve the nuclear power plant. The reliability of digital I&C system is very important. Combining the functional safety concept and safety integrity level requirements of IEC61508, this paper predicts the mean time between failures (MTBF), studies the failure mode and effects analysis (FMEA) of the hardware of the digital I&C system of nuclear power plants, and finds and eliminates the hardware failures of the digital I&C system of nuclear power plants. Weak links can reduce the effects to improve the reliability of the nuclear power plant digital I&C system hardware and provide an effective verification method for hardware reliability verification.

Keywords: The digital I&C system · Failure mode and effects analysis · Fault insertion test · Failure mode · Hardware · Reliability

1 Preface

The digital I&C system of the nuclear power plant integrates a number of technologies such as computer, communication, control, and display. It optimizes the monitoring and operation of nuclear power plants and provides more advanced control and management means [1]. Hardware is the basic component of the digital I&C system of nuclear power plants. The level of hardware reliability directly determines whether the system can run safely, reliably and smoothly. This paper firstly predicts the module mean time between failure (MTBF) according to the research characteristics of the nuclear power digital I&C system, and then uses the hardware failure mode and effect analysis (FMEA) method to verify the prediction result of MTBF. Finally, the hardware FMEA is verified by fault insertion test, so as to improve the hardware reliability of nuclear power digital I&C system.

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 281–289, 2023.
https://doi.org/10.1007/978-981-99-3455-3_28

2 Background and Role

A high-reliability control system required by nuclear power plants with high safety standards [2]. In order to meet the requirements of safe and reliable operation of the system, the instrument control system should adopt effective design methods and technical solutions to improve the reliability of the system. In the design process of the digital I&C system, we should fully apply the theory and method of electronic reliability design. In order to build a high-reliability platform that satisfies the R&D and manufacturing of nuclear power hardware products. We should extensively learn from the best practices of electronic reliability design in communication, aviation, aerospace and other fields [3]. Electronic components are the smallest unit of nuclear power digital I&C system, and its quality and reliability are the basis for ensuring the reliability of the entire digital I&C system [4].

The digital I&C system in this paper is in the order of composition: system— > module— > component.

This paper firstly expounds the estimated steps and calculation methods of the hardware reliability index of the digital I&C system.The first step is to assign system reliability indicators to modules.

Secondly, the paper introduces the estimation steps and calculation process of the hardware reliability of the digital instrument control system module.In this paper, the hardware failure mode and effects analysis method is used for research, and the potential failure of hardware is analyzed from the bottom up at the component level [5]. Finally, we perform a fault insertion test design based on the failure mode and effects analysis, thereby verifying the reliability of products and systems.This paper introduces the method of identifying and analyzing the hidden hardware failure mode in the system in detail, and analyzes the influence of the known hardware failure mode on the system. This paper also provides reference information for product testing to help further verify the hardware reliability of the digital I&C system.

3 Prediction and Calculation Method of Hardware Reliability of the Digital I&C System

3.1 Prediction of Hardware Reliability of Digital I&C System

From a system-level perspective, RAMS indicators (i.e. reliability, availability, and maintainability) include three, namely, rejection rate, misoperation rate, and availability rate [6].

The main quantitative indicators of the module include MTBF and diagnostic coverage (DC). The MTBF and the DC can obtain the undiagnosable rejection rate, the undiagnosable malfunction rate, and the diagnosable failure rate.

We can make indicator assignments to the quantitative indicators of the module, after linking the system-level quantitative indicators refusal probability, misoperation rate, usability, and module quantitative indicators MTBF and diagnostic coverage DC.

This paper defines the undiagnosable refusal failure rate and the undiagnosable malfunction failure rate λ_U = (1-DC)*1/MTBF. The diagnosable failure rate λ_D = DC*1/MTBF。

It can be seen from the above formula, in the final analysis, the MTBF and DC of the board module need to be allocated in order to meeting the requirements of system-level refusal probability, misoperation rate, and availability.

Steps to predict the hardware reliability of the digital I&C system are as follows.

1) A clear system definition, including system functions, tasks, system components and their interfaces.

The system is divided into modules according to functions, and then the system reliability diagram is drawn according to the series-parallel relationship of each module.
(2) Clarify the failure criteria of the system.

By distinguishing the normal operation or fault state of the system, the fault propagation relationship between modules can be clearly recognized, which provides a basis for the reliability diagram. The general system fault criterion is determined according to the operating limits of the system, such as the function, performance index, operating environment and working characteristics. The main basis for the failure of the digital I&C system is that under the specified working environment, all the functions listed in the serial number (1) cannot be completed or some performance indicators cannot be kept within the scope specified in the requirements specification.
(3) Clarify the working conditions of the system.

Clarifying the working conditions of the system is beneficial to the parameter selection of the component-level reliability prediction model.
(4) Draw the reliability diagram of the system (with the module as the smallest unit), and establish the system reliability model.
(5) Draw the reliability diagram of the module (with the module hardware component as the smallest unit), and establish the module reliability model.
(6) Predict the reliability of each module.
(7) Predict the reliability of each module according to the module reliability model.
(8) Predict the reliability of the system according to the system reliability model.

3.2 Calculation of Two Basic Relationships of MTBF in Digital I&C System

The series relationship and the parallel relationship are the two basic relationships in the reliability diagram.Regardless of the size of the system, the reliability diagram can be constructed according to the composition of the modules.Therefore, the method for drawing the system reliability diagram will not be described again. The MTBF calculation methods for these two basic reliability diagrams are as follows.

(1) Series model.

The characteristic of a series system is that the failure of any one of the constituent units will lead to the failure of the entire system [7]. Its reliability diagram is shown in Fig. 1.

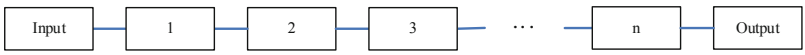


Fig. 1. Reliability diagram of series system

The failure rate of a series system λ_S is the sum of the failure rates of each unit in the system λ_i, which can be expressed as follows.

$$\lambda s = \sum_{i=1}^{n} \lambda i, \ MTBF = \frac{1}{\lambda s} \tag{1}$$

(2) Parallel model.

The characteristic of a parallel system is that fails of the all constituent units will lead to the failure of the entire system [8]. Its reliability diagram is shown in Fig. 2.

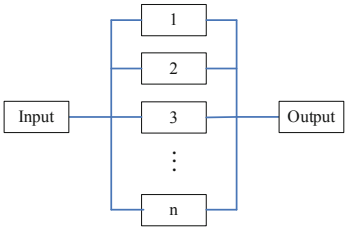


Fig. 2. Reliability diagram of parallel system

The failure rate of a parallel system, which can be expressed as follows.

$$MTBF = \sum_{i=1}^{n} \frac{1}{i\lambda} \tag{2}$$

4 Prediction and Calculation Method of Hardware Reliability of Digital I&C System Module

The main quantitative indicators of the module include MTBF and diagnostic coverage (DC). Both of these metrics are derived through the module-level FMEA.

In order to meet the requirements of module-level hardware reliability indicators.

(1) Before the module hardware FMEA, first determine the failure mode of components and the basic failure rate of components.
(2) Then execute the module hardware FMEA to confirm that the module design meets the MTBF and DC indicators.
(3) Finally, verify the validity and correctness of the FMEA through the fault insertion test.

4.1 Digital I&C System Module Hardware FMEA Preparation

The smallest component of a module is an electronic component. The quality and reliability of components are the basis for ensuring the reliability of the entire instrument control system [4]. The stress analysis method is a method for predicting the failure rate of electronic components based on probability statistics. The reference standard for

the prediction model of component failure rate is "GJB299C-2006 Electronic Equipment Reliability Prediction Manual". Imported electronic components can be based on Appendix A of the standard [9]. First, the basic failure rate of the components is obtained according to the device model of the components. The basic failure rate is then corrected for factors such as component quality grade, stress level, and environmental conditions.

In this paper, the stress analysis method and the parts count method are used for prediction, and the stress coefficient is mainly based on the actual stress analysis. There are three main sources of component failure rate data.

(1) Reliability data provided by component suppliers.
(2) Estimated according to MIL-HDBK-217 standard.
(3) Predict the failure rate according to the experimental data provided by the manufacturer.

Most manufacturers conduct accelerated experiments according to the JESD22 standard, and perform mathematical statistics on the results according to the JEP122D/JESD85 standard to obtain the failure rate of components. The failure rate data is based on the exponential distribution of the component life distribution, and the mathematical model of the failure rate mathematical statistics is the Arrhenius equation.

The Arrhenius equation [10] used for component failure rate estimation is as follows:

$$\lambda = \frac{\chi^2(\alpha, 2n+2) \times 10^{-9}}{2 \times AF \times DH} \tag{3}$$

$\chi^2(\alpha, 2n+2)$ is the chi-square distribution model failure prediction.The α is the confidence level, generally 60%. The n is the number of sample failures. DH is the equivalent working time, which is essentially the number of samples multiplied by the acceleration time. AF is the overall acceleration factor, where TAF is the temperature acceleration factor and VAF is the voltage acceleration factor. The expression of the working failure rate λ is as follows.

$$\lambda_{PS} = \sum_{i=1}^{n} N\lambda_{pi} \tag{4}$$

The λ_i is the working failure rate of the ith componen. N is the number of the same component.The n is the number of types of components.

4.2 Digital I&C System Module Hardware FMEA

The steps of module hardware FMEA are as follows.

(1) Function analysis: describe the function to be completed by the module, decompose the function of the module, divide the module into relatively independent functional units according to functions, and find out the basic devices that complete this functional unit. Indicate the relationship between the various functional units.
(2) Draw a functional diagram: The functional diagram reflects the correspondence between functions and devices, and the functional units are completed by those devices.

(3) Draw a reliability diagram: indicate the input and output relationship between each functional unit, so as to distinguish the mutual influence relationship between the failures of each functional unit.
(4) Definition of failure mode: Determine the failure mode and failure mode percentage of the component.
(5) Failure mode level: Hardware failures can be classified into categories according to the severity of module failures.
(6) Failure analysis: analyze the cause of failure and calculate the probability of failure.
(7) Calculate MTBF and DC.

This article refers to the concept of functional safety and the evaluation method of safety integrity level in IEC 61508, and takes the digital output terminal module as an example to carry out FMEA.

(1) Function analysis: The digital output terminal module can support digital output transfer, the output signal is 24VDC voltage signal and contact type signal, and the IO module constitutes a complete IO processing unit.
(2) Draw the function diagram as shown in Fig. 3.

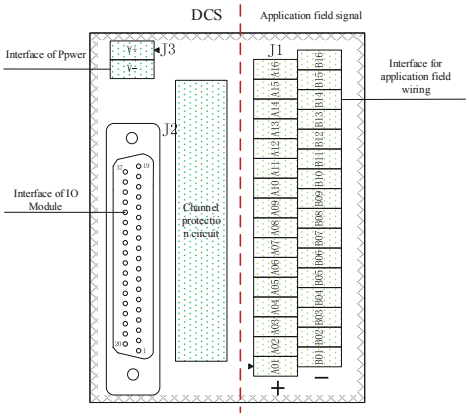


Fig. 3. Example of functional diagram

(3) Draw the reliability diagram as shown in Fig. 4.

Fig. 4. Example of reliability diagram

(4) Definition of failure mode: According to the Mil-Hdbk-338B standard, the failure mode and failure mode percentage of the component are determined as shown in Table 1.

Table 1. Example of failure modes and percentage of failure modes

Board function block	Failure mode	Failure Rate	Mode Percent	Mode Failure Rate
Output connector	Open circuit failure	0.91	0.61	0.55
Output connector	Poor contact failure	0.91	0.23	0.21
Output connector	Short circuit failure	0.91	0.16	0.15

(5) Failure mode level.

Class S1 failures: failures affecting safety functions. Type S1 failures are divided into undiagnosable failures and diagnosable failures. Undiagnosable failures refer to failures that cause the board's security functions to be unavailable when required and cannot be discovered by board diagnostics or system diagnostics. A diagnosable failure refers to a fault that renders a board's security functions unavailable when required, but can be discovered by board self-diagnostic measures or system diagnostics.

Class S2 failures: failures unrelated to the safety function, the failure does not affect the realization of the safety function. Such as signal indication, and failure of self-diagnosis function.

(6) Failure analysis: The specific analysis example of FMEA is shown in Table 2.

Table 2. FMEA example

Material	Tag number	Board function block	Failure mode	Local influence	Final impact	Severity	Diagnosable	Diagnosis method	Mode Failure Rate
Plug-in double row screw connection terminal block	J1	Output connector	Open circuit failure	Channel output signal disconnected	Output to field switch signal error	S1	0	None	0.55
	J1	Output connector	Poor contact failure	Channel output signal is unstable	Output to field switch signal error	S1	0	None	0.21
	J1	Output connector	Short circuit failure	Channel output signal is unstable	Output to field switch signal error	S1	0	None	0.15

(7) Finally, calculate the MTBF and DC of the board according to the quantitative statistical calculation formula of the board.

$$DC = \frac{\lambda_{S1D}}{\lambda_{S1D} + \lambda_{S1U}} \tag{5}$$

$$MTBF_{S1}(Year) = \frac{1}{\lambda_{S1D} + \lambda_{S1U}} \times \frac{1}{8760} \tag{6}$$

$$MTBF(Year) = \frac{1}{\lambda_{S1} + \lambda_{S2}} \times \frac{1}{8760} \tag{7}$$

The λ_{S1D} is the diagnosable failure rate of type S1. The λ_{S1U} is the undiagnosable failure rate of type S1. The λ_{S1} is the failure rate of type S1. The λ_{S2} is the failure rate of type S2. The $MTBF_{S1}$ is the mean time between failures of type S1 fault. The MTBF is the mean time between failures of the entire board.

4.3 Module Hardware Component Level Failure Verification Process

The component-level fault insertion test is carried out on the real board, and the code of the board under test is not modified in principle.

For large systems, it is not practical to verify failures at the entire component level. In the actual verification process, the key links that affect the security function of the module can be sorted out according to the module schematic diagram and reliability diagram. According to the failure modes of the components in the module FMEA analysis, the corresponding real component failures are manufactured on the critical links affecting the module's safety function [11]. Observe the local and final effects to verify the correct processing of the module.

Figure 4 "Application Field Wiring Connector" function block has open circuit, poor contact and short circuit failure modes, then the design fault insertion test is to manufacture open circuit, poor contact and short circuit failure faults. Verify whether the local impact and final impact of the functional block are consistent with the analysis in Table 2, and the test case design is shown in Table 3. After the fault insertion test, the result of the component failure is verified on the real board, and the local and final effects of the component failure are recorded to verify the reliability of the module.

Table 3. Fault Insertion Test Example

NO	Test Instructions/Procedures/Data	Desired result
1	Open the positive and negative terminals of the signal output in the output connector respectively	The channel output signal is disconnected, and the output to the field switch signal is wrong
2	Open and conduct the signal output positive and negative terminals in the output connector respectively	The channel output signal is disconnected, and the output to the field switch signal is wrong
3	Short-circuit the positive and negative terminals of the signal output in the output connector to the adjacent pins respectively	The channel output signal is disconnected, and the output to the field switch signal is wrong

5 Concluding Remarks

In this paper, after assigning the hardware reliability index of the digital instrumentation and control system to the modules, the hardware failure mode and impact analysis method are studied, and it is found that the failure of the system is from the perspective of the lowest component, and this inductive analysis method is used to predict the hardware reliability of the module., to demonstrate the module hardware FMEA process with an example, and finally use the fault insertion test to verify the validity and correctness of the FMEA [12, 13].

This paper provides a complete set of hardware reliability analysis, calculation and verification process of nuclear power digital I&C system. This paper introduces the concept of functional safety and the assessment method of safety integrity level in IEC 61508 into the life cycle of nuclear power digital I&C system. This paper further introduces the steps of hardware fault insertion test, which broadens the ideas and methods for effectively evaluating the hardware reliability of nuclear power digital I&C system, and has important reference significance for hardware reliability research.

References

1. Yang,C., Lu, C.: Development and application analysis of digital instrument control system in nuclear power plants. Shandong Industr. Technol. **2016**(4), 1
2. Zheng,Y.-B., Peng, X.-Q., Dong, Z.-B.: Application analysis of high reliability technology for AP1000 I&C System. In: China Nuclear Power I&C Technology Conference (2011)
3. Ren, L.-H., Lang, A.-G., Li, S.-X., et al.: Analysis and calculation of reliability and availability of nuclear power plant I&C system. Autom. Instrum. **36**(11), 127 (2015)
4. Bai,T., Jin, C.-R., Zhang, C.-L.: Discussion on element screening in the development of instrument and control equipment in nuclear power plants. Autom. Panorama **2013**(4), 5
5. Wang, X.-Y., Zhang, Y.-D., Zhou, X.-B.: research and practice of software FMEA in nuclear level I&C system platform (Harmony System). Autom. Panorama **34**(3), 5 (2017)
6. Xu, B., Liu, M.-X., Han, W.-X., et al.: Analysis and calculation of reliability parameter test scheme for safety level DCS system of nuclear power plant. Instr. Users **25**(11), 4 (2018)
7. Shen, W., Lu, B., Yang, B.-Q., et al.: Research on reliability evaluation method of nuclear power safety injection system. Power Gener. Equipm. **31**(4), 5 (2017)
8. Zhang,W., Jia, Y.: System reliability analysis method and comparative study. Envir. Technol. (2021)
9. General Equipment Department of the Chinese People's Liberation Army GJBZ299C-2006 Electronic Equipment Reliability Prediction Manual. Military Standard Publishing and Distribution Department of General Equipment Department, Beijing (2007)
10. Yang, X.-Q., Wu, Q., Zhou, L.: Study on residual life of analog card in Qinshan No.1 factory [J]. Instr. Users **26**(1), 5 (2019)
11. Tong,X.-P., Wang, W.-F.: System test method and application based on fault injection. In: Building a well-off society in an all-round way and China's aviation development - China Aviation Science and Technology Conference (2013)
12. Chen, S.-C.: Research on hardware design of nuclear power digital instrument control system. Xi'an University of Electronic Science and Technology (2020)
13. Shen, W.-W., Hu, Y.-W., Tian, M.: Research on the evidence collection of HAF601, a FPGA based instrument control system platform for safety level in nuclear power plants. Comput. Knowl. Technol. **013**(006), 255–258 (2017)

Research on Verification Method of PCIe IP Core Based on Programmable Logic

Ling-Ling Dong[1(✉)], Jun-Long Huang[1], Jun-Qing Zhang[1], Xian-Yin Xu[1], Guo-Yun Wang[2], Chao Peng[2], and Li-Hua Liu[2]

[1] China Techenergy Co., Ltd., Beijing 100094, China
donglilingabcd@126.com
[2] Guangdong Nuclear Power Joint Venture Co., Ltd., Shenzhen 518124, China

Abstract. With the development of nuclear power digital instrument control technology, IP core, as an indispensable part of FPGA chips, is more and more involved in the realization of important functions of instrument control products. Due to the high reliability requirements in the nuclear power field, it is necessary to fully verify the logical functions of IP cores. Traditional verification methods cannot meet the requirements of complex IP core verification quality and efficiency due to the use of directional testing and poor reusability. This paper proposes a method based on UVM construction of IP core verification platform, through the analysis of IP core application scenarios, and uses UVM components to realize the hierarchy and reusability, and finally, random test excitation generated by components is injected into the tested IP through the verification module, and the output data is monitored to check whether it is consistent with the expected value. This method can quickly build a verification platform, and the random excitation generated by the platform can fully verify IP. The paper takes the PCIe X4 IP verification of domestic FPGA as an example to explain how to use this method to build a verification platform and execute test cases. By practice, this method shortens the verification time and improves the verification efficiency.

Keywords: Functional verification · PCIe IP core · UVM verification · Verification efficiency

1 Introduction

At present, the development of smart boards in digital instrumentation and control systems in the nuclear power field is mostly completed by FPGA chips. The IP core is a part of the FPGA chip, it is mainly used for the realization of complex design function modules. The designer can avoid repetitive work and shorten design time by calling IP cores. Therefore, FPGA design based on IP core also participates in the realization of important functions of instrument control products. According to the relevant standards of nuclear power, the products developed for FPGA need to be fully verified. As a pre-development item, the IP core needs to be proved to meet the requirements through operating experience and necessary supplementary tests. The verification of the IP core is essential work before the product delivery.

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 290–301, 2023.
https://doi.org/10.1007/978-981-99-3455-3_29

As the complexity of IP design increases, the verification work becomes more complicated. Due to the defects of low coverage and poor reusability in the past directional verification, it is difficult to be competent for the current large-scale IP core verification [1]. Building a fast and efficient general verification platform can improve test coverage and reusability, and is an important means to solve IP core verification. One such complex IP core is the PCIe IP core.

The PCIe bus interface is widely used in the design of data stream transmission that requires high speed and large data volume. Compared with the PCI interface, the transmission speed of the PCIe interface has been greatly increased, and its performance improvement has also made its verification work more arduous. A main control smart board of nuclear power uses the PCIe protocol to complete the communication between the FPGA and the CPU, and is implemented with the PCIe IP core. The PCIe protocol is complex, and it is difficult to verify the IP core alone, and it cannot quickly build a verification platform to meet the needs of the project schedule. Aiming at this problem, this paper proposes to use the PCIe verification module, simulate the PCIe protocol interface, connect with the tested IP, and the test incentives are given from the other end of the verification model. The framework solves the problems of reusability and standardization of the verification platform and improves the verification efficiency.

2 Validation Platform Design

2.1 IP Core Introduction

The localized PCIe IP core verified in this paper is a high-performance FPGA product (PGT180H) with completely independent property rights architecture and mainstream 40nm process. The FPGA is developed by Shenzhen Pango Microsystems Co., Ltd. The company provides a self-developed kit for the chip. PCIe IP is an IP designed to implement the PCIe protocol in FPGA products, and can be instantiated and generated by the IP Compiler tool in the kit [2].

The PCIe protocol is divided into three layers: transaction layer, data link layer and physical layer. Each layer has two functions of sending and receiving at the same time. The hierarchy is shown in Fig. 1:

In the PCIe architecture, data packets are generated at the core layer of the device, then pass through the transaction layer and data link layer of the device to the physical layer, and are output through high-speed differential signals. The data at the receiving end is also transmitted to the transaction layer through the physical layer and the data link layer, and finally reaches the device core layer for processing.

The internal programmable logic design structure of PCIe IP is shown in Fig. 2:

The *pgs_pciex4_ui_top* module in the IP core implements a part of the transaction layer functions, and also completes the interface conversion function between the PCIe protocol and the AXI interface. The *pgs_pciex4_axi_slave* module receives the commands of AXI initiated by the user side, converts them into commands corresponding to the PCIe protocol and sends them to the *pgs_pciex4_tl* module, and then sends the response returned by the other point to the user side. The *Pgs_pciex4_axi_master* module converts the received commands such as MRd/MWr from the other point into commands of AXI, and sends the response returned by the user side to the *pgs_pciex4_tl* module.

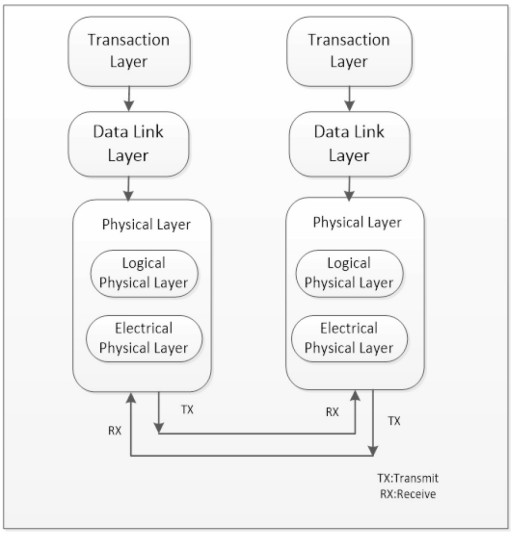


Fig. 1. PCIe layered architecture

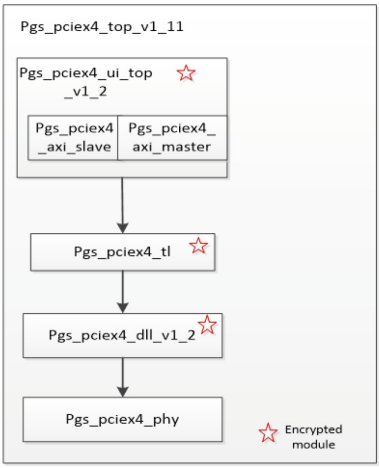


Fig. 2. PCIe programmable logic implementation architecture

The *Pgs_pciex4_tl* module implements the functions of the PCIe protocol transaction layer, the *pgs_pciex4_dll* module implements the functions of the PCIe protocol data link layer, and the *pgs_pciex4_phy* implements the PCIe protocol physical layer functions [2].

2.2 Verification Framework

The implementation of the PCIe IP core is relatively complex. Most of the code inside the IP core provided by the manufacturer is encrypted and invisible. This verification treats the IP core as a black box. The bottom layer of the PCIe IP core communicates through differential signals. After analysis, the external interfaces of the PCIE IP core are AXI Interface and APB interface. The APB interface can configure some parameters of the PCIe IP core, and AXI implements the communication with the user side. The verification platform uses a verification model to connect with the tested IP. It injects test incentives from the verification model, and checks whether the function of the tested object is correct. The overall verification framework is shown in Fig. 3:

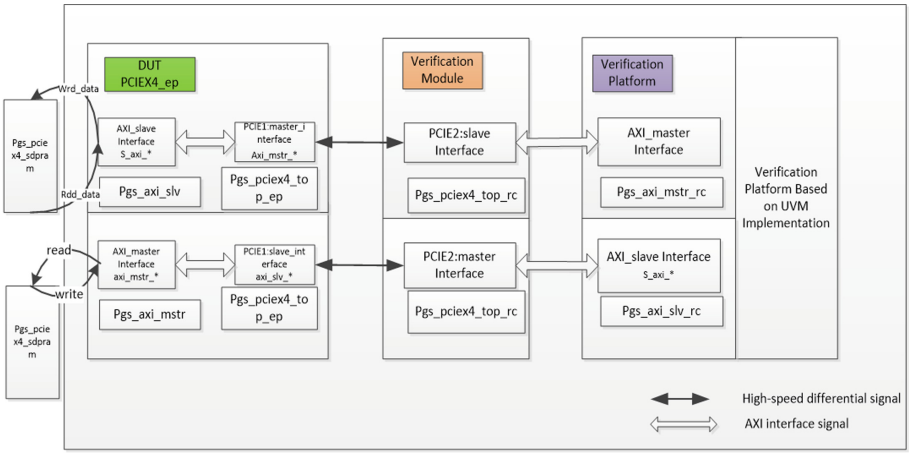


Fig. 3. Integrated validation framework

The DUT under test is used as the EP node of PCIe, and the verification IP is used as the RC node. The verification platform injects test incentives through the AXI slave interface of the verification model to check whether the DUT side can receive normally, and simulates the process of reading and writing data from the RC node to the EP node; at the same time, it can also inject incentives from the DUT side to check whether the verification model can receive normally, and simulates the process of reading and writing data from the EP node to the RC node.

2.3 Introduction to Verification Methods

In this paper, the UVM method is used to build the IP core verification platform. The test stimulus is generated by the Sequence and input to the Sequencer, then sent to the DUT of the tested object through the driver, and the Monitor monitors the data returned by the DUT.

There are two main base classes in UVM methods: uvm_component and uvm_object. An actual verification platform is derived from the base class, including basic components such as uvm_driver, uvm_sequencer, uvm_monitor, uvm_agent, uvm_scoreboard,

uvm_env, and uvm_test [3]. The operation of the UVM verification platform requires two mechanisms, namely the factory mechanism and the sequence mechanism. The existence of the factory mechanism is to more easily replace the instance or registered type in the verification platform, and the configuration flexibility brought by the factory registration mechanism [4]. The run_test command can only be run at the top level of the test if all used components are loaded into the factory. After the UVM verification platform is built, it is impossible to execute the test, there is no data flow, just like the introduction of water flow after the pipeline is connected, and the sequence is the source of incentives for the entire environment, starting a sequence starts the operation of the verification platform [5]. A basic verification platform built by the UVM method is shown in the figure (see Fig. 4):

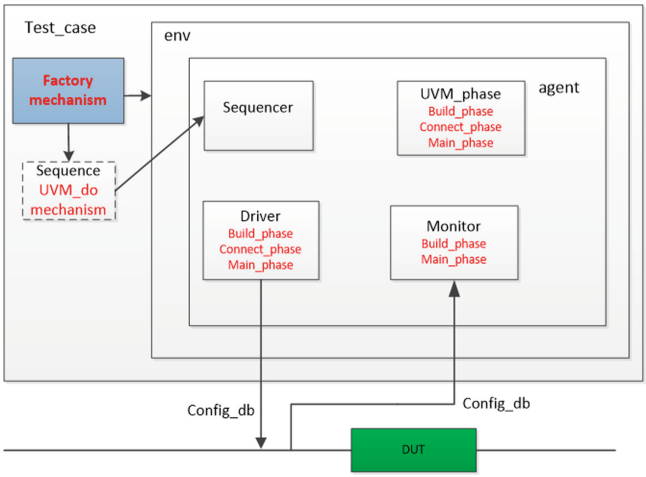


Fig. 4. Verification platform based on UVM method

3 PCIe IP Core Verification

According to the characteristics of the PCIe IP module, the UVM verification method is used to build a simulation verification platform for the PCIe IP module. The components of the verification platform are inherited from the UVM base class, and the hierarchy is clear, which is convenient for inheritance and extension [6].

3.1 Verification Platform Construction

The nuclear power instrumentation and control equipment MPU board adopts the PCIe IP in the FPGA to complete the communication between the embedded CPU and FPGA. In actual design, PCIe IP is used as the endpoint device in the protocol topology. The interfaces of PCIe IP to the user side include APB interface and AXI interface. The

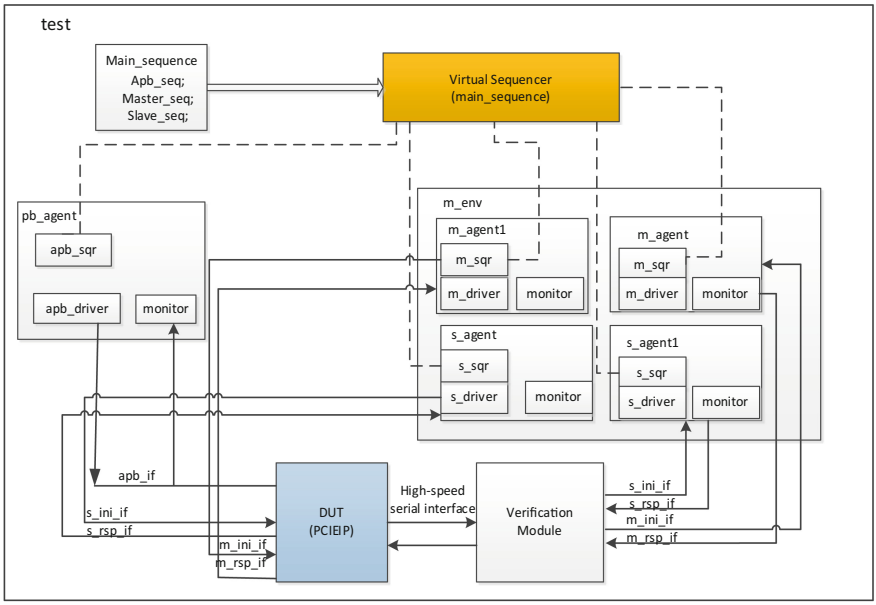


Fig. 5. Validation platform block diagram

interface timing driver of APB is written in the verification platform, and the PCIe IP register under test is read and written through the APB bus port.

The platform needs to write the interface timing driver of AXI, construct m_agent and s_agent to simulate the master and slave modes of AXI, and use the reusability of the UVM method to generate two pairs of master/slave signals, which are connected to the PCIe IP core under test and the IP core port of the verification module. The PCIe communication situation is tested by constructing various timing sequences.

The master-slave port and APB port of the IP core support full-duplex communication. In the verification platform, the Virtual Sequencer is used to schedule and control the Sequencer of the APB and the master-slave port to achieve synchronization between different sequences. The specific verification framework is shown in Fig. 5.

3.2 Determining the Interface Signal

The verification platform communicates with the tested IP through a virtual interface. After analysis, the virtual interface is an AXI interface. The AXI interface has 5 channels, namely, write address channel, write data channel, write response channel, read address channel and read data channel. According to the flow of data or address information, the five channels of the AXI bus can be divided into two categories, one is from the master interface to the slave interface, which is the write address channel, the write data channel, and the read address channel, and the other is from the slave interface. The flow to the main interface is the write response channel and the read data channel.

The interface of AXI is divided into master interface and slave interface. The signals of the master and slave interface are divided into two groups. One group is the data sent to the tested object, which is defined as m_ini_if/s_ini_if, and the other group is the data returned by the tested object, which is defined as m_rsp_if /s_rsp_if. The APB interface between the environment under test and the DUT is apb_if. The establishment interface signals are as follows:

Interface m_ini_if#(ADDR_WIDTH = 64, DATA_WIDTH = 128)(input clk, input rst_n);

Master interface flows to slave interface:

write address channel signal;

write data channel signal;

read address channel signal;

……

endinterface

Interface s_ini_if#(ADDR_WIDTH = 64, DATA_WIDTH = 128)(input clk, input rst_n);

Flow from interface to main interface:

write response channel signal;

read data channel signal;

…

endinterface

Interface apb_if(input clk, input rst_n);

address signal;

Chip select enable signal;

write enable signal.

write data 1;

write data 2;

…

endinterface

3.3 Constructing Test Incentive Data

The data mode of AXI transmission is transmitted in the way that burst is 1, that is, a start address is sent, a burst length is sent, and then a group of data with the length plus 1 is sent. First establish a basic transaction as m_burst_trans, which contains signals such as addr, len, data, etc. The data size of data is determined by len. According to the IP, it supports 15 ID numbers, randomizes 15 m_burst_trans, and each time a sequence is sent, data is extracted from the 15 m_burst_trans and sent to the AXI interface. The process of generating test incentive data is shown in Fig. 6.

3.4 Sequence Scheduling

Because there are three types of external interfaces of the tested object, each type of interface has its corresponding sequence, such as apb_sequence, which realizes the function of reading and writing to the internal registers of PCIe, master_sequence realizes

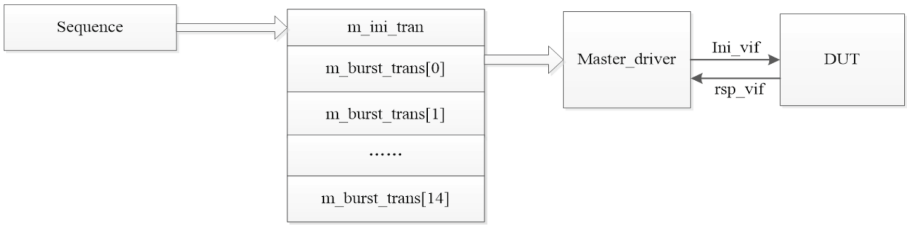


Fig. 6. Test stimulus generation

reading and writing data to the master interface of the DUT, and slave_sequence realizes reading and writing data to the slave interface. For the scheduling of different Sequences, use the virtual sequencer to schedule the sequencers in the respective Agents to achieve full-duplex communication (see Fig. 7).

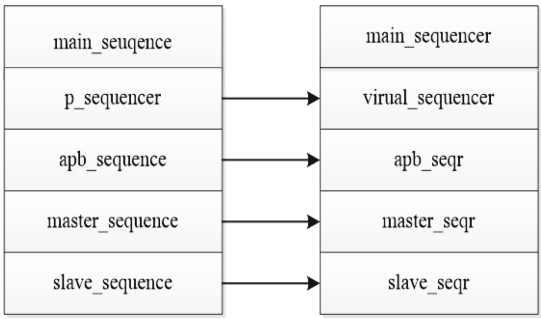


Fig. 7. Schematic diagram of sequence schedule

Sequence operation is in the test module, indicating which sequence needs to be run for the environment to run. The following code indicates running main_sequence, and the content in main_sequence will be automatically executed after the test platform is started.

Write it as follows:

Virtual function void build_phase (uvm_phase phase);

Super. Build_phase (phase);

uvm_config_db#(uvm_object_wrapper)::set(this,"main_sqr.main_phase", "default_squence",main_sequence::type_id::get());

endfunction

3.5 Data Processing

When m_agent initiates a write instruction to write data, the slave_agent1 receives data; when m_agent initiates a read instruction, it needs to read data from slave_agent1. Slave_agent1 stores the received data, if the m_agent reads it, it sends data out. In order to realize the communication between two threads with asynchronous reading and

writing, the mailbox mechanism in system Verilog is adopted, slave_agent1 stores the received data in the mailbox according to the starting address and data format. After receiving the reading instruction, slave_agent1 searches the specified starting address and sends all its corresponding data.

4 Validation Results

This verification platform is built with UVM. For similar interfaces, the same agent can be reused. The reusability of UVM verification components improves the efficiency of building the verification platform. In addition, using the verification module to connect with the tested object does not need to consider the high-speed serial interface, and also reduces the time of building the verification platform. The functional verification results and analysis are as follows:

1) Verification of rate

The PCIe module of the tested object supports the communication rate of 2.5GT/S and 5GT/S. Parameter SUPPOT_5G is the signal that controls the rate. When the value is 0, it means that it is in GEN1 state, that is, the transmission rate is 2.5GT/S. When the value is 1, it means that it is in Gen2 state, that is, the transmission rate is 5GT/S. By modifying the parameter SUPPORT_5G value, check whether the single signal transmission time of differential signal is consistent with the requirements. As Fig. 8 shows the Gen2 state, it can be seen that the single signal transmission time is 0.2ns, that is 5GT/S; As Fig. 9 shows the GEN1 status, it can be seen that the single signal transmission time is 0.4ns, that is 2.5GT/S. The verification results are shown in Fig. 8 and Fig. 9.

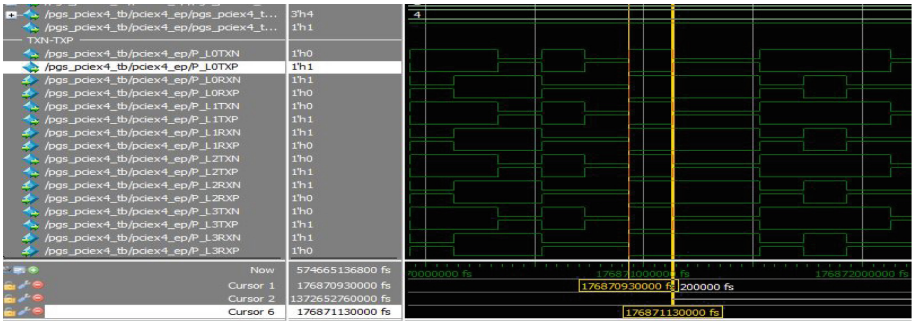


Fig. 8. PCIe Gen2 status rate waveform

2) Read/Write Configuration space register

The verification platform can read the PCIe IP control / status register through the interface of APB. According to the operation manual of PCIe IP, the address space distribution of APB is as follows (see Fig. 10):

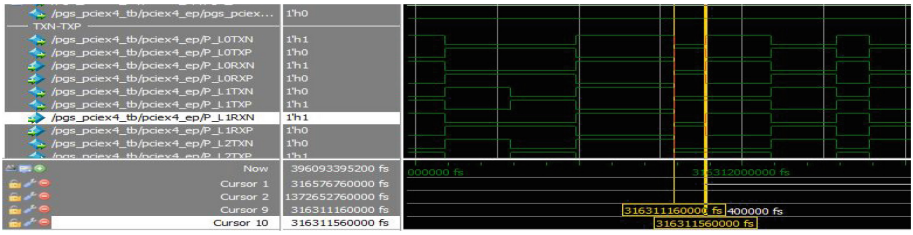


Fig. 9. PCIe Gen1 status rate waveform

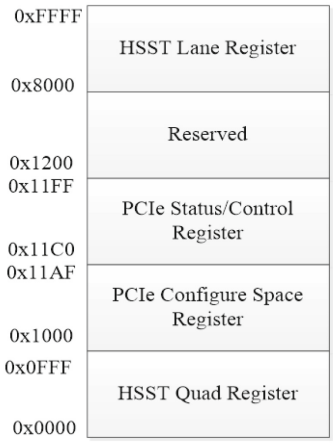


Fig. 10. Address space of APB

The address of PCIe configuration space register is 0x1000 ~ 0x11af, the register of 0x1064 address is device capabilities, the bit width of this register is 32 bits, and 2 ~ 0 bits represent Max_payload_size (maximum data load length).

As shown in the Fig. 11, the address of the read data is 0x1064, the read data is 32 'h0000. Then, the data written to this address is 32' h0004, and the value read again is 32 'h0004. Through this test, the reading and writing function of the configuration space register can be verified.

3) Memory read / write function

The verification platform uses burst mode to read and write memory, verifying two data flow directions: the first is that the verification platform reads and writes data to the tested object; second, the tested object reads and writes data to the verification platform. The test case is addressed according to 64 bits.

The verification platform reads and writes data to the tested object, m_agent sends data to the tested object, slave_ Agent1 receives the data transmitted by the tested object through PCIe, and then m_agent initiates a read request, and the data read by the test is consistent with the data written. The verification results are shown in the Fig. 12.

