Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
©2023 ESREL2023 Organizers. *Published by* Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P700-cd

A Fault Simulation and Monitoring Method of DCS in Nuclear Power Plant Based on Virtual Platform

Chao Guo

Institute of Nuclear and New Energy Technology of Tsinghua University, Collaborative Innovation Center of Advanced Nuclear Energy Technology, Key Laboratory of Advanced Reactor Engineering and Safety of Ministry of Education, Beijing, China. E-mail: guochao@tsinghua.edu.cn

Duo Li

Institute of Nuclear and New Energy Technology of Tsinghua University, Collaborative Innovation Center of Advanced Nuclear Energy Technology, Key Laboratory of Advanced Reactor Engineering and Safety of Ministry of Education, Beijing, China. E-mail: liduo@tsinghua.edu.cn

Ronghong Qu

Institute of Nuclear and New Energy Technology of Tsinghua University, Collaborative Innovation Center of Advanced Nuclear Energy Technology, Key Laboratory of Advanced Reactor Engineering and Safety of Ministry of Education, Beijing, China. E-mail: qu-rh@tsinghua.edu.cn

Fan Chen

Institute of Nuclear and New Energy Technology of Tsinghua University, Collaborative Innovation Center of Advanced Nuclear Energy Technology, Key Laboratory of Advanced Reactor Engineering and Safety of Ministry of Education, Beijing, China. E-mail: chen_fan@tsinghua.edu.cn

Yuan Chen

Huaneng Shandong Shidao Bay Nuclear Power Co., Ltd., Shandong, China. E-mail: chenyuan@sdwgs.chng.com.cn

Xiaojin Huang

Institute of Nuclear and New Energy Technology of Tsinghua University, Collaborative Innovation Center of Advanced Nuclear Energy Technology, Key Laboratory of Advanced Reactor Engineering and Safety of Ministry of Education, Beijing, China. E-mail: huangxj@tsinghua.edu.cn

Reliable operation of the distributed control system (DCS) is an important guarantee for the economy and safety of nuclear power plants (NPPs). Due to the complexity of functions and structures, the diversity of equipment and interfaces, there may be random faults or systematic faults in