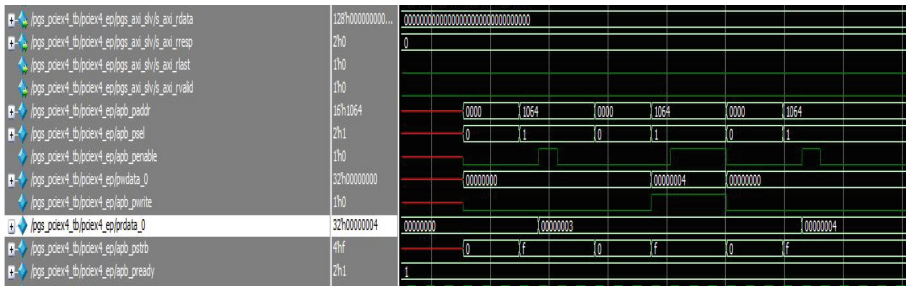


Fig. 11. Verification waveform of configure register read-write

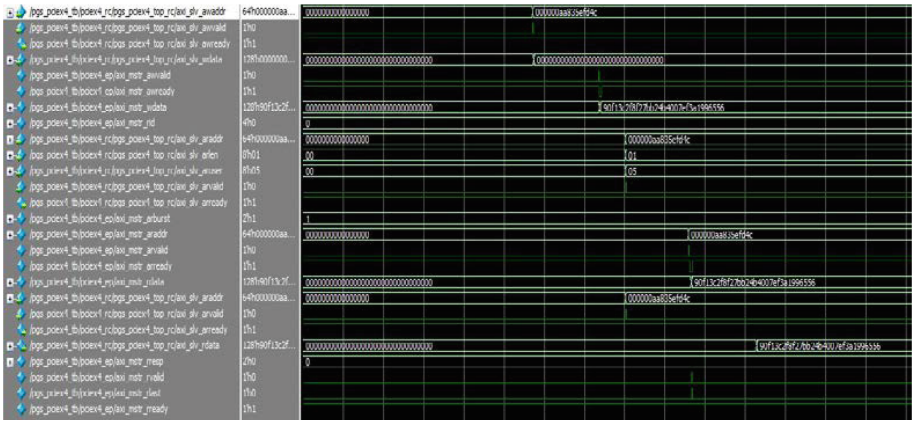


Fig. 12. RC initiates a request to read and write data

The PCIe IP core verified in this paper has been successfully applied in the domestic nuclear power DCS products to complete the communication between the processor and the peripheral FPGA. The FPGA receives the data transmitted by PCIe and converts it into data of other protocols, such as local bus, to communicate with other devices. The burst length, address and data used by the verification platform are all randomized, which can cover more test scenarios. This verification platform tests the completion rate, read-write configuration space register, read-write memory and other functional items. The verification work is expected to be completed in 3 months. Using this method, the simulation test time is saved by about 30% and the verification efficiency is improved.

5 Conclusions

This paper introduces the verification method based on programmable logic PCIe IP, using the verification IP to simulate the interface timing of PCIe to connect with the DUT under test, and inject data through the AXI protocol of another port of the verification IP. This method is an efficient method for complex IP verification, and the verification method can be applied to the verification of other similar interfaces. This method has

been applied to nuclear power instrumentation and control products, and the verification results show that using the UVM verification platform to verify the PCIe IP core can effectively improve the verification efficiency and shorten the verification time.

References

1. Juan, P.H.: Simulation verification of FPGA logic based on PCIe IP core. J. Inf. Commun. **4**(2020), 81–83
2. Titan Series PCIe x4 IP User Guide (UG_IP_Sys_00d, Version 1.0). Shenzhen pango Microsystems Co.,Ltd., China (2016)
3. Xu, Y., et al. (ed): Nuclear Power Plants: Innovative Technologies for instrumentation and Control Systems, vol. 507, pp.17–27. LNEE, Berlin (2019)
4. Yao, A.H., Sun, M.Z., Zhang, Z.J., Yuan, L.N.: Assertion-based functional verification for compact PCI IP core. J. Chin. Comput. Syst. **35**(3), 676–678 (2014)
5. Liu, H.T., Zhou, Y., Dai, Z.B., et al.: Design of coverage-guiding and reusable verification platform for PCIe. J. Comput. Eng. Des. **37**(6), 1675–1695 (2016)
6. Zhou, Q., Xuan, X.L., He, G.H., et al.: Design and verification of PCIE interface for FPGA. J. Microelectr. Comput. **36**(7), 17–21 (2019)

Determination of the Inputting Data Length for the Diagnosis of the Operation Trend Based on Wavelet Analysis

Wen-Ji Zhang, Shu-Qiao Zhou(✉), Duo Li, and Xiao-Jin Huang

Collaborative Innovation Center of Advanced Nuclear Energy Technology, Key Laboratory of Advanced Reactor Engineering and Safety of Ministry of Education, Institute of Nuclear and New Energy Technology of Tsinghua University, Beijing 100084, China
zhousq@tsinghua.edu.cn

Abstract. The trend features, which are named trend symptoms later, of the operation conditions of critical equipment in a nuclear power plant can reflect its operation conditions, especially the potential failures. The trend features can be acquired based on the related physical quantities, such as temperatures, pressures, and flows, measured by sensors. When judging the trend symptoms of the operation and equipment, it is often necessary to select a suitable inputting data length. This paper proposes a method to determine the inputting data length based on wavelet analysis. The equipment history data are filtered by wavelet analysis to remove the noise and burr, then the smooth data curve after filtering will be segmented by a time series segmentation method based on local maximum and minimum, and the analysis results are obtained by linear fitting of the data within each segment. Then, the shortest segment of the segmentation results is conservatively selected as the reference value for the inputting data length of the corresponding equipment. The effectiveness of the proposed method is demonstrated by testing with several pieces of equipment history data. The results show that the proposed method can improve real-time performance while ensuring the accuracy of determining the symptom of equipment operation data.

Keywords: Input data length · Trend diagnosis · Wavelet denoising · Extreme point

1 Introduction

Nuclear power plant is a complex facility with high safety requirements. The traditional nuclear power plant alarm is often realized by setting appropriate thresholds for different equipment measuring points. Once the physical quantity of the measuring point exceeds or falls below a specific threshold, it is considered that the current equipment is abnormal and needs further attention and verification by the operator. However, when this threshold alarm occurs, it generally means that the abnormality of the equipment has occurred for some time. Diagnosing the operation trend of the current equipment through the algorithm can advance the alarm time and further improve the operation safety of the nuclear power plant. Therefore, the diagnosis of equipment operation trends in a nuclear power plant can be used for equipment fault prediction.

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 302–309, 2023.
https://doi.org/10.1007/978-981-99-3455-3_30

In previous research, fault detection and diagnosis (FDD) are widely used in industry [1, 2]. In the field of the nuclear industry, the model-based method and data-based method are the two main methods in FDD [4]. The model-based method is generally used in application scenarios with a clear mechanism and mature model. Data-based methods are generally used in scenes with complex mechanisms or unable to model, and relevant conclusions are directly summarized from the data. According to the types of data and how the data are processed, the FDD methods are classified into three categories: model-based online data-driven methods, signal-based methods, and knowledge-based history data-driven methods [3]. He, Q. P., et al. (2005) used PCA and clustering method to diagnose the fault of data, the input data length of the 2000s is selected [2]. Ding, S. X. (2014) [5] studied fault analysis using partial least squares regression with 48h input data length. Jia, Lei, et al.(2016) use a deep neural network to train on the fault data set of rotating machinery, in which each fault data contains 2400 data points [6]. In these studies, some of the input data lengths are limited by the data set, some are to meet the needs of the corresponding algorithm, and some are determined by experience.

However, in the process of diagnosing the equipment operation trend, the different lengths of the selected input data will directly affect the judgment results. The too-large length will reduce the timeliness of the judgment of the algorithm, while the too-short length will reduce the accuracy of the algorithm. Therefore, this paper designs and implements the input data length determination method of operation trend judgment based on wavelet analysis, which can give the reference value of the input data length (Fig. 1).

2 Determination of Input Data Length for Operation Trend Diagnoses

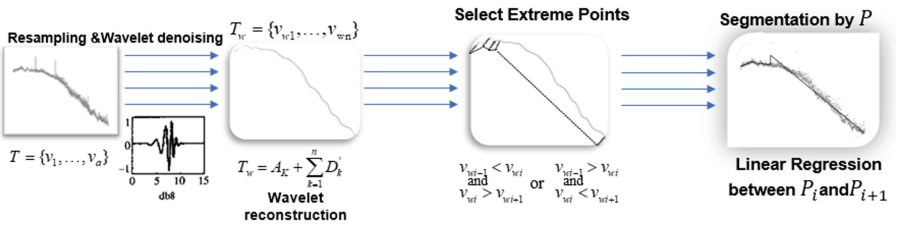


Fig. 1. Input Data Length Determination Framework

2.1 Resampling

In general, for the data detected by the sensor, to save storage space, only the physical quantity corresponding to the change time will be retained. Therefore, it can be considered that the data not recorded in the sensor is consistent with the data recorded at the previous time. For the original data with uneven time intervals, resampling shall be carried out first.

It is assumed that the original timeseries of the history data is $T = \{v_1, \ldots, v_a\}$ which contains with a data points. If x is the time interval:

$$N = \frac{|t_{i+1} - t_i|}{x} \tag{1}$$

where t_i is the time point of data value v_i. Then N same data points as v_i are filled in between t_i and t_{i+1} The timeseries after resampling is recorded as $T_R = \{v_{R1}, \ldots, v_{Rn}\}$.

2.2 Wavelet Denoising

Fourier transform and wavelet transform are often used to analyze the state of equipment with frequent changes, such as mechanical seal leakage [7, 8] or the main pump of the nuclear power plant [9, 10]. These kinds of equipment are often accompanied by strong vibration. However, for the equipment to run relatively smoothly, wavelet denoising is also a good method to remove industrial noise. Whether it is used for analysis or denoising, wavelet packet decomposition is needed at the beginning. The diagram of data decomposition using wavelet in this paper is as follows:

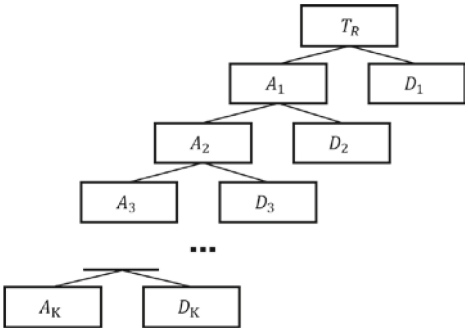


Fig. 2. Wavelet Data Decomposition

In this research, the mother wavelet function is chosen as Daubechies 8 (db8), because the data related to the pressure measuring points analyzed in the experimental process in this paper have a good performance when using that wavelet function[11, 12]. The mother wavelet function can be flexibly adjusted according to the situation (Fig. 2).

As for T_R, the data decomposition process is as follows:

$$\begin{cases} T_R = A_1 + D_1 \\ A_{k-1} = A_k + D_k \end{cases} \tag{2}$$

where A is the low-frequency component and D is the high-frequency component. According to the different mother wavelet functions, a total of K times of decomposition will be carried out, and the data decomposition after the first layer only carries out the decomposition of low-frequency components A.

Set threshold Y in denoising, for all high-frequency components D:

$$D_k^{'} = D_k - Y(1 \le k \le K) \tag{3}$$

where $D_k^{'}$ is the high-frequency component after denoising. Therefore, the data reconstruction is as follows:

$$T_w = A_K + \sum_{k=1}^{n} D_k^{'} \tag{4}$$

where $T_w = \{v_{w1}, \ldots, v_{\mathrm{wn}}\}$ are the data after wavelet denoising.

2.3 Segmentation

The data after denoised preserves the original trend features and usually includes multi-stage rise and fall. Therefore, it is necessary to separate different trend features in historical data.

In this paper, extreme points are used for data segmentation. The main idea of selecting extreme points is that if $\exists v_{wi} \in T_w$,then if it has $v_{wi-1} < v_{wi}$ and $v_{wi} > v_{wi+1}$ or $v_{wi-1} > v_{wi}$ and $v_{wi} < v_{wi+1}$(Extreme point condition),the data value point v_{wi} is a extreme point.

Algorithm 1 Steps for data segmentation

1: t_{wi} goes into sequence P
2: **while** $w_i \le w_n$:
3: **if** t_{wi} satisfies the extreme point condition **then**
4: t_{wi} goes into sequence P
5: **end if**
6: t_{wn} goes into sequence P
7: **end while**
8: **for** $P_i = P_1 : P_n$ **do**
9: Linear fitting v_{wi} between P_i to P_{i+1}
10: Record the slopes S_i and the time intervals L_i of each segment
11: **end for**

The linear fitting method uses the linear expression algorithm package from Sklearn in the Python environment.

2.4 Input Data Length Determination

Assuming that the selected data for determining the length of input data is long enough to include a feature period in its operation, the shortest independent trend segment will be conservatively selected as a reasonable reference value for the length of input data.

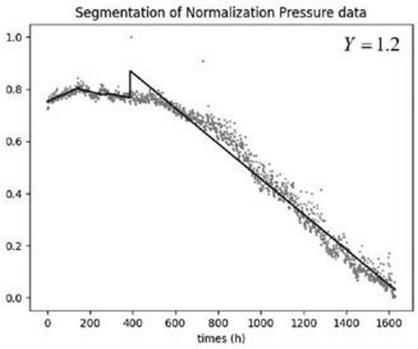


Fig. 3. Input Data Length Analysis Results of Normalized Pressure Data

As shown in Fig. 3, there are several trend features before the pressure begins to decline continuously, and when these feature segments are considered to be part of the anomaly, their time is much smaller than the last feature segment of continuous decline. Therefore, when the shortest time interval among these segments is selected (five days in the result of Fig. 3), the occurrence of anomalies can be diagnosed in a faster time, and these feature segments with shorter lengths will not be misjudged.

3 Experimental Investigation

The minimum time interval for original data is seconds and the time interval selected for resampling is one hour. To promote the experiment, the artificially generated data are used in the test process. The artificial data used in the denoising experiment is the data of adding different levels of white noise with the quintic function as the main body. At the same time, the sine wave with white noise is generated in the data segmentation experiment. The real data used in the experiment is the pressure measuring point data after normalization.

3.1 Wavelet Denoising Performance

The effect of wavelet denoising becomes better with the increase of threshold Y, but there is an upper limit so that the denoised data sequence will not change after the threshold Y continues to increase. When the result of noise reduction processing is unchanged, it means that all separated high-frequency separation is filtered out (Fig. 4).

Wavelet denoising performs best when the noise level is 5, while the real data generally does not fluctuate as the generated data with the noise level of 15, because such a large range of noise reflects the possible faults of the sensor. The real data is similar to the generated data with the noise level of 5, but there are some peaks once in a while which leads to a slight increase in the threshold Y. On the other hand, the peak value deviates greatly from the normal data value, it can also be removed by filtering at first.

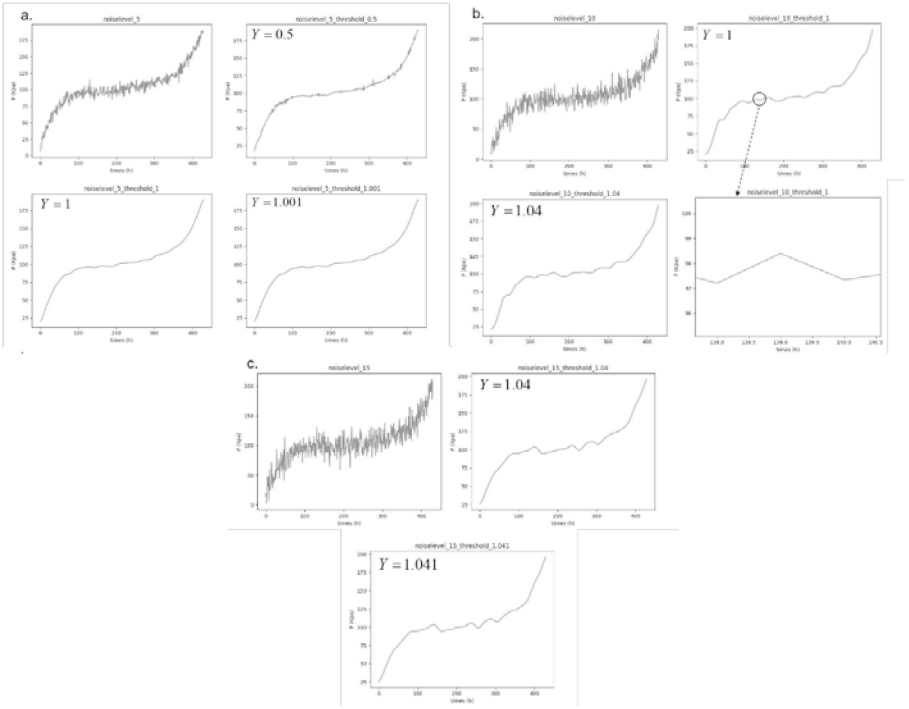


Fig. 4. Wavelet Denoising Performance in Difference Noise Level. The White Noise Levels in a, b and c are 5, 10, and 15.

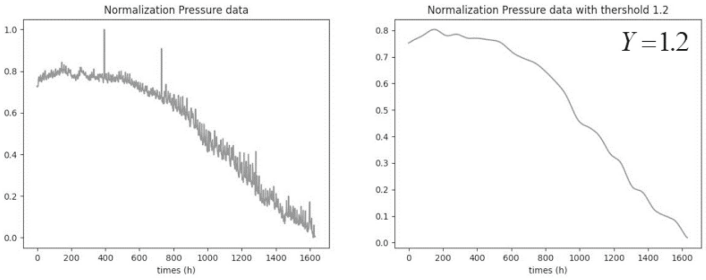


Fig. 5. Wavelet Denoising of Normalized Pressure Data

3.2 Segmentation Performance

The generated sine wave with added noise is taken as the test object of data segmentation, and the segmentation performance divides the rise and fall of the sine wave each time. For the data segmentation in Fig. 5, the results are shown in Fig. 3.

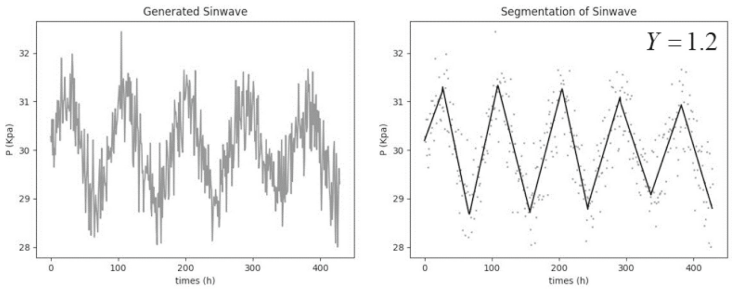


Fig. 6. Segmentation of Generated Sin wave Data

4 Conclusion

In this research, a method was proposed to determine the input data length of operation trend diagnosis based on wavelet analysis, which is committed to solving the problem that it can not be considering both the timeliness and accuracy of diagnosis results due to the uncertain input data length in the operation trend diagnosis of nuclear power equipment. Firstly, after resampling the original data, wavelet denoising is carried out to obtain a smooth filter curve. Then, the maximum and minimum points in the equipment operation curve are found. After that, segmentation and linear fitting are carried out according to these points. Finally, the part with the shortest time interval in the segmentation result is conservatively selected as the reference value of the input data length of the current measuring point of the equipment (Fig. 6).

References

1. Chiang, L.H., Russell, E.L., Braatz, R.D.: Fault Detection and Diagnosis in Industrial Systems. Springer, Berlin (2002)
2. He, Q.P., Qin, S.J., Wang, J.: A new fault diagnosis method using fault directions in fisher discriminant analysis. AIChE J. **51**(2), 555–571 (2005)
3. Dai, X., Gao, Z.: From model, signal to knowledge: a data-driven perspective of fault detection and diagnosis. IEEE Trans. Industr. Inf. **9**(4), 2226–2238 (2013)
4. Ma, J., Jiang, J.: Applications of fault detection and diagnosis methods in nuclear power plants: a review. Prog. Nucl. Energy **53**(3), 255–266 (2011)
5. Ding, S.X.: Application of partial least squares regression to fault diagnosis. In: Ding, S.X. (ed.) Data-driven Design of Fault Diagnosis and Fault-tolerant Control Systems. AIC, pp. 95–116. Springer, London (2014). https://doi.org/10.1007/978-1-4471-6410-4_6
6. Jia, F., Lei, Y., Lin, J., et al.: Deep neural networks: a promising tool for fault characteristic mining and intelligent diagnosis of rotating machinery with massive data. Mech. Syst. Signal Process. **72**, 303–315 (2016)
7. Jin, Y., Shan, C., Wu, Y., et al.: Fault diagnosis of hydraulic seal wear and internal leakage using wavelets and wavelet neural network. IEEE Trans. Instrum. Meas. **68**(4), 1026–1034 (2018)
8. Lin, G.B., Fu, P., Zhang, E.Q., et al.: A new classifying method for mechanical seal condition based on acoustic emission and wavelet neural network. Lubr. Eng. **000**(009), 40-45 (2014)

9. Gu, J., He, P., Liu, C.X.: On -line vibration monitoring system of nuclear reactor main pump based on PXI. Nucl. Electr. Detect. Technol. **33**(12), 1498–1501 (2013)
10. Shu, X.T., Yang, Z., Xu, Y.Z., et al.: Fault diagnosis of vibration induced by fluid of 100D main pump for CPR1000 unit. Nucl. Power Eng. **42**(3), 5 (2021)
11. Zhao, X., Zhang, S., Zhou, C., et al.: Experimental study of hydraulic cylinder leakage and fault feature extraction based on wavelet packet analysis. Comput. Fluids **106**, 33–40 (2014)
12. Goharrizi, A.Y., Sepehri, N.: Application of fast fourier and wavelet transforms towards actuator leakage diagnosis: a comparative study. Int. J. Fluid Power **14**(2), 39–51 (2013)

Research on Defence-in-Depth of Nuclear Power Plant DCS Based on Swiss Cheese Model

Yingjie Lin(✉), Xudong Liu, Yanxiong Yang, Hongtao Sun, and Dandan Zhang

China Techenergy Co., Ltd., Beijing 100094, China
1048951681@qq.com

Abstract. After the Fukushima nuclear accident, the design concept of Defence-in-Depth of the nuclear power plant has further developed, and the safety requirements for level setting of Defence-in-Depth and for independence of inter-level have further improved. In order to ensure current Defence-in-Depth analysis always meets the latest international nuclear safety requirements, this paper analyzes the Defence-in-Depth level of DCS of nuclear power plant based on Swiss Cheese Model, and make a comparison with the Defence-in-Depth analysis schemes before and after a domestic project improvement, and proposes a Defence-in-Depth level-setting method on the premise of meeting the regulatory standards, which provides a valuable reference for the continuous improvement of the digital I&C system design of third generation of nuclear power reactor.

Keyword: Defence-in-Depth · Swiss Cheese Model · Independence

1 Introduction

Since the 21st century, the digital Distributed Control System (DCS) in the nuclear power plant has gradually replaced traditional analog system to ensure the safety and steady operation of plant. Nuclear safety is the first consideration, and the concept of Defence-in-Depth forms a significant constituent of nuclear safety. Defence-in-Depth is widely used in all activities related to safety to ensure these activities are under the multi-level protection logic.

Especially after the Fukushima nuclear accident, the design concept of Defence-in-Depth for nuclear power plant has been further developed at home and abroad, and higher technical requirements has been raised on the independence and other aspects of Defence-in-Depth. Take HAF102 as an example of domestic regulations and requirements, for the I&C system of nuclear power plant, the design of Defence-in-Depth has 2 meanings: first, as a support system, I&C should provide monitoring and control means for the process systems at all levels of Defence-in-Depth of the nuclear power plant; second, I&C system should also meet the requirements of Defence-in-Depth design concept to ensure that the failure of one level can be compensated by the next level. This paper firstly summarizes the design requirement of Defence-in-Depth of I&C system at home and abroad, and introduces the design and practice of Defence-in-Depth of the I&C system of a practical nuclear project combined with Swiss Cheese Model, and gives suggestions on the issues that should be paid attention to in design of Defence-in-Depth of I&C system of nuclear power plant.

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 310–317, 2023.
https://doi.org/10.1007/978-981-99-3455-3_31

2 Regulatory Requirements for Defence-in-depth

2.1 IAEA

The International Atomic Energy Agency (IAEA) issued the safety standard SSR 2-1 in 2016, which summarizes the lessons of the Fukushima nuclear accident and raises higher requirements on the independence of Defence-in-Depth levels. Chinese HAF102 has largely referred to this standard. At the same year, IAEA published the technical document IAEA-TECDOC-1791, which further interpreted the SSR 2-1 standard and provided guidance for practical application. SSG-39 is the lower level standard of SSR 2-1 in the field of I&C design. It provides guidance on how to meet the Defence-in-Depth requirements of nuclear power plant and I&C system in the overall structure design of I&C system. It is stated that the overall structure design of I&C shall not affect the overall Defence-in-Depth concept and diversity strategy of the power plant. The overall structure design of I&C shall define the Defence-in-Depth concept and diversity strategy of the I&C system (Table 1).

2.2 WENRA

RHWG, a subsidiary of WENRA, released a technical report SNND in 2013, which clarified the technical insights of Western European nuclear power regulators on key safety issues of nuclear power plants, including Defence-in-Depth design methods, independence between Defence-in-Depth levels, and multiple failure response measures for new nuclear power plants (Table 2).

2.3 NRC

According to the branch technical requirements BTP 7–19 in NUREG 0800, NRC standard review plan for nuclear power plant safety analysis report discusses the requirements and response measures to be followed by the digital I&C system of nuclear power plant on Defence-in-Depth and diversification. BTP 7–19 is the guidance document for NRC to review the Defence-in-Depth and diversity of the I&C system of nuclear power plants. In BTP 7–19, the Defence-in-Depth level of I& C system is referred to the definition of Defence-in-Depth level of nuclear power protection system in NUREG/CR 6303 (Table 3).

It's obvious that NRC classification of the Defence-in-Depth level of the I&C system is simpler. The four levels are classified into the disassembling and further deepening of the logic of the I&C system, without considering the melting of the DBC and DEC cores. This inspires our defence logic on the DCS side.

By reviewing the above IAEA\WENRA\NRC Defence-in-Depth principles and technical requirements for the whole power plant and I&C, we can get two ways of Defence-in-Depth for current situation:

a) Take Defence-in-Depth as the overall requirement of nuclear power plant, then sort out and refine the defence level according to the design conditions. Or
b) Sort out the Defence-in-Depth level from the control logic based on the design of I&C system.

Table 1. IAEA's DiD

	Overall Defence-in-Depth level of power plant	Defence-in-Depth level of I&C system
Level1	Prevent deviation from normal operation and failure of safety significant item	Operate power plant under normal operation mode, and keep the main parameters of power plant within specification
Level2	Monitor and control the deviation of normal operation, and prevent expected operation events from evolving into accidents	The automatic control design basis accident shall not exceed the requirements of acceptance criteria, and the reactor shall be brought into and maintained at safe shutdown state after design basis accident
Level3	The consequences of accidents are limited through engineered safety feature, safety systems, procedures and other measures, to prevent core damage and radioactive release to bring power plant back to safe state	The automatic control design basis accident shall not exceed the acceptance criteria, and the reactor shall be brought into and maintained at safe shutdown state after design basis accident. The backup function used to deal with common cause failure of I&C system and the superimposed condition of expected initial event belongs to Level3b of Defence-in-Depth
Level4	Mitigate the consequences of accidents caused by the failure of the level3 defence, including preventing the evolution of accidents and mitigating the consequences of serious accidents, avoiding or minimizing off-site radioactive pollution, and "practically eliminating" early radioactive leakage or large-scale radioactive leakage	An independent DC power supply is required to monitor and mitigate the core melting accident through an independent system
Level5	The consequence of radioactive release is limited through adequate on-site and off-site emergency response facilities, plans and procedures	None

Table 2. WENRA's DiD

	The overall Defence-in-Depth level of power plant
Level1	Prevent abnormal operation and failures through conservative design, high-quality construction and operation, control of parameters of nuclear power plant
Level2	Control abnormal operation and failure through control and limit system and other monitoring facilities
Level3	3a: Limit the accidents consequences, radioactive release and prevent core melting accident through protection system, safety system and procedures, etc. Single initiating event is in consideration 3b: Limit the accidents consequences, radioactive release and prevent core melting accident through additional safety features and procedures. Multiple initiating event is in consideration
Level4	Mitigate core melt, manage core melt accident and limit off-site release through supplemental safety features
Level5	Mitigate the consequences of large-scale radioactive release through on-site and off-site emergency response and intervention

Table 3. NRC's DiD

	Defence-in-Depth level of I&C system
Level1	Control system: The control system level usually consists of non-safety related equipment and is used for routine nuclear power plant operational control and accident mitigation routine operations
Level2	Reactor shutdown system: The reactor shutdown system level consists of safety-related equipment. In the event of an accident, the reactivity in the reactor is quickly reduced and the reactor can be emergency shutdown
Level3	Engineered safety facility: The engineered safety facility level is composed of safety-related equipment. In the event of an accident, heat in the reactor is discharged by driving the safety related equipment, and the integrity of the three physical boundaries (fuel cladding, pressure vessel, primary circuit cooling system and containment) that prevent radioactive release is protected and maintained. The engineered safety facility level usually refers to the engineered safety facility driving system;
Level4	The monitoring and indication system level is composed of sensors, safety parameter display, data communication system and independent manual control (for the operator's response to the operation time of the nuclear power plant)
Level5	None

3 Swiss Cheese Model

Swiss Cheese Model is an accident causation model proposed by James Reason, a professor of psychiatry at the University of Manchester in the United Kingdom. From the perspective of organizational management, he has carried out research on the mechanism of accident causation. From his opinion, accidents are usually not caused by isolated factors, but a series of loopholes or defects in the system, which are caused by the failure and the superposition of risk defence. Defencive failures are divided into latent failures and evident failures. Latent failures include 3 factors, organizational factors, unsafe supervision, and precursor of unsafe acts. Evident failures mainly refer to unsafe acts. Based on this concept, Reason proposed an accident causation model. The far left of the model is the danger (hazard source) that may lead to an accident. The various measures taken to prevent accidents are called defences, and the holes in each defence layer refer to loopholes or defects in risk management and control. The position and size of these holes will change. When the holes in each defence layer are arranged in a straight line (occurring at the same time), the loopholes or defects in the defence system form "opportunistic accident ballistics", danger will pass through this "ballistic" and cause an accident. Swiss cheese has large and small holes due to the addition of Propionibacterium that can produce pores in the production process. In the accident causation model proposed by Reason, the defence model with holes in each layer is similar to Swiss cheese, so this accident causation model is called Swiss Cheese Model, as shown in Fig. 1 below.

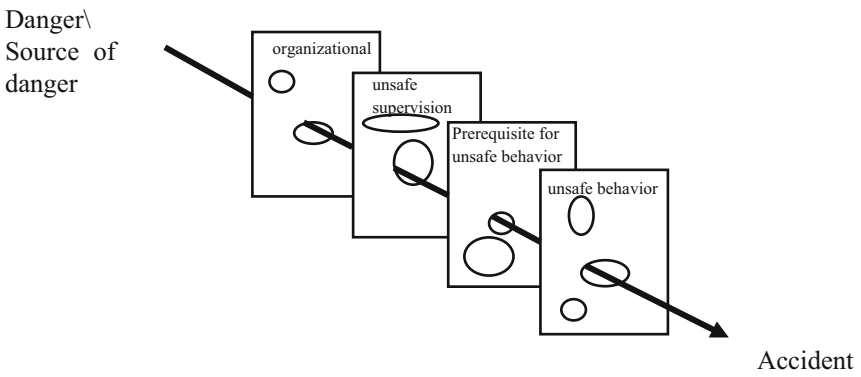


Fig. 1. Swiss cheese model

The Swiss Cheese accident causation model can also be used in the nuclear power DCS Defence-in-Depth analysis, and the design of each defence layer can be fully considered, thus to improve the rationality of each level of Defence-in-Depth.

Several layering principles of Swiss Cheese Model are summarized: 1. The next layer of cheese can block the holes of this layer of cheese. 2. To form intolerable accidents from hazard sources and dangerous events, it is necessary to break through all levels of cheese and form opportunistic accident ballistics. 3. There should be a level of protection

against certain specific issues. 4. In order to ensure the effectiveness of each layer setting, each layer of cheese should have sufficient independence.

4 Model Application

4.1 Defence-in-Depth Analysis of a Domestic Project

The I&C system of a project adopts digital DCS platform, F-SC1 adopts FirmSys platform, and F-SC3 adopts SH_N platform, the diversity protection system adopts FitRel platform. Referring to the previous project experience, and according to the design requirements of HAF102 for Defence-in-Depth, functions of the I&C system side at each stage are divided into five levels, from bottom to top they are - level 1: reactor control function; Level 2: emergency shutdown function; Level 3: engineered safety facilities; Level 4: serious accident control; Level 5: emergency response of the whole power plant, as shown in the following table. This level can reflect the operation of the process system and I&C after the accident, but it can not demonstrate function description, independence and diversity between levels (Table 4).

Table 4. Defence-in-Depth analysis of a domestic project

DiD	Function description	F-SC3 DCS	Reactor protection system (RPS)	Diversity drive system (DAS)	Serious accident system (SA I&C)
1	Reactor control function	√			
2	Emergency reactor trip function		√	√	
3	Engineered safety facilities		√	√	
4	Serious accident control				√
5	Emergency response of the whole power plant	-	-	-	-

4.2 Optimized Defence-In-Depth Analysis

According to the above summarized principles, the Defence-in-Depth analysis of a domestic project in Chapter 4 is optimized. Considering that each layer of cheese needs to play a role in this layer,

The first layer is composed of F-SC3 systems as the prevention layer, which is mainly used to prevent further evolution of events. LEVEL2 is composed of KIC and ACP-VDU;

The second layer is composed of RPS and SAS system as the main defence layer, which is mainly used to bring the reactor back to the safe state. LEVEL2 is composed of SCID and ECP;

The third layer is composed of KDS system as the diversity defence layer, and LEVEL2 is composed of DHP, aims to prevent the common cause failure of the second main defence layer. Therefore, it is set up for a specific issue. Other opportunistic accident ballistics cannot be effectively blocked at this level;

The fourth layer is the serious accident prevention layer, which aims to reduce the accident consequences caused by the failure of the second layer, and realize the fourth layer defence by controlling the accident progress and reducing the consequences of the serious accident. The fourth layer is composed of KDA and LEVEL2 is composed of DCP (Fig. 2).

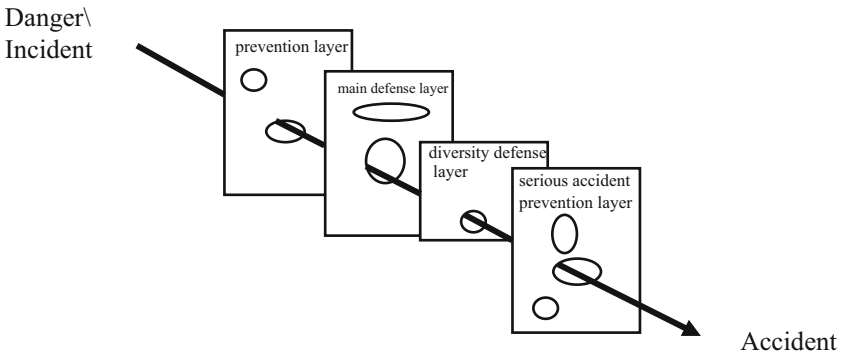


Fig. 2. Optimized Defence-in-Depth analysis

5 Conclusion

The application of digital control system in the industrial control system is very mature. If nuclear power DCS is only used to realize control function, it is not different from other industrial public service systems. However, if the special requirements of nuclear industry for its safety and other aspects are considered, the requirements of Defence-in-Depth will be derived. If independence and diversity are considered everywhere in the design of nuclear power DCS, high cost is required. Therefore, a reasonable Defence-in-Depth analysis can meet both safety and availability to a certain extent. This is an important factor to measure whether the design scheme is mature and can be widely used.

In order to ensure the effectiveness of the four Defence-in-Depth levels, the levels divided by the improved Defence-in-Depth analysis compared with the initial scheme not

only illustrate the main functions of each defence level, but also reflect the overall process of the on-site events evolving into serious accidents. The Defence-in-Depth analysis based on the Swiss Cheese Model can further clarify the criteria of independence and diversity among various I&C systems. This paper provides a layered Defence-in-Depth method, which can meet the requirements of nuclear power plant safety better.

References

1. Reason, J.: A system approach to organization error. Ergonomics **38**(8), 1708–1721 (1995)
2. Branch Technical Position (BTP) 7–19, Guidance on Evaluation of Defence-in-Depth and Diversity in Digital Computer - Based Instrumentation and Control Systems, U. S. NRC. July 2012
3. NUREG/CR -6303,Method for Performing Diversity and Defence-in-Depth Analyses of Reactor Protection Systems, U. S. NRC, December 1994
4. Xu, L., Li, Z., Jiang, G.: Study on the diversity and defense-in-depth of EPR I&C architecture. Nucl. Sci. Eng. **32**(S2), 134–138 (2012)
5. Jiang, G., Li, F., Mo, C., Ma, G.: The research and development of self-diagnostic function for NPP I&C system. Nucl. Sci. Eng. **39**(01), 146–154 (2019)
6. Zhou, J., Zhu, P., Xiao, P.: Defense-in-Depth and diversity design of instrumentation and control system in nuclear power plant. Nucl. Power Eng. **35**(1), 122–124 (2014)
7. Vaurio, J.K.: Uncertainties and quantification of common cause failure rates and probabilities for system analyses. Reliab. Eng. Syst. Saf. **90**(2–3), 186–195 (2005)
8. Long, M., Luo, S., Yan, X.: Application of Swiss cheese model in fall prevention management for elderly patients. Chin. Nurs. Res. **32**(7), 1053–1056 (2018)

Application Development and Research of 3D Parametric Intelligent Design System for Double Sheathed Liner Sumps

Zi-Shen Huang(✉), Shi-Lei Li, Dong Zhao, and Xiao-Dong Jing

State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment, China Nuclear Power Engineering Co., Ltd., Shenzhen 518172, Guangdong, China
6005688@qq.com

Abstract. The parametric design method is applicable to the series, generalization and standardization of nuclear power major equipment, that can helps to improve the modeling efficiency in the 3D model modeling stage. The Double Sheathed Liner Sumps in the nuclear power plant, it's has the above structural characteristics. This paper proposes the method and technology of parametric design, to carry out parametric analysis and Research on the dimension and assembly relationship of Double Sheathed Liner Sumps. Through the development technology based on C software, the purpose of parametric design for the 3D model of Double Sheathed Liner Sumps is realized. The application of this system tool, it's can improves the efficiency of 3D design of Double Sheathed Liner Sumps, the 3D model generated by this system, can meet the standardization requirements of the design criteria in the design process, and effectively reduce the manual errors. Therefore, the parametric design concept and research results can be applied to other similar nuclear power equipment.

Keywords: Parameterization · 3D design · Double Sheathed Liner Sumps

1 Introduction

The Double Sheathed liner Sumps has high safety performance, so it has been widely used in the nuclear power plant. The main reason for adopting 3D model as design means is that, with the development of technology, CAD design software is widely used in China when design nuclear power equipment. The data of 3D model can be widely used, such as mechanical calculation, output of engineering drawings and data sharing. Therefore, the requirements of data application on 3D models are also constantly improving, such as unified standardized management model, efficient modeling and 3D model utilization. According to the investigation, in the process of creating the 3D model of Double Sheathed Liner Sumps, the engineers mainly rely on the pure manual modeling method, such like "building blocks" to create the 3D model of the equipment. Basically,

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 318–331, 2023.
https://doi.org/10.1007/978-981-99-3455-3_32

to create 3D model of each Double Sheathed liner Sumps, it needs to be built from purely manual. The main problems of this method are as follows.

1) Low work efficiency.

Purely manual takes a long time, is prone to manual errors, repeats many assembly steps, and is inconvenient to modify later.

2) No unified standardization has been formed.

Since each model is built by the different engineers, there is no unified standardized model between the models, which is inconvenient for the standardized management in the design process. The model data was not reasonably utilized. For the 3D model that is not parameterized, the dimensions in the model data, their relationships, and constraints are "lonely data islands", which is not conducive to the subsequent management and reference of the data in the information design.

3) Lack of competitiveness of the industry.

The Double Sheathed Liner Sumps is the major equipment in nuclear power plants. If the 3D modeling link affects the design efficiency and design quality in the design process, the project cost will increase, which is not conducive to competition in the same industry.

4) Model standardization.

The 3D model of Double Sheathed Liner Sumps has never formed a standardized series of template models. The Leak Detection Pipe, Leak Detection Groove, Channel Steel and other components used in the assembly are all created by engineers in different ways. Therefore, the 3D model can't reach a unified standard in standardization and quality assurance, and lacks effective management.

5) Parameterization of model.

The parameterization [1] of 3D model is a decisive factor for the rapid and effective design of 3D model. Since the 3D model of Double Sheathed Liner Sumps has never been standardized, its 3D model is not a parametric model, and the size, correlation and assembly relationship of the model are not defined. Therefore, the design software can't rely on the parameter driven to realize the modeling of the 3D model, which is the core of the technical problem to be solved this time.

6) Repetitive modeling problems.

In the 3D modeling of Double Sheathed Liner Sumps, there are a lot of repetitive works, such as Channel Steel assembly. For example, the assembly process of reinforcement is one of the main reasons for the low efficiency of 3D model modeling. To sum up, the design process of the 3D model of Double Sheathed Liner Sumps needs an effective 3D design system tool to improve the above problems and improve the design efficiency.

2 Main Technical Scheme

Through investigation, most of the existing 3D models of Double Sheathed Liner Sumps are created using C software. Therefore, this paper takes C software as the core to explore and study its related technologies.

2.1 Toolkit Technology

Toolkit [2] is a secondary development tool provided by C software and is the application system program interface of the software. Toolkit encapsulates many library functions and header files called for the underlying resources of C software in the background, so that external application programs can access their databases and application programs safely and effectively. Developers can form seamless integration of application system programs and software function modules through C programming, so that users or third parties can add and use the system programs developed to meet the requirements in C software system.

Toolkit includes two development modes: synchronous mode and asynchronous mode. The synchronization mode is divided into spawn (multi process mode) and d11 (dynamic link library mode). The dynamic link library can easily integrate the developed system program into the C software function module. Moreover, in the dynamic link library mode, the information interaction between toolkit application and C software is realized through direct function call, which has the characteristics of high development flexibility and relatively complete functions. Therefore, the secondary development of C software in this paper is mainly based on dynamic link library mode.

The use of asynchronous development mode is complex and rarely used in practice, which does not meet the requirements of this system development.

2.2 Model Parameterization

The 3D parametric model is the core foundation of the development of this application system. It needs to have a strict hierarchical relationship, and the setting of parameters should be based on the condition that the minimum number and all deformation requirements are met. Focusing on the preconditions of the 3D parametric model and aiming at “rapid design” and “optimal design”, the specific technologies and methods are described below.

Top-Down design. In the assembly function of C software, “Top-Down design” [3] is a method of transferring the design specifications to all relevant components through the top-level structure, controlling the deformation of the overall structure of the model due to size change in the whole design, effectively managing the assembly reference, and strictly restricting the overall model, It can improve the accuracy of 3D design model assembly and effectively reduce the fatal error of model collapse after deformation. The Top-Down design method is to create a top-level skeleton at the top of the model tree area of the model component file, and then form a hierarchical assembly under the inheritance of the top-level skeleton. The assembly of each layer takes the skeleton as a closed reference to expand more detailed assembly, such as the assembly of parts. The skeleton and assembly hierarchy are shown in Fig. 1.

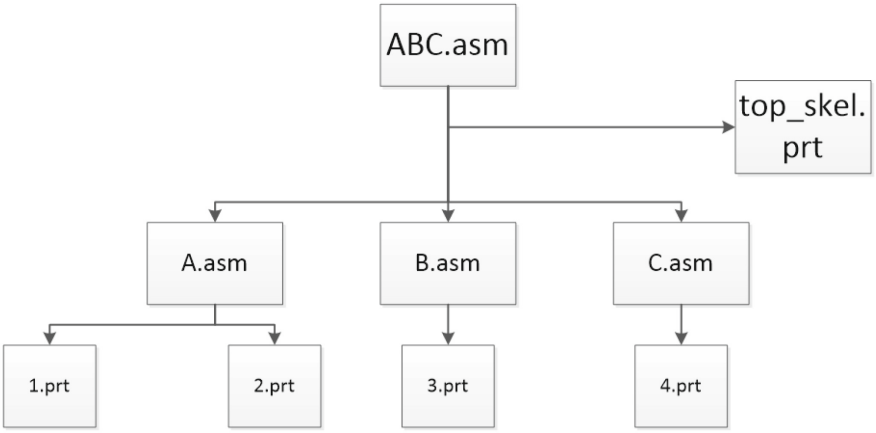


Fig. 1. Top-Down design

2.3 Sorting Out the Relationship Between Model Size and Parameters [4]

Carding of Model Size. The size sorting is the basis for parameterization of the 3D model. Through the structural analysis and research of the steel cover of Double Sheathed Liner Sumps, it is mainly composed of seven parts, including the Longitudinal Channel, the Channel Support, the Transversal Channel, the Channel Anchor Reinforcement, the pump Embedded Parts, the Leak Detection Groove and the Leak Detection Pipe. Based on the analysis and statistics of the four most representative Double Sheathed Liner Sumps in the project, it is known that, the steel cladding dimensions of different sizes of Double Sheathed Liner Sumps are mainly different in the positioning of Channel, Leak Detection Pipes and Embedded Parts. Therefore, the parameters are set in these three types of components. The specific analysis dimensions are listed in Table 1.

Table 1. The parameters of Double Sheathed Liner Sumps

Type	Channel					Tank		Embedded parts			
	Length -A	Width -B	Height -C	Height -D	Flat -Y	Deviation -Y1	Deviation -Y2	Distance -X3	Distance -Y3	Distance -X4	Distance -Y4
Type1	2500	1650	2500	2500	886	1046	496	1250	950	1950	950
Type2	2800	2100	3500	3500	1176	1846	1446	950	1450		
Type3	2600	2200	2904	2904	1230	1846	1446	1450	900	1450	1700
Type4	1400	2100	2850	1804	1030	746	1696	1250	700		

Sorting Out the Relationship Between Model Parameters. In C software, a mathematical operation formula is provided to describe the relationship between parameters, mainly through the indirect relationship between parameters to cause changes in other parameter values. The parameters in the software support normal addition (+), subtraction (−), multiplication (*) and division (/) mathematical operations, and can perform

square, square, trigonometric functions and other operations. The syntax rules follow the syntax rules of general program language system for formula calculation, ensuring that the 3D model is saved reasonably and updated in time under the constraint of parameter relations. The styles are listed in Fig. 2.

```
/*==============CHANNEL=========*/
D1:0 = MAIN_CHANG  /*=LENGTH=*/
D2:0 =  MAIN_KUANG /*=WIDTH=*/
D0:0 =  MAIN_GAO /*=HIGH=*/
D11:0 = MAIN_HOUDU /*=THICKNESS=*/

/*================================*/

/*==============CHANNEL=========*/

D40:2 = MAIN_CHANG - MAIN_HOUDU
D39:2 =  MAIN_KUANG - MAIN_HOUDU
D1:2 = D39:2 - 100
D0:2 = D40:2 - 100
D57:2 = MAIN_HOUDU
```

```
/*==========================*/

/*================TANK==========*/
D0:14 = MAIN_CHANG + 100
D0:16 = MAIN_KUANG + 100

P82:14 = FLOOR(D0:14/2/200) + 1
P38:16 = FLOOR(D0:16/2/200) + 1

P491 = WAI_WEI_CAO_GANG_NUM1

/*===============TANK============*/

/*==========================*/
```

Fig. 2. Parameter setting and relationship setting

Through combing and analysis, the parameter correlation of the steel cover of Double Sheathed Liner Sumps mainly includes the following: the length of the Channel; Observe the length of the Pipe and the height of the Channel; Location of Leak Detection Groove and Process Hole; Positioning of Leak Detection Pipes and Observation Pipes. In terms of quantity, the quantity relationship between Channel Steel and other parts is the main one. Through research and analysis, the main relationships are listed in Table 2.

Automatic Generation of Feature UDF User Defined Feature Technology. User defined feature (UDF) is a user-defined feature function provided in C software [5, 6]. It is usually used to combine one or several general features into a whole feature group and save them as user-defined feature files to provide system calls. It plays a role in generating specific features and rapid assembly. Generally, the UDF feature group contains the pre-defined features and the reference relationship between their relevant dimensions and the selected features. According to the structural characteristics of Double Sheathed Liner Sumps, its characteristics are defined as such common standard components as openings, Leak Detection Pipe, Leak Detection Grooves and Channel Steel, and can be used as a unified standard library. The reference relationship between its size and assembly is defined in the data of UDF files. The use of this technology is the basis for realizing automatic generation of features and automatic assembly. The workflow of UDF is shown in Fig. 3.

Table 2. Main relationships of Double Sheathed Liner Sumps

Name of part	Dimensionrel	Assemrel	Amount
Walls stainless steel anchor plate	The length is related to surface A/B of the longitudinal channel	The bottom edge is coincided with the fixed edge of the longitudinal channel	4
Walls steel anchor plate	The length is related to surface A/B of the longitudinal channel	The top is 10mm higher than the edge wrapped angle steel bottom	4
Walls	Unchanged	At the 4 corners of angel steel	4
Ceiling	Unchanged	At the 4 corners of angel steel	4
Leak detection system	The length is 120mm longer than the long axis of the corresponding hole	Top of transversal channel 20mm	Same as holes total
Transversal channel steel at the low	Length = A \ B (length \ width of transversal channel), fixed value of cross-sectional dimension	The bottom of the steel is 100mm away from the longitudinal channel, and the bottom of the top steel is flush with the longitudinal channel. Uniformly distributed, n in total	C/500 ≤ n ≤ C/400,n is an integer
Transversal channel steel at the bottom	Length = A(transversal channel length) - 140mm, fixed value of cross-sectional dimension	The first one is 200mm away from the edge of the longitudinal channel, and the last one is 200mm away from the edge of the longitudinal channel, totaling n-1	(B-400)/500 ≤ n ≤ (B-400)/400

(*continued*)

Table 2. (*continued*)

Name of part	Dimensionrel	Assemrel	Amount
Leak detection	Length = C + 294mm	The distance between the center and the outer wall of the longitudinal channel is 278mm	1
Observation	Length = C + 294mm	The distance between the center and the outer wall of the longitudinal channel is 278mm	1
Connector	Unchanged	Between leak detection, observation and longitudinal channel	2
Flan & pipe	Unchanged	Top of leak detection and observation	2
Support	Length = 60mm	20mm away from the leak detection and observation	6 or others
Longitudinal channel at the side	Length = C-156mm	The longitudinal side is parallel to the longitudinal channel; The width direction is parallel to the transverse channel	(B-296)/500 ≤ n ≤ (B-296)/400, (B-400)/500 ≤ n ≤ (B-400)/400
Longitudinal channel at the bottom	Length = Y-60mm	The first one is away from the tank of longitudinal channel 148mm and the last one is away from that 148mm. n-1 in total	(B-296)/500 ≤ n ≤ (B-296)/400
Longitudinal channel at slope section	Length = B - Y-60mm	Parallel to the horizontal section the bottom of the longitudinal channel. n-1 in total	(B-296)/500 ≤ n ≤ (B-296)/400

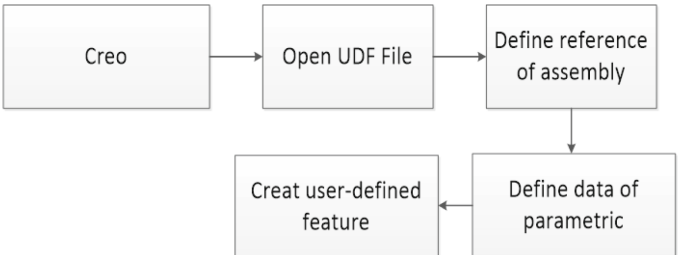


Fig. 3. UDF workflow

2.4 Automatic Assembly Method

The steel rib layout of the Channel of Double Sheathed Liner Sumps has the largest workload in the 3D design. Therefore, in the development process of the system, the automatic reinforcement layout concept of "automation" and "intellectualization" is adopted to realize the automatic generation and assembly of the Anchor Rib Channel Steel of Double Sheathed Liner Sumps. After analyzing the logic of rib placement and the constraint conditions of assembly, the computer language algorithm for the automatic assembly function of the form cost application system is developed. The specific analysis is as follows.

Logic of Reinforcement Arrangement. In the project, the method of "sectional reinforcement distribution" and "empty reinforcement distribution are mainly used for the reinforcement distribution of the outer layer of Double Sheathed Liner Sumps. This method is used to formulate rules to ensure that the Anchor Rib Channel Steel does not interfere with the process holes on the Channel. The application system analyzes and obtains the required total number of Channel Steel sections and the specific size and relative positioning data set of each section

of Channel Steel through the algorithm. The analysis rules and logic adopted by the algorithm are shown in Fig. 4.

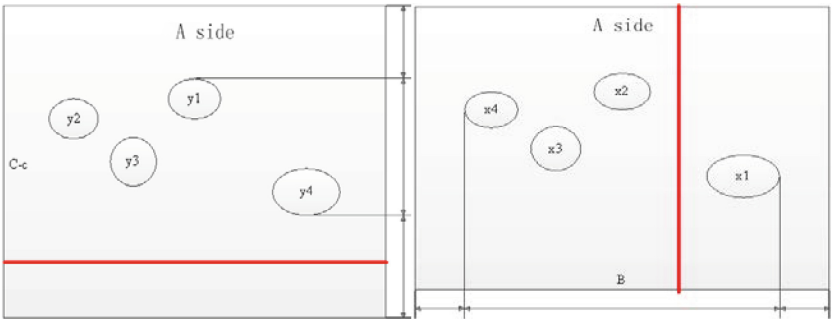


Fig. 4. Schematic diagram of reinforcement layout logic

Scheme of 3D parametric intelligent design system for Double Sheathed Liner Sumps. There are four surfaces A, B, C and D on Double Sheathed Liner Sumps that need to be assembled with Channel Steel. The assembly of each section of Channel Steel on each surface needs to have reference surface, overlapping object and normal direction as constraints, as shown in Fig. 5. These constraints are defined into the constraint objects of UDF custom features as constraints for assembling reinforcement. The application system calculates the constraint condition data of each section of Channel Steel on each surface according to the above "Logic of rib layoutl" algorithm. The data includes the total number of Channel Steel and the size and location of each section of Channel Steel. It circulates the parameter data of constraint conditions to UDF user-defined features for use, and combines the two to realize the function of "automatic rib layout".

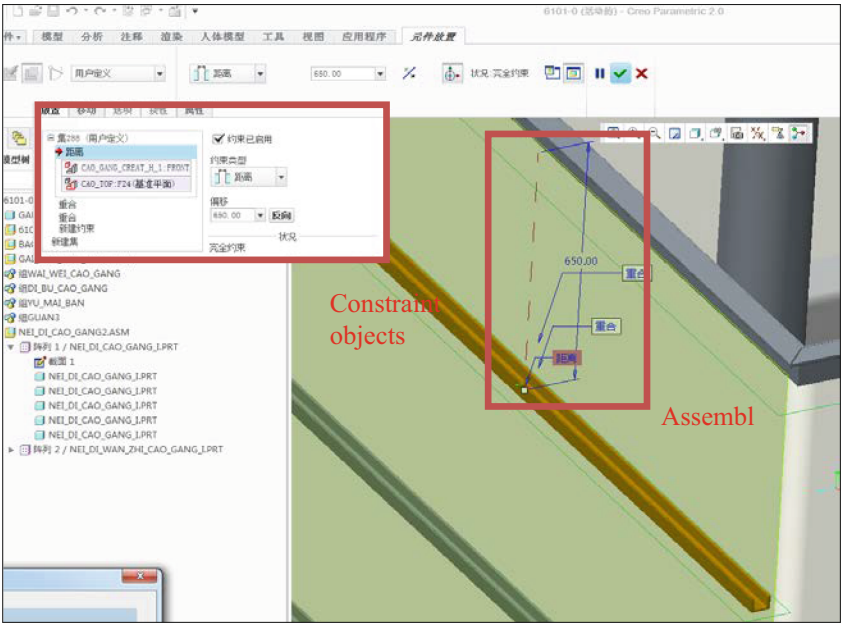


Fig. 5. Schematic diagram of constraint conditions for channel steel assembly

3 Scheme of 3D Parametric Intelligent Design System for Double Sheathed Liner Sumps

3.1 System Framework

In combination with the document composition requirements and operating environment characteristics of C software 3D design software, the 3D intelligent parametric design system architecture of Double Sheathed Liner Sumps is divided into four parts. They are the model file part, the resource file part, the system function library part, and the

compiled DLL file part. The system architecture is shown in Fig. 6. The contents and functions of each part are described below.

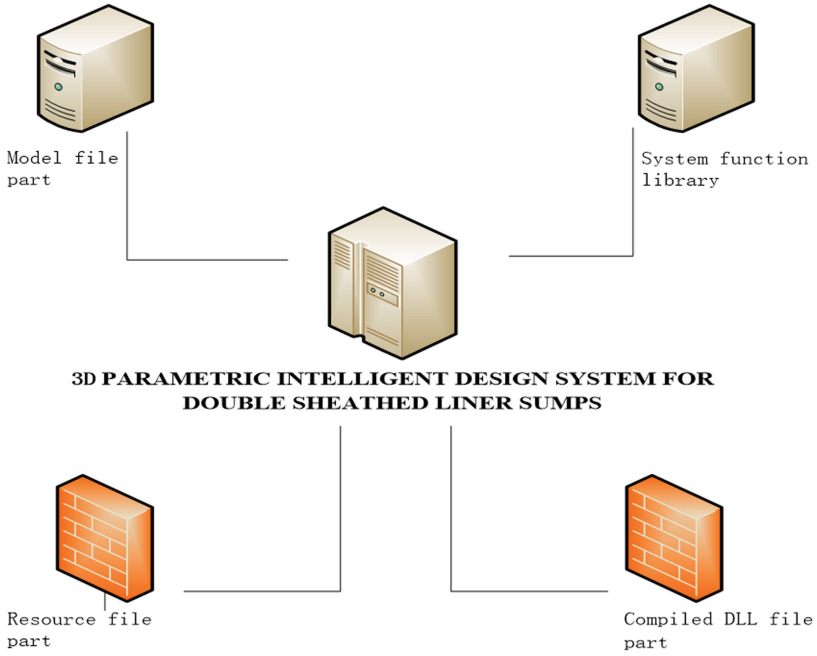


Fig. 6. System architecture

Model File Part. Model files are mainly parameterized 3D model files, including parameterized template models, standardized part models such as Leak Detection Pipe, Leak Detection Grooves and Channel Steels.

Resource File Part. Resource files mainly include specific attribute files that generate custom feature shapes and constrain their assembly relationships.

System Function Library. This part mainly provides the internal package function library file of 3D design software for the system tools to realize the operation, which is used to support the system's operation of 3D design software.

Compiled DLL File Part. After the source code of the 3D design software is edited, the DLL format file generated by the source code is compiled by the project programming tool, which is used to provide the 3D design software to call and start the 3D design system.

3.2 Workflow

The working flow chart of the 3D intelligent parametric design system for Double Sheathed Liner Sumps is shown in Fig. 7.

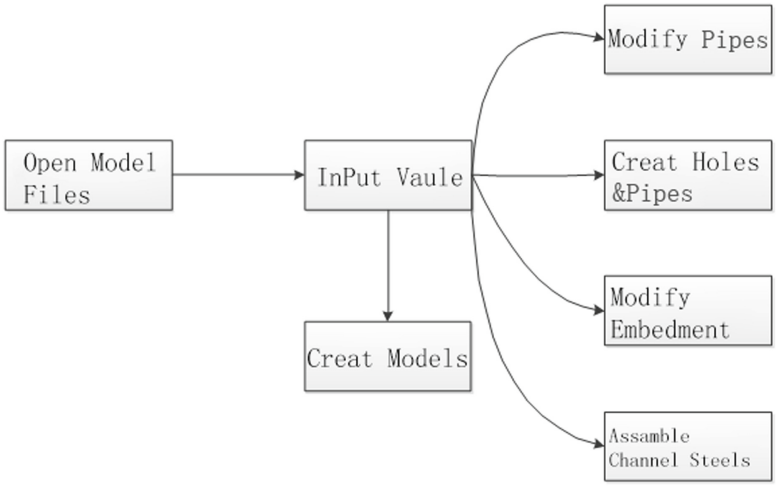


Fig. 7. Work flow chart

3.3 Main Functions of the Interface

The main function interface of the system is shown in Fig. 8. The main interface is the input of Channel size, and has the functions of generating model, saving model and restoring model.

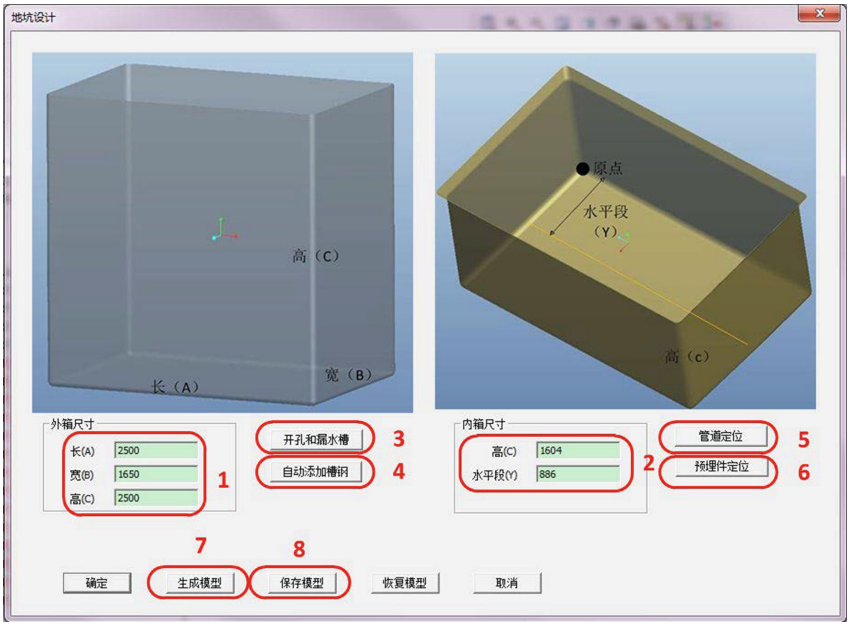


Fig. 8. Main interface of the platform

Interface Description. 1) basic dimension input part of Longitudinal Channel; 2) Basic size input part of Transversal Channel; 3) Opening and generating Leak Detection Groove; 4) Automatic addition of Channel Steel is the function of "automatic reinforcement arrangement"; 5) Pipeline positioning; 6) Positioning of Embedded Parts; 7) Generating a model; 8) Save the model.

As shown in Fig. 9, the sub interface is used for inputting hole parameters and generating holes and Leak Detection Grooves, inputting Leak Detection Pipe and Observation Pipe parameters, and inputting pump Embedded Parts parameters. In order to prevent the error of human input parameters, the interface is also set with the function of importing hole parameters, which can automatically add holes and Leak Detection Slots by reading the CSV format file carrying hole parameters.

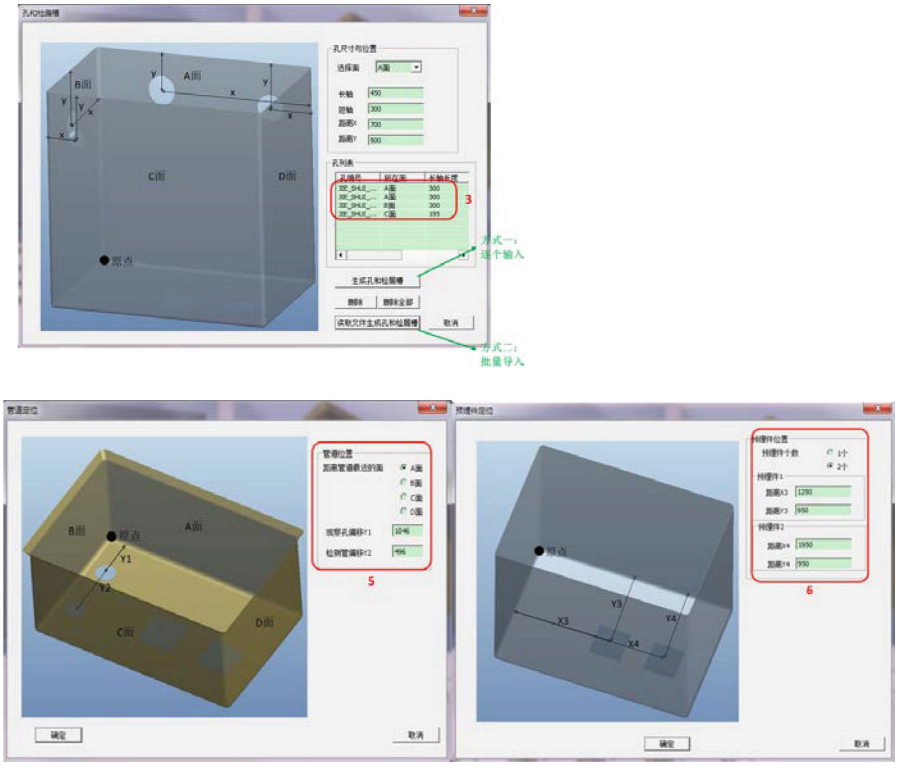


Fig. 9. System sub interface

4 Application Effect

As shown in Fig. 10, Type1 - and Type2 - are typical Double Sheathed Liner Sumps, Type3 - is the Double Sheathed Liner Sumps without process pipes access, and Type4 - is the Double Sheathed Liner Sumps with the most process pipes. The four sets of

Double Sheathed Liner Sumps are representative and can represent the other 25 sets of Double Sheathed Liner Sumps.

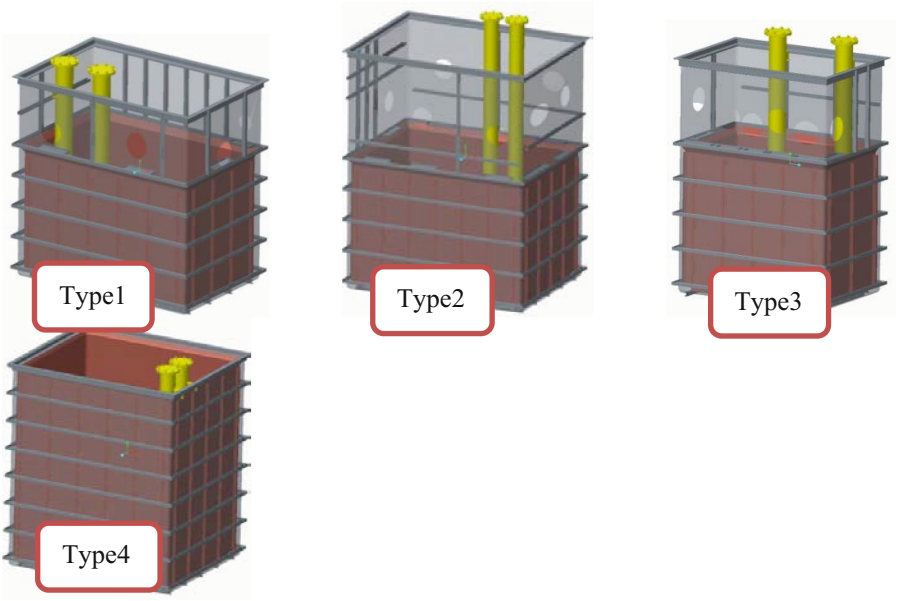


Fig. 10. 3D Model of Double Sheathed Liner Sumps

5 Conclusion

The completion of the 3D intelligent parametric design system for Double Sheathed Liner Sumps not only improves the efficiency of the 3D model creation, but also standardizes the 3D model and establishes a standardized model library, which provides favorable conditions for the standardized management of the design process, and is also conducive to the effective application of the 3D model data. It realizes the goal of the rapid design of Double Sheathed Liner Sumps and meets the requirements of the development of information technology. It provides an effective method of rapid design for nuclear power equipment which is designed with CAD software, and it is worthy of reference and promotion.

References

1. Yang, X., Xu, S.: Modeling and Simulation of Digital Prototype. Tsinghua University Press, pp. 81–89 (2014)
2. Lin, L.: Pro/Toolkit Wildfire 2.0 Plug-in Design. Electronic Industry Press, pp. 7–10 (2005)
3. Lin, L.: Pro/Engineer Wildfire 5.0 Advanced Design. Tsinghua University Press, pp. 246–281 (2010)

4. Wang, Z., Wang, H.: Application research on parametric design technology of C software secondary development. Mech. Res. Appl. **3**, 183–186 (2014)
5. Wang, H., Zhang, X., Wang, T.: Secondary development of Pro/E using MFC. J. Comput. Aid. Des. Graphics **6**, 869–872 (2004)
6. Hu, Y., Guo, Z.: Research on the application of parametric design and automatic assembly for secondary development of C software. Mod. Manuf. **9**, 90–99 (2017)

Research on Software Reliability of Nuclear Power Plant Instrument Control System

Ning Qiao and Jin-bing Liu(✉)

I&C Department, Nuclear and Radiation Safety Center, Beijing, China
iujingbinjob@163.com

Abstract. The reliable operation of the digital I&C system of nuclear power plants is of great significance to nuclear safety, but there is no industry-recognized method for evaluating and improving software reliability. This paper proposes a method which is depend on software reliability growth model, to calculate software reliability. At first this paper analyzes the cause and mechanism of software failure,then demonstrates how to descript software reliability mathematically. The second part of this paper explains two way to reduce software failures: fault-tolerant design and error-avoidance design. Furthermore, the third part proposes a software reliability assessment and improvement method based on the reliability growth model, which is used for the digital I&C system of nuclear power plants.

Keywords: Reliability · Software · Nuclear plant

1 Introduction

While the digital I&C technology has been developing, the traditional plant simulation technology of nuclear power plants has been gradually replaced, making the reliable operation of the digital I&C system the key to ensuring the safety of nuclear power plants and improving its reliability is of great significance. The digital I&C system is a complex system including hardware, software, and firmware. When evaluating its reliability, it is necessary to consider the influence of hardware failure and software error. Due to the inherent characteristics of aging, the trend of hardware failure rate can be predicted, and its reliability can be improved through circuit design, component selection, structural design, noise suppression, and redundancy design. However, software reliability assessment has limitations because of the system's complexity, the uncertainty of interactions with the external, and the credibility of test data. Presently, there are no global standards or methods to assess nuclear safety level software's reliability effectively. This paper first analyzes the mechanism of software failure and then introduces the software's error avoidance design and fault tolerance design method in the second part. In recent years, evaluating software reliability using the reliability growth model has received more and more attention. The third part of this paper proposes a method for reliability assessment and improvement of the core-level software based on the reliability growth model.

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 332–342, 2023.
https://doi.org/10.1007/978-981-99-3455-3_33

2 The Mechanism of Software Failure

2.1 Definition of Software Failure

Figure 1 defines software failure. Software failure means that the program's operation deviates from the requirements, such as crashes, wrong output results, and failure to respond within the specified time. It is the reflection of the software fault at the user end. The cause of the failure is that the software execution encounters software defects. Software defects refer to the existence of codes that can cause software failures, that is, software errors. Software defects are static and remain in the program as long as the program is not modified, such as incorrect functional requirements, missing performance requirements, etc. Software errors are mistakes made by developers during software development, including startup errors, input errors, input range errors, algorithm errors, and boundary errors. Software failure is the gradual manifestation of software defects in continuous testing and use, which is inevitable but can be improved by learning to reduce the number of errors in the program as much as possible, especially the number of significant errors.

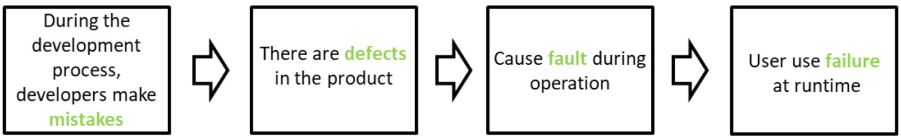


Fig. 1. Definition of software failure

There are three direct ways to reduce software failures based on the different life cycles of the software. The first is error avoidance design, which aims to reduce software defects by preventing or avoiding the occurrence or introduction of errors. The second is fault-tolerant design, which means that system functions can still be completed in the presence of errors. The third is failure detection and troubleshooting by reducing the number and severity of failures in software testing. This report mainly introduces the methods of the reliability growth model. In the following section, the paper will describe in detail how the three methods improve software reliability.

2.2 Mathematical Description of Software Reliability

Software reliability is defined as the ability of software not to cause system failure under specified conditions and within a specified period. It can be described intuitively with mathematics, and the program is regarded as the mapping from the input space to the output space. The software running error can be seen as some inputs do not get the expected output mapping. Assuming that there are I points in the input space, whether the program runs correctly has the following relationship expressed as Eq. 1,

$$Y(i) = \begin{cases} 1, & \textit{the program runs correctly} \\ 0, & \textit{else} \end{cases} \tag{1}$$

Let P(i) be the probability that the input point i occurs, the probability that output will cause the program to run correctly can be written as

$$\sum_{i=1}^{\mathrm{I}} \mathrm{P}(i)\mathrm{Y}(i) \tag{2}$$

Assuming that the expected time of each execution of the program is T, then the number of times the program runs in [0, t] time is t/T times, and the probability of non-failure in a given environment and a given time can be expressed as follows,

$$\mathrm{R(t)} = \left[\sum_{i=1}^{I} \mathrm{P}(i)\mathrm{Y}(i)\right]^{\frac{\mathrm{t}}{\mathrm{T}}} \tag{3}$$

Since I is a very large number, and P(i) is difficult to determine, Eq. (3) can only essentially reflect the definition of software reliability.

Let n represent the number of times the program runs in a particular application, which is a large number, and $\mathrm{C_n}$ represents the number of correct runs, then the software reliability during (0, t) based on running performance can be expressed as,

$$R(t) = \left[\lim_{n\to\infty} \frac{c_n}{n}\right]^{\frac{t}{T}} \tag{4}$$

Let λ(t) represent the risk function, which is the probability that the program runs correctly until the program fails at time t per unit time. Suppose T represents the time elapsed between the program's start and failure, then T is a continuous random variable. Thus,

$$\lambda(t) = \lim_{\Delta t\to 0} \frac{Pr\{(t+\Delta t) \geq T > t | T \rangle t\}}{\Delta t} \tag{5}$$

So,

$$\begin{aligned} &R(t+\Delta t) = Pr\{T > (t+\Delta t)\} \\ &= \Pr(T > t) \cap \Pr(\text{non - failure in}[t, t+\Delta t]) \\ &= R(t)(1-\lambda(t)\Delta t) \end{aligned} \tag{6}$$

Then there is,

$$\frac{dR(t)}{R(t)} = -\lambda(t)dt \tag{7}$$

And

$$R(t) = e^{-\int_0^t \lambda(x)dx} \tag{8}$$

According to the definition of reliability, R(0) = 1, R(∞) = 0. As the testing progresses, the faults are continuously corrected, and λ(t) can be optimistically viewed as a decreasing function, and the reliability function R(t) is an increasing function.

3 Software Design Method

3.1 Error Avoidance Design

To eliminate software failure, one of the common solutions in the industry is to avoid or reduce defects as much as possible during the software development process, which is the starting point of software error avoidance design. Software error avoidance design is implemented through rigorous software development methods, specifications, and process, which closely integrates the software reliability and conventional design. It runs through the conventional design process, including plan formulation, requirement analysis, and the final implementation. There are significant differences in the reliability of software and hardware, which are reflected in the failure causes, failure rates, and abandonment reasons, so the design quality has special significance for software reliability. Compared with hardware, software reliability depends more on design. It is crucial to develop the reliability design of software to ensure its reliability.

NUREG/CR6101-1993 Reliability and Safety of Nuclear Power Plant Protection System Software puts forward the qualitative evaluation terms of software reliability from the perspective of the whole life cycle of software. These terms are derived from key industrial software design and production activities, which are summaries of existing and similar engineering experiences, and have been adopted by the US Electric Power Industry Special Report. NRC believes that when the reliability requirements listed in NUREG/CR6101 are implemented, it is of great significance to the reliability of the safety-level software in nuclear power plants, which can effectively avoid or reduce the introduction of software defects and improve the inherent reliability of software. Taking the "requirements stage of the safety-level software in nuclear power plants" as an example, as the starting point of software reliability design, the software requirements specification (SRS) records all the requirements of the software, which is very important to ensure the reliability attributes of the final product. In order to ensure the reliability requirements of safety software in nuclear power plants, both the requirements of regulations and standards and the experience from the design and construction of nuclear power plants need to be considered. In addition to the conventional functional description, attention should also be paid to the following aspects when making the SRS:

- whether the changes to hardware or software are documented in the SRS, and whether the functional requirements have been independently verified;
- whether each requirement is expressed unambiguously, and whether the functional requirements as a whole can be coordinated with each other;
- whether each functional requirement can be checked, or passed inspection and testing;
- whether the communication channel is clearly expressed in subroutine calls and remote procedure calls;
- whether the transmission method and medium of each message are defined;
- whether the static operation requirements are adequately described, and whether there are complete and precise timing requirements;
- whether each software requirement is testable, and whether reliability and safety requirements are independently defined;
- whether each hazard identified in the system risk analysis can be traced to one or more software requirements that would prevent, suppress or mitigate those hazards;

- whether the level of detected errors will be rated if the software is required to diagnose hardware or software errors.

3.2 Fault-Tolerant Design

As software systems are getting increasingly large and complex, there will be inevitable software defects, no matter how well-designed. The software error avoidance design discussed in Sect. 3.1 embodies the idea of prioritizing prevention. Error avoidance design applies to all types of software and should run through the entire software development process. However, the software cannot be free of defects through error avoidance design and can only achieve a certain degree of reliability. For systems with high-reliability requirements or their failure consequences may be catastrophic, using only error avoidance design cannot meet the requirements. Therefore, it is necessary to introduce the software fault-tolerant design, which allows the system to detect errors and avoid failures, or to detect and recover itself from errors. As "the other line of defense" of software error avoidance design, software fault-tolerant design plays the role of defense in depth.

Take a nuclear power plant's digital I&C protection system as an example, the system adopts the fault-tolerant design, and the Watchdog timer monitors the running status of each program. When the program failure occurs due to external disturbances or other reasons, the working step of the process exceeds its Watchdog timing value, and the Watchdog can capture this state. Then the interrupt service subroutine recognizes the process and executes a series of identification and repair steps. Specifically, firstly check whether the RAM protection zone set by the system has been rewritten and whether the collected data is within a reasonable range.

For example, the first byte of the temperature value at the outlet of the primary circuit must be within a specific range, and any other value indicates corrupted illegal data. Rereading the control output feedback value determines whether the control output is correct, and the operation processing result is compared with a set of standard values the system sets to determine whether it needs corrections. Different repair strategies can be made depending on the type and nature of the fault diagnosed. If irreparable faults occur, such as repeatedly destructions of the RAM working area, the main control room alarm will be triggered. The backup disk will be switched, and manual intervention measures such as error correction and system reset will be implemented.

4 Software Reliability Growth Model

4.1 Overview

The reliability growth model is a mathematical model based on the error or failure time data found in the software testing stage. It is a theory that uses failure data to estimate and predict the failure intensity. Essentially, it describes the relationship between software defects and software failure and reflects the increasing trend of software reliability with defect elimination. It is realized by establishing the mathematical equation of the relationship between software failure and operating profile. It can be used as an indicator to evaluate whether the reliability of the current software meets the deliverable target, predict the reliability level in actual operation in the future, and estimate the time

required for testing before delivery. It is independent of the programming language and the specific software development method used. According to the uniform specification, the same software reliability model should give the same estimates regardless of which programming language is used.

So far, the research on the software reliability model has been more than 40 years, and nearly 100 kinds of models are published nationally and internationally. There are currently no complete and systematic classification methods, and some common classification methods are as follows.

< 1 > By analyzing the role of the software reliability growth model, the preconditions for its establishment, the factors affecting the accuracy of the model, the applicable reliability assessment scope, and the advantages and limitations of the model, *IEEEStd1633-2008* divides the current reliability growth models into three classes: (1) Exponential Non-homogeneous Poisson Process (NHPP) model, (2) Non-exponential NHPP model, (3) Bayesian model.

< 2 > The random process classification method: The random process classification method is a common classification method, as shown in Fig. 2. Stochastic process models are often called macroscopic models, and others are called microscopic models. Generally speaking, the macroscopic model's benefits are much greater than those of the microscopic model. The macroscopic model measures the software performance and behavior more comprehensively and extensively than the microscopic model, and the advantage of the microscopic model is its local relative precision.

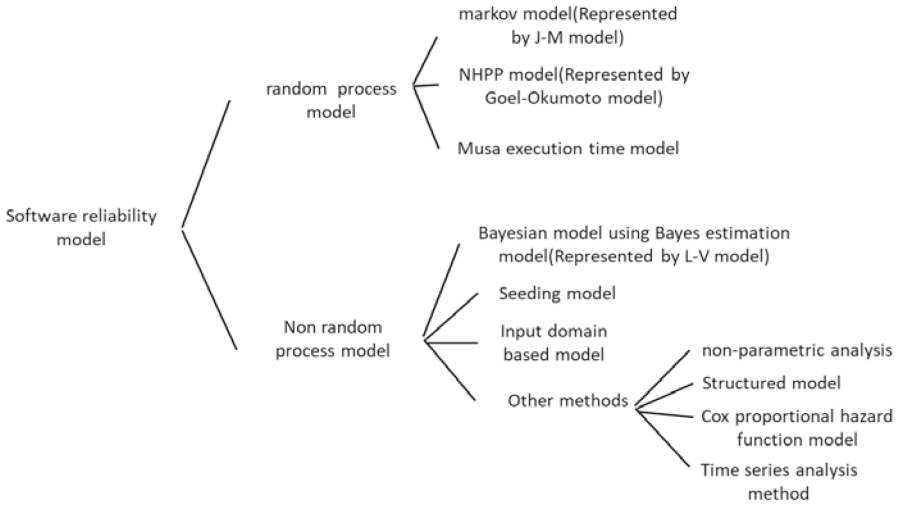


Fig. 2. Reliability models classified by random processes

< 3 > Classification by fault characteristics:

(1) Time interval between faults model: study the time interval between fault and assume it follows a specific distribution.

(2) Faults counting model: study the number of software faults in a specific time interval, and assume it follows a consistent random process. The NHPP reliability growth model belongs to this category.
(3) Faults seeding model: For a program with an unknown number of inherent faults, artificially implant a specific number of faults and then test it to estimate the program's reliability and other software performance measures based on the number of faults.
(4) Model based on the input domain: According to the usage of the program, find out the probability distribution of the input domain, randomly select test cases on the input domain, and observe the program faults to infer the program's reliability.

< 4 > Classification by data domain and time domain model (Fig. 3):

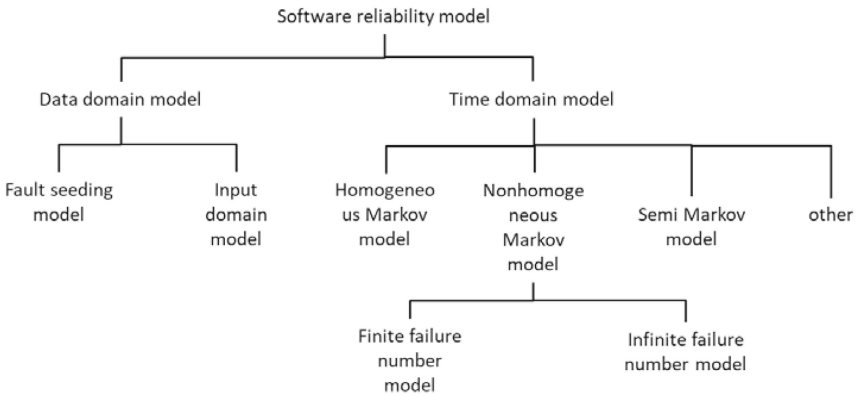


Fig. 3. Classification method of data domain and time domain model

4.2 Modeling and Application of Reliability Growth Model

The primary process of establishing a reliability growth model is shown in Fig. 4.

In most cases, obtaining a suitable model through such a process is complicated. If the fitting accuracy does not meet the requirements, repeat the process of selecting an appropriate reliability model. If the final reliability does not meet the requirements, repeat the entire process until the requirement is met.

For the various software reliability growth models, NHPP is very important and the most attractive model for managing and improving software reliability. It can quantitatively describe the reliability-related attributes in software testing, such as the number of software faults, changes in software reliability, etc. It has been verified as the most suitable and straightforward model for evaluating software reliability in engineering practice.

Take the establishment of the reliability growth model of a nuclear power plant protection system software as an example. The model is based on data recorded during the development process and focuses on the severity level of errors, dividing errors

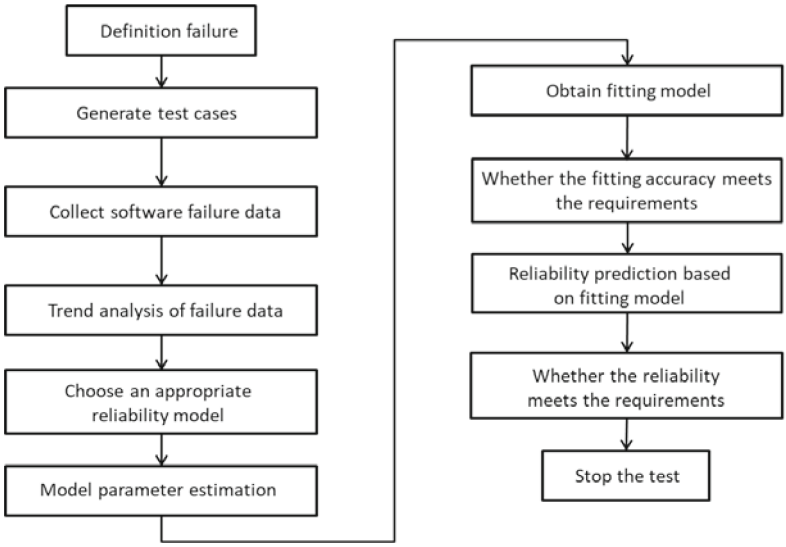


Fig. 4. Reliability model modeling process

into critical and non-critical errors. Let the critical error ratio function ρ_1 (t) and the non-critical error ratio function ρ_2 (t), as shown in Fig. 5. The error severity level ratio function can be expressed as Eq. 9 using the logistic function (a sigmoid function).

$$\begin{cases} \rho_1 t = \frac{1}{1+\beta e^{-\alpha t}} \alpha, \beta > 0 \\ \rho_2 t = \frac{\beta e^{-\alpha t}}{1+\beta e^{-\alpha t}} \alpha, \beta > 0 \end{cases} \tag{9}$$

where α and β are the parameters of the logistic function.

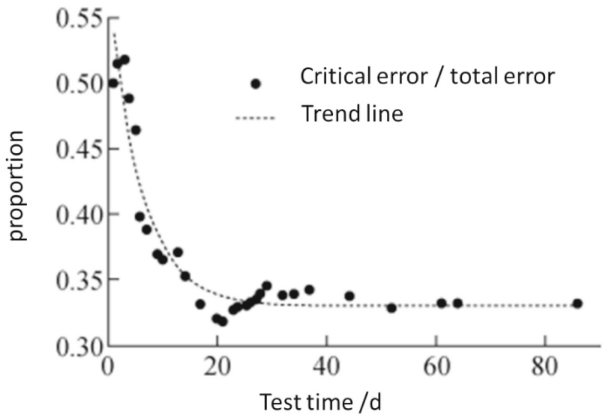


Fig. 5. Severity level of error ratio function

Make the following assumptions,

(1) Assuming that the error detection process is a Poisson process, and the cumulative number of detected errors at time t is N(t), then N(t) follows a Poisson distribution with the mean function m(t). The expected number of errors detected per unit time interval is proportional to the number of undetected errors. Therefore, the mean value function is a bounded non-decreasing time function;
(2) The errors found in software are divided into two categories according to their contribution to the failure, namely critical errors and non-critical errors;
(3) The number of errors detected in each time interval is independent of each other;
(4) Errors are corrected immediately after they are discovered, and no new errors are introduced;
(5) Errors of different severity, in the time interval of (t, Δt + t), the proportion of the expected number of detections and the number of undetected errors is different.

Then there is,

$$\begin{gathered} m_c(t+\Delta t) - m_c = b(N - m(t))\rho(t)\Delta t \\ c = 1, 2 \end{gathered} \tag{10}$$

where b is the expected detection rate given by the error detection model, and

$$\begin{cases} m(t) = \sum_{c=1}^{2} m_c(t) \\ \sum_{c=1}^{2} \rho(t) = 1 \end{cases} \tag{11}$$

when ρ(t) is fixed, the expectation function of the cumulative number of errors can be written as,

$$m_c(t) = \rho_c(t)m(t) \tag{12}$$

Based on the above assumptions, according to Eq. 10, $\Delta t \to 0$, solve the differential equation,

$$m_c(t) = N\int_0^t b\rho_c(\tau)e^{\int_0 \tau bdx}d\tau \tag{13}$$

where τ is the time integration variable, and the expected function of the cumulative number of errors with different severity is finally solved as,

$$\begin{cases} m_1(t) = Nb\int_0^t \frac{e^{b\tau}}{1+\beta e^{-\alpha\tau}}d\tau \\ m_2(t) = Nb\int_0^t \frac{e^{-\alpha\tau-b\tau}}{1+\beta e^{-\alpha\tau}}d\tau \end{cases} \tag{14}$$

According to the inhomogeneous Poisson process, for errors with different severity, the reliability is defined as

$$R_c(x|t) = e^{(-(m_c(t+x)-m_c(t)))} \tag{15}$$

The above reliability model includes four parameters N, b, α, and β. There are three commonly used parameter estimation methods,

(1) Least Squares Estimation (LSE): It has fast convergence and small deviation, and is suitable for small or medium-sized samples.

(2) Maximum Likelihood Estimation (MLE): The most widely used estimation method, suitable for large samples.
(3) Bayesian Estimation: A method of integrating prior knowledge into the estimation process, its analysis and calculation are more complicated than the LSE and MLE.

Different parameter estimation methods give different results for the same set of software failure data and may even vary greatly. Therefore in practical application, for a good software reliability model, it is better to use different parameter estimation methods and give the results after comparative analysis.

Least Squares Estimation:

$$\min S^2 = \sum_{i=1}^{k_1} \left(m_1(t_i,\theta) - n_i^1\right)^2 + \sum_{i=}^{k_2} \left(m_2(t_i,\theta) - n_i^2\right)^2 \tag{16}$$

where n_i^c is the cumulative number of errors with severity c at the end of time t_i in the testing process.

Maximum Likelihood Estimation:

$$L(\theta) = \prod_{i=1}^{k} (e^{-m_1 t_i - m_1 t_{i-1} + m_2 t_i - m_2 t_{i-1}} \frac{(m_1 t_i - m_1 t_{i-1})^{n_i^1}}{n_i^1!} \frac{(m_2 t_i - m_2 t_{i-1})^{n_i^2}}{n_i^2!}) \tag{17}$$

where $m_1 t_i + m_2 t_i$ is the overall expected cumulative number of errors.

The collected data were compared with the reliability models obtained from the LSE and MLE parameter estimation, and the results are shown in Fig. 6.

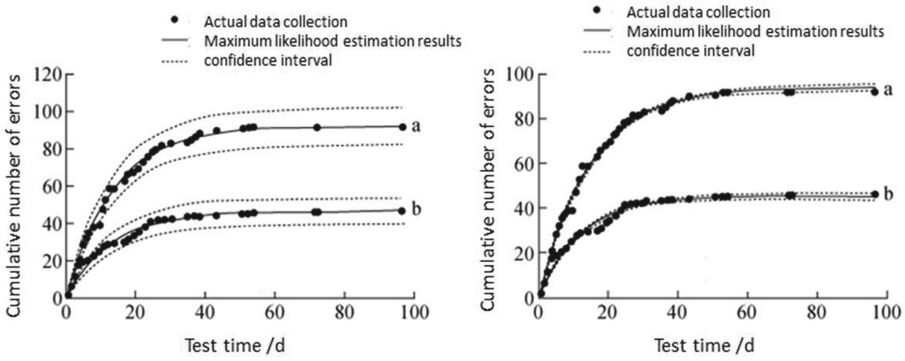


Fig. 6. Comparisons between the collected data and the reliability models

Errors of the reliability model can be calculated by comparing the average variance and the coefficient of determination between the predicted data and the collected data to evaluate the quality of the model. Another basis for evaluating the model is its predictive performance, which is not detailed here.

Select the corresponding reliability model for different software according to the modeling process given above. However, the current software reliability model may have the following limitations,

① There is a delay in the correction of faults. Fault detection and correction are two different stages in the software development process. It is ideal to assume that faults are eliminated immediately after detection, but it does not fully reflect the software testing situation and reduces the practical significance of the model.

② Software error detection and troubleshooting is a complex process, which may introduce new errors while troubleshooting due to inexperienced developers.

5 Summary

Currently, more and more software-based systems and equipment have been applied on a large scale in nuclear power plant I&C systems. Therefore, software reliability has become a critical safety issue that must be solved in designing and manufacturing digital nuclear power plants. Under the above background, this paper introduces three implementation schemes of error avoidance design, fault-tolerant design, and reliability growth model to improve software reliability in order to provide a reference for the implementation of safety-level software reliability improvement in the digital I&C system.

References

1. Li, S., Dohi, T., Hiroyuki, O.: Burr-type NHPP-based software reliability models and their applications with two type of fault count data. J. Syst. Softw. **191,** 111367 (2012). ISSN:0164-1212
2. Zhang, C.E., et al.: Review of research on software reliability growth model. J. Softw. **28**(09), 2402–2430 (2017). https://doi.org/10.13328/j.cnki.jos.005306
3. GJB/Z161-2012 military software reliability evaluation guide. National Military Standard, China (2012)
4. IEEEStd1633-2008 IEEE Recommended Practice on Software Reliability[S] .U.S.:Standards Committee of the IEEE Reliablility Society (2008)
5. IEEE Std 982.1-2005 IEEE Standard Dictionary of Measures of the Software Aspects of Dependability U.S.:Software Engineering Standards Committee (2005)
6. NUREG/CR-6901-2006 Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments. U.S.: Nuclear Regulatory Commission (2006)
7. Xian, Z., Hanyu, L.: Summary of research on quantitative reliability evaluation method of safety level DCS software. Nucl. Stand. Measure Qual. (03), 64–71 (2021)

An Algorithm of Nuclide Number Identification for Environmental Radioactivity Monitoring

Jing Xu(✉)

China Nuclear Control System Engineering Co., Ltd., Beijing, China
xujing@cncs.bj.cn

Abstract. The traditional nuclide identification algorithm based on the characteristic peak has high requirements for users' specialization, many steps and slow recognition speed. In recent years, although the new methods such as artificial neural network and Bayesian theory based on full spectrum analysis have high recognition speed and low requirements for user specialization, they rely on a large number of training samples, and the accuracy of measurement results will be affected when the measurement conditions of training samples and measured samples deviate. To solve this problem, an algorithm of nuclide number identification based on singular value method is designed. The algorithm is to analyze the time series of the collected data, which is mainly divided into the steps of acquiring array signals, constructing incidence matrix, calculating and sorting eigenvalues. The experiments show that the nuclide recognition time is short and the recognition is accurate. It can provide fast and accurate information in case of abnormal nuclear radiation.

Keyword: singular value · time series · nuclide recognition

1 Introduction

As an efficient and clean energy, nuclear energy plays an important strategic role in coping with climate change, ensuring energy security, optimizing energy structure and improving the atmospheric environment. Of course, the environmental problems brought by it can't be ignored. Radionuclides will spontaneously release α、β and γ rays in the process of decay of radionuclides into stable state. And γ rays have strong penetration, carry high energy, and have lethality to biological cells. Therefore, γ radioactivity monitoring in the environment is particularly important.

As we know, γ spectrometer is an important tool to detect γ rays and identify radionuclides. According to different uses, γ spectrometer can be divided into aviation γ spectrometer, indoor γ spectrometer and portable γ spectrometer. Portable γ spectrometer is generally used for environmental radioactivity monitoring to realize nuclide identification.

Currently, nuclide identification algorithm adopted by portable γ spectrometer is divided into two types: one is the traditional spectrum analysis algorithm based on the characteristic peak. The algorithm searches the nuclide library according to the calculated

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 343–350, 2023.
https://doi.org/10.1007/978-981-99-3455-3_34

energy value through the steps of smoothing, background deduction, peak search and energy calibration, so as to identify the type of nuclide. Portable γ spectrometer with this algorithm requires users' high professional knowledge, and has many steps and slow recognition speed; the other is the full spectrum analysis method developed in recent years, such as artificial neural network and Bayesian theory, and these methods are more efficient in nuclide identification and have lower requirements for the "threshold" of users' nuclear technology specialization.

2 Portable γ Spectrometer

NaI(Tl) detector can work and store at normal temperature. It is not only convenient to use, but also has the advantages of short detection time and high detection efficiency. It is also the very classic detector used in portable γ spectrometer. In this study, γ spectrometer is mainly composed of NaI(Tl) detector, multichannel analyzer and spectrum analysis software, as shown in Fig. 1.

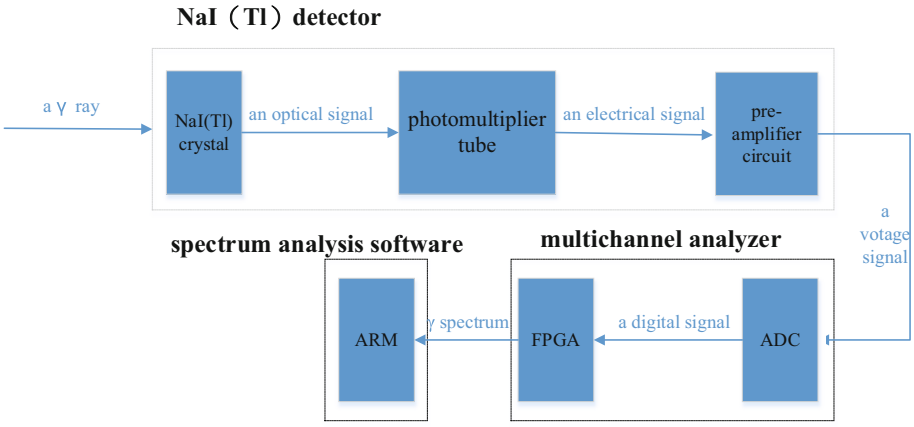


Fig. 1. The principle block diagram of portable γ spectrometer

When a γ ray is incident on the NaI(Tl) detector, it first becomes an optical signal through the NaI(Tl) crystal, then is converted into an electrical signal through the photomultiplier tube, and finally is output by the preamplifier circuit in the way of a voltage signal. The amplitude of the voltage signal is proportional to the energy value of the γ ray. After the voltage signal enters the multichannel analyzer, the FPGA controls the ADC chip to perform analog-to-digital conversion on the signal and convert it into a digital signal. The FPGA extracts the converted digital value of each voltage signal peak and transmits the data to the spectrum analysis software for display in the form of γ spectrum. The spectrum analysis software is developed based on ARM, which is convenient to design nuclide identification algorithm to realize the identification of radionuclides.

The process of nuclide identification by traditional energy spectrum analysis software is generally as follows: measure for a period of time so as to make the count of

each channel reach a certain statistical fluctuation, then successively adopt the steps of smoothing, background deduction, peak search and energy calibration, and finally the energy value obtained from the calibration is compared in the nuclide library, and then the nuclide identification is realized. Because the premise of this algorithm is characteristic peak search, there are some problems such as false and missing reports of radionuclides.

Although the γ spectrometer using Bayesian theory or artificial neural network is simple to operate and fast to identify, these algorithms need a large number of training samples. If the measurement conditions of the measured samples and the training samples are inconsistent, it is often difficult to ensure the accuracy of the nuclide identification.

The characteristic of environmental radioactivity monitoring is that it needs to monitor a wide range. The monitoring object is the environmental background of nature, and the presence of radionuclides in the environment is very rare. Based on this, this paper studies the algorithm of nuclide number identification for environmental monitoring, and judges whether there is nuclear radiation anomaly in the environment by identifying the nuclide number.

3 Algorithm

This algorithm is based on singular value decomposition method to identify the number of nuclides. It uses spectral information to estimate the number of nuclides in the field. The algorithm is mainly divided into the following steps: acquire array signals, construct incidence matrix, calculate and sort eigenvalues.

3.1 Acquire Array Signals

The data measured by the γ spectrometer are the cumulative value in the measurement time. First, they are processed to obtain the time array sequence. For example, hypothesis the output data of the γ spectrometer are expressed as formula (1), where n = 1,2…represents time sampling.

$$s(n) = [s_1(n), s_2(n), \cdots, s_k(n)] \tag{1}$$

Convert it to a time array as formula (2).

$$x(n) = [x_1(n), x_2(n), \cdots, x_k(n)] \tag{2}$$

Formula (2) satisfies formula (3) and formula (4).

$$x(1) = s(1) \tag{3}$$

$$x(n) = s(n) - s(n-1) n = 2, 3, \cdots, \tag{4}$$

3.2 Construct Incidence Matrix

Using time array sequence, construct covariance matrix as formula (5).

$$R = E\left[(x(n) - \overline{x})(x(n) - \overline{x})^H\right] \tag{5}$$

The R matrix is decomposed into a normal orthogonal matrix and an upper triangular matrix by using the orthogonal triangular decomposition method in numerical analysis, and the eigenvalues λ_i of $R^H R$ are obtained. The singular values of R matrix are further obtained as shown in formula (6).

$$\sigma = [\sigma_1, \sigma_2, \cdots, \sigma_n] = \left[\sqrt{\lambda_1}, \sqrt{\lambda_2}, \cdots, \sqrt{\lambda_n}\right] \tag{6}$$

3.3 Calculate and Sort Eigenvalues

Hypothesis the signal array x(n) received by the γ spectrometer is the sum of the signal source array o(n) and the white noise array N(n), that is, its model can be expressed as formula (7).

$$\mathrm{x(n)} = \mathrm{Ao(n)} + \mathrm{N(n)} \tag{7}$$

The signal source array o(n) is uncorrelated with the white noise array N(n) or the correlation is very low, that is, $\mathrm{E}\left[\mathrm{o(n)N^H(n)}\right]$ is less than a certain threshold. Thus, formula (8) is obtained.

$$\mathrm{R} \approx \mathrm{R_o} + \mathrm{R_N} \tag{8}$$

$\mathrm{R_o} = \mathrm{AE}\left[\mathrm{x(n)x^H(n)}\right]\mathrm{A^H}$ is the similarity transformation of the covariance matrix of the signal source array o(n), and $\mathrm{R_N}$ is the similarity transformation of the covariance matrix of the white noise array N(n). When $\|\mathrm{R_N}\| \ll \|\mathrm{R_o}\|$, there is formula (9).

$$\lambda_\mathrm{i} \approx \lambda_\mathrm{i}^\mathrm{o} + \lambda_\mathrm{i}^\mathrm{N} \tag{9}$$

The eigenvalues of the covariance matrix of the signal source array are $\lambda_\mathrm{i}^\mathrm{o}$, the eigenvalues of the covariance matrix of the white noise array are $\lambda_\mathrm{i}^\mathrm{N}$. So, if λ_i or σ_i is very small and it can be estimated that there is only noise; On the contrary, it is estimated that there is a signal source, that is, the measured sample has a corresponding nuclide.

The obtained singular values are sorted from small to large, and the singular value sequence as formula (10) which are greater than a certain threshold C is obtained.

$$\sigma_1^{'} \geq \sigma_2^{'} \geq \cdots \geq \sigma_\mathrm{m}^{'} \geq \mathrm{C} \geq \sigma_{\mathrm{m+1}}^{'} \geq \cdots \geq \sigma_\mathrm{n}^{'} \geq 0, \mathrm{m} \leq \mathrm{n} \tag{10}$$

Hypothesis $\gamma_\mathrm{k} = \sigma_{\mathrm{k-1}}^{'}/\sigma_\mathrm{k}^{'}$ and $\mathrm{k} \geq 2$, then when formula (11) is satisfied and γ_t is greater than a certain threshold, the value of γ_t is the estimated number of nuclides.

$$\gamma_\mathrm{t} = \max(\gamma_2, \gamma_3, \cdots, \gamma_{\mathrm{n-2}}) \tag{11}$$

4 Experiment and Analysis

A portable γ spectrometer with NaI(Tl) detector is used for this experiment. ^{241}Am, ^{137}Cs and ^{60}Co are the radiation sources. The radiation sources are all facing the detector with a distance of about 1cm when they are measuring. Measure the background, mixed sources of ^{241}Am and ^{137}Cs, mixed sources of ^{241}Am, ^{137}Cs and ^{60}Co respectively for 5 min and store these spectrums, as shown in Fig. 2, Fig. 3 and Fig. 4.

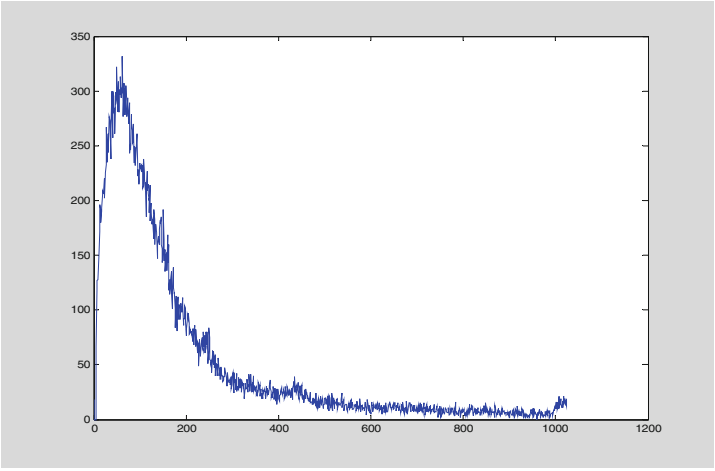


Fig. 2. Background spectrum.

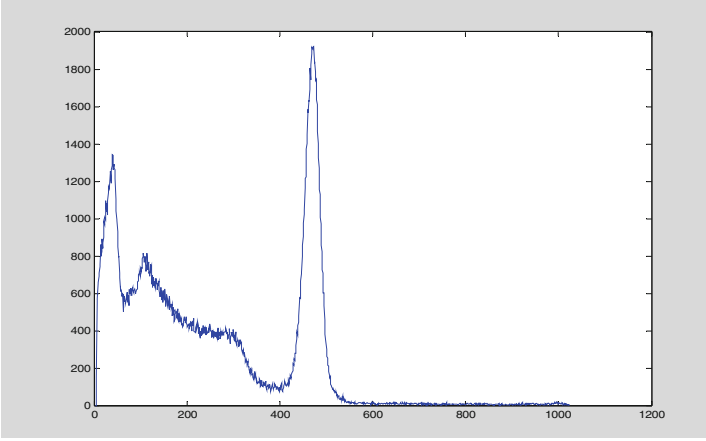


Fig. 3. ^{241}Am and ^{137}Cs spectrum.

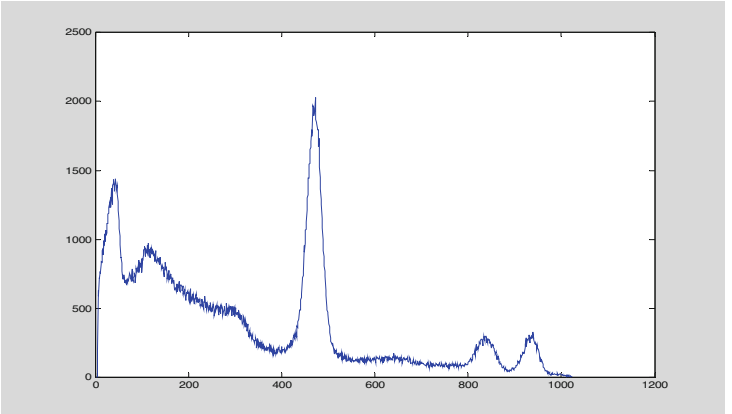


Fig. 4. ^{241}Am, ^{137}Cs and ^{60}Co spectrum.

4.1 Analysis

Each measured spectrum is converted into the corresponding time array sequence, and then the covariance matrix can be obtained according to formula (5). Calculate the singular values of the covariance matrix and sort them. See Table 1 for the results of the first eight singular values. See Table 2 for the ratios of the first eight singular values.

Table 1. The first eight singular values of three groups.

Singular values	Background	^{241}Am and ^{137}Cs	^{241}Am、^{137}Cs and ^{60}Co
σ_1'	21.2201	820.1957	1660.3578
σ_2'	1.4578	28.0384	41.5230
σ_3'	1.4168	13.3142	39.7787
σ_4'	1.375	13.2340	15.6898
σ_5'	1.3475	12.6852	15.0088
σ_6'	1.3335	12.5457	14.4568
σ_7'	1.3143	11.7257	14.0776
σ_8'	1.2917	11.2971	13.8479

It can be seen from Table 2 that if the threshold value is set to 1.1, there is no nuclide in the background, while the mixed sources of ^{241}Am and ^{137}Cs, and the mixed sources of ^{241}Am, ^{137}Cs and ^{60}Co take the maximum value at γ_2 and γ_3 respectively and meet the threshold condition. According to this algorithm, there are 2 and 3 nuclides in the two samples, which are consistent with the expectation.

Table 2. The ratios of the first eight singular values of three groups.

Ratios of singular values	Background	^{241}Am and ^{137}Cs	^{241}Am、^{137}Cs and ^{60}Co
$\gamma_2 = \sigma_2^{'}/\sigma_3^{'}$	1.0289	2.1059	1.0439
$\gamma_3 = \sigma_3^{'}/\sigma_4^{'}$	1.0304	1.0061	2.5353
$\gamma_4 = \sigma_4^{'}/\sigma_5^{'}$	1.0204	1.0433	1.0454
$\gamma_5 = \sigma_5^{'}/\sigma_6^{'}$	1.0105	1.0111	1.0382
$\gamma_6 = \sigma_6^{'}/\sigma_7^{'}$	1.0146	1.0699	1.0269
$\gamma_7 = \sigma_7^{'}/\sigma_8^{'}$	1.0175	1.0379	1.0166
$\gamma_2 = \sigma_2^{'}/\sigma_3^{'}$	1.0289	2.1059	1.0439
$\gamma_3 = \sigma_3^{'}/\sigma_4^{'}$	1.0304	1.0061	2.5353

5 Conclusion

This algorithm is to analyze the time array sequence of γ spectrum. Compared with the traditional nuclide identification algorithm using the characteristic peak analysis method, the accuracy of nuclide number identification is high in a short time. It does not have these problems that has many steps and high professional requirements for characteristic peak analysis method. At the same time, it also avoids the problem that the nuclide identification algorithm based on the full spectrum analysis has great dependence on training samples.

It is suggested to try to use less time array sequence (i.e., less than 5 min of collected data) to verify this nuclide number identification algorithm, so as to further shorten the time required for nuclide number identification algorithm. It is also suggested to deeply study the theory of Blind Source Separation, and then design the nuclide type identification algorithm so as to improve the nuclide identification algorithm.

References

1. Kim, J., Park, K., Cho, G.: Multi-radioisotope identification algorithm using an artificial neural network for plastic gamma spectra. Appl. Radiat. Isot. **147**, 83–90 (2019)
2. Kimoto, N., et al.: Precise material identification method based on a photon counting technique with correction of the beam hardening effect in X-ray spectra. Appl. Radiat. Isot. 1**24**, 16–26 (2017)
3. Liang, D., et al.: Rapid nuclide identification algorithm based on convolutional neural network. Ann. Nucl. Energy **133**, 483–490 (2019)
4. Shahabinejad, H., Vosoughi, N.: SGSD: a novel sequential gamma-ray spectrum deconvolution algorithm. Ann. Nucl. Energy **132**, 369–380 (2019)
5. Zhang, C., et al.: Identification of SNM based on low-resolution gamma-ray characteristics and neural network. Nucl. Inst. Methods Phys. Res. A **927**, 155–160 (2019)
6. Lele, A.: Challenges for the chemical weapons convention (CWC). Strat. Anal. **35**(5), 752–756 (2011). https://doi.org/10.1080/09700161.2011.591766

7. Li, J., Jia, W., Hei, D., Cai, P., Cheng, C., Tang, Y.: The optimization of coal on-line analysis system based on signal-to-noise ratio evaluation. J. Radioanal. Nucl. Chem. **318**(2), 1279–1286 (2018). https://doi.org/10.1007/s10967-018-6173-x
8. Li, J.T., Jia, W.B., Hei, D.Q., Tang, Y.J., Cheng, C., Cai, P.K.: Design of the explosion-proof detection integrated system based on PGNAA technology. J. Radioanal. Nucl. Chem. **322**, 1719–1728 (2019). https://doi.org/10.1007/s10967-019-06837-7
9. Marrone, P.A., Cantwell, S.D., Dalton, D.W.: SCWO system designs for waste treatment: application to chemical weapons destruction. Ind. Eng. Chem. Res. **44**(24), 9030–9039 (2015). https://doi.org/10.1021/ie0506670
10. Reber, E.L., Blackwood, L.G., Edwards, A.J., Egger, A.E., Petersen, P.J.: Idaho explosives detection system: development and enhancements. Sens. Imag. Int. J. **8**(3–4), 121–130 (2007). https://doi.org/10.1007/s11220-007-0038-7

Prevention and Treatment of Network Storm in Control Station of Digital I&C System in Nuclear Power Plants

Wang Dong(✉), Leng Qiang, and Xiang Yuan

China Nuclear Control Systems Engineering Co., Ltd., Beijing, China
wangdong@cncs.bj.cn

Abstract. In the design of non-safety I&C system of nuclear power plants, different safety classification and power supply sequence design need to meet the characteristics of system network redundancy and self-healing. Therefore, engineers often use ring network configuration in system network design. When the ring network design or network wiring is wrong, it is easy to cause a network storm, resulting in the abnormal operation of the main control unit of the first-floor control network control station, and the mis-operation of the control unit on the field equipment, resulting in nuclear power safety accidents. This requires that the main control unit of the control station could resist the attack of network storm. This paper provides a method to prevent network storm based on link layer. The abnormal packets are filtered in the network protocol layer of the control unit, and the network storm threshold detection algorithm is used to monitor the network storm attack in time, and the network loopback protection control unit is set. Experiments show that this method can effectively resist the attack of network storm. When the main control unit is attacked by network storm, it can normally complete the task of logic unit, ensure that the field instrument and control equipment is in safe working mode, and the system can automatically return to normal state after the network storm stops. At present, this technology has been realized and applied in the digital I&C system of nuclear power plants, which has good adaptability and broad development space.

Keywords: Nuclear power plants · I&C · network storm · link layer · threshold detection algorithm

1 Introduction

Digital I&C system is widely used in nuclear power plants with its high reliability, flexibility, coordination, complete control functions and easy maintenance [1, 2]. It includes DCS nodes such as field controllers, server, operator station and engineer station. These nodes are mainly distributed in different locations such as cabinet rooms, main control rooms and computer centers. Bidirectional data transmission between each control node and operation node is real-time based on the communication network with switchboard composed of these devices [3, 4].

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 351–359, 2023.
https://doi.org/10.1007/978-981-99-3455-3_35

The communication network is the basis and key of the safety-grade digital I&C system. The reliability design includes more redundant structures with loops. It inevitably leads to massive replication and propagation of data, and the result cause network outages, which is known as a network storm. Guaranteeing the reliability of network data communication and avoiding the problem of network storm, it is necessary to design the communication network of Digital I&C system in nuclear power plants and propose corresponding countermeasures [5].

The paper provides an identifying mechanism with the master processing unit based on the embedded operating system for resisting network storms. The master processing unit of the control station can guarantee that its logical operations can still work normally by improving the network link layer when a network storm occurs in the first layer of communication.

2 The Network Structure of DCS Systems and Analysis of Network Storm in Control Station

2.1 The Network Structure of DCS Systems

The non-safety DCS system for nuclear power plants is divided into two parts by safety classification: NC and NC*. NC* is the non-safety class with special requirements, such as independent power supply, seismic resistance, and routine test. The power supply can be divided into columns A and columns B. Each column is fed by the power supply system of the corresponding sequence. The equipment supplied by different power columns usually must be redundant. Some equipment requires special power supplies, for example emergency diesel engines and 72-h battery power. When the whole plants are in electrical loss condition, it needs to guarantee the continuous operation of the necessary functions.

To achieve the inter-device network communication, the switches are also divided into different security levels and power supply types to guarantee the independence of the corresponding functional groupings. It needs to consider the fact that the remaining network can still operate normally in the event of the loss parts of the network. For example, NC* can still operate normally after the loss of NC and column B can still operate normally after the loss of column A power. Based on the looped network, the switches in columns A and columns B are each configured as a small, looped network. The additional network connections are made between the specially powered switches.

The looped Ethernet is made by the hardware devices on the first floor and the man-machine software on the second floor via Ethernet switches. The system network is a redundant dual-looped network structure. The network A and network B are working simultaneously without any master-slave distinction. All service terminals, including operator stations, engineer stations, servers, communication stations and controllers, connected to the redundant network have two independent network interfaces. They are connected to the switches on the different loops. The network structure of DCS systems is shown as Fig. 1.

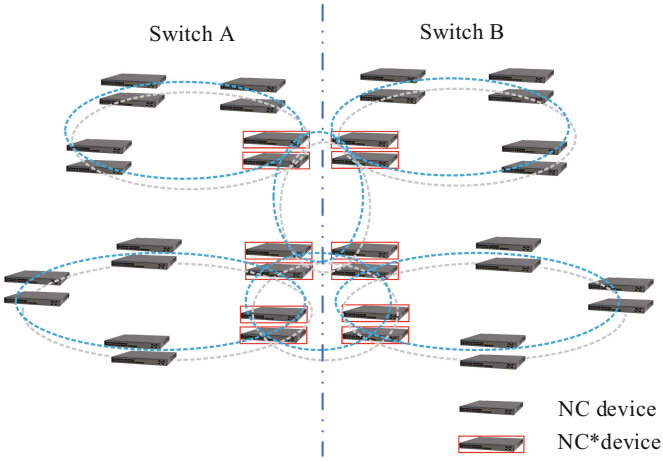


Fig. 1. The network structure of dcs systems in nuclear power plants

2.2 The Analysis of Network Storm

In the processing of the engineering system integration, the switches are equipped with the appropriate protection against network storms, which is the rapid spanning tree protocol (RSTP) set up at all switch connection ports. The protocol can be applied to a loop network to achieve path redundancy by means of a matching algorithm. The protocol prunes the loop network into a loop-free tree network, thus avoiding the proliferation of messages and infinite loops in the loop network.

When the devices on the loop network are working normally, the switch automatically sets a breakpoint through the RSTP protocol. When one device on the loop network is not working properly or an open circuit is formed, the network fault-tolerance mechanism can detect the network failure and connects the automatically set breakpoint. At the same time, the reserve link is activated instantly so that the network can work normally in the event of a transmission medium failure.

When the actual project is implemented, it is extremely vulnerable to several defects such as incorrect network connection, unconfigured or incorrectly configured switches. This can cause the network storm between the master processing unit on the ground floor of control station and the communication network on the second floor of software. In this case, the network between the master processing unit and the second layer communication is down state. According to the requirements of the nuclear power plants, the network failure of the master processing unit should not cause mis-operation of the field devices. This requires the master processing unit to be able to withstand network storms, while its logic operations and bus communication inputs and outputs with I/O modules are maintaining normal operation.

3 The Design of the Master Processing Unit Identification Based on Improved Link Layer

The paper proposed a master processing unit design method based on improved link layer, which consists of three main parts: the communication design of master processing unit, the design of network storm resilience mechanism and the processing of packet classification.

3.1 The Communication Design of Master Processing Unit

As shown in Fig. 2, it is the main components of the network structure of the master processing unit. The external communication network of the master processing unit is divided into three parts: communication with the second level man-machine software, inter-station communication and logic configuration software with the engineer station.

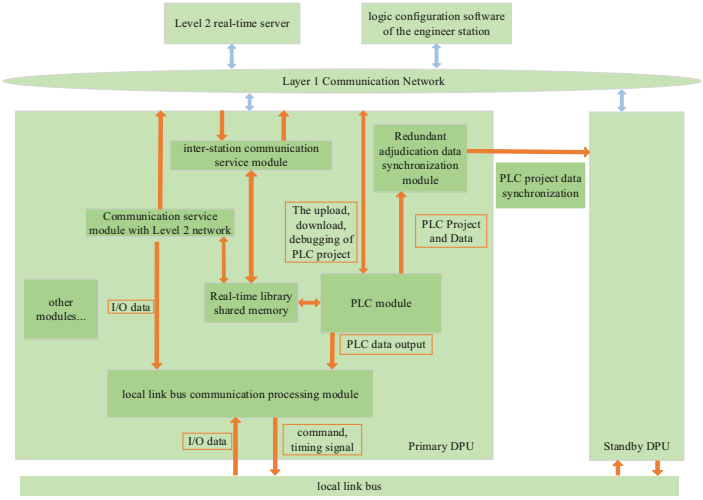


Fig. 2. The main components of the network structure of the master processing unit.

The master processing unit is connected to the switch via the Ethernet port. It is also unified with the other master processing units, the man-machine software unit on Level 2 and the engineer station to work within the ground floor communication network. The master processing unit acquires the logic configuration project via network communication with the engineer station. After starting the master processing unit, it runs the PLC module and uses local link communication to obtain the I/O module data within the control station. The I/O data is stored into the real-time library shared memory by means of logic operations. Other functional modules such as inter-station communication or communication modules on Level 2 can obtain data from the real-time library for external communication. The same mechanism is generally used for the external network communication processing of the main control processing unit to ensure uniformity in design development and maintenance.

3.2 The Design of Network Storm Resilience Mechanism

By monitoring the number of messages and data flow received by the Ethernet, a network storm is determined to occur on the network when it exceeds a threshold value.

The setting of the threshold is the basis for the determination of network storms. The data flow under normal operating conditions needs to be monitored, and it can identify the network flow under the busiest conditions when the master processing unit is in the maximum load capacity with communications on Layer 2, inter-station communications and engineering configuration download .

According to the tested, the maximum network usage of the one-layer network did not exceed 20% when the instrumentation and control system was working under maximum load conditions. Even under heavy load conditions such as using file transfer protocol (FTP) to transfer larger files or using logic configuration software to download PLC projects, the maximum flow did not reach 15%. Therefore, the program determines that if the flow of network packets reaches 20%, when the network load rate is 1s, it is determined that the conditions for the occurrence of a network storm have been met. The flowchart of network storm determination is shown in Fig. 3.

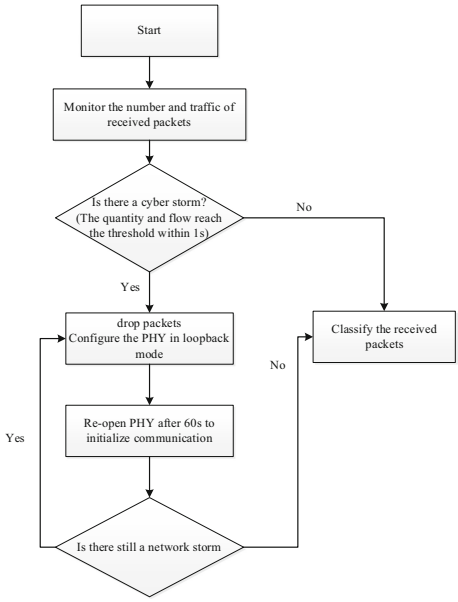


Fig. 3. The flowchart of network storm determination

When the network storm is occurred, the packets received by Ethernet are dropped directly and not sent to the TCP/IP stack to protect the embedded operating system stack program. The PHY of the master processing unit will be set to loopback mode. In this mode, the network communication will no longer respond to outside network data, only network communication data within the master unit will be processed. On a reduced system CPU usage, the system will no longer keep responding to interruptions from

incoming network communication packets. When a storm has occurred for a period, the master processing unit attempts to restore the network. If the network storm is detected to still exist, the network continues to be shut down and if the network is restored, the master processing unit can resume normal operation. This mechanism is effective against the network storm scenario that occurs briefly after the initial power-up of all switches when the entire instrumentation and control system is re-powered. Without this protection, the master processing unit has been tested in practice with a network stack crash due to a brief network storm.

3.3 The Processing of Packet Classification

To protect the network protocol stack, packets received by Ethernet are classified and processed as shown in Fig. 4. Ethernet packets are divided into Spanning Tree Protocol packets, ARP protocol packets and IP protocol packets, which has a different processing strategy. IP packets are also divided into ICMP packets, TCP packets and UDP packets, with slightly different processing strategies.

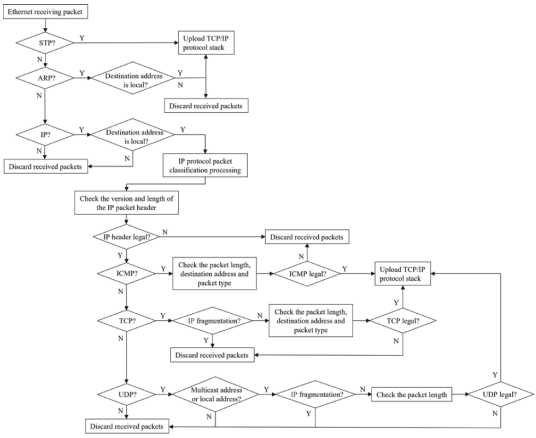


Fig. 4. The flowchart of packet classification and processed

By the classifying and processing of packets, the master processing unit can use flow thresholds to determine the network storms and protect the network. It can also provide protection against the flooding attacks of some network. When a network storm occurs, data such as illegal tree protocol packets, ARP protocol packets and IP protocol packets are transmitted across the network more than normal communication thresholds due to the mis-configuration of some network switches. It causes the master processing unit to be flooding attacks with ARP when attempting to re-communicate after the network storm has stopped, and it causes the network protocol stack to crash. The classification processing method solve the network anomaly attacks caused by network storms besides flow thresholds.

4 The Experimental Analysis and Results

Based on the network storm protection mechanism described above, the mechanism for running network communications of master processing unit based on the embedded real-time operating system is as follows. When the system starts up, embedded operating system generates the tUsrRoot task to implement the following functions.

Firstly, the network task queue is initialized, then a tNetTask is generated in netLibInit() to handle the tasks in the network task queue.The tNetTask task loads the network interface driver and defines the network driver device access point in tNetTask. By adding a pointer to the network interface driver in the embedded operating system, it points to the function that can complete sending the data to the upper layers of the MUX. The MUX adds the returned END_OBJ pointer to the structure chain table of END_OBJ. This chain table includes all the available network devices in the system. When returned from muxDevLoad(), the network device is ready for use.

The system implements network interrupt registration by calling the sysIntConnect() function, which is to register the network interface device for interrupt processing. When the system starts up, the device is used through the interrupt procedure. When a network device interrupt arrives, embedded operating system activates the interrupt service registered by the device driver and calls the netJobAdd() function. NetJobAdd() places the function call (including its parameters) into the task queue of tNetTask. Embedded operating system implements task-level network processing functions via tNetTask. After a call to netJobAdd(), when data is transmitted over the network, netJobAdd() starts the task to request resources for processing and generates system overhead.

The embedded operating system receives a large number of network packets in a short period of time and its netJobAdd() function is called frequently. This causes the network stack to crash, and the result is not operating properly in embedded operating system. The logic configuration processing of the main processing unit also does not work properly and trigger mis-operation of field devices. In some cases, the terminal will give error messages, and the error message is shown in Fig. 5.

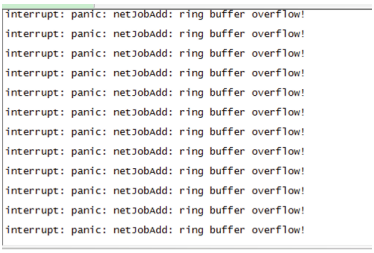


Fig. 5. The error message of embedded operating system

Ten network storm tests were conducted for the network components of embedded operating system under actual working conditions, and the actual test results are shown in Table 1.

As shown in Table 1, the network components of embedded operating system can withstand network storms and maintain normal operation within 3s. Therefore, the master

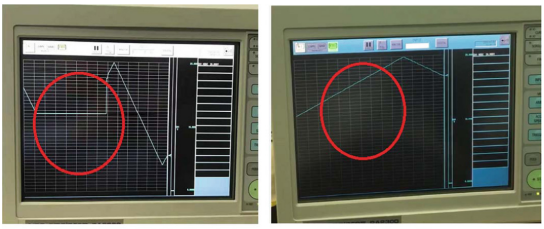
Table 1. The network component crash time from network storm generation to embedded operating system.

	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10
Time (S)	6.7	3.1	4.4	5.4	11.2	3.2	4.2	6.6	6.1	8.3

processing unit needs to identify network storms and initiate defensive measures as soon as possible within 3s.

Using the protection mechanism described in Sect. 2, the master processing unit in the control station can take the initiative to shut down the network in case of a network storm and guarantee normal logic operation. At the same time, it tries to open the network interface once every 60s to check whether the storm exists. If the network is back to normal, the system continues to work normally, and if the storm still exists, the network continues to be shut down to keep the field I/O modules running normally.

After testing, by following an AI acquisition through the analog output signal of the field configuration, the analog output is still continuous after the storm as shown in Fig. 6.



(a) (b)

Fig. 6. (a) Results of not implementing the network storm resilience mechanism. (b) Results of implementing the network storm resilience mechanism

5 Conclusion

The network structure of DCS system with different safety classification and power supply sequence of non-safety DCS equipment in nuclear power plants ensures the independence of corresponding classification and sequence, and the remaining networks can still operate normally in the case of losing some networks. Due to the need of network redundancy configuration, there is a physical loop in the network topology, resulting in the possibility of network storm. Based on this working condition, this paper puts forward the scheme of preventing network storm by the main control processing unit in the first layer control station of DCS system. Through the detection of the threshold, judge the occurrence of network storm, to take corresponding protective measures to ensure that the on-site processing side of the main control processing unit can still work normally.

This makes the on-site equipment of the nuclear power I&C system will not malfunction when it is attacked by the network storm, to improve the reliability of the nuclear power non safety I&C system.

References

1. LI, Z.: The network security analysis and protection strategy for AP1000 nuclear power plants fully digitalized instrumentation and control system. In: The Conference of ICSP'2013, pp. 621–624 (2013)
2. Yue, C., Wang, X.: Analysis communication network of digital instrumentation and control system in nuclear power plants. Plant Maint. Eng. **18**, 106-108 (2018)
3. Jiujin, A.I.: Cyber security analysis for nuclear power plants digital control system. Int. Combust. Engine Parts **03**, 137–138 (2017)
4. Wang, Y.: The fault analysis and preventive measures of DCS network broadcast storm in nuclear power plants. Elect. Saf. Technol. **18**(09), 12–14 (2016).
5. Zhan, X., Li, J., Liu, Y.: Research of network topology for nuclear power plants non-safety DCS. Autom. Panorama (006), 72–77 (2017)

Design of Robot System for Grinding the End of Reactor Core in Heavy Water Reactor Nuclear Power Plant

Jin Wang[1], Lixing Jin[1], Zhao Gao[2], Tengfei Cui[1], Hao Wen[1], and Xingguang Duan[1(✉)]

[1] Beijing Advanced Innovation Center for Intelligent Robots and Systems, School of Mechatronic Engineering, Beijing Institute of Technology, Beijing 100081, China
duanstar@bit.edu.cn

[2] Qinshan Nuclear Power, China National Nuclear Corporation, Zhejiang 314300, China

Abstract. The operation space for grinding the end of reactor core is very narrow in heavy water reactor nuclear power plant. The traditional manual grinding method are low efficiency, high radiation dose and poor grinding effect. This paper designed a teleoperation robot system for grinding the end of reactor core. The robot operates in a linear Delta configuration at the slave end. The robot system integrates irradiation camera and surface detection sensor which can provide compact configuration, real-time monitoring, precise positioning and good overall results. This design greatly reduces radiation risk and provides a safe and reliable automation system solution for grinding tasks.

Keywords: heavy water reactor · the end of reactor core · grind · teleoperation · linear Delta · robot

1 Introduction

If there is any defect on the sealing surface of the fuel channel in the reactor core of the heavy water reactor nuclear power plant, it will cause sealing failure, and the heavy water in the channel will leak, causing serious accident potential. Since the fuel passage is an inaccessible area during the normal operation of the unit, maintenance personnel can only enter it for inspection during each overhaul. This will lead to the failure to detect the end defects of reactor core in time, resulting in refueling interruption. In addition, when the defects of the channel sealing surface are found, the maintenance personnel use the self-made special grinding tools to grind the channel, which is not only time-consuming and laborious, but also very unfavorable to the radiation pollution control of the maintenance personnel in the environment of high dose and high pollution of the end of reactor core.

This research was supported by the National Key R&D Program of China (Grant no. 2019YFB1310500).

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 360–372, 2023.
https://doi.org/10.1007/978-981-99-3455-3_36

The dose control of personnel has always been the main objective of the nuclear power plant, while the end of reactor core is a high dose area, and work has always been strictly controlled in that area. How to reduce the working task and working time in the area of the end of reactor core is the most important part of dose control. In addition, it is also the goal to realize non shutdown maintenance in the inaccessible area of the end of reactor core in nuclear power plants at home and abroad. In view of the above problems, it is proposed to design and develop a robot system for grinding the end of the reactor core in heavy water reactor nuclear power plant. At the same time, after the preliminary feasibility analysis and the necessity evaluation of the robot system, it is considered that the project has practical application value and great design significance.

The main content of this paper is the design and analysis of robot system for grinding the end of reactor core in heavy water reactor nuclear power plant.

2 Functional Requirement Analysis of Grinding the End of Reactor Core in Heavy Water Reactor Nuclear Power Plant

2.1 Introduction of Heavy Water Reactor Nuclear Power Plant

Heavy water reactor is a reactor with heavy water as moderator. Therefore, it is referred to as heavy water reactor. It can directly use natural uranium as nuclear fuel. Heavy water reactor nuclear power plant is a kind of nuclear power plant with early development. Light water or heavy water can be used as coolant, which can be divided into pressure vessel type and pressure tube type. At present, only CANDU type pressure tube heavy water reactor nuclear power plant developed in Canada has achieved industrial scale promotion.

The nuclear power unit of heavy water reactor is a kind of reactor type with characteristics in the nuclear power family. Its technical characteristics include high inherent safety, high fuel utilization rate, diversified fuel utilization forms, strong adaptability for refueling without shutdown, and large-scale production of isotopes [1].

The benefits of non-shutdown refueling are manifold. It not only avoids the mandatory shutdown that requires a long time due to fuel replacement, but more importantly, it provides a powerful and flexible fuel management method, and also can timely take out the damaged fuel assembly from the core.

The nuclear fuel of CANDU Reactor is a simple and short fuel rod bundle assembly. Each fuel rod bundle is about 50 cm long and about 10 cm outer diameter. The reactor core is composed of 380 horizontal pressure tube fuel channels, and each pressure tube is generally equipped with 12 fuel rod bundle assemblies [2].

Qinshan Phase III (heavy water reactor) nuclear power plant project is a key construction project during the Ninth Five Year Plan period, and is the first commercial heavy water reactor nuclear power plant in China. Mature Canadian CANDU-6 heavy water reactor nuclear power technology is adopted in the project, and South Korea Yuecheng units 3 and 4 are taken as reference power plant.

2.2 Functional Requirement Analysis of Grinding the End of Reactor Core in Heavy Water Reactor Nuclear Power Plant

The on power fueling function of the heavy water reactor is mainly realized by the reload fuel machine located on both sides of the reactor end, and the fueling function is realized by clamping the reload fuel machine with the fuel passage. The action of the reload fuel machine depends on the action of the bridge and its components. As shown in Fig. 1.

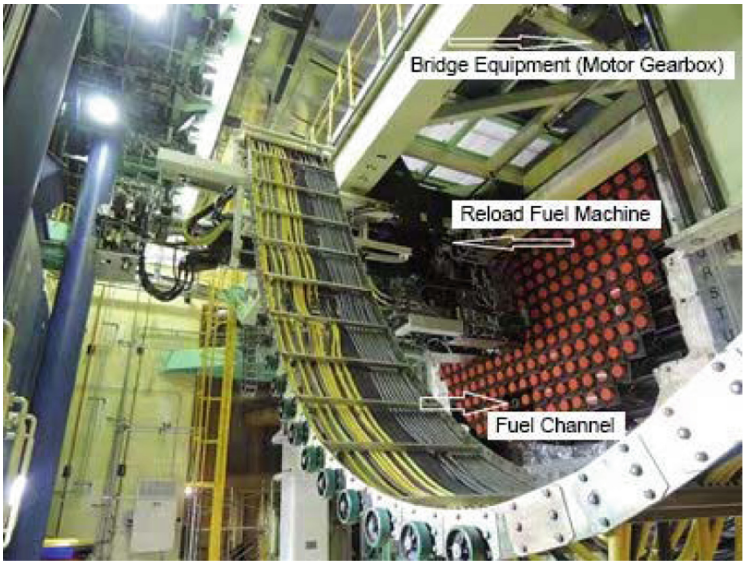


Fig. 1. Refueling Equipment of Heavy Water Reactor Nuclear Power Plant

When the reload fuel machine clamps the fuel passage, the sealing surface of the fuel channel contacts the central support cylinder inside the nozzle of the reload fuel machine to form a seal. When the sealing surface of the channel is defective, it will cause sealing failure and heavy water leakage in the channel. When the leakage reaches a certain value, refueling cannot be carried out [3].

Since the fuel passage is an inaccessible area during the normal operation of the unit, maintenance personnel can only enter it for inspection during each overhaul. This will make it impossible to judge whether the defect exists in the channel or on the reload fuel machine when the nozzle clamp fails, which will lead to misjudgment, fuel interruption and large consumption of static seal ring spare parts. In addition, when the defects of the channel sealing surface are found, the maintenance personnel use the self-made special grinding tools to grind the channel, which is not only time-consuming and laborious, but also very unfavorable to the radiation pollution control of the maintenance personnel in the environment of high dose and high pollution of the end of reactor core. It is difficult to ensure the consistency of shape accuracy and processing quality in manual grinding or polishing. The application of intelligent equipment has become a trend. The grinding robot system has been applied in many fields because of its high grinding accuracy and high consistency of machining quality.

In May 2015, «made in China 2025» mentioned intelligent manufacturing for the first time, opening the way of artificial intelligence in China. In July 2017, the State Council issued «the development plan for the new generation of artificial intelligence», which clearly pointed out the strategic goal of the development of the new generation of artificial intelligence in three steps. In 2019, the central comprehensive Deepening Reform Commission deliberated and adopted the «guiding opinions on promoting the deep integration of artificial intelligence and the real economy». In terms of national top-level design, more and more attention has been paid to artificial intelligence as a basic technology, which can penetrate into all walks of life, help traditional industries achieve leapfrog upgrading, and improve industry efficiency [4].

Considering the above factors, it is necessary to develop a robot system for grinding the end of reactor core in heavy water reactor nuclear power plant, and this robot system is the first set of this type of product in the world, with independent intellectual property rights.

The system should have following functions:

1) Grinding the end of reactor core in heavy water reactor nuclear power plant;
2) Visual observation of the end of reactor core in heavy water reactor nuclear power plant;
3) Scanning and measurement of roughness of the end of reactor core in heavy water reactor nuclear power plant.

The end of reactor core is ground, and the number is about 3–4 each time, and the position is random. Abrasive paper with different roughness is used for grinding the end surface of reactor core.

In consideration of electromagnetic compatibility and site conditions, referring to manual grinding tools, pneumatic grinding head or electric grinding head is selected as the grinding head, and pneumatic grinding head is preferred.

The equipment of the end of reactor core is invisible and most of them are key sensitive equipment. The reactor needs to be shut down for equipment maintenance. The system can directly observe the equipment status, quickly and accurately locate the defects that cannot be accurately located at ordinary times, and grind the sealing surface of the fuel passage to provide support for the safe and stable operation of the unit.

3 Analysis of the Design Scheme of Robot System for Grinding the End of Reactor Core in Heavy Water Reactor Nuclear Power Plant

3.1 Difficulty Analysis

Difficulty 1: How to position the end of reactor core by the robot system?
Difficulty 2: Judge whether the end of reactor core needs to be ground.
Difficulty 3: Judge whether the grinding is completed and meets the requirements.
Difficulty 4: The reserved installation space and operation space are very small. The distance from the reload fuel machine to the end of reactor core is only about 300 mm. It puts forward higher requirements for the compactness of the system scheme.

Difficulty 5: The non-parallelism between the grinding joint and the grinding end caused by the assembly error will greatly interfere with the lapping effect.
Difficulty 6: The volume of space mobile equipment is huge, and it is very difficult to feed and adjust the position by relying on the reload fuel machine.
Difficulty 7: At the moment of contact between the grinding joint and the end, rigid connection will lead to great impact force. The design scheme should have flexible cushioning function.

3.2 Function Realization Method Analysis

Thinking and analysis of the installation and positioning of the grinding robot system, First of all, we will introduce the important equipment in nuclear power plant - reload fuel machine. The reload fuel machine is the key equipment of the fuel operation and storage system (PMC system) of the nuclear power plant, It is mainly used to perform the work related to fuel assembly loading and unloading in the reactor building. The correct positioning of fuel assemblies in the reactor core is not only the core function of the reload fuel machine, but also the foundation of fuel handling in nuclear power plants. One of the bases for the reload fuel machine to achieve the above functions is to establish the core coordinates in its control PLC, which is the main content of the reload fuel machine core positioning test in the construction phase of the nuclear power plant.

The hardware part of the core positioning system of the reload fuel machine is mainly composed of PLC, frequency converter, absolute value encoder, etc. And all core coordinate parameters are stored in PLC. When the equipment is in operation, after the movement target position is given, the core positioning system will read the current position value measured by the encoder in real time, and control the frequency converter to drive the trolley to move after comparing with the target position value until the reload fuel machine moves to the error range of the target position [5].

The reload fuel machine is the most critical equipment in the heavy water reactor refueling equipment, The two reload fuel machines cooperate with each other to complete the refueling task of the unit. The reload fuel machine is operated by the operator in the main control room remotely operating the computer, Except for the refueling operation on the reactor, the rest of the time is spent in the refueling maintenance room (inside the reactor containment) where personnel can normally enter.

Under normal circumstances, the refueling maintenance room and the refueling room (the end of reactor core) are isolated by a screen door weighing about 180 tons. The reload fuel machine is suspended on the pulley and transmitted to the refueling room along the guide rail driven by the pulley. The vertical movement is realized by the bridge moving up and down. With the cooperation and assistance of the bridge, pulley, catenary and other systems, the transfer and positioning functions of the reload fuel machine are completed.

Although the reload fuel machine is huge and complex in structure, it can complete various very delicate actions under the control of the control system, realize loading, transfer, fuel string separation, unloading and other functions, its function and accuracy are no less than a modern robot. The whole system is composed of tens of thousands of parts and components. 8500 actions are required to complete the refueling task of a fuel

channel. Failure of any part or action will lead to interruption of the refueling process and even fuel damage.

As a special device of the heavy water reactor, the reload fuel machine is the guarantee for realizing the feature of refueling without shutdown of CANDU-6 heavy water reactor, Its unique fuel operation system and unique refueling operation mode are also not available in other reactor types, At present, there is almost no mature experience can be used for reference in China [6].

The commonly used grinding machines are divided into pneumatic and electric ones according to the driving mode. The choice of grinder is actually the choice of grinder performance. Generally speaking, the selection of the grinder is determined by the sealing surface and material to be ground, as well as the site environment and installation mode.

3.3 Advantage Analysis

1) During the overhaul, The γ dose rate is 200–300 μ Sv/h within 1 m of the end of reactor core, the use of robots instead of manual can greatly reduce the dose received by personnel at the end of reactor core or even eliminate the dose irradiation.
2) The robot replaces the manual, and the grinding is more stable and accurate, which can avoid the uneven grinding force caused by human factors and the secondary damage of the channel sealing surface caused by angular deviation.
3) In case of emergency during the normal operation of the unit, the robot can also enter the end of reactor core with the reload fuel machine to grind and repair the channel.

4 Design of Robot System for Grinding the End of Reactor Core in Heavy Water Reactor Nuclear Power Plant

According to the functional analysis, the robot system for grinding the end of reactor core in heavy water reactor nuclear power plant is mainly divided into the grinding part, the video part and the plane measurement part. The grinding part is the main part of the overall tool, which will be described below.

4.1 Grinding Robot Mechanism Function

The grinding robot system is fixed in a way that the tail is designed with the same overall dimension as the grinding end interface. It is supported on the reload fuel machine, and the reload fuel machine is used to locate the position to be grinded [7]. The interface part is shown in Fig. 2.

According to the demand analysis, the functions and actions of the grinding mechanism are divided into the following parts:

1) Moved to the worn end of reactor core by the reload fuel machine, complete large range translation and positioning;
2) Secondary accurate alignment by grinder, cover the end of reactor core with the grinding head;
3) Moving forward by the grinder, elastic end start pressure pre tightening;

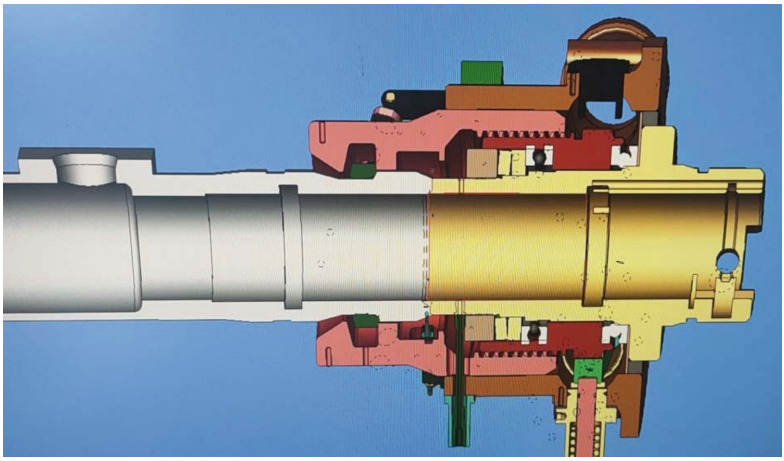


Fig. 2. The Interface of Robot System for Grinding the End of Reactor Core in Heavy Water Reactor Nuclear Power Plant

4) Grinder adaptive end face angle, adjust the angle offset caused by assembly error and gravity;
5) The reload fuel machine moves to the next end of reactor core in turn, complete all rough grinding procedures of the end of reactor core;
6) The reload fuel machine moves to the sandpaper replacement position, automatic prepressing to replace fine sandpaper;
7) Repeat the above process until the fine grinding of all worn ends of reactor core is completed.

To sum up, the grinding mechanism has three features: 3 translational degrees of freedom, Flexible end connections provide preload, Angle adaptation. According to these requirements, the designed grinding mechanism adopts a linear delta mechanism, which is compact and suitable for the current environment. It has 3 degrees of freedom of spatial translation, stable posture of the moving platform, and meets the functional requirements. As shown in Fig. 3.

The installation position of the grinding head adopts the spring bed structure to meet the angle adaptation and flexible preloading. When working, the grinding head is installed on the reload fuel machine, and the reload fuel machine is positioned at the interface to be grinded. The grinding robot then fine tunes the position of the grinding head through the translation of the linear Delta mechanism to align it with the end of reactor core to be grinded. Through the translation of linear delta mechanism, video observation and end profile measurement can also be carried out. As shown in Fig. 4.

4.2 Video Part (Vision Sensor)

Radiation resistant cameras are selected for the video part. The selection of radiation resistant cameras refers to the use of nuclear power plants. The camera shall be small in size and suitable for placing on the actuator or tool for inspection and monitoring in

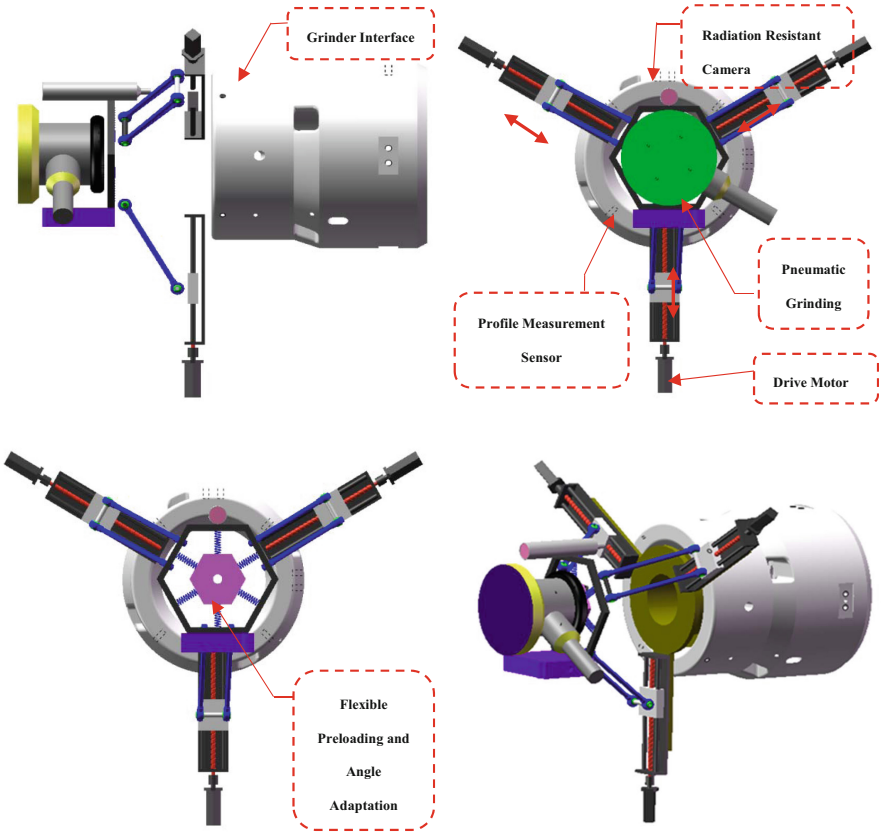


Fig. 3. Schematic Diagram of Mechanism of Robot System for Grinding the End of Reactor Core in Heavy Water Reactor Nuclear Power Plant

confined space. The monitoring area of the camera can be easily adjusted by changing the lens and setting the focal length from the outside.

4.3 Measurement Part

The sensor is installed on the grinding tool. It can scan the end of reactor core before and after grinding, establish a 3D model of the end of reactor core, analyze the situation of the end of reactor core before and after grinding, and compare the grinding thickness.

This part also needs to be verified by repeated tests during the specific implementation of the project.

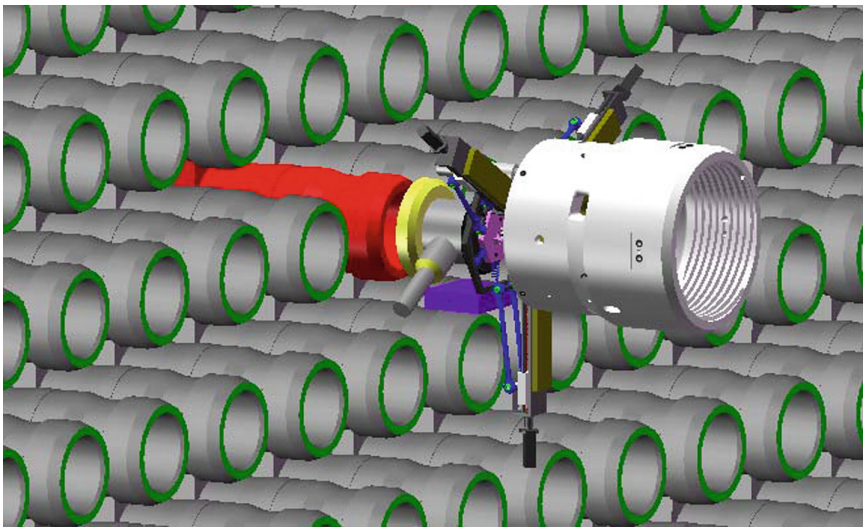


Fig. 4. Working Diagram of Robot System for Grinding the End of Reactor Core in Heavy Water Reactor Nuclear Power Plant

4.4 Project Technology Breakthrough

1) The Scheme Design Based on Linear Delta Parallel Mechanism Meets the Requirements of Narrow Space Operation Tasks

In view of the narrow space in the actual working environment and the difficulties in equipment installation and operation, the system adopts a new linear delta mechanism, which distributes the driving device on the vertical surface, greatly saving the installation space and providing a compact solution; This configuration can provide 3 spatial translational degrees of freedom to meet the task requirements of precise positioning and work feeding of the grinder. The attitude of the moving platform remains constant during the movement, providing stable installation conditions for the irradiation camera and the end of reactor core detection sensor; The flexible connection of the integrated spring on the moving platform can greatly reduce the contact impact, and realize the adaptive alignment of the end of grinder and the end of reactor core, avoiding the uneven grinding caused by attitude deviation [8].

2) Real Time Monitoring of The End of Reactor Core Condition and Automatic Recognition of Damage Based on System Multi-sensor Fusion

The system has built-in radiation resistant camera (visual sensor) and end detection sensor, which can monitor the end state in real time during reactor operation and grinding operation. The off-line database of the end of reactor core state is established by using the data collected by the sensor, and the current end of reactor core image data is calculated and analyzed by an intelligent algorithm to determine the wear state in real time, so as to

realize the real-time monitoring of the end of reactor state and the automatic recognition of the damage situation.

3) Stable and Reliable Automatic Intelligent Operation System Integration and Function Development

The proposed system provides a compact, automatic, intelligent and safe operation scheme, and realizes system integration and function integration through sensor fusion and control system development. The operator can remotely inspect and grind the end of reactor core, which is far away from the irradiation environment and reduces the irradiation dose and risk.

5 Dynamic Modeling of Robot System for Grinding the End of Reactor Core in Heavy Water Reactor Nuclear Power Plant

The robot system for grinding the end of reactor core in heavy water reactor nuclear power plant is a three degree of freedom delta parallel robot. The mechanism characteristics of parallel robot make it have unique kinematic and dynamic characteristics [9]. Dynamics research mainly describes the relationship between the torque and motion of each joint of the robot, which plays a very important role in the performance analysis and actual motion control of parallel robots [10].

In an ideal state, the output torque of the delta parallel robot can be divided into three items from the perspective of dynamics: inertia torque, velocity torque and gravity torque.

Moment of inertia refers to the inertia of each robot arm in motion due to its own mass; The speed torque is related to the moving speed of the robot; The gravitational moment is the gravity of the robot itself and is related to the position and attitude of the moving platform [11].

The dynamic expression of delta parallel robot is:

$$\tau_n + \sum_{i=1}^{3} \tau_{a,i} + \sum_{i=1}^{3} \tau_{bc,i} = 0 \tag{5.1}$$

In Eq. (5.1): τ_n refers to the force acting on the moving platform, $\tau_{a,i}$ represents the toque of the active arm, $\tau_{bc,i}$ is the force of the driven arm.

For the delta robot, its own gravity G_n and inertial force F_n play a role in the translational motion of the moving platform.

$$G_n = m_n[00 - g]^T \tag{5.2}$$

$$F_n = m_n \ddot{x}_n \tag{5.3}$$

The sum of the acting moments of these two forces on the force of the moving platform can be obtained through the Jacobian matrix:

$$\tau_n = J^T(m_n \ddot{x}_n - G_n) \tag{5.4}$$

The force of delta robot's active arm, which only rotates:

$$\tau_a = I_A\ddot{q} - G_A - \tau \tag{5.5}$$

where τ is the joint driving torque,

$$G_A = (m_A + m_C)r_{gA}g\left[\cos q_1 \cos q_2 \cos q_3\right]^T \tag{5.6}$$

$$r_{gA} = l_1\frac{\frac{1}{2}m_A + m_C}{m_A + m_C} \tag{5.7}$$

Force of driven arm of Delta robot:

$$\tau_{bc,i} = \frac{1}{3}m_{bc}\left[J^T\left(\ddot{x}_n + \frac{1}{2}a_{1,i}\right) + J_{1,i}^T(\frac{1}{2}\ddot{x}_n + a_{u,i})\right] - \frac{1}{2}(J + J_{u,i})^T m_{bc}\begin{bmatrix}0\\0\\-g\end{bmatrix} \tag{5.8}$$

Acceleration at the upper driven arm:

$$a_{u,i} = -{}_i^R R\left[\begin{bmatrix}l_1\sin q_i\\0\\l_1\sin q_i\end{bmatrix}\ddot{q}_i + \begin{bmatrix}l_1\cos q_i\\0\\-l_1\cos q_i\end{bmatrix}\dot{q}_i\right] \tag{5.9}$$

The joint driving torque is:

$$\tau = I_A\ddot{q} + J^T m_n\ddot{x}_n - G_A - J^T G_n + \sum_{i=1}^{3}\tau_{bc,i} \tag{5.10}$$

According to the previous analysis of inertia and mass, formula 5.10 is adjusted as:

$$\tau = I_B\ddot{q} + J^T m_{na}\ddot{x}_n - J^T m_{ng}\left[00 - g\right]^T - G_{ag} \tag{5.11}$$

In the formula:

$$I_B = I_m + l_1^2(\frac{m_a}{3} + \frac{2m_{bc}}{3} + m_c) \tag{5.12}$$

$$m_{ng} = m_n + \frac{3m_{bc}}{2} \tag{5.13}$$

$$G_{ag} = l_1(\frac{1}{2}m_a + m_c + \frac{1}{3}m_{bc})g\left[\cos q_1 \cos q_2 \cos q_3\right]^T \tag{5.14}$$

$$\ddot{x}_n = \frac{d^2 f(q)}{dt^2} \tag{5.15}$$

After finishing, formula 5.16 is obtained:

$$\tau = (I_B + J^T m_{na}J)\ddot{q} + J^T m_{na}\dot{J}\dot{q} - J^T m_{ng}\left[00 - g\right]^T - G_{ag} \tag{5.16}$$

In formula 5.16 , $(I_B + J^T m_{na} J)\ddot{q}$ is the inertia term, $J^T m_{na} \dot{J} \dot{q}$ is the speed term, $J^T m_{ng}\left[00 - g\right]^T$ and G_{ag} is the gravitational term. These three items can be calculated by the previous model, so the delta robot dynamics model has been completed [12].

Dynamics research is very important for designing the mechanical system of parallel robot and realizing the precise control of the robot. In this paper, the dynamic model of the 3-DOF parallel robot is established based on the delta robot mechanism. Thus, it provides theoretical support for the follow-up implementation of the robot system for grinding the end of reactor core in heavy water reactor nuclear power plant, and provides certain experimental support for the related research of the robot system for grinding the end of reactor core in heavy water reactor nuclear power plant in the future. It has important practical significance [13].

6 Summary

At present, there is no relevant equipment for end equipment inspection and channel grinding in domestic and foreign heavy water reactor nuclear power plants during unit operation. After the feasibility, practicability and stability of the robot system designed in this project are fully verified, it can be popularized and used as a fully independent intellectual property equipment to other nuclear power units of heavy water reactors around the world.

References

1. Chen, B.: Brief introduction of heavy water reactor nuclear power plant technology. Energy Knowl. **3**, 47–48 (1996)
2. Kan, X.: Development strategy of heavy water reactor nuclear generator set in current nuclear power market. Shanghai Jiaotong University, ShangHai (2009)
3. Xi, M., Mi, L.: Fuel operation system of CANDU6 unit in Qinshan phase III project. Nucl. Sci. Eng. **21**(2), 176–181 (2001)
4. Hua, Z., Fan, J., Guo, R., Wang, Y., Xiaoxiang, W.: Application of artificial intelligence technology in thermal power industry. China Electric Power **54**(7), 198–207 (2021)
5. Cheng, W., Liyan, X., Wang, L.: Improvement of nuclear power plant reload fuel machine core positioning test method. Lifting Transp. Mach. **12**, 164–167 (2017)
6. Liu, D.: Application of reliability centered maintenance in the loader system of Qinshan Phase III heavy water reactor nuclear power plant. Shanghai Jiaotong University, ShangHai (2006)
7. Lu, X., Wang, J.: Research on improvement of reactor core positioning system in Daya Bay Nuclear Power Station. Power Equipment **12**(9), 60–62 (2008)
8. Weng, Z., Liu, S., Xiaoyu, W., Hanghang, Y., Wang, W., Zhu, F.: A new type of vibration isolation platform with quasi zero stiffness for 3-D translational freedom delta mechanism and its characteristics. Acta Armamentarii **3**, 667–675 (2022)
9. Tsai, L.W.: Robot Analysis: The Mechanics of Serial and Parallel Manipulators, pp. 5–40, 55–60. Willey (1999)
10. Dong, X.: Research on Key Technologies of 3-DOF Translational Parallel Robot. Harbin Institute of Technology, ShenZhen (2010)
11. Li, X.: Research on control method of 3-DOF delta robot. Liaoning University of science and technology, AnShan (2019)

12. Wang, W.: Dynamics simulation of an autonomous grinding robot. J. Changchun Inst. Eng. (Nat. Sci. Ed.) **3**, 30–33 (2014)
13. Rachedi, M., Bouri, M., Hemici, B.H.: Feedback control for parrallel mechanism and application to delta robot. In: Control & Automation (2014)

Research on Common Problems of Safety-Grade Batteries in Nuclear Power Plants

Zi-Xi Chen, Jia-Kang Zheng(✉), Jing Kong, Jing-Bin Liu, and Ning Qiao

Nuclear and Radiation Safety Center, Beijing 100082, China
zhlc135@sina.com

Abstract. The battery supplies power to the safety-level equipment and instruments of the nuclear power plant in the event of a power outage in the entire plant. At present, many nuclear power plants in China have the problems of unmeasured connection resistance, lack of quarterly inspection and lack of operation test in the three links of battery installation and debugging, daily maintenance and regular test. This leads to the shortening of the life cycle of the battery due to the lack of effective measurement, maintenance and testing, and the premature replacement of the battery is a waste of resources and increases the cost of equipment.

Keywords: Battery. · Connection resistance · Quarterly inspection · Run the test · Solution

1 Introduction of Lead-Acid Battery

The DC power supply system of the nuclear power plant supplies power for control, signal, protection and automatic devices (collectively referred to as control loads), as well as electromagnetic closing of circuit breakers, DC motors, inverters, emergency lighting (collectively referred to as power loads), etc., involving emergency diesel engine control Important loads such as disks, nuclear reactor protection groups, rod power circuit breaker panels, shutdown circuit breakers, and nuclear instruments play a vital role in the safe and stable operation of nuclear power plants [1]. The battery is an important equipment in the DC power system of the nuclear power plant. During normal operation, the battery is always in the floating charge state, the charger supplies power to the downstream load, and provides a floating charge current for the battery. When the battery is discharged for a short time to provide inrush current, so that the voltage of the system remains stable; when the charger itself fails or loses the AC power supply, the charger stops working and the battery starts to discharge to ensure that the downstream load can be supplied within a specified time. Stable power supply ensures continuous power supply for important loads and ensures the safety of nuclear power plants [2].

Commonly used batteries include lead-acid batteries, nickel-cadmium batteries, nickel-hydrogen batteries, and lithium-ion batteries. Among them, lead-acid batteries have mature technology, high reliability, low price, high and stable discharge voltage, and large discharge current. Therefore, lead-acid batteries are generally used as backup power sources in the DC system of nuclear power plants.

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 373–377, 2023.
https://doi.org/10.1007/978-981-99-3455-3_37

The positive active material of the lead-acid battery is lead dioxide, the negative active material is spongy lead, and the electrolyte is dilute sulfuric acid. When the electrolyte is injected, the positive electrode generates a higher potential (about 1.69 V), while the negative electrode generates a lower potential (about −0.358 V), the potential difference between the positive and negative electrodes is the electromotive force of the battery. During discharge, the lead dioxide and spongy lead of the positive and negative electrodes react electrochemically with the dilute sulfuric acid solution to generate lead sulfate. The electrochemical reaction equation of lead-acid battery is as follows:

$$\text{Positive} : PbO_2 + 3H^+ + HSO_4^- + 2e^- \rightleftarrows PbSO_4 + 2H_2O \tag{1}$$

$$\text{Negative} : \text{Pb} + HSO_4^- \rightleftarrows PbSO_4 + H^+ + 2e^- \tag{2}$$

$$\text{Overall reaction} : PbO_2 + 2H_2SO_4 + Pb2 \rightleftarrows PbSO_4 + 2H_2O \tag{3}$$

Although the basic principles of lead-acid batteries are the same, after more than 150 years of development, lead-acid batteries have produced many types. Classified by use, there are mainly starting, traction, stationary, and other uses. Classified by air-tightness, there are mainly open type, acid-proof exhaust type, acid-proof hydrogen elimination type, valve-controlled closed type, etc. According to the state of electrolyte, there are mainly rich liquid type and lean liquid type [3].

2 Common Problems of Safety-Grade Batteries

2.1 The Problem that the Connection Resistance Measurement of the Safety-Grade Battery is not Carried Out After the Commissioning and Installation

After the battery is sent from the manufacturer to the nuclear power site, it must be stored for a long time until the site meets the installation conditions before installation. During installation, the poles and connecting strips need to be wiped to meet the installation requirements, and the measurement of connection resistance is precisely [4, 5]. It is an effective method to judge whether the installation is correct, but the nuclear power field engineer will not measure the connection resistance of the battery, which causes the following common problems:

(1) Whether the battery is installed correctly.
(2) The original record of the initial value of the battery connection resistance of the nuclear power plant, which makes it difficult to judge whether there is looseness between the batteries in the future.
(3) If the connection resistance of the battery increases due to improper installation, the connection will be overheated due to the effective connection, resulting in a heat accumulation effect. Because the battery is the only electrical equipment that undergoes thermal aging in a mild environment, the life of the battery will be greatly reduced, and in severe cases, there may even be a risk of fire.

2.2 The Problem of the Lack of Quarterly Inspections in the Daily Regular Inspection of Safety-Grade Batteries

After the battery is charged and discharged for the first time, the nuclear power plant needs to formulate an effective battery maintenance program to maximize the battery life, prevent avoidable failures and reduce premature replacement to ensure that the battery can meet the design requirements. However, the lack of quarterly inspections in the actual maintenance of the power plant causes the nuclear power plant to check and record the voltage and electrolyte specific gravity of a single battery that is not an indicator battery during the annual inspection (if the float current of the battery is not used to monitor the state of charge) and electrolyte temperature. This will prolong the time for discovering the abnormality of the above three data of non-indicating battery, thus detracting from the life of the battery.

2.3 The Problem of Lack of Operational Tests in Periodic Tests of Safety Grade Batteries

After the nuclear power plant conducts a battery capacity test performance test within the first two years of battery operation, a performance test is performed every 5 years (the performance test interval should not be greater than 25% of the expected operating life). During the test interval, the operation test is regularly arranged arbitrarily, and the battery performance test alone cannot accurately reflect the actual level of battery maintenance, and the deterioration of battery performance cannot be found in time.

3 Solution

3.1 Solution for Safety-Grade Batteries Without Connection Resistance Measurement After Commissioning and Installation

There are clear requirements for the battery to measure its connection resistance during installation. According to IEEE484, during the operation of the nuclear power plant battery after commissioning and installation, a micro-ohmmeter is used to measure and record the connection resistance between the batteries. This verifies the correctness of the initial installation and provides a reference for future maintenance testing; review records of resistance measurements for each connection, sorted by connection type (ie: battery-to-battery, tier-to-rack, or rack-to-rack). Calculate the average resistance value for each type of connection. Identify the connections whose measured resistance value is greater than 10% of the average resistance value of each type of connection or which is greater than the average resistance of a certain type of connections plus 5 $\mu\Omega$, and these connections should be reconnected and measured.

The measurement of battery connection resistance is not only an important detection method to detect whether the battery is installed correctly and whether the various parts of the battery are in good condition without rust, but also provides original records for the subsequent judgment of whether the connection parts of the battery are loose to facilitate proofreading.

In this paper, it is suggested that the connection resistance of each battery should be measured and recorded for the Hualong nuclear power unit after the battery is installed, and the original record is left for the convenience of subsequent proofreading.

3.2 Solutions for Safety Grade Batteries Missing Quarterly Inspections in Routine Periodic Inspections

During the operation of the battery at the nuclear power site, it is necessary to conduct regular tests to verify whether the performance of the battery meets the requirements. According to the requirements of IEEE450 battery maintenance, monthly inspection, quarterly inspection, annual inspection and special inspection should be carried out for the battery. The quarterly inspection requires checking and recording the voltage of each battery, the specific gravity of 10% of the battery electrolyte in the battery (if the float current of the battery is not used to monitor the state of charge), and the temperature of at least 10% of the battery electrolyte in the battery.

If quarterly inspections are not carried out, the nuclear power plant staff will only monitor the above three data indicating the battery, rather than indicating that the battery can only be found during the annual inspection if these three data are abnormal. Thus, the time to find non-indicative battery abnormality is prolonged, thereby depleting the life of the battery.

This paper recommends adding quarterly inspections to the battery maintenance program of the Hualong nuclear power plant to more effectively monitor the status of non-indicating batteries, to maximize battery life, prevent avoidable failures and reduce premature replacement.

3.3 The Solution for the Lack of Running Test in the Periodic Test of Safety Grade Battery

According to IEEE450, the battery performance test is a test to measure the battery capacity, using a constant current or constant power load, and the discharge rate is equal to the battery rating specified by the manufacturer corresponding to the selected test time; the operation test is to verify that the battery has the ability to meet its working cycle, The discharge rate and test time are consistent with the actual working cycle of the battery. Running tests are special battery discharge tests used to determine whether their duty cycle requirements are met. System designers should develop test procedures and acceptance criteria prior to running tests. The tests shall be carried out under actual operating conditions without temperature or aging corrections for the tests.

The battery itself has a certain margin considering factors such as temperature, load growth and aging, which is used to make the battery meet the requirements of the working cycle during the entire working life. During the severe part of the duty cycle, the trend of battery voltage will provide the user with a basis for predicting when the battery will no longer meet the design requirements. Successful test results can be used to evaluate the performance of the battery and its degree of deterioration.

In this paper, it is suggested that the battery of Hualong nuclear power plant should carry out the operation test before the two performance tests of the battery, so as to verify that the working conditions of the battery on site meet the requirements of the working cycle.

4 Safety Significance

In addition to supplying power to the control and signal systems, the battery also generates uninterrupted 220 V AC power through the DC/AC inverter after the loss of off-site power and on-site AC power systems. Therefore, as 1E-level electrical equipment, the battery plays an important role in the retreat of the unit and the safe shutdown of the reactor.

This technical opinion analyzes the current problems of nuclear power plants from three aspects of battery on-site commissioning and installation, daily maintenance inspection and regular testing, and describes its technical requirements according to regulations. Finally, improvement suggestions are put forward for the Hualong nuclear power plant, so as to prolong the life of the battery in the nuclear power plant, effectively prevent the risk of battery failure, and reduce the cost of premature battery replacement in the nuclear power plant.

References

1. Bai, Z., et al.: Power Engineering DC System Design Manual, 2nd edn. China Electric Power Press, Peking (2009)
2. Zhu, S.-R.: Battery Brochure. Tianjin University Press, Tianjin (1998)
3. GB/T 14546-2008 Design criteria for safety-grade DC power systems in nuclear power plants
4. IEEE450-1995 Recommended Practice for Maintence, Testing, and Replacement of Vented Lead-Acid Batteries for Stationary Applications
5. IEEE484-1996 Recommended Practice for Installation Design and Installation of Vented Lead-Acid Batteries for Stationary Applications

Research and Application of Key Technologies of Nuclear Power Civil Engineering Design Platform

Fenghua Guan(✉), Dong Zhao, Zhigang Zhou, and Liang Fu

State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment, China Nuclear Power Engineering Co., Ltd., Shenzhen 518172, Guangdong, China
namegfh@163.com

Abstract. The civil engineering design of nuclear power plants has a long cycle, involves many disciplines, and the design process is complex. The traditional design methods and technical means are backward, mainly two-dimensional design means. The design activities are lack of specifications and coordination. The design data are stored and managed in the form of drawings, tables, calculation instructions, etc., scattered on personal computers, and difficult to share and reuse. This paper has carried out the research on the key technologies of nuclear power civil engineering design. It has proposed to manage design tasks in the way of task map. It has realized the standardized management of design tasks and calculation activities. It has unified management and scheduling of nuclear power civil engineering design tools. It has opened the data connection with external systems. It has eliminated information islands. It has realized the structural management and intelligent application of design data. It has constructed the refined collaborative design of nuclear power civil engineering, It has strengthened business collaboration. It has controlled design process and accumulated design data among various disciplines, improved the efficiency of nuclear power civil engineering collaborative design. It has not only saved costs, but also laid a solid foundation for nuclear power projects to go abroad.

Keywords: Nuclear power plant · Civil design · Collaborative design · Structured management · Standardized management

1 Introduction

Civil engineering design of nuclear power plant includes nuclear island structure, conventional island and BOP structure, architecture, hydraulic structure, general drawing and plant site. It has a vital impact on the construction, operation and safety of the nuclear power plant. The finished product entity is the carrier of the owner, material, flow and field of the nuclear power plant. It has interface information exchange with all disciplines of the power plant. The design task is heavy and the data volume is large. With the development of science and technology, digital collaborative design is the inevitable trend of future nuclear power plant design. The three-dimensional information model based on the concept of life-cycle information management is the fundamental element of intelligent power plants.

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 378–386, 2023.
https://doi.org/10.1007/978-981-99-3455-3_38

After years of development, the civil engineering design of the domestic nuclear power industry has accumulated rich design experience the design method and design theory have been very mature, and special design tools have been improved through self research, scientific research, procurement, etc. However, the civil engineering design is still mainly based on discrete software design. The digital collaborative design function is weak, and the collaboration and sharing of data and knowledge are poor. Some professional designs still rely on traditional design review, manual experience and a small amount of theoretical calculation methods. The repetitive workload is large, the management is difficult, and the efficiency is low.

In recent years, with the continuous development of electronic information technology and the Internet, the engineering construction field is entering the digital era in an all-round way [1]. In all aspects of civil design of nuclear power plants, the sources of data are diverse. Designers need to interact with multiple systems, such as the data extraction system, the design and production management platform, and the high-performance computing platform. More importantly, the design data storage, process data interaction, data level results release, and project management based on a unified data source have not yet been realized [2]. At present, some mature and effective management models or methods in nuclear power projects are often constrained by the loss of core talents and cannot be effectively retained and promoted. If a set of standardized management processes can be realized, a reproducible standardized management model can be realized, and the overall management ability of the enterprise can be improved, the dependence on core talents will be greatly reduced [3]. With the improvement of users' requirements for products and the intensification of market competition, the concept of product life cycle management and related network technologies have been further developed [4–6]. How to use a unified platform to effectively integrate these numerous systems has become very important.

In view of the drawbacks and shortcomings of traditional civil design, this paper makes full use of existing resources, proposes to standardize the civil design process driven by process and data. It realizes the integration and unified call of design tools, structural organization of data and intelligent application of experience and knowledge. It achieves the goal of refined collaborative design of nuclear power plant civil engineering. This method effectively solves the complex design collaboration problem and information island problem of multi discipline and multi discipline in the nuclear power civil engineering design process, realizes the collaborative engineering design process of civil, the traceability of design results, and the collaboration between design disciplines, improves the efficiency of nuclear power civil engineering design, and saves costs.

2 Key Technology Research

2.1 Standardized Management of Design Tasks and Calculation Activities

As the source of design activities, design task management is very important. There are many nuclear power civil engineering design disciplines (see Fig. 1). The design types and design results involved in each discipline are complex, covering a long design cycle and a wide range. The design task management mode has great defects. The design input is mainly based on document submission, and is modeled by specialized personnel.

The existing platform is not fully used for data exchange. The layout, calculation and drawing models are disconnected. The design process relies on the task list or oral communication of design indicators, and the design knowledge and experience are recorded by themselves. Drawings, forms and process achievements are stored locally without centralized control.

By sorting out the design achievements of each design stage of each discipline, this paper creatively manages the design tasks by means of task maps, and displays the progress of current design nodes with node colors and percentages to visually display the design progress. Tasks are associated with design activities and design results, so as to realize the standardized management of design tasks, calculation and analysis processes and design results. The design task is managed through task map, and the complex design task is decomposed, making the civil design process clearer and clearer. At the same time, it also provides reference for the civil design process of other nuclear power projects to achieve the accumulation and sharing of experience.

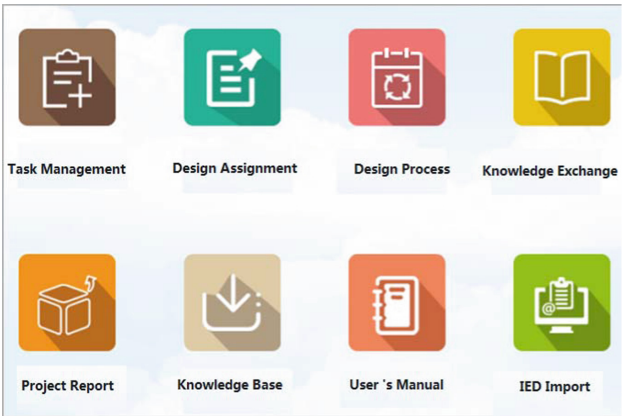


Fig. 1. Main Interface

The platform task flow, first create top-level tasks, and then assign tasks according to the individualization of each discipline (see Fig. 2). Designers receive design tasks, refer to the platform knowledge base online, and finally close the design tasks through the editing and proofreading process. After receiving the task, designers can carry out relevant design work in the workbench. The workbench contains sub modules such as task information, design input, design tools, process documents, design output, reference documents, feedback information, etc.

2.2 Unified Management and Scheduling of Nuclear Civil Engineering Design Tools

Design tools are an important part of nuclear power civil engineering design. The integration of design tools is an important link to ensure the smooth implementation of the design process and the automatic transfer of documents and parameters. The calculation

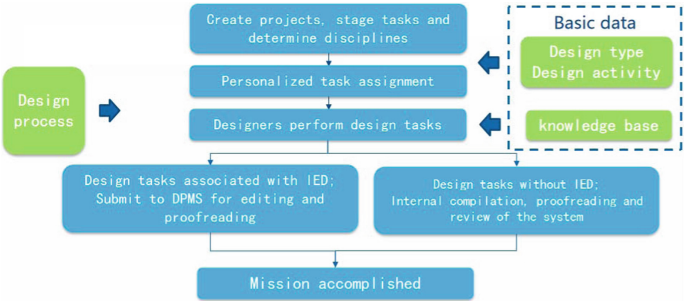


Fig. 2. Design task flow diagram and design workbench interface

and analysis software of each discipline is basically complete, but there is not unified collaborative design platform.

Through the integration and encapsulation of design activities and design tools, this paper realizes the unified integration and encapsulation of commercial, self-made and various professional analysis tools. It realizes the unified management and scheduling of tools, and the automatic warehousing management and correlation of input and output files and parameters (see Fig. 3).

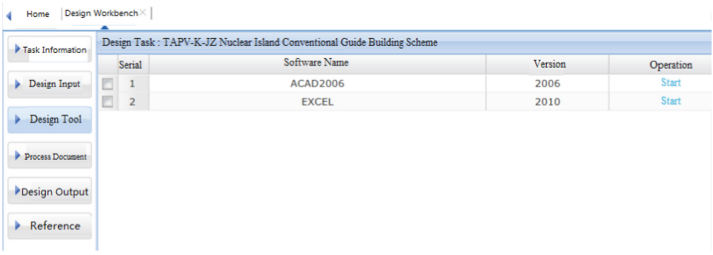


Fig. 3. Tool Integration Management Diagram

2.3 Research and Development of Civil Design Tools

Intelligent 3D Reinforcement Modeling and Drawing of Civil Structure of Nuclear Island

The number of reinforcement drawings of nuclear island civil engineering structures accounts for more than 50% of the total structural drawings. In the past, the two-dimensional manual drawing of reinforcement drawings was inefficient, repetitive and difficult to guarantee quality. The nuclear island structure has a large amount of reinforcement, and the reinforcement is dense. The two-dimensional drawing cannot realize the reinforcement collision inspection. It is difficult to find the reinforcement collision problem, which is not conducive to the on-site construction. The 2D reinforcement can not

make use of the existing 3D solid model results, resulting in the process disconnection, which is a major reason restricting the efficiency of reinforcement drawing.

In order to solve the above difficulties, this paper uses 3D technology to superimpose the reinforcement information into the solid model. Through the reinforcement solid simulation, collision inspection, 3D drawing and material statistics functions, it achieve effective control of the production process and improve the efficiency and quality of reinforcement design (see Fig. 4).

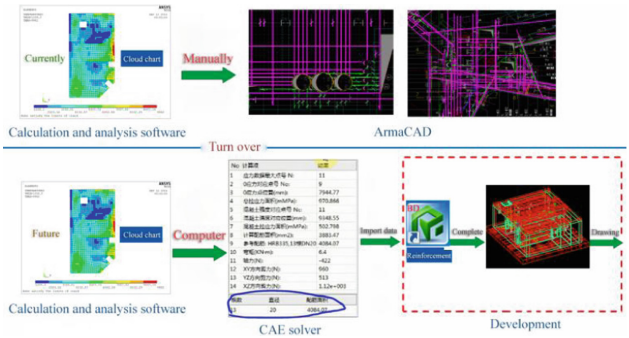


Fig. 4. Intelligent 3D reinforcement modeling and drawing of nuclear island civil structure

Development of Civil Structure Calculation Tool Set

Equipment foundation analysis, calculation and analysis of simple components, embedded calculation and analysis are important design activities of nuclear island plant. There are many problems such as tight time, many tasks and long time consuming, which consume a lot of manpower and time, and the accuracy can not be effectively guaranteed.

In this paper, by sorting out the design analysis process, the standardization of core design activities such as anti equipment foundation is formed, and the process based design analysis is carried out according to the specific process of developing user-friendly computing software. From calculation analysis to report generation, the labor intensity of engineers is reduced, and the time for design and analysis activities is reduced to meet the requirements of engineering design progress (see Fig. 5).

Post Processing of Nuclear Power Plant Floor Response Spectrum Calculation

After Fukushima nuclear accident in Japan, the seismic performance of nuclear power plant structures has received great attention in the industry. It is of great significance to carry out structural dynamic analysis of nuclear power plant structures and related sub structures. Floor response spectrum analysis, that is, the response curve of each floor of a building to a specific seismic vibration frequency. It is the seismic input for seismic analysis of equipment or pipes on the floor slab. It plays an important role in the structural dynamic analysis of nuclear power plants. The domestic nuclear power design industry often conducts floor response spectrum calculation based on SAP2000 software. Because SAP2000 itself lacks perfect post-processing function. The software cannot

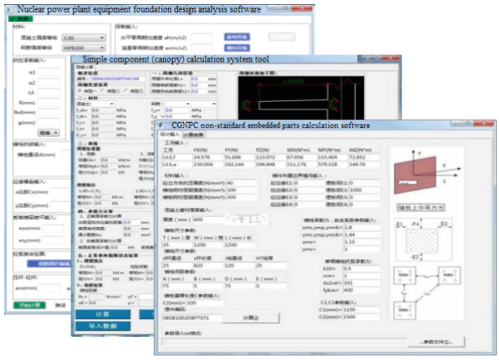


Fig. 5. Toolset presentation

automatically extract, customize and generate data and regional envelope according to user needs. In order to obtain the floor response spectrum, designers often face a large number of data processing, data export, multi-point fitting and envelope smoothing. Usually, the calculation of the floor response spectrum of a factory requires a lot of time for repetitive work, which is low in efficiency, high in labor cost, and prone to human error.

Based on SAP2000 API development interface, this paper combs and puts forward the idea and method of post processing of response spectrum. It develops a post processing system of nuclear power plant floor response spectrum, which can solve the problem from repeated and inefficient data processing. So that, the designers can focus more on the evaluation of results, improve the accuracy of calculation, and greatly improve the post processing efficiency of floor response spectrum calculation (see Fig. 6).

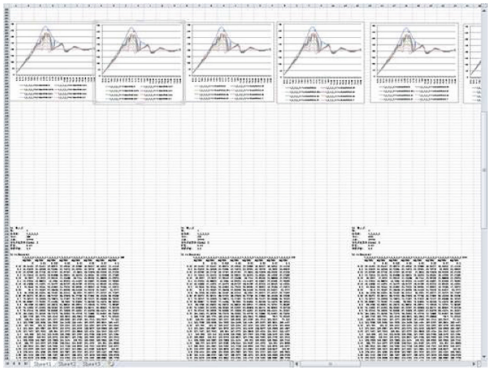


Fig. 6. Comparison chart of automatically generated response spectrum curve results

2.4 Structured Management and Intelligent Application of Design Data

Traditional finished design documents and data are mainly stored and managed by AutoCAD drawings, Excel tables and calculation instructions in a decentralized manner without centralized control. Data and knowledge collaboration and sharing are poor. Data retrieval is difficult. Data security and sharing management are low. And many experiences and knowledge may be lost.

In this paper, process data, reference data and finished product data in the platform are stored in the database in a structured form. All kinds of data are related to each other and displayed in the platform in the form of forms. At the same time, the platform controls the use of data. For similar operations of the same type of data, it can also provide the functions of batch viewing data and process information and batch processing to ensure the quality of data. This method ensures the real-time, effectiveness and uniqueness of data, reduces the number of interfaces between disciplines, and greatly improves the work efficiency and design quality of designers (see Fig. 7).

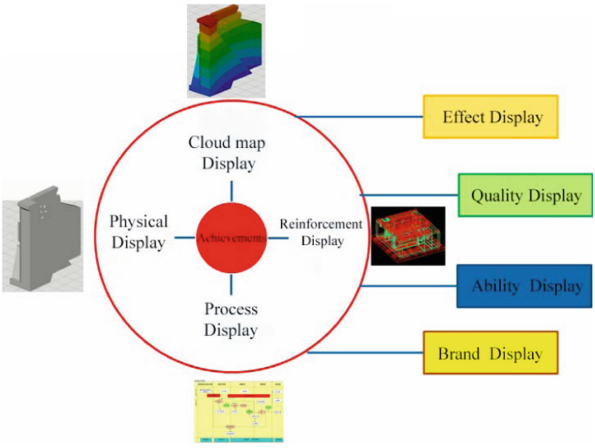


Fig. 7. Data Structure Management Diagram

The data is stored in the database in a structured form, which greatly improves the efficiency of users to obtain the required data and ensures the real-time effectiveness of the data. All kinds of design activities are based on unified and effective data, which reduces the number of interfaces between disciplines and improves the work efficiency and design quality.

All kinds of data are related to each other and are determined during creation or application. For example, when users carry out design work. Relevant parameter data can be pushed to corresponding design activities according to the defined design types to realize the value of design data.

2.5 Data Connection with External Systems

The civil design of nuclear power plant uses PDMS as a three-dimensional layout design platform, which greatly improves the work efficiency and design quality. However, as the

functional scope of PDMS does not cover such fields as general layout design, structural calculation, steel structure deepening design and drawing. It cannot fully meet the needs of civil design, and even through in-depth secondary development. It cannot better meet the complete needs of civil engineering related professional and technical work. At the same time, the PDMS civil engineering model is relatively closed, and the model format has poor compatibility with its mainstream 3D design software. The 3D civil engineering design must be modeled again with other software, resulting in repeated work, increasing the workload of civil engineering design, and adversely affecting the collaboration between disciplines and real-time information exchange.

In this paper, the data formats of Bentley and PDMS are converted to each other through customized development. The data interface between civil design model and process layout PDMS model is opened. The data source is unified. The design model is multi available. The real civil design data integration is realized. At the same time, the integration of the civil design platform, the design and production management platform, the project document management platform and other external information platforms related to the design process is realized through Web services. It eliminates information islands, and realizes seamless connection of design data and interconnection between platform systems (see Fig. 8).

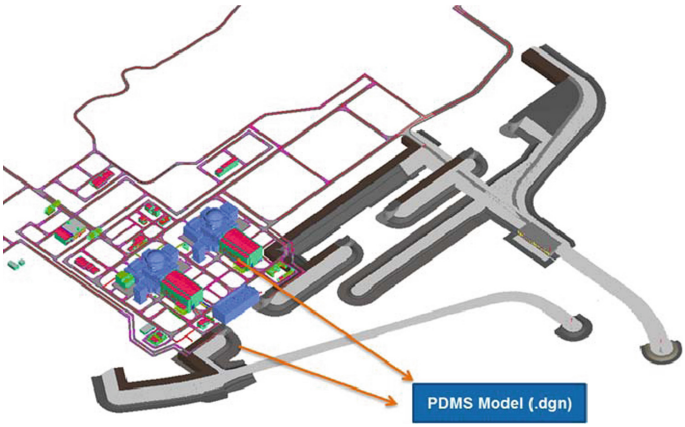


Fig. 8. PDMS model data is converted into Bentley model data

3 Conclusion

The establish of Collaborative Engineering Platform for Civil of nuclear power plant has been deeply applied in the civil engineering design of nuclear power plant. It covers all design activities of six civil engineering disciplines, including civil nuclear island structure, conventional island and BOP structure, architecture, hydraulic structure, general drawing and plant site. The project achievements have been widely praised and highly recognized. It realizes the flow and standardized management of the design process. It realizes the transformation of the traditional design method. It promotes the

development of collaborative design. It improves the nuclear civil engineering design information system. It improves the nuclear civil engineering design information level.

References

1. Yang, W.: Digital handover of "hualong-1" pressurized reactor nuclear power plant engineering data. Sci. Technol. Eng. **20**(36), 14935–14943 (2020)
2. Shen, T., Li, X.: Configuration and data management of nuclear power digital design system. Instrum. Users 24(11), 528–551 (2017)
3. Li, B., Fan, G., Shao, K., Wang, H., Wang, X., Yang, X.: Application of digital construction technology in civil engineering of HPR1000. China Nuclear Power (11), 68–72 (2017)
4. Huang, S., Fan, Y.: Overview of product lifecycle management. Comput. Integr. Manuf. Syst. **10**(1), 1–9 (2004)
5. Gao, N., Zhao, S., Gao, C.: Product life cycle management and manufacturing industry informationalization. Mod. Manuf. Eng. (09) 16–18 (2006)
6. Gao, J., Du, H., Zhao, X.: A survey of network collaboration technology based on product lifecycle management. Technol. Econ. Guide (01), 23–25 (2017)

Self-stability Analysis of Fluoride Salt Cooled High Temperature Reactor Based on Shifted-Ectropy Approach

Yi-Ran Liu(✉), Wei Zhang, and Dan-Jing Wei

China Nuclear Power Technology Research Institute, Shenzhen, China
yiran@teamyoungtech.com

Abstract. Fluoride salt cooled high temperature reactor (FHR) is a promising advanced fourth generation reactor. Self-stability of FHR focus on the ability to converge to an equilibrium point without control loop, which is crucial for the design of control system and operation strategy of FHR. In this paper, the self-stability of the FHR is analyzed based on its physical characteristic using shifted-ectropy approach. Through theoretical analysis, it is proved that the equilibriums of FHR dynamics are globally asymptotically stable.

Keywords: self-stability · fluoride-salt-cooled reactor · Lyapunov function

1 Introduction

Fluoride salt cooled high temperature reactor (FHR) combines many technologies in fourth-generation reactors, such as the high temperature and high burn-up tolerant fuel technology from high temperature gas cooled reactor, and the high temperature molten salt cooling technology from molten salt reactor, passive safety technology of liquid metal reactor. FHR has advantages in safety performance, economical efficiency and environmental adaptability comparing with the traditional reactors.

The concept of FHR is first proposed by Charles and W. Forsberg from Oak Ridge National Laboratory (ORNL) in American, they carried out the first conceptual designing of FHR which is called advanced high temperature reactor (AHTR), with the coolant as FLiBe the aim of the design is to provide high-temperature heat which facilitates hydrogen generation and electric power generation in a relative low cost. And then the university of California, Berkeley (UCB) combined with ORNL kept on researching the FHR. The design team made a big improvement for the AHTR in 2006, they proposed the conceptual design of advanced pebble bed FHR (PB-FHR), using the graphite pebbles permeated with TRISO fuel particles. In 2010, ORNL developed the small modular AHTR (smAHTR) which is easy to assemble and transport, and suitable for the application in many communal facilities. Soon afterwards, the U.S. Department of Energy Office of Nuclear Energy (DOE-NE) cooperated with the UCB, the Massachusetts Institute of technology (MIT), the university of Wisconsin, Madison (UWM) to carried out

The research is sponsored by Chinese national key research project (2020YFB1902000).

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 387–395, 2023.
https://doi.org/10.1007/978-981-99-3455-3_39

an integrated study project which goal is to develop a FHR with commercial competitiveness. And in 2014, UCB put forward the 236MW modular commercial PB-FHR reactor system which is a relatively complete commercial design. Additionally, Shanghai Institute of Applied Physics carried out the study of thorium molten salt reactor with liquid fuel, and the experimental reactor is under construction. In 2015, based on the requirement of modularity and portability, Xi'an jiaotong university proposed the 20MW TFHR conceptual design. And in 2020 Xi'an jiaotong university proposed the Fluoride salt cooled high temperature advanced Reactor (FuSTAR), with the property of integration and flexibility aiming at the application in remote area and military base. The analysis of this paper is based on the design of FuSTAR.

The FuSTAR plant consist of an integrate reactor with reactor core and primary heat exchanger in the reactor vessel, and the coolant of primary loop is FLiBe, the intermediate loop is consist of FLiNaK as coolant and intermediate heat exchanger, the intermediate heat exchanger transfers the heat to the supercritical CO2 power conversion system. The schematic structure of the FuSTAR is shown in Fig. 1.

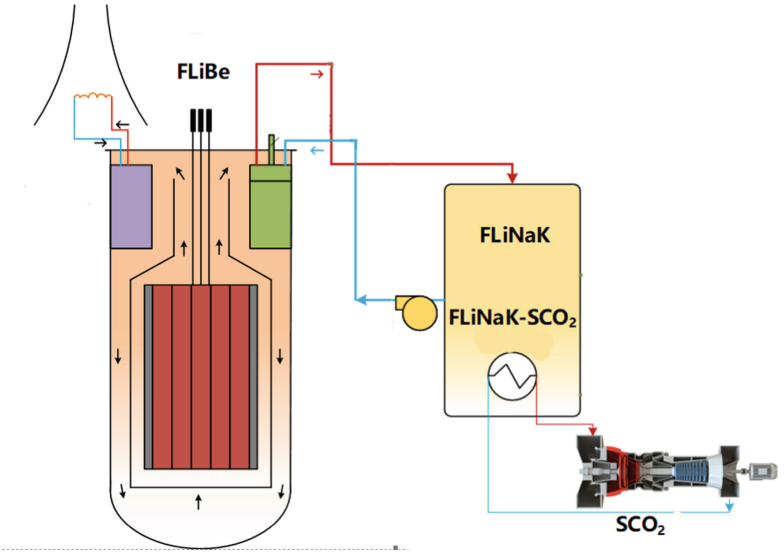


Fig. 1. The schematic structure of FuSTAR

Reactor control is very important for the safety and economic competiveness of the nuclear plant. And power-level regulation is one of the key technologies which guarantee safe, stable in PWR. Although there has been an extensively study of nuclear power control in PWR. The PWR nuclear power control can't be used directly to the FuSTAR because:

1) The moderator and the coolant of FuSTAR are quite different from those of the PWR:
2) Thermal capacity of the FuSTAR is much larger than that of PWR, which makes the FuSTAR's maneuverability weaker than that of PWR.

3) The module-coupling effect need carefully redesigned based on its own dynamics characteristic.

Thus, the controllers of the FuSTAR need to be designed based on its own dynamic properties.

Self-stability is the most important dynamic property of nuclear power plant. And it is the base of the power level control design. Through the study of self-stability, we can know how to strengthen the closed-loop stability and to improve the maneuverability.

In this paper, the self-stability of FuSTAR plant is analyzed based on Lyapunov direct method. And the Lyapunov function is construct based on the concept of irreversibility function and shifted-ectropy of general thermodynamic systems. The theoretical results shows that equilibriums of the FuSTAR dynamics are globally asymptotically stable.

2 Nonlinear State-space model for FuSTAR

2.1 Modeling

In FuSTAR plant, there are three loops as we can see from Fig. 1, the reactor vessel of FuSTAR contains reactor core and primary heat exchanger and primary coolant, in the PHX heat transfer from primary loop to intermediate loop, and the intermediate loop contains FLiNaK as the intermediate coolant. In the intermediate heat changer, the CO_2 is been heated up to be super critical CO_2, and transport to generator to generate electricity. Based on the above description, the simplified nodalization of FuSTAR is presented in Fig. 2.

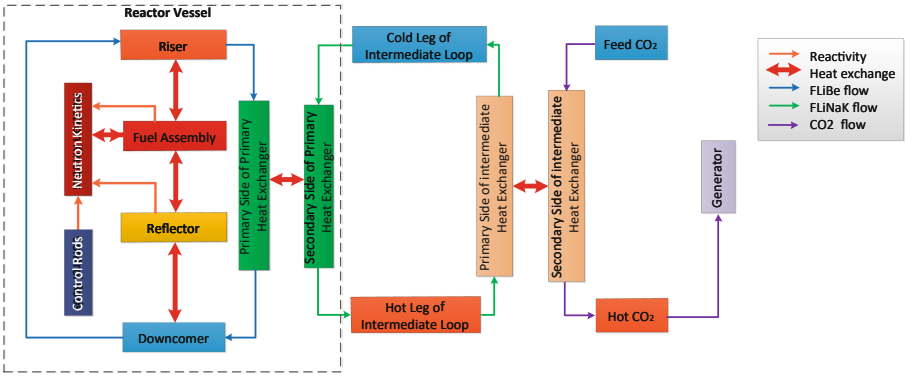


Fig. 2. Nodalization of FuSTAR

The model considers the point neutron kinetics and with one equivalent delayed neutron with the feedback given by the change of fuel temperature and coolant temperature.

And the state space model for analysis can be written as:

$$\begin{cases} \frac{dn_r}{dt} = \frac{\rho_r-\beta}{\Lambda} n_r + \frac{\beta}{\Lambda} c_r + \frac{n_r}{\Lambda}[\alpha_f (T_f - T_{f,m}) + \alpha_r (T_r - T_{r,m})] \\ \frac{dc_r}{dt} = \lambda (n_r - c_r) \\ \frac{dT_f}{dt} = -\frac{\Omega_{fu}}{\mu_f}(T_f - T_u) - \frac{\Omega_{fr}}{\mu_f}(T_f - T_r) + \frac{P_0}{\mu_f} n_r \\ \frac{dT_r}{dt} = -\frac{\Omega_{rd}}{\mu_r}(T_r - T_d) + \frac{\Omega_{fr}}{\mu_r}(T_f - T_r) \\ \frac{dT_u}{dt} = \frac{\Omega_{fu}}{\mu_u}(T_f - T_u) + \frac{M_p}{\mu_u}(T_{pp} - T_u) \\ \frac{dT_d}{dt} = \frac{\Omega_{rd}}{\mu_d}(T_r - T_d) + \frac{M_p}{\mu_d}(T_{pp} - T_d) \\ \frac{dT_{pp}}{dt} = -\frac{M_p}{\mu_{pp}}(T_{pp} - T_d) + \frac{M_p}{\mu_{pp}}(T_u - T_{pp}) - \frac{\Omega_p}{\mu_{pp}}(T_{pp} - T_{ps}) \\ \frac{dT_{ps}}{dt} = -\frac{\Omega_p}{\mu_{pp}}(T_{pp} - T_{ps}) + \frac{M_i}{\mu_{ps}}(T_{ic} - T_{ps}) - \frac{M_i}{\mu_{ps}}(T_{ps} - T_{ih}) \\ \frac{dT_{ih}}{dt} = \frac{M_i}{\mu_{ih}}(T_{ps} - T_{ih}) - \frac{M_i}{\mu_{ih}}(T_{ih} - T_{sp}) \\ \frac{dT_{ic}}{dt} = \frac{M_i}{\mu_{ic}}(T_{sp} - T_{ic}) - \frac{M_i}{\mu_{ic}}(T_{ic} - T_{ps}) \\ \frac{dT_{sp}}{dt} = -\frac{\Omega_i}{\mu_{sp}}(T_{sp} - T_{ss}) + \frac{M_i}{\mu_{sp}}(T_{ih} - T_{sp}) - \frac{M_i}{\mu_{sp}}(T_{sp} - T_{ic}) \\ \frac{dT_{ss}}{dt} = -\frac{\Omega_i}{\mu_{ss}}(T_{sp} - T_{ss}) - \frac{2M_s}{\mu_{ss}}(T_{ss} - T_{fs}) - \frac{P_m}{\mu_{ss}} \end{cases} \tag{1}$$

where n_r is the normalized neutron concentration, c_r is the normalized equivalent delayed neutron precursor, β is the total fraction of delayed fission neutrons. Λ is the effective prompt neutron lifetime, ρ_r is the reactivity inserted by control rods, λ is the decay constant of the equivalent delayed neutron precursor. α_f is the reactivity feedback coefficient of average fuel temperature. α_r is the reactivity feedback coefficient of reflector temperature. P_0 is the thermal power, T_f is the average temperature of the fuel, T_r is the average temperature of the reflector, T_u is the average temperature of the FLiBe inside the riser of primary loop, T_d is the average temperature of the FLiBe inside the downcomer of the primary loop, $T_{f,m}$ and $T_{r,m}$ are the initial equilibrium values of fuel temperature and reflector temperature. T_{pp} is the primary side temperature of PHX, T_{ps} is the secondary side temperature of PHX, T_{ih} is the temperature of FLiNaK in the hot leg of intermediate loop, T_{ic} is the temperature of FLiNaK in the cold leg of intermediate loop, T_{sp} is the temperature of the primary side of intermediate heat exchanger, T_{ss} is the temperature of the secondary side of intermediate heat exchanger, T_{fs} is the temperature of feed CO_2, P_m is the output power of the FuSTAR, Ω_{fu}, Ω_{fr}, Ω_{rd}, Ω_p and Ω_i are heat transfer coefficients between the fuel and riser, the fuel and reflector, the reflector and downcomer,the PHX, the IHX, M_p and M_i are primary mass flowrate times heat capacity of FLiBe and intermediate mass flowrate times heat capacity of FLiNaK, μ_f, μ_r, μ_u, μ_d, μ_{pp}, μ_{ps}, μ_{ih}, μ_{ic}, μ_{sp}, μ_{ss} are the total heat capacity of fuel, reflector, riser, downcomer, primary side of PHX, secondary side of PHX, hot leg of intermediate loop, cold leg of intermediate loop, primary side of IHX, secondary side of IHX.

Furthermore, the difference between the actual values of n_r, c_r, T_f, T_r, T_u, T_d, T_{pp}, T_{ps}, T_{ih}, T_{ic}, T_{sp}, T_{ss}, T_{fs}, ρ_r and equilibrium values, n_{r0}, c_{r0}, T_{f0}, T_{r0}, T_{u0}, T_{d0}, T_{pp0},

T_{ps0}, T_{ih0}, T_{ic0}, T_{sp0}, T_{ss0}, T_{fs0}, ρ_{r0} are defined as:

$$\begin{cases} \delta n_r = n_r - n_{r0} \\ \delta c_r = c_r - n_{r0} \\ \delta T_f = T_f - T_{f0} \\ \delta T_r = T_r - T_{r0} \\ \delta T_u = T_u - T_{u0} \\ \delta T_d = T_d - T_{d0} \\ \delta T_{pp} = T_{pp} - T_{pp0} \\ \delta T_{ps} = T_{ps} - T_{ps0} \\ \delta T_{ih} = T_{ih} - T_{ih0} \\ \delta T_{ic} = T_{ic} - T_{ic0} \\ \delta T_{sp} = T_{sp} - T_{sp0} \\ \delta T_{ss} = T_{ss} - T_{ss0} \\ \delta T_{fs} = T_{fs} - T_{fs0} \\ \delta \rho_r = \rho_r - \rho_{r0} \end{cases} \tag{2}$$

For the purpose is to analysis self-stability, it is obviously that

$$\delta \rho_r = \rho_r - \rho_{r0} \equiv 0 \tag{3}$$

Define the state-vector $\vec{x}$ as

$$\vec{x} = \begin{bmatrix} \delta n_r & \delta c_r & \delta T_f & \delta T_r & \delta T_u & \delta T_d & \delta T_{pp} & \delta T_{ps} & \delta T_{ih} & \delta T_{ic} & \delta T_{sp} & \delta T_{ss} \end{bmatrix}$$

And the nonlinear state-space model of FuSTAR can be written as

$$\begin{cases} \frac{dx_1}{dt} = -\frac{\beta}{\Lambda}(x_1 - x_2) + \frac{n_{r0}+x_1}{\Lambda}[\alpha_c x_3 + \alpha_r x_4)] \\ \frac{dx_2}{dt} = \lambda(x_1 - x_2) \\ \frac{dx_3}{dt} = -\frac{\Omega_{fu}}{\mu_f}(x_3 - x_5) - \frac{\Omega_{fr}}{\mu_f}(x_3 - x_4) + \frac{P_0}{\mu_f} n_r \\ \frac{dx_4}{dt} = \frac{\Omega_{rd}}{\mu_r}(x_4 - x_6) + \frac{\Omega_{fr}}{\mu_r}(x_3 - x_4) \\ \frac{dx_5}{dt} = \frac{\Omega_{fu}}{\mu_u}(x_1 - x_5) + \frac{M_p}{\mu_u}(x_7 - x_5) \\ \frac{dx_6}{dt} = \frac{\Omega_{vd}}{\mu_u}(x_4 - x_6) + \frac{M_p}{\mu_u}(x_7 - x_6) \\ \frac{dx_7}{dt} = -\frac{M_p}{\mu_{pp}}(x_7 - x_6) + \frac{M_p}{\mu_{pp}}(x_5 - x_7) - \frac{\Omega_p}{\mu_{pp}}(x_7 - x_8) \\ \frac{dx_8}{dt} = \frac{\Omega_p}{\mu_{pv}}(x_7 - x_8) + \frac{M_i}{\mu_{ps}}(x_{10} - x_8) - \frac{M_i}{\mu_{px}}(x_8 - x_9) \\ \frac{dx_9}{dt} = \frac{M_i}{\mu_{hh}}(x_8 - x_9) - \frac{M_i}{\mu_{ih}}(x_9 - x_{11}) \\ \frac{dx_{10}}{dt} = \frac{M_i}{\mu_{ic}}(x_{11} - x_{10}) - \frac{M_i}{\mu_{ih}}(x_{10} - x_8) \\ \frac{dx_{11}}{dt} = -\frac{\Omega_i}{\mu_{sp}}(x_{11} - x_{12}) + \frac{M_i}{\mu_{sp}}(x_9 - x_{11}) - \frac{M_i}{\mu_{sp}}(x_{11} - x_{10}) \\ \frac{dx_{12}}{dt} = \frac{\Omega_i}{\mu_{ss}}(x_{11} - x_{12}) - \frac{2M_{ss}}{\mu_{ss}}\left(x_{12} - \delta T_{fs}\right) - \frac{\delta P_m}{\mu_{ss}} \end{cases} \tag{4}$$

2.2 Stability Analysis

Here we will briefly introduce the concept of system stability base on Lyapunov function.

Consider a system can be expressed as

$$\frac{d\vec{x}}{dt} = \vec{f}(\vec{x}, \vec{u}) \tag{5}$$

If there exist a value function $V\left(\vec{x}\right)$:

$$\begin{cases} V(0) = 0 \\ V(x) > 0, \quad \forall \vec{x} \neq 0 \end{cases}$$

Satisfy $\frac{dV\left(\vec{x}\right)}{dt} < 0, \forall \vec{x} \neq 0.$

en $\vec{x} = 0.$ is globally asymptotically stable.

After constructing the dynamic model of the FuSTAR for self-stability analysis and introduction of globally asymptotically stability, the problem to be solved in this paper can be summarized as below:

Consider the FuSTAR dynamics, Is the equilibrium point of this system globally stable?

Find a Lyapunov function that satisfied $\begin{cases} V(0) = 0 \\ V(x) > 0, \ \forall \vec{x} \neq 0 \end{cases}$

Proof the derivative of the Lyapunov function along the system (9) is negative definite.

3 Construction of the Lyapunov function

The concept of shift ectropy in nuclear reactor is propose by Dong, here we just give the form of the shift ectropy and not going to the details.

The shift ectropy of the neutron kinetics is

$$\zeta_N = \Lambda\left[n_{r0} + x_1 - n_{r0}\ln\left(1 + \frac{x_1}{n_{r0}}\right)\right] + \frac{\beta}{\lambda}\left[n_{r0} + x_2 - n_{r0}\ln\left(1 + \frac{x_2}{n_{r0}}\right)\right] \tag{6}$$

The shift ectropy of thermal hydraulic loop of the reactor can be express as

$$\zeta_T = \frac{1}{2}\left(\mu_f x_3^2 + \mu_r x_4^2 + \mu_{li} x_5^2 + \mu_d x_6^2 + \mu_{pp} x_7^2 + \mu_{px} x_8^2 + \mu_{ih} x_9^2 + \mu_{ic} x_{10}^2 + \mu_{sp} x_{11}^2 + \mu_{ss} x_{12}^2\right) \tag{7}$$

Here we will give some assumption to make the system globally stable.

1) The feed CO2 temperature T_{fs} is constant.
2) Tss is larger, Pm is larger, i.e.

$$\delta T_{ss} \delta P_m \geq 0 \tag{8}$$

3) The temperature feedback effect caused by the reflector is much weaker than that caused by the fuel, i.e.

$$|\alpha_c \delta T_c| << |\alpha_r \delta T_r| \tag{9}$$

4 Self-stability analysis

The ectropy of the neutron kinetics is:

$$\zeta_N = \Lambda\left[n_{r0} + x_1 - n_{r0}\ln\left(1 + \frac{x_1}{n_{r0}}\right)\right] + \frac{\beta}{\lambda}\left[n_{r0} + x_2 - n_{r0}\ln\left(1 + \frac{x_2}{n_{r0}}\right)\right] \tag{10}$$

Differentiate (11) along the trajectory of the system (4), we have:

$$\begin{aligned}\frac{d\zeta_N}{dt} =& \Lambda\frac{x_1}{n_{r0}+x_1}\frac{dx_1}{dt} + \frac{\beta}{\lambda}\frac{x_2}{n_{r0}+x_2}\frac{dx_2}{dt}\\ =& [-\beta(x_1-x_2) + (n_{r0}+x_1)(\alpha_c x_3 + \alpha_r x_4)]\frac{x_1}{n_{r0}+x_1} + \beta(x_1-x_2)\frac{x_2}{n_{r0}+x_2}\\ =& -\frac{\beta(x_1-x_2)^2}{(n_{r0}+x_1)(n_{r0}+x_2)} + x_1(\alpha_c x_3 + \alpha_r x_4)\end{aligned} \tag{11}$$

The ectropy of the hydraulic thermal loop is:

$$\zeta_T = \frac{1}{2}\left(\mu_f x_3^2 + \mu_r x_4^2 + \mu_k x_5^2 + \mu_d x_6^2 + \mu_{pp} x_7^2 + \mu_{px} x_8^2 + \mu_{hh} x_9^2 + \mu_c x_{10}^2 + \mu_{pp} x_{11}^2 + \mu_s x_{12} x_2^2\right) \tag{12}$$

Differentiate (12) along the trajectory of the system (4), we have:

$$\begin{aligned}\frac{d\zeta_T}{dt} =& \mu_f x_3\frac{dx_3}{dt} + \mu_r x_4\frac{dx_4}{dt} + \mu_{lc} x_5\frac{dx_5}{dt} + \mu_d x_6\frac{dx_6}{dt} + \mu_{pp} x_7\frac{dx_7}{dt} + \mu_{ps} x_8\frac{dx_8}{dt} + \mu_{ii} x_9\frac{dx_9}{dt} + \mu_{ic} x_{10}\frac{dx_{10}}{dt} + \mu_{sp} x_{11}\frac{dx_{11}}{dt} + \mu_{ss} x_{12}\frac{dx_{12}}{dt})\\ =& \mu_f x_3\left[-\frac{\Omega_{fu}}{\mu_f}(x_3-x_5) - \frac{\Omega_{ff}}{\mu_f}(x_3-x_4) + \frac{P_0}{\mu_f}x_1\right] + \mu_r x_4\left[\frac{\Omega_{nd}}{\mu_r}(x_4-x_6) + \frac{\Omega_{fr}}{\mu_r}(x_3-x_4)\right]\\ &+ \mu_u x_5\left[\frac{\Omega_{fu}}{\mu_u}(x_1-x_5) + \frac{M_p}{\mu_u}(x_7-x_5)\right] + \mu_d x_6\left[\frac{\Omega_{rd}}{\mu_u}(x_4-x_6) + \frac{M_p}{\mu_u}(x_7-x_6)\right]\\ &+ \mu_{pp} x_7\left[-\frac{M_p}{\mu_{pp}}(x_7-x_6) + \frac{M_p}{\mu_{pp}}(x_5-x_7) - \frac{\Omega_p}{\mu_{pp}}(x_7-x_8)\right] + \mu_{ps} x_8\left[\frac{\Omega_p}{\mu_{ps}}(x_7-x_8) + \frac{M_i}{\mu_{ps}}(x_{10}-x_8) - \frac{M_i}{\mu_{ps}}(x_8-x_9)\right]\\ &+ \mu_{ih} x_9\left[\frac{M_i}{\mu_{ih}}(x_8-x_9) - \frac{M_i}{\mu_{ih}}(x_9-x_{11})\right] + \mu_{ic}\left[\frac{M_i}{\mu_{ic}}(x_{11}-x_{10}) - \frac{M_i}{\mu_{ih}}(x_{10}-x_8)\right]\\ &+ \mu_{sp} x_{11}\left[-\frac{\Omega_i}{\mu_{pp}}(x_{11}-x_{12}) + \frac{M_i}{\mu_{sp}}(x_9-x_{11}) - \frac{M_i}{\mu_{sp}}(x_{11}-x_{10})\right] + \mu_{ss} x_{12}\left[\frac{\Omega_i}{\mu_{ss}}(x_{11}-x_{12}) - \frac{2M_{ss}}{\mu_{ss}}(x_{12}-\delta T_{fs}) - \frac{\delta P_m}{\mu_{ss}}\right]\\ <& -\Omega_{fu}(x_3-x_5)^2 - \Omega_{fr}(x_3-x_4)^2 - \Omega_{rd}(x_4-x_6)^2 - \Omega_{nd}(x_4-x_6)^2 - M_p(x_7-x_6)^2 - M_p(x_7-x_5)^2\\ &- \Omega_p(x_7-x_8)^2 - M_i(x_{10}-x_8)^2 - M_i(x_{11}-x_{10})^2 - M_i(x_{11}-x_9)^2 - M_i(x_9-x_8)^2 - \Omega_i(x_{11}-x_{12})^2 - 2M_s x_{12}^2 + P_0 x_1 x_3\end{aligned} \tag{13}$$

The Lyapunov function of the whole system can be constructed as:

$$V(x) = \zeta_T + \frac{P_0}{|\alpha_c|}\zeta_N \tag{14}$$

Differentiate (14) along the system of (4), combine (13) with (11), because the α_C is negative, then we can cancel out the term consist of x_1x_3, we have

$$\begin{aligned}\frac{dV(x)}{dt} <& -\Omega_{fu}(x_3-x_5)^2 - \Omega_{fr}(x_3-x_4)^2 - \Omega_{rd}(x_4-x_6)^2 - M_p(x_7-x_6)^2 - M_p(x_7-x_5)^2\\ &- \Omega_p(x_7-x_8)^2 - M_p(x_7-x_6)^2 - M_i(x_{11}-x_{10})^2 - M_i(x_9-x_8)^2 - \Omega_i(x_7-x_8)^2\\ &2M_{ss}x_{12}^2 - \frac{P_0\beta(x_1-x_2)^2}{|\alpha_c|(n_{r0}+x_1)(n_{r0}+x_2)}\end{aligned} \tag{15}$$

Because the deviation of normalized neutron concentration x_1, the deviation of normalized equivalent delayed neutron precursor x_2 are all less than 1, then $(n_{r0} + x_1)(n_{r0} + x_2)$ is positive. So it is proven that the derivation of the whole system's Lyapunov function satisfied the requirement of negative define:

$$\frac{dV(x)}{dt} < 0 \tag{16}$$

Which is to say that the state vector of the equilibrium points is globally asymptotically stable in the entire definition domain.

Remark 1. In the FuSTAR, the value of the reactivity feedback of temperate of reflector is much smaller than that of fuel, and what's more, the heat capacity of the reflector is so large that the temperature of the reflector are almost constant comparting to fuel temperature. So these facts lead to the rational assumption (9), which means the feedback caused by reflector is negligible.

Remark 2. For FuSTAR, the feed CO2 temperature is decided by the capacity signal, and will not change is a definite equilibrium state. So it is evident that when CO2 temperature is higher, the CO2 enthalpy is larger, that results in a larger output power. So the assumption (8) is explained.

Remark 3. From inequality (15), we can see that if the negative temperature feedback is larger, the power-density is smaller, the heat transfer coefficient is larger, the FuSTAR is more stable. This observation find the main factors of the system's stability.

Remark 4. Although we have proven that FuSTAR has the ability of self-stability, we have not yet analyze the effect exterior disturbance. Some uncontrolled exterior disturbance may threaten the stability of the FuSTAR. Thus it is very necessary to design feedback control to suppress the disturbances and uncertainties in the future.

5 Conclusion

The FHR is promising candidate among the fourth-generation nuclear energy systems. Self-stability is a curial dynamic feature of the reactor. In this paper we analyzed the self-stability of an advanced FHR named FuSTAR, the key is to find a proper Lyapunov function. Since the nuclear plant is a thermodynamic system with fission reaction, the Lyapunov function is constructed in Sect. 3 based on the concept of shifted-ectropy. In Sect. 4, it has been proved theoretically that the equilibriums of FuSTAR dynamics are globally asympototic stable. The future work is to design control laws for strengthening the stability in uncertain exterior disturbance.

References

1. Forsberg, C.W., Peterson, P.F., Pickard, P.S.: Molten salt cooled advanced high-temperature reactor for production of hydrogen and electricity. **144**(3), 289–302 (2003)
2. Fratoni, M.: Development and application of methodologies for the neutronic design of the pebble bed advanced high temperature reactor. University of California, Berkeley (2008)
3. Greene, S.R., Gehin, J.C.: Pre-conceptual design of a Fluoride-salt-cooled modular advanced high temperature reactor. Oak Ridge National Laboratory, Oak Ridge (2010)

4. Scarlat, R.O., Laufer, M.R.: Design and licensing strategies for the fluoride salt cooled, high temperature reactor technology. Prog. Nucl. Energy **77**, 406–420 (2014)
5. Andreades, C., Cisneros, A.T.: Technical description of the Mark 1 pebble-bed fluoride salt cooled high temperature reactor power plant. Berkeley: Department of Nuclear Engineering, University of California (2014)
6. Dalin, Z., Hao, Q., et al.: Preliminary concept design of integral inherently safe fluoride-salt-cooled high-temperature advanced reactor FuSTAR. China Basic Sci. **4**(2021), 15–20 (2021)
7. Khlil, H.K.: Nonlinear Systems, 3rd edn. Prentice Hall, Upper Saddle River (2002)
8. Haddad, W.M., Chellaboina, V., Nersesov, S.G.: Thermodynamics: A Dynamical Systems Approach. Princeton University Press, Princeton (2005)
9. Dong, Z.: Self-stability analysis of MHTGRs: a shifted-ectropy based approach. Nucl. Eng. Des. **248**(2012), 137–148 (2012)

Design of Static Semantic Analyzer for Code Generator Applied in Safety-Level I&C of NPPs

Lin Lan[1], Gang Wang[1], Jun Tu[1], Zhe Li[1], Di Huang[1], Jia-Cheng Zhang[1], and Wei Jiang[2(✉)]

[1] Nuclear Power Institute of China Institute of Reactor Operation and Application Leshan, Beijing, China

[2] Science and Technology on Reactor System Design Technology Laboratory, Nuclear Power Institute of the China Chengdu, Sichuan, China

jiangwei.chn@gmail.com

Abstract. In the nuclear safety level I&C (Instrument and Control) area, the code generator plays an important role in developing the application software. The main function of the code generator is to translate the Lustre program corresponding to the graphical control algorithm into C code. Therefore, the reliability and quality of the code generator will directly affect the safe and reliable operation of nuclear power plants. In order to ensure the correctness of Lustre code, a static semantic analyzer is designed and developed to find the errors in source Lustre code. Its function is to check the correctness of the input source Lustre code, including identifier-checking declarations, identifier-checking programs, type-checking expressions and equations, clock-checking expressions and equations. According to the characteristics of Lustre language, the static semantic analyzer is designed and developed, and its function and correctness are verified by a large number of test cases. In this paper, mainly introducing the design and implementation of the static semantic analyzer.

Keywords: I&C · code generation · semantic analyzer · Lustre

1 Introduction

Nuclear Advanced Safety Platform Instrument Control system (NASPIC) is a set of devices used to ensure the safe and reliable operation of nuclear power plants. As an important part of NASPIC, the function of NASPES is to provide a high assurance application software development environment for I&C engineers. It is a design platform integrating control algorithm design, simulation, verification and code generation. Its interface is shown in Fig. 1. The I&C engineers design the graphical control algorithm in NASPES. Then, the functional correctness of the algorithm is verified in simulation tools. Finally, the graphical control algorithm is transformed into the target C code by the trusted code generator. And after the generated C code is compiled, it is downloaded to the controller to run. At present, the code generators used in the nuclear safety level I&C system are all imported from abroad, such as SCADE KCG. Based on the formal method

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 396–409, 2023.
https://doi.org/10.1007/978-981-99-3455-3_40

and compilation technology, a code generator is designed and developed in the auxiliary theorem prover Coq [1, 2]. Its function is to transform the Lustre code corresponding to the function block diagram into C code equivalently. Formal methods are mainly used to develop trusted software in safety critical fields. Because of its difficulty and high cost, people has not paid much attention to this technology. With the increasing requirements of software security in the safety critical fields, formal methods have gradually attracted people's attention again. At present, there are many outstanding software developed by formal methods. Jourdan [3] et al. developed a formally verified static semantic analyzer of C language. X.Leory [4] et al. use formal method to develop CompCert compiler in Coq. Its function is to translate C code into assembly code.

Fig. 1. The interface of NASPES

Graphical control logic developed in NASPES includes control logic information and graphical information. Among them, the control logic is described by Lustre language. Therefore, in fact, the function of the code generator is to translate Lustre code into C code equivalently. The code generation process is shown in Fig. 2. In order to ensure the correctness of the translation from graphical control logic to C code, firstly, static semantic analysis of Lustre code is needed to ensure that Lustre code has no syntax and semantic errors. Then, the translation module of code generator is called to translate Lustre code into C code equivalently. According to the characteristics of Lustre language, this paper completes the design and implementation of static semantic analyzer used in code generator. Static semantic analysis is an important stage in the process of code generation. This paper briefly introduces Lustre language and solves the following technical problems: (1) type-checking expressions and equations. (2) clock-checking expressions and equations. (3) identifier-checking declarations. (4) identifier-checking program. The remainder of the paper is structured as follows: Sect. 2 briefly introduces the grammatical characteristics and special function operators of Lustre language. Section 3 introduces the design of symbol table. Section 4 introduces the functional design of static semantic analyzer. Section 5 gives some test cases to verify the function and correctness of the static semantic analyzer. Section 6 briefly summarizes the above work.

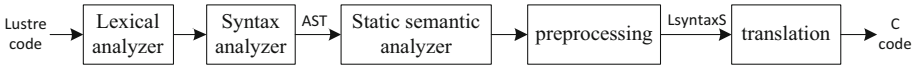


Fig. 2. The process of code generation

2 The Synchronous Data Flow Language Lustre

2.1 Lustre Syntax Features

In this section, the extended Backus Naur Form (BNF) is used to briefly describe the syntax rules of Lustre language. The detailed introduction of Lustre language can be found in literature [5, 6]. Lustre program structure described by BNF is shown in Fig. 3. It's mainly composed of three parts, including user-defined type declarations, global constant declarations and function declarations.

```
<Lprogram> ::= <Lnode>*
<Lnode>::=
                <LtypeDecs>        /*type declarations*/
              | <LconstDecs>       /*const declarations*/
              | <LnodeDecs>        /*function declarations*/
```

Fig. 3. The structure of Lustre program

1. **User-defined type declaration**

The basic data types supported by Lustre language include int, bool, real, float and char. I&C engineers can use the above basic data types to define some complex data types, such as structures, arrays and enumerations. The user-defined type declarations described by BNF are shown in Fig. 4. And the word *type* is the keyword of type declaration. For example, declaring a structure data type *type analog = {value: real, status: bool}*.

```
<typeDecs>::= type  <typeDecList>   /*type declaration*/
<typeDecList>::= <typeDec>*
<typeDec>::= ident = <type>;
```

Fig. 4. The declaration of type

2. **Global constant declaration**

The global constant declaration described by BNF is shown in Fig. 5, where the word *const* is the keyword. For example, declaring an integer constant *const _L1:int = 5*.

3. **Function declaration**

The concept of function in Lustre program corresponds to a basic block in FBD programming. The function declaration described by BNF is shown in Fig. 6. There

```
<constDecs>::= const  <constDec>*        /* const declaration*/
<constDec>::=ident:type=<const>;
```

Fig. 5. The declaration of const

are two kinds of functions in Lustre language, one is a function that supports temporal operations, and the keyword is node. The other is a function that does not support temporal operations and the keyword is function.

```
<LnodeDecs>::=<LndType><ident><LndArgs><LndRets><LndBody>     /* function declaration* /
<LndArgs>::=[<ident>:type]+                                    /* input parameters*/
<LndRets>::=[<ident>:type]+                                    /* output parameters*/
<LndBody>::= <varBlk> let <LeqStmt>tel                         /* function body*/
<LndVarDecs>::= var [<ident>:type]*                            /* local variables*/
<LeqStmt>::=<lhs>=<expr>                                       /* equations*/
<lhs>::=<ident>+                                          /* right value of equations*/
```

Fig. 6. The declaration of function

2.2 Lustre Special Function Operator

In addition to basic arithmetic operators and logical operators, commonly used special function operators include temporal operators and *when* operators. This section will briefly introduce the usage and semantics of commonly used special function operators. The detailed introduction of special function operators can be found in literature [7, 8].

The *pre* operator is a basic operator and its function is to access the value of the previous period of expression. It should be noted that the value of the previous cycle of the first cycle is undefined, so it is generally necessary to initialize it first. *Pre* operator can act on either a single expression or multiple expressions at the same time and produce the same type and number of outputs as inputs.

The - > (arrow) operator is often used together with the *pre* operator, and its function is to initialize the value of the first period of the data flow. It can act on either a single expression or a list of expressions. The number, type and clock of the two input parameters must be the same. The- > operator will not affect the clock of the input parameters, and the number, type and clock of the output values are consistent with the input parameters.

The *fby* operator can be equivalently expressed as *fby*(b) by pre operator and- > operator. *Fby*(b) = a- > *pre fby*(b; n-1; a). if n = 1, it means binary *fby* operator, whose function is to delay the input data by one cycle. if n is not equal to 1, it means ternary *fby* operator, whose function is to delay the input data for multiple periods.

The *when* operator is a filter operator, whose function is to filter out the data of a specific period according to the value of the clock. The *when* operator has two input parameters, a data flow and a clock expression. If the calculation result of the clock expression is true, the result of the *when* expression is equal to the result of the current period of the first parameter.

3 The Design of Symbol Table

This section mainly introduces the data structure that needs to be constructed in the process of static semantic analysis. In order to develop the static semantic analyzer, it's necessary to construct corresponding data structure to collect identifier information. First, modeling the binary sorting tree in Coq, and the corresponding node access and storage operations are defined. Second, based on the definition of binary sorting tree, a symbol table for storing identifier information is constructed. The binary sorting tree defined by inductive type in Coq is shown in Fig. 7.

```
Inductive NasTree (A : Type) : Type :=
  | Leaf : NasTree A
  | Node : NasTree A -> option A -> NasTree A -> NasTree A.
```

Fig. 7. The inductive definition of binary sort tree

Binary sorting tree *NasTree* is defined as polymorphic type, which can store any type of data. Its definition contains two constructors, among which the constructor Leaf represents a leaf node and does not store any data. The constructor Node represents an internal node, where the first parameter *NasTree* A represents the left subtree, the second parameter stores data, and the third parameter *NasTree* A represents the right subtree. This binary sorting tree has the following characteristics: (1) the index value of any left child node in the tree is twice larger than that of its parent node (one more constructor *XO*). (2)The index value of any right child node is larger than the index value of its parent node by 2 times and 1(one more constructor *xI*). Basing on the above definition, binary tree related operations are defined in Coq, including the function *visitchild (a: type) (id: positive) (t: NasTree a)* is defined to access binary tree nodes and the function *insertchild (a: type) (id: positive) (val: a) (t: NasTree a)* to store data to the binary tree nodes.

Symbol table is an important data structure for storing semantic information of Lustre program, and its main task is to collect as much information as possible related to identifiers. In the process of semantic analysis, the symbol table saves the identifier and the attribute information of the identifier, including type, clock, value and so on. All identifiers in Lustre program are mapped as a sub-item in symbol table, but the attribute information of different kinds of identifiers is different. For example, the information of variable identifiers only includes type and clock information. The contents stored in the symbol table are the basis for the static semantic analysis.

According to the scope of identifier and the need of subsequent algorithm development, the whole symbol table is divided into six parts, including a type declaration symbol table, a global constant declaration symbol table, a function declaration symbol table, a function input parameter declaration symbol table, a function output parameter declaration symbol table and a local variable declaration symbol table. The structure of symbol table is shown in Fig. 8. A Lustre program has a global scope and multiple local scopes, that is, each function has a local scope.

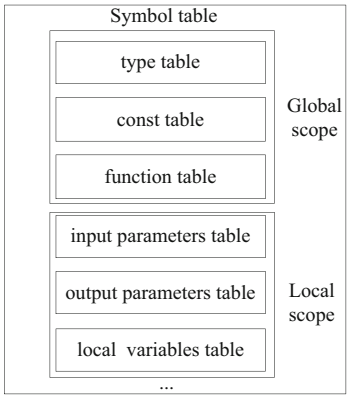


Fig. 8. The structure of symbol tables

The six parts of the symbol table are all realized based on the constructed binary sorting tree. Taking the following code as an example, the specific design and implementation of symbol table are given in Fig. 9.

```
Definition constEnv:Type := nasTree (Ltype*const).
Definition varsEnv:Type := nasTree  (Ltype*clock).
Definition ndEnv:Type:= nasTree  (bool* list Ltype).

Record symbTable : Type := generalSymbTable
  { tyDecsSymtbl: varsEnv;                    /*type table*/
    constDecsSymtbl: constEnv;                /* const table*/
    nodeDecsSymtbl: ndEnv;                    /* function table*/
    ndInputsSymtbl: varsEnv;      /*input parameters table*/
    ndOutputsSymtbl:varsEnv;   /*output parameters table*/
    ndVarSymtbl: varsEnv              /*local variables table*/
}
```

Fig. 9. The design of symbol tables

Among them, the symbol table *tyDecsSymtbl* registers user-defined data type information, including type name (type name is expressed by Coq binary number), type and clock. In addition, if the declared type is a structure, the information of the structure member list also needs to be registered in the symbol table *tyDecsSymtbl*. Symbol table *constDecsSymtbl* registers global constant declaration information, including global constant name, type and constant value. In addition, if the declared global constant is of enumeration type, the information of enumeration member list also needs to be registered in the symbol table *constDecsSymtbl*. Symbol table *nodeDecsSymtbl* registers function declaration information, including the type of function and the type list corresponding to the output parameter list. Symbol table *ndInputsSymtbl* registers function input parameter list information, including input parameter name, type list of input parameter list and clock list. The symbol table *ndOutputsSymtbl* registers the function output parameter list information, including the output parameter name, the type list of the output parameter

list and the clock list. The symbol table *ndVarSymtbl* registers the function local variable declaration information, including variable name, variable clock and type.

4 The Design of Static Semantic Analyzer

4.1 Identifier-Checking Declarations

The function of identifier-checking declarations is mainly to check whether there are any syntax errors of repeated definition of identifiers in Lustre program. According to the structural characteristics of Lustre program, a Lustre program is divided into a global scope and multiple local scopes, where the global scope includes a type declaration area, a global constant declaration area and a function declaration area. And each function is a local scope. According to the characteristics of function definition, a function declaration is divided into input and output parameter areas and function local variable declaration areas. It is required that the identifiers registered in the three symbol tables in the global scope cannot be repeated with each other. The identifiers registered in the three symbol tables in the local scope cannot be repeated with each other and can be repeated with the identifiers registered in the symbol tables in the global scope.

The description of the algorithm: The method of registering while checking is adopted to check the identifier declarations. During the process of parsing, Coq binary numbers are used to represent each identifier abstractly. However, the same identifier has the same Coq binary numbers. Therefore, based on this, the uniqueness check task can be completed when the identifier is registered in the symbol table. The uniqueness check of identifier becomes the uniqueness check of Coq binary number corresponding to identifier. The principle of checking the uniqueness of identifiers in programs is similar. Here, taking the identifier-checking in constant declaration statements as an example, the algorithm flow chart is shown in Fig. 10. The specific procedures are shown as follows:

Step1: Traversing the abstract syntax tree AST and registering the constant declaration identifier into the symbol table *constDecsSymtbl*. Before registration, look up whether Coq binary number corresponding to this identifier exists in the symbol table. if it has been existed, entering step 2. Otherwise, entering step 3.
Step 2: Reporting the error message "*This identifier has been defined repeatedly*".
Step 3: Registering the constant declaration identifier information into the symbol table *constDecsSymtbl*.
Step 4: Repeating steps 1, 2, 3 and 4 until finishing the identifier-checking of all constant declaration identifiers.

4.2 Identifier-Checking Programs

It's main function is to ensure that identifiers are used correctly in Lustre program. The task includes three parts: (1) the definition of identifier, only allowing letters or underscores at the beginning. (2) Check whether the identifiers used in the program have been declared already. (3) Global identifiers and input parameters cannot be used as the left value of equation.

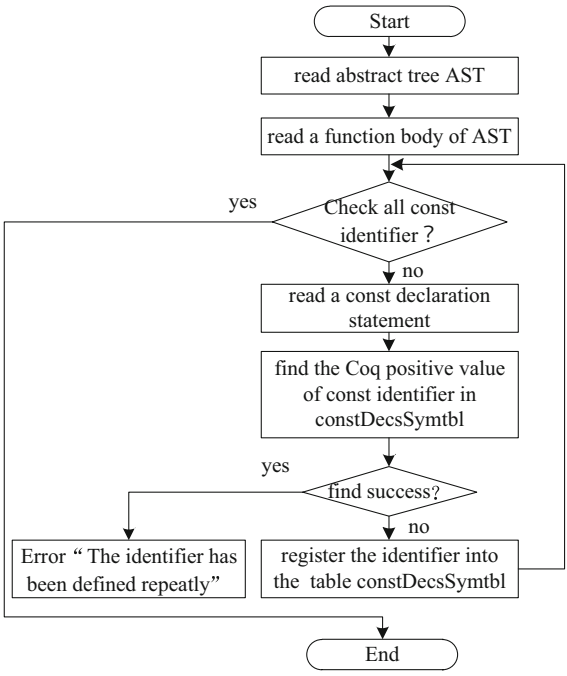


Fig. 10. The process of checking const identifier

The description of the algorithm: based on the symbol table, the algorithm of identifier-checking program is realized in Coq. According to the index value *coqName* corresponding to identifiers appearing in different areas of the program structure, the corresponding symbol table is traversed. If the identifier is not found, it means that the identifier has not been declared before, and the error message should be output, and the subsequent processing of the code generator should be stopped. The flowchart of identifier-checking program on the left side of the equation is shown in Fig. 11. The checking principle of the identifier on the right side of the equal sign of the equation is similar, so it is not repeated here.

4.3 Type-Checking Expressions and Equations

The function of type-checking Lustre program mainly includes two parts: (1) type checking expressions. (2) type checking equations. The task of type checking expressions is to check the legality and consistency of the types of operands acted by arithmetic and logical operators. For example, the equation $s = e\ and\ 42$, where the type of e is *bool* and the type of operator *and* is bool $\times$ bool $\rightarrow$ bool. If two *bool* type inputs are provided to operator *and*, then output a *bool* type value. However, the type of second input parameter in the equation is *int,* which Auxiliary theorem prover Coq is selected to accomplish the development of the code generator. And it can also be used to prove the semantic

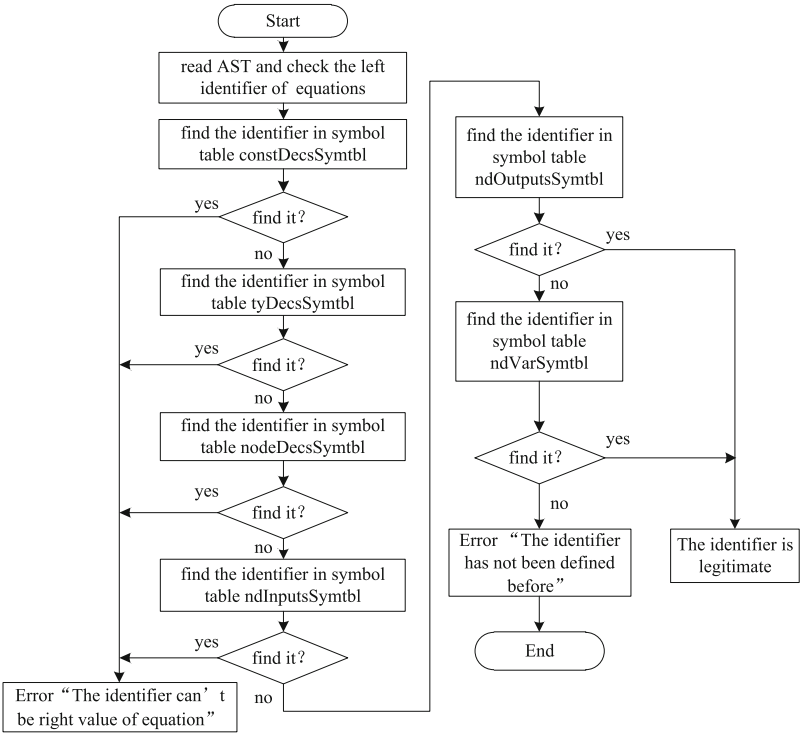


Fig. 11. The flowchart of identifier validity check

preservation of transformations. According to the compilation technology and the characteristics of Lustre language, the overall architecture of code generator is divided into three parts including auxiliary function module, front-end and back-end. [9].

The description of algorithm: The type checking expressions is realized by the created symbol table, the information registered in the symbol table includes the type information of identifiers, and the identifiers defined in the program and the types of identifiers are classified and recorded in the symbol table. For the specific implementation of the algorithm, it is still based on Coq matching pattern. If different kinds of basic expressions are matched, the corresponding types of operands in the expressions are checked. The flowchart of type-checking is shown in Fig. 12.

The result of type-checking expression is the basis of type checking equation. After finishing type-checking expressions in the program, the type of expression is saved in the abstract syntax tree *LsyntaxS*. For example, after type-checking the expression $a + b$, in which the types of a and b are both *int*. The type of the expression will be saved as *int*. Based on the result of type-checking expression, we can check the consistency of the types on the left and right sides of the equation. The flow chart of type-checking equation is shown in Fig. 13.

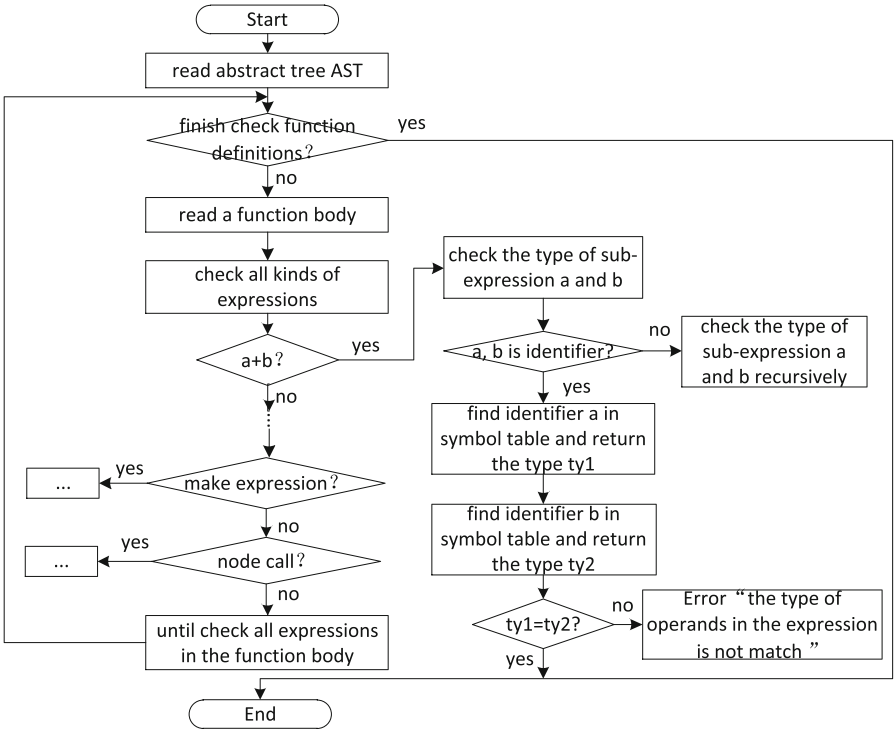


Fig. 12. The flowchart of expression type consistency check

4.4 Clock-checking Expressions and Equations

The function of the operator *when* is to filter the data flow periodically, so the data flow in the program may have different rates. Specifically, the filtered data stream may have no data in some periods. If the clocks in expressions or equations are different, this may lead to the problem that some variables have no data in the current period. For example, two data streams a and b are shown in Table 1, we can see that the rate of a is faster than that of b. And the expression $a + b$ does not meet the requirements, because some periods of b have no corresponding values. The purpose of clock-checking is to find such errors in Lustre program.

The task of clock-checking mainly includes clock-checking expressions and clock-checking equations. Clock-checking expressions requires that the clocks of operands acting on operators are the same. The clock-checking expression flow chart is shown in Fig. 14. In order to finish clock-checking equation, it is required that the clocks on both sides of the equation are the same, and the clock-checking principle is familiar with the type-checking equation, so it is not repeated here.

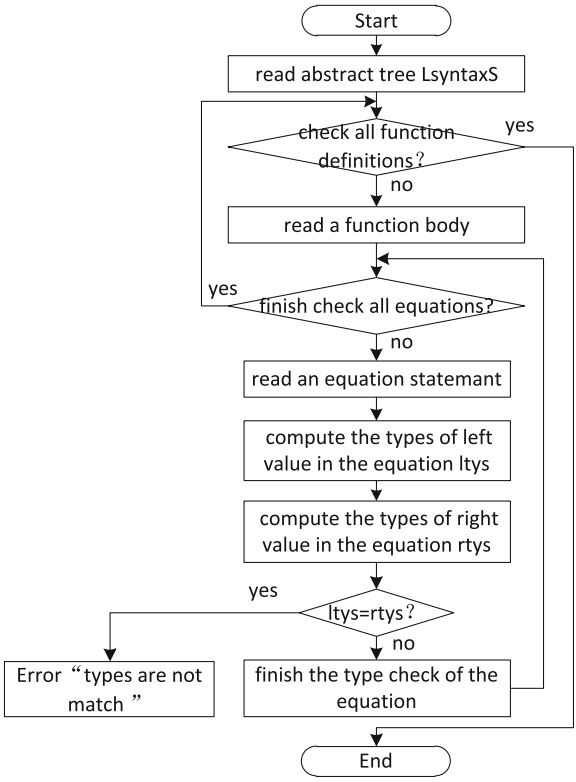


Fig. 13. The flowchart of type-checking equation

Table 1. Two data flows a and b with different clocks

a	1	2	1	5	7	9	5	4	…
b		8		3		2		7	…

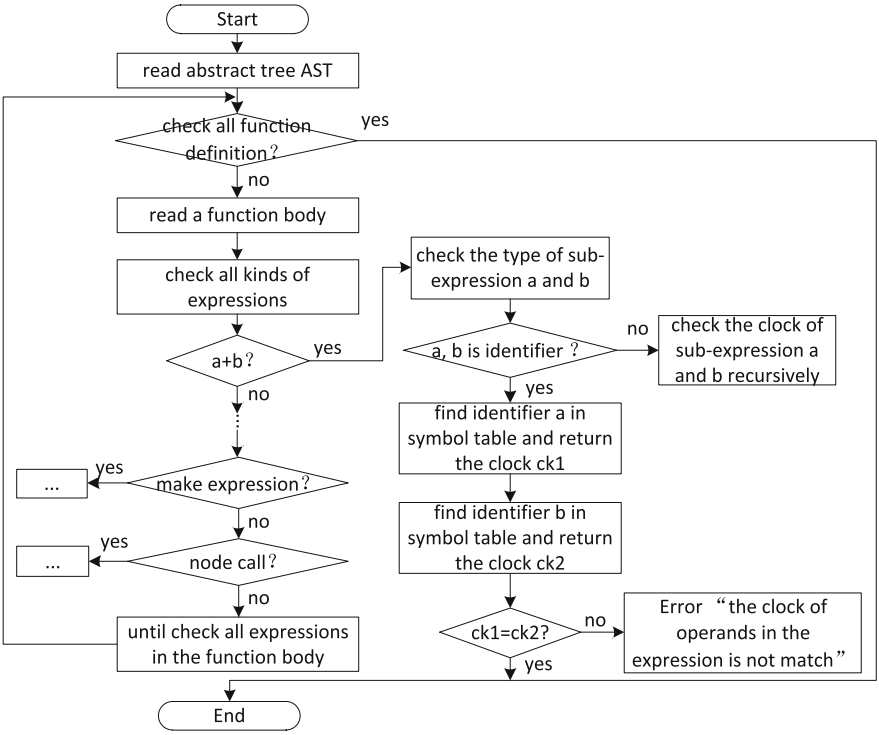


Fig. 14. The flowchart of clock-checking expression

5 Case Analysis

The function of the static semantic analyzer is to find the syntax and semantic errors of the input Lustre program. In order to test the function of static semantic analyzer, mainly writing test cases with specific errors to verify the correctness of function algorithms. When the static semantic analyzer finds that there exists errors in the program, it should immediately stop code generation and report the corresponding error message. The four test cases shown in Fig. 15 are introduced to four different kinds of errors. They are used to test the function of static semantic analyzer and show the effect of each checking algorithm. The test results are shown in Fig. 16. First, Executing the code generation command "./NASCG…". Then, the screen gives an error message "Error:…" and stops the code generation.

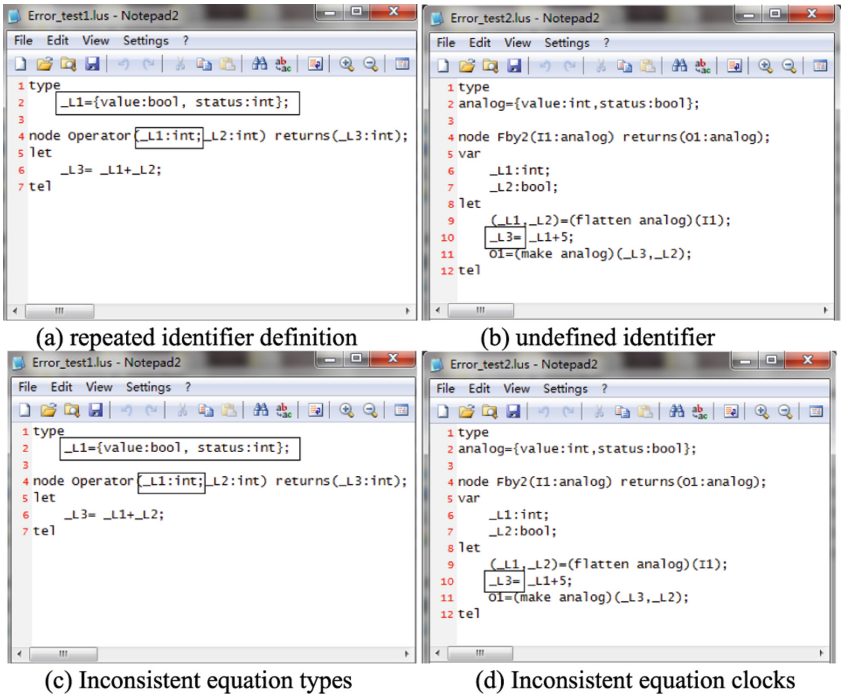


Fig. 15. The Lustre code of test cases

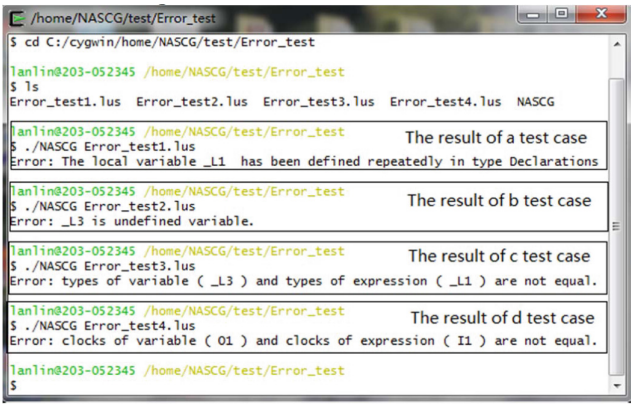


Fig. 16. The results of test cases

6 Conclusions

Code generators are widely used in developing application software of nuclear safety DCS system. And its function is to transform Lustre program corresponding to graphical control logic into C program. So the correctness of generated C program is directly

decided the safety and assurance of nuclear power plant operation. In this paper, the static semantic analyzer is designed and developed to make sure the correctness of the source Lustre code of the input code generator. It is the basis of ensuring the correctness of the translation from Lustre to C. The final test results show that this code generator based on the static semantic analyzer can translate Lustre program into C program correctly.

References

1. The Coq Development Team. The Coq Proof Assistant Reference Manual Version V8.3 [EB/OL]. http://coq.inria.fr/
2. Interactive theorem proving and program development: Coq-Art: the calculus of inductive constructions (2004)
3. Jourdan, J.H., Laporte, V., Blazy, S., et al.: A formally-verified C static analyzer. Acm Sigplan Notices **50**(1), 247–259 (2015)
4. Bourke, T., Brun, L., Dagand, P.-É., et al.: A formally verified compiler for lustre. Acm Sigplan Notices **52**(6), 586–601 (2017)
5. Colaco, J.L., Pagano, B., Pouzet, M.: Scade 6: a formal language for embedded critical software development. In: International Symposium on Theoretical Aspects of Software Engineering. IEEE Computer Society (2017)
6. Scade-suite home [WB/OL]. http://www.esterel-technologies.com/products/scade-suite
7. Caspi, P., Pilaud, D., Halbwachs, N.: Lustre: a declarative language for programming synchronous systems. Symp. Principles Program. Lang. Acm **259**(89), 911 (1987)
8. Caspi, P., Pilaud, D., Halbwachs, N., Plaice, J.: LUSTRE: a declarative language for programming synchronous systems. In: 14th ACM Symposium on Principles of Programming Languages, January 1987
9. Wei, J., Lin, L., Bin, Y., Hou, R.B.: Design of code generator for safety level I&C software of NPPs. In: Xu, Y., Sun, Y., Liu, Y., Gao, F., Gu, P., Liu, Z. (eds.) Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems. ISNPP 2021. Lecture Notes in Electrical Engineering, vol. 883, pp 479–489. Springer, Singapore (2022). https://doi.org/10.1007/978-981-19-1181-1_46

Main Instrumentation and Control Systems for Units 7&8 of Tianwan Nuclear Power Station

Wan-Chun Yang(✉)

China Techenergy Co., Ltd., Beijing, China
yangwanchun@cgnpc.com.cn

Abstract. Tianwan Nuclear Power Station (TNPS) Units 7&8 with total capacity of 2 × 1200 MW, is located in Lian Yun Gang City, Jiang Su Province in China, which will apply the pressurized water reactor of VVER-1200 (AES-2006). China Techenergy Co., Ltd. (CTEC) is the supplier of the main instrumentation and control system (Main I&C) for Units 7&8 of Tianwan Nuclear Power Station.

Keywords: VVER-1200 · Nuclear Power Station · Digital I&C System

1 Introduction

The VVER-1200 (AES-2006), which is the generation 3+ nuclear power technology of Russian, is widely applied in Russia and international market. The main instrumentation and control systems of VVER-1200 projects adopted in the Russia and international market are distributed control systems from European company. It is first time to propose that the instrumentation and control system solution for VVER1200 projects based on the Platforms from China Techenergy Co., LTD, the Platforms from CTEC are met the requirements of code and standard, defense in depth and diversity, and system requirements of VVER-1200. This paper is mainly focused on the overall architecture of the solution based on CTEC's technology, FirmSys Platform, HOLLiAS-N and FitRel platform.

FirmSys platform is a safety digital I&C system based on CPU technology to meet all the requirements for Class I systems in nuclear power plant (NPP). It is a Distributed Control architecture specifically designed for, functions of top safety classification which include reactor trip system, engineered safety feature actuation system. The most strictly Codes and standards and government regulations are applied for Generic qualification of FirmSys platform.

HOLLiAS-N is a distributed control system for process automation in power plant control. The plant operation is monitored and controlled by HOLLiAS-N platform, including NPP normal operation, reactor and Turbine Generator start-up and shutdown, to adjust automatically and prevent plant operational transients. In addition, HOLLiAS-N platform is applied to the BDBA I&C system which is designed to cope with nuclear power plant severe accident.

FitRel platform is applied to the Diversity Protection System (DPS) which is designed to perform safety functions in case of software Common Cause Failure (CCF) of RPS.

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 410–414, 2023.
https://doi.org/10.1007/978-981-99-3455-3_41

2 Overall Main I&C Architecture for TNPS Units 7&8

Figure 1 shows the overall architecture of main digital I&C systems of TNPS Units 7&8.

The main digital I&C systems/functions are distributed and implemented on 4 levels:

- L0, field level. It consists of sensors, transmitters, limit switches) and the actuator interface equipment (pilot valves and their associated interface relay, electro-pneumatic converters, drive actuators, switch-gear, and power electronic equipment);
- L1, automation level. It implements signal conditioning, calculation and automatic adjustment, all plant equipment and systems are controlled;
- L2, human-machine interface (operation and monitoring) level. It includes computerized equipment by which the plant operator can operate the plant (manual control and information means), monitor the status of plant operation, and maintenance and service operations are fulfilled on the digital I&C itself;
- L3, UNIT management (or Plant Management) level. It consisted of computerized equipment, fulfills the site management including normal maintenance, periodic tests, spare parts

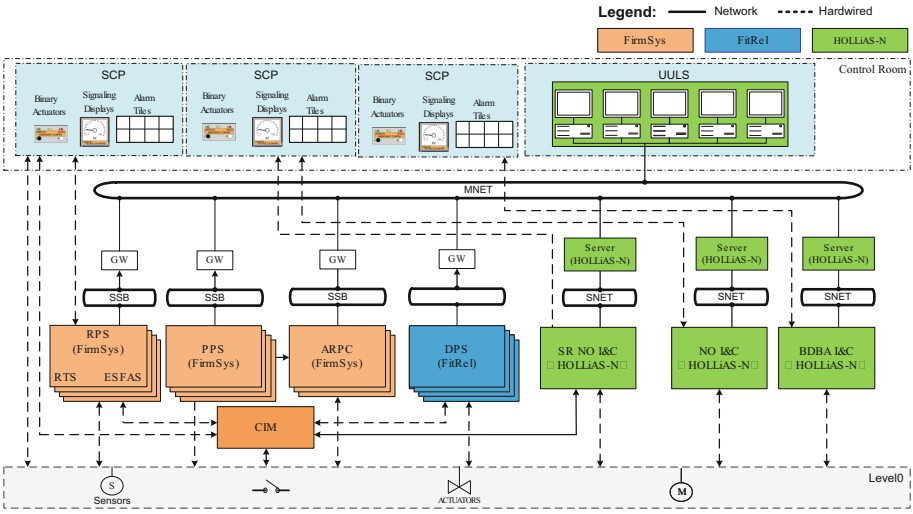


Fig. 1. The Overall Architecture of Main I&C System of TNPS Units 7&8

The RPS (Reactor Protection System) is realized by FirmSys platform based on CPU technology, and includes of Signal Process Cabinet (SPC), Reactor Protection Cabinet (RPC), Engineered Safety Feature Actuation Cabinet (ESFAC), Priority Actuation Control (PAC) and Gateway. The brief descriptions are as follows:

- SPC performs the signal conditioning, isolation and distribution functions.
- RPC mainly performs the initiating functions of reactor trip which includes fourfold redundant and independent divisions. Each RPC division consists of two sets of controller with sensors/transmitters' diversity.

- ESFAC receives the partial actuation signals from RPC and performs the voting functions of ESF and the control functions of supporting systems, and send the actuation signals to PAC. ESFAC also includes fourfold redundant independent divisions and each division has two sets.
- PAC mainly performs the functions of priority management, component drive and information collection. The priority management among different commands from RPS, DPS, PPS, manual operation and SR NO I&C, is accomplished by CPLD in the Component Interface Modules (CIM), which is diverse from the microprocessor technology and will not be impacted by CCF of RPS. The Gateway performs the signal transmission and protocol transfer from RPS to UULS. Information (such as the related parameters and trigger signals) are transmitted to the control room (MCR/SCR) to indicate and alarm through gateway.

The PPS and ARPC are also realized by FirmSys platform. PPS consists of Preventive Protection Cabinet (PPC) and Gateway. The brief descriptions are as follows:

- PPC mainly performs preventive protection functions to reduce and/or to limit the reactor power in order to prevent the actuation of RPS in case of operational occurrences. PPC includes fourfold redundant independent division. As the function of PPC is assigned to safety category B, there are no diverse sets in PPC.
- Gateway of PPS performs the signal transmission and protocol transfer from PPS to UULS. Information (such as the related parameters and trigger signals) is transmitted to the control room (MCR/SCR) to indicate and alarm.
- ARPC consists of Automatic Reactor Power Controller (ARPC) and Gateway, which is designed to adjust reactor power according to the TG power while maintaining the specified steam pressure, to keep the value pre-set for neutron reactor power and limit steam pressure increase. ARPC is implemented as one three-train set arranged in one separate cabinet using microprocessor equipment with generation of control commands to move the control rod groups based on 2-out-of-3 majority logic. Gateway of ARPC performs the signal transmission and protocol transfer from ARPC to UULS. Information (such as parameter and status) is transmitted to the control room (MCR/SCR) to indicate and alarm.

On the automation level in the middle of Fig. 1, DPS is shown. This system is classified as category B. DPS performs the function of diverse reactor trip and ESF actuation, which is to cope with software common cause failure (CCF) of RPS and anticipated transient without scram (ATWS). DPS is independent from the I&C platform used by RPS, which is realized by FitRel platform based on PFGA technology to avoid CCF of RPS, and consists of fourfold redundant divisions.

On the automation level on the right of Fig. 1, BDBA I&C is shown. This system is classified as category B. BDBA I&C is to cope with severe accidents, and considers the experience feedback from Fukusima NPP accident. BDBA I&C is realized by HOLLiAS-N platform based on microprocessor technology, and configured with two redundant divisions.

SR NO I&C is classified as category B. NO I&C is classified as category C.

The SR NO I&C is realized by HOLLiAS-N platform and configured with four redundant divisions. The NO I&C is realized by HOLLiAS-N platform and configured with two divisions.

Main Control Room (MCR) is the monitoring center of the nuclear power plant. It is consisted of workplace for operational control of the process and acquisition of information (OWP), large-screen displays for representation of the main information (LSD) and traditional mosaic monitoring and control panels.

OWP is designed for monitoring and control of technological process tasks of the unit in all modes of normal operation, abnormal operation and severe accidents. Traditional mosaic monitoring and control panels are designed to control technological process on NPP in case of the failure of the OWP.

If MCR is damaged (in case of fire, etc.), power unit will be shut down and controlled by the same safety functions (as in MCR), operation and control carried out from the Standby Control Room (SCR).

SCR is designed to bring the power unit into sub-critical cooled down condition (cold state) and maintain that state. It is consisted of OWP and traditional mosaic monitoring and control panels.

3 Main I&C System in TNPS Units 7&8

Defense-in-Depth is a design principle which ensures multiple layers of the I&C structure and architecture, consisting of redundant components or diverse control systems to act processively against the controlled variables deviation from the set value, as anticipated operational occurrences and postulated initiating accidents. This design principle is applied in the safety-important I&C systems for main I&C of TNPS Units 7&8.

The Main I&C system can be subjected to software and hardware common cause failures (CCFs) which could render the entire system inoperable. CCFs is a key interest for an I&C system design, which is required in nuclear safety-related applications and functions including RPS and ESFAS. While CCFs are considered being beyond design basis, the digital RPS functions should be protected against CCFs.

The Main I&C System in TNPS Units 7&8 is designed to meet following requirements:

- I&C system is implemented as integral design solutions, proven systems and technical principles are used.
- t shall enhance the NPP possibilities to fulfil safety functions.
- I&C system shall implement automatic monitoring and controlling of operational conditions of the NPP. In case of the controlled de variables deviations from the set values or the conditions defined in the NPP general design, the I&C system shall adjust in returning to normal conditions to keep the UNIT ensuring safety.
- I&C system shall be designed as a distributed architecture according to hierarchical structure and different levels.
- It shall have the functions of self-diagnostics and good survivability.
- Safety I&C systems should meet requirement of testability, fail safe, periodic test, redundancy, isolation of electric and communication and physical, diversity.
- The digital I&C system performs the following functions:

- Data measuring and processing.
- Providing loop control.
- Monitoring plant parameters (safety and non-safety variables), alarm functions and initiating appropriate actions.
- Information display at the center control room.
- Data logging.

4 Conclusion

In TNPS Units 7&8, the state-of-art total integrated solution of Digital I&C systems are supplied by CTEC, including three advanced PLATFORMs. Some new powerful components and devices, software packages are used to meet the high demands on VVER-1200 safety, reliability and availability.

We can conclude that the I&C systems of TNPS Units 7&8 are mature and proven, and their performance can assure the safe and efficient operation of the plant.

References

1. ATOMPROEKT, Preliminary Safety Analysis Report for TNPS Unit 7&8. Section 7.8
2. IAEA NP-T-1.5, Protecting Against Common Cause Failures in Digital I&C Systems of Nuclear Power Plants. Vienna (2009)
3. U.S. NRC, NUREG-0800, Section 7.8 Diverse Instrumentation and Control Systems. Rev.6, August (2015)
4. U.S. NRC, NUREG-0800, BTP 7-19 Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based I&C Systems. Rev.8, January 2021
5. 10 CFR 50.62 Requirements for reduction of risk from ATWS events for light-water-cooled nuclear power plants. August 28, 2007

Study on Updating and Modification of Computer-Based Procedure System of Nuclear Power Plant

Jie-Mei Zhang(✉), Yong-Quan Xie, and Yan-Tong Luo

China Nuclear Power Design Co., Ltd., I&C Department, Shenzhen, Guangdong, China
354002030@qq.com

Abstract. This paper describes the development process of the computer-based procedure system (CBPs) and the requirements of regulation and standards. Based on the operating experience of the digital control system in CPR1000 nuclear power plants, it puts forward the user needs of the CBPs of the second generation nuclear power plants in service in China to improve the level of automation, the convenience of operation and maintenance management, and the friendliness of human-computer interface. The requirements and constraints for updating and modification of nuclear power plants in service are analyzed, including consideration of six aspects, such as software and hardware platform performance, operator operation habits, operation procedure architecture, power plant operation and maintenance plan, verification and training, and safety and economic benefits. Different types of CBPs is compared and analyzed, and the updating scheme of the CBPs of the nuclear power plant in service is proposed, which is divided into three stages. The first stage is to realize a well used computer-based procedure system. The second stage is to realize a computer-based procedure system with higher level of automation. The third stage is to realize a highly intelligent computer-based procedure system. This paper introduces the development and implementation process of the first level updating scheme of the CBPs of CPR1000 nuclear power plants. And it briefly describes the design principles and main technical points of the transformation scheme. The verification plan is proposed based on different platforms and different objects. The future development direction of the CBPs is analyzed. And personal prospects and solutions are proposed.

Keywords: Digital · Procedures · Computer-based Procedure · Human-machine Interface · Intelligence

1 Introduction

Operating procedure consists of a series of standard instructions that operators of nuclear power plants refer to and execute in order to operate reliably and efficiently under normal operation state or abnormal accidents. According to Rasmussen's human error classification method, the guidance of operation procedure can change knowledge-based behavior into rule-based behavior, reduce the accidental risk introduced by operators'

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 415–422, 2023.
https://doi.org/10.1007/978-981-99-3455-3_42

knowledge-based decision-making, and significantly reduce the probability of human error, especially in complex accident conditions, which can reduce the negative impact caused by the degradation of operators' knowledge capacity under stress.

As the first self-designed digital main control room in China, Ling'ao Phase II nuclear power plant adopts Computer-Based Procedures systems (CBPs) to maximize the advantages of digital control system (DCS). A good Computer-Based Procedures system can significantly improve the efficiency of personnel and reduce the unnecessary extra tasks brought by the implementation of paper-based procedures, such as document switching, task tracking, information searching, etc. Operators need to read, memorize and implement paper-based procedure while performing monitoring tasks, which may lead to human errors. However, due to the independent design of the CBPs for the first time, the lack of experience in the design and operation of digital operation strategy, and the limitation of software and hardware platforms, the CBPs of Ling'ao Phase II nuclear power plant has some shortcomings, such as low automation level, inflexible and inconvenient use, and the structure of procedure is not conducive to the implementation of digital strategy. With the accumulation of operation experience in applying digital man-machine interface operation strategy, the rapid development of information and intelligent technology in recent decades, and the successive commissioning of advanced three-generation nuclear power reactors, the updating and modification of CBPs in plant in service has been put on the agenda.

2 Standard and Regulations

Regulations and standard have been formulated at different levels and dimensions.

Chapters 7, 8 and 9 of HAD 103/01 expounds the requirements of operating procedures, including the safety standard, approval process, operation limitation requirements, qualifications of compilers, etc., but do not involve the detailed requirements of CBPs [1].

Chapter 8 of NUREG 0700 expounds characteristic elements of CBPs, detailed CBPs design and human factors engineering review guidelines of human-machine interface [2]. NUREG 6634 further expands the technical basis of CBPs compilation guidelines and human factors engineering design guidelines, and suggests the method of developing procedure design according to human factors engineering design process [3].

NB/T 20270 is compiled with reference to IEEE-1786, stipulates the human factors engineering criteria for various CBPs designs [4], and gives the human factors engineering requirements that should be followed by a more detailed and enforceable CBPs.

IEC 62646 stipulates the whole life cycle requirements of CBPs, including the principle of CBPs, classification of types, use environment, system function requirements, detailed design requirements, operation and maintenance, etc. [5].

On the basis of IEC 62646, NB/T 20267 refers to the experience of CBPs design, operation and maintenance of nuclear power plants in China, puts forward the requirements of display format, functional design, design implementation and regular operation and maintenance that CBPs of nuclear power plants should follow [6].

The regulations and standard of CBPs vary from country to country, and the design methods of CBPs of different nuclear plant are also quite different. However, the classification definitions of CBPs in various regulations and standard systems are basically the same, as shown in Table 1 for details.

Class I CBPs only provide procedure display on the computer, and do not provide any real-time data display, logic processing or equipment functions, but can provide navigation links within the procedure.

Class II CBPs is characterized by embedding dynamic process data in the procedure, and can evaluate the execution conditions or logic of the procedure according to the dynamic process data, which can support the operator to make decisions, but does not have direct control function.

Class III CBPs include embedded soft control unit, which can be used to issue control instructions to plant equipment. Operators can complete actions required by procedures without leaving CBPs, and should also have automation functions, that is, automatic task sequence execution based on procedures.

Table 1. Classification of CBPs

Function	CBP system		
	Class	Class II	Class III
Select and display procedures on a computer	Yes	Yes	Yes
Provide navigation links within or between procedures	Yes	Yes	Yes
Display process parameters of procedure steps	No	Yes	Yes
Evaluate procedure step logic and display valuation results	No	Yes	Yes
Provide operation links to call process display and soft operation functions realized by other systems besides CBP system	No	Yes	Yes
Provide embedded soft operation and issue operation instructions	No	No	Yes
Start procedure-based automation according to operator instructions	No	No	Yes

3 Operating Experience

Class I CBPs in the regulations are generally adopted in the second-generation and second-generation + nuclear power plants that have been put into production in China, that is, the electronic and navigation functions are realized, and special procedure matching displays are designed to assist the implementation of CBPs. After decades reactor year of accumulated operation experience of digital system, users put forward opinions on the shortcomings in the use of CBPs through simulator training and actual unit application, which pointed out the direction for the updating and modification of CBPs.

3.1 Improvement of Automation Degree

Class I CBPs can't give full play to the advantages of DCS informationization. The route of procedures needs to be judged manually by operators, and operators need to switch between CBPs and monitoring display repeatedly. There are risks of human factors, such as wrong selection of monitoring display, wrong positioning of equipment, wrong judgment of information cognition, etc. At the same time, the high workload in the implementation of procedures is not solved, and the automation degree can be greatly improved.

3.2 Improvement of Operation and Maintenance Management

Execution and preservation in CBPs adopts the way of management procedure to indicate people's behavior, while execution, preservation and repeated execution in labelling does not unify standard, which is not conducive to management of recording, training assessment and technical support of procedures. At the same time, the synchronization and timeliness of updating procedures between CBPs and paper-based procedure need to be ensured, and the invalid procedures are marked and downloaded online, to ensure the accuracy and effectiveness of CBPs.

With the rapid development of informationization and intelligence technology in recent ten years, human-computer interface has been revolutionized in mobile phones, automobiles and other industrial fields. More human-computer interaction technologies such as multi-touch, intelligent association, voice and image recognition have been applied maturely. The human-computer interface of CBPs just possess the basic functions of early computers, which introduces unnecessary tasks to operators, such as screen configuration, picture information search, etc., which is inconvenient for efficient task execution and distracts operators' attention.

4 Analysis of Limitation Conditions of Modification

Different from the newly-built plant, for the updating and modification of the in-service plant, in addition to meeting the requirements of regulations, standard and user requirement, it is also necessary to consider the specificity of the in-service plant, and formulate a detailed implementation plan in combination with the operation and maintenance period. The following six limitations need to be considered.

4.1 Capability of Software and Hardware Platform

The technical scheme of updating and modification needs to be realized on the existing software and hardware platform, or can be realized by updating some software and hardware, and does not affect the safety and reliability of the original system. For example, the CBPs of CPR1000 plant is integrated in DCS system, and the technical scheme needs to consider DCS system architecture and server capability capability support.

4.2 Operator's Operating Habits

Users often do not use products according to the original intention and plan of designers, especially nuclear power operators who have undergone high-intensity study, repeated intensive training and long-term operation tasks, and have formed relatively stable personal operation habits. The use of CBPs is closely related to the habits of operators, and violating the inertia thinking of operators may lead to human errors. Therefore, the updating and modification of CBPs should pay attention to the impact on operators' operation habits and the risks brought by inconsistency.

4.3 Architecture of Operation Procedure

CBPs need to be developed based on operating procedure architecture, and a good technical scheme under one operating procedure architecture may not suitable for another. The in-service plant is based on the existing operation procedure architecture in procedure compilation, operator training, operation supervision and other aspects, and the system design and equipment configuration are also matched with the operation procedure. The updating and modification of CBPs should be implemented under the existing operation procedure architecture system as far as possible to reduce other adverse effects brought by the updating.

4.4 Plant Operation and Maintenance Plan

The modification of CBPs usually has an impact on the normal operation of plant, which generally needs to be implemented during the overhaul period with a long time window. Before implementation, it is necessary to formulate a detailed modification work plan in combination with plant operation and maintenance plan, and carry out a preview of the modification implementation.

4.5 Validation and Training

The updating and modification of CBPs has changed the implementation mode of the original operation procedure, which requires complete and sufficient validation on simulator. The system after modification can support operators to complete various operation tasks, and it is necessary to retrain all operators, so that operators can skillfully use the new system to perform operation tasks.

4.6 Safety and Economic Benefits

The purpose of updating is to improve the safety and economy of nuclear power plants. At the same time, it will increase manpower and equipment investment, and it may introduce uncertain risks. Before the implementation of the modification, it is necessary to comprehensively analyze the necessity and comprehensive benefits of the modification. Therefore, the modification scheme should be comprehensively analyzed and considered in combination with relevant information in order to achieve the optimal goal.

5 Updating and Modification of CPR1000 Plant

5.1 Upgrading and Modification Plan

Combined with the opinions of CPR1000 unit users, and considering all aspects of limitations and the advanced experience of the third generation nuclear power plant, the modification plan divided into three stages.

a) The first stage mainly solves the shortcomings of CBPs, improves the convenience of application, increases automatic diagnosis auxiliary reminders, and forms a more easy-to-use CBPs;
b) In the second stage, make appropriate adjustments to the operation procedure architecture, establish an operation procedure architecture that meets the digital operation strategy, and upgrade and reconstruct the CBPs to realize the automatic diagnosis of accident, supplemented by the automatic execution of the procedure sequence of high-load tasks, and form CBPs, which meets the Class III CBPs regulations and standard, and has high automation degree;
c) In the third stage, more intelligent operation and maintenance method and human-computer interaction technology are introduced to realize analog and real-time load analysis of the procedure route, reduce the peak workload of the operator, avoid the decline of the operator's perception and understanding of the overall state of the plant during the procedure execution, introduce diversified human-computer interaction technologies, and increase the technical means of human error prevention, identification and error correction to form a more intelligent CBPs.

5.2 Modification Design Principle

Considering the standard and regulations, DCS product capability, operation habits of in-service power stations, modification implementation time window, operation and maintenance and other influencing factors, the following design principles are formulated for the first stage transformation:

a) It does not change the existing procedure structure and does not affect the procedure usage habits of operators;
b) It does not affect the stability of DCS system and guaranty the calculation margin of DCS system;
c) Improve the execution efficiency of procedures, reduce the workload of operators by increasing automatic diagnosis, automatic monitoring and improving supporting display, improve the execution efficiency, and strengthen the monitoring of key safety parameters of units in accidents;
d) Reduce the risk of human error, and reduce the deviation by reducing the number of personnel judgments and navigation, increasing information auxiliary reminders, and arranging equipment information nearby;
e) Meet the standard of procedure execution record without increasing the extra burden on the operator;
f) It does not affect the rapid transformation of procedure and online upgrade and downloading;
g) Information security/network security issues are not introduced.

5.3 Validation and Confirmation

The modification scheme is validated and confirmed by validation platform, factory test prototype and full-scale simulator, and commercial PWR operators who have obtained operation licenses are used as test subjects. Validation data is collected through workload metrics, questionnaires, observer checklists, post-test personnel interviews, event records, data operation records or video and audio records, then analyzes these data and complete the confirmation report.

6 Future Study

The rapid development of information and intelligent technology provides technical support of software and hardware platform for updating the CBPs of nuclear power plants. The continuous improvement of the public and regulatory authorities' attention to nuclear safety also urges the designer to seek safer, more reliable and convenient means operation monitoring. Intelligence and human-friendly will be the two main directions for research and development and improvement of new systems at present. At the same time, the linkage between design and user operation and maintenance, and the scheme meeting the requirements of plant operation and maintenance management are also the crucial factors for the CBPs to be put into use in the unit. At present, the research and development of the new system is mainly carried out in the following directions:

a) The application of more intelligent technologies, such as automatic screen configuration and automatic information positioning;
b) More friendly operation display, such as richer function of displaying icons;
c) More complete auxiliary support functions, including procedure execution and operation and maintenance management;
d) Human error prevention, such as operation deviation reminder, missing item reminder, etc.;
e) Modular procedure design and online flexible configuration of tasks;
f) Perform route deduction, and carry out dynamic load analysis based on the deduced route to identify the high-load tasks;
g) Large data learning iterative optimization and ultra-real-time computing simulation early warning.

7 Conclusion

This paper describes the development process and requirements of CBPs, analyzes the updating requirements and limitations of plant in service, expounds the updating limitations and modification direction of CBPs, introduces the research and development plan of CBPs modification of CPR1000 nuclear power plant, and looks forward to the future development direction. The updating of CBPs can help reduce the load of operational tasks and improve the nuclear power plant safety.

References

1. HAD 103/01, Operating Limits, Conditions and Operating Procedures of Nuclear Power Plants (2004)
2. NUREG-0700, Human-System Interface Design Review Guidelines (2020)
3. NUREG/CR-6634, Computer-Based Procedure Systems: Technical Basis and Human Factors Review Guidance (2000)
4. NB/T 20270, Application Criteria of Human Factors Engineering in Computerized Operation Procedure System of Nuclear Power Plants (2014)
5. IEC-62646, Nuclear power plants -Control rooms-Computer-based procedures (2016)
6. NB/T 20267, Design Criteria for Computerized Operation Regulations System of Nuclear Power Plants (2014)

Research and Application of BIM + GIS Technology for Underground Pipeline of Nuclear Power Plant

Hui Chang(✉), Dong Zhao, Jiafu Yan, and Zhigang Zhou

China Nuclear Power Engineering Company Ltd., Shenzhen, Guangdong, China
2302624561@qq.com

Abstract. In recent years, nuclear power project management mode of underground pipeline applied gradually BIM to save costs and improve efficiency. GIS technology was applied to show geographical environment and spatial position relationship of underground pipeline. In the article, through in-depth study of BIM and GIS technical theory, application platform for underground pipeline by opening source technology was built. The design rules and model characteristics of underground pipeline were taken as the research objects, and the technical feasibility for BIM + GIS technology was verified. The research would provide basic guarantee for intelligent management of nuclear power's underground pipeline.

Keywords: BIM · GIS · underground pipeline

1 Introduction

The underground pipeline of nuclear power plant was an important part of the construction, and the whole nuclear power plant were distributed, such as water supply pipe, drain pipe, oily wastewater, sewage, HVAC and electric pipe and so on. Most of them were buried underground and had strong concealment. Furthermore, in the same area of nuclear power plant was often repeatedly excavated by different specialties, excavation accidents of directly buried pipes were occurred from time to time. During the construction process, it was found that there was inconsistencies between actual position of pipeline and planning of CAD drawing. The current situation of nuclear power underground pipeline was as follows: on the one hand, the CAD drawings of each specialty planning and construction in the early stage of power plant construction were relatively scattered, and the spatial distribution and position cross relationship of pipeline were not invisibility, on the other hand, with the progress of the project, the underground pipeline would become more and more dense and complex, and the actual construction and planning drawings couldn't be updated at the same time, so these would bury construction hidden dangers for subsequent construction, and even directly cause construction delay and loss serious economic. In view of this, it was urgent to carry out intelligent management of underground pipeline in nuclear power plants to avoid the recurrent of excavation accidents.

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 423–429, 2023.
https://doi.org/10.1007/978-981-99-3455-3_43

With the wide application of BIM technology, Internet of things technology, UAV technology, space-time big data storage technology, GIS technology and so on. Many Scholars had researched BIM and GIS in different angles, such as the research of data transformation and integrated application between BIM and GIS [1], the research of collecting data and building three-dimensional models and constructing BIM + GIS platform, it was important of achieving significant results. Furthermore the application of many enterprises at home and abroad has been quite mature in urban or in plant of underground pipe network. The application and management experience of underground pipe network provided us with valuable reference, and comprehensive integration of existing data resources of underground pipeline, predicting in advance and commanding the site construction by technical means could be fully realized.

2 BIM + GIS Advantage

Building Information Modeling (abbreviate BIM) was a methodology, which could transform the construction object into a unified information model. On the one hand, it could be used to guide all participants to work together based on 3D model, on the other hand, it could be used to manage the whole project information throughout its life cycle [3, 4]. Geographic Information System (abbreviate GIS) was a computer-based tool. 3D GIS could not only express the plane and vertical relations between spatial objects, but also perform spatial query, analysis and statistics [5]. BIM could provide simulated analog of underground pipeline and could provide convenience for modelers to formulate measures of construction and control in advance, and it could also provide information such as cost, progress, operation and maintenance for underground pipeline, and it could also realize integrated management and intelligent maintenance of underground pipeline, and it could realize design, coordination, construction, operation and maintenance [6]. GIS could provide the spatial position information of underground pipeline and simulate the spatial position relationship between underground pipeline and its surrounding environment, and it could realize the query and analysis and management of the spatial information of underground pipeline.

For nuclear power plant, underground pipeline has planned pipeline and temporary pipeline, some pipelines were buried deeply, some pipelines were buried shallowly. At present, BIM was widely used in nuclear power project management, furthermore GIS has been used in nuclear power data for many years. Through research, it was found that the basic idea of BIM design was parametric modeling, BIM payed attention to the presentation of model details, and focused on 3D modeling and information management of model itself. GIS laid emphasis on the external environmental geographic information. Using BIM + GIS technology, the combination of macro and micro management of underground pipeline could be realized, and real-time validity sharing and transmission of internal and external data could be realized, and the real scene of the construction site could be reflected. Finally, the informationize of site construction was promoted and the capacity of facility management was enhanced and the capacity of prediction and command construction was increased.

3 Key Technologies

3.1 Model Data Optimization

3D models were essential to create a realistic world that could be browsed 360 degrees. 3D models of geographic environment of nuclear power plant could be modeled by oblique photography, or by using Maya, 3DMax and other software according to construction drawings, and BIM models of underground pipeline could be modeled by manual modeling or by using Bentley, PDMS, Maya and 3DMax.

The BIM model without optimization was large in volume and with more triangular patches, in order to improve the loading speed and rendering efficiency, BIM model was simplified, transformed and reduced in geometric entity with carrying information or building logic by means of simplify facet. The triangle patches of the BIM model were removed by manually operated at first, only the structure and geometric topological relationship of the BIM model was retained, so as to greatly reduce the storage space occupied by the 3D file. The 3D graphics were viewed by browser or GIS software client, and the operation was repeated until the loading speed was acceptable. Later, the technology of simplifying geometric entity was developed to use hollow shell, it only cared about the geometric representation of the model without considering the process information of modeling, and it achieved optimization by simplifying the internal structure and thickness of the three-dimensional model, but it caused loss of model information. Recently, the technology of simplifying geometric entity was developed to use level of detail(abbreviate LOD) to deal with model, the components were sorted in spatial position to determine the outline of the model, in order to guarantee users could see the overall outline of the model when it was loaded initially. In the geometric data rendering stage, BIM model was displayed dynamically of contour model and loaded gradually and rendered solid model by calculating the distance between the viewpoint and the model in real time, so as to improve the efficiency of rendering BIM models on local computers without affecting visual effects, and realize the effect similar to the human eye observation. Comparison of advantages and disadvantages of BIM model optimization technology were shown in the Fig. 1.

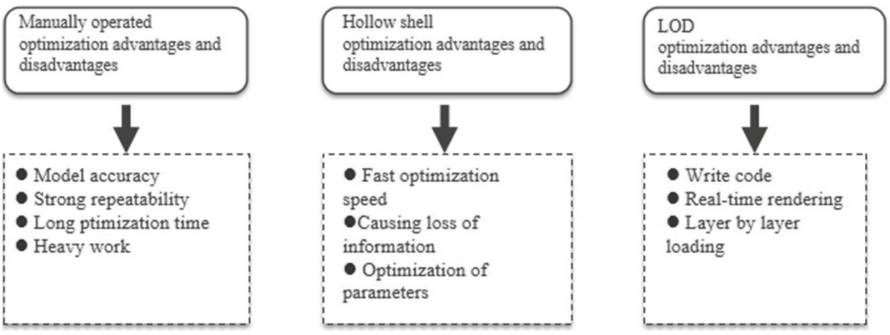


Fig. 1. Advantages and disadvantages of three-dimensional model optimization technology

3.2 Model Data Transformation and Fusion

At present, there was mature GIS application software on the market. If the BIM model of underground pipeline was displayed and browsed on the platform, it needed to be converted into a data format acceptable to GIS software. Most domestic mainstream GIS software has its own plug-in for three-dimensional model format conversion. Discovered through application and comparison, the plug-in showed the disadvantages of slow parsing speed and poor rendering effect. However, BIMBase software with complete independent intellectual property rights was developed basing on autonomous 3D graphics kernel P3D and has multi-source data conversion tool. The tool realized the effect of multi-source data fusion by means of converting BIM model with different data formats into a unified PModel format. For the 3D model, it achieved the purpose of fast parsing speed and good rendering effect.

Considering that BIM focused on 3D modeling and information management of underground pipeline itself, GIS focused on terrain model and above-ground building, BIM data and GIS data were converted into unified format storage by BIMBase plug-in. The application platform applied the same parsing and rendering methods to GIS and BIM data, regardless of its source and storage mode, thus the complete integration of BIM data and GIS data were realized. As shown in the Fig. 2.

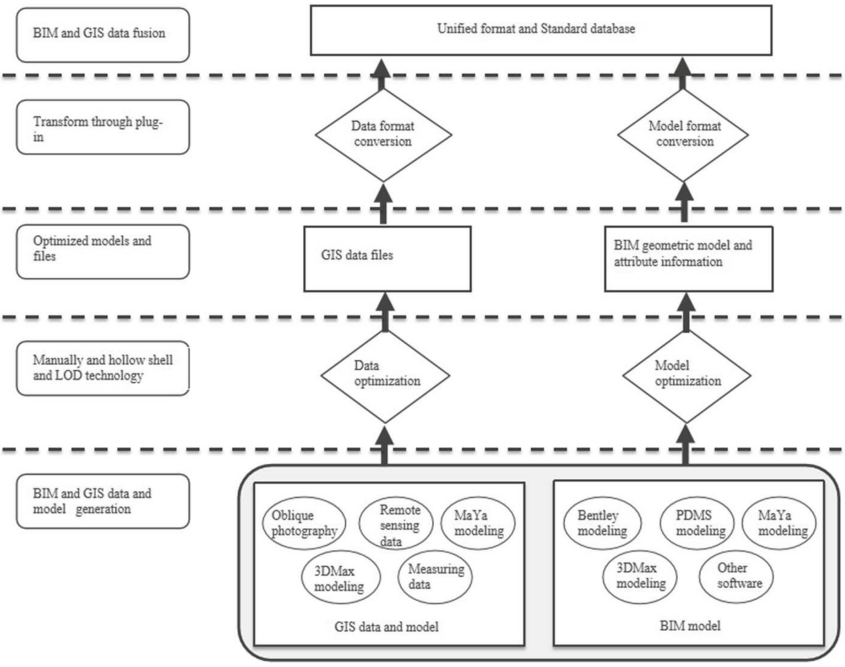


Fig. 2. BIM data and GIS data fusion

3.3 Integrated Platform

At present, purchasing the mainstream application platform on the market could realize the application of BIM + GIS, so we could focus on BIM modeling, collecting and applying directly platform functions for customized application. But customized development was limited by the interface API of software itself, and the cost of purchasing and post-maintenance was very high. With the development of open source technology at home and abroad, such as World Wind or Leaflet, a self-developed BIM + GIS application platform could be built. Basic ideas and techniques as shown in Fig. 3.

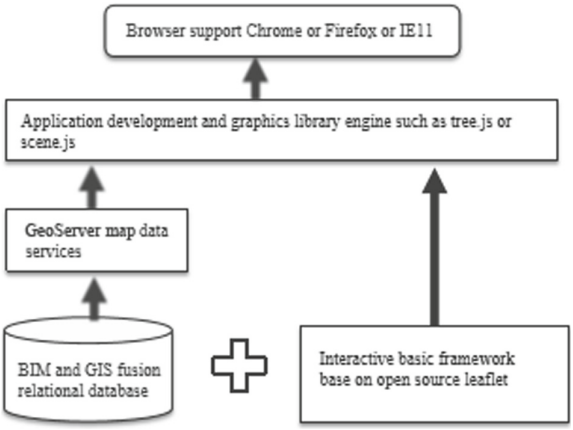


Fig. 3. Basic ideas and techniques of building application platform

Among them, BIM was displayed based on the different browser environment, and there were many problems, such as low carrying capacity of data, low browsing efficiency and poor graphic effect and so on. 3D hardware of HTML5 be used to accelerate rendering, So many open source 3D graphic library based on HTML5 have emerged, such as three.js and scene.js. Especially, three.js was widely used, on the one hand, it used with lower threshold, on the other hand, it supported directly for several common 3D file formats such as 3ds, obj, dae and fbx and so on.

4 Application Cases

For example, taking the data of underground pipeline of a nuclear power plant as an example. There were two ways to get business data, first according to the CAD drawings of underground pipeline planning and combining with on-site maintenance records, BIM model was built by Bentley, secondly converting the CAD drawing information to Excel pipeline table by Hong Ye software, and mass 3D models on SuperMap software were produced. Then geometric data with attribute data were associated by unique ID. According to oblique photography modeling, data of geographical environment was got, according to using Maya or 3D max, model of building model and nuclear power plant area was generated. Data format was converted by transform plugin and was optimized by LOD. Data services on Geoserver were published.

The application platform was developed with open source leaflet technology, data services were connected by tree.js, BIM and geographic information were displayed on Browser such as IE11, Chrome and Firefox. At last, an application platform with 3D browsing interface was built. As shown in the Fig. 4 and Fig. 5.

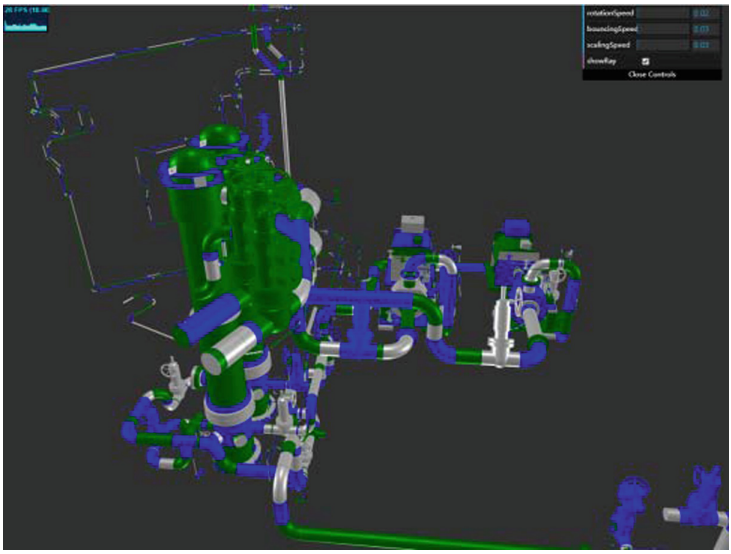


Fig. 4. BIM Model

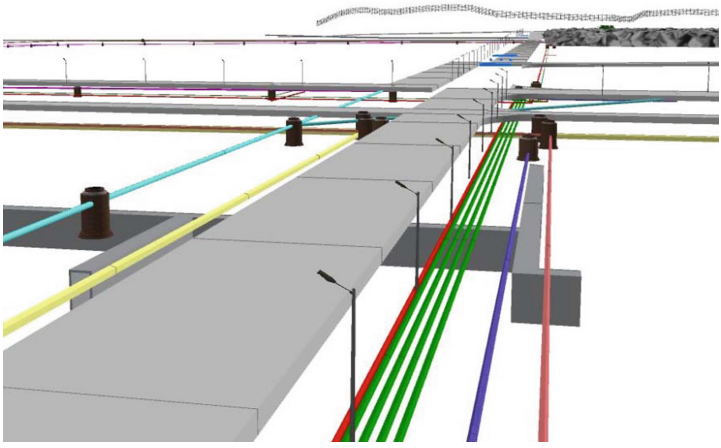


Fig. 5. Application example of underground pipeline

Research and application platform based on open source technology, fusing BIM and GIS technology, it achieved certain results by means of taking the actual data of a nuclear power plant. Compared with other more mature application software, there is

still a big gap, but the advantages are also very obvious,mainly reflected in the low cost, not restricted by licensing, strong portability, flexible function customization.

5 Summary

In this paper, the application of BIM + GIS technology in underground pipeline of nuclear power plant was explored, the modeling of underground pipeline and geographic environment were researched, application platform was built, feasibility of BIM + GIS technology was validated, there provided technical support for the intelligent management of nuclear power plant, and provided experience and reference for excavation accident and pipeline maintenance.

With the application of BIM + GIS technology more and more widely and its advantage more and more obviously, deeper and deeper was applied in nuclear power application. Such as BIM + GIS + AR technology, it would to realize accurate matching between pipeline model and actual position, and it could unobstructed inspect of underground pipeline like the real world by human movement on virtual scene, it could achieve accurate real-life matching maintenance. Through the research and application of BIM + GIS technology, the capacity of facility management and predict and command construction was improved, and the intelligent management level of nuclear power plant could be improved comprehensively.

References

1. Shumin, L., Yufeng, C.: The application of BIM+GIS technology in the information management of urban underground pipelines. Econ.·Manage.·Summary 157–158 (2019)
2. Xiaoyu, L., Dandan, Z.: Research on digital technology system of underground heating pipe network based on GIM+GIS. Eng. Sci. Technol. 63–65 (2021)
3. Yujin, X., Changyun, X.: Application conception of BIM technology in nuclear power deficiencies and corrective actions management. Manage. Inf. Chin. 49–50 (2016)
4. Yan, H.: Applied research of BIM in engineering quantity calculation of nuclear power civil work construction management. Inf. Technol. Inf. 193–195 (2018)
5. Yong, Z.: Conceptual framework of building information modelling (BIM). Value Eng. **31**(8), 33–34 (2012)
6. Xumingm, C., Shitong, Z.: Application of BIM Technology in Electromechanical Construction Stage. Architectural Technol. **44**(10), 909–912 (2013)

Author Index

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 431–433, 2023.
https://doi.org/10.1007/978-981-99-3455-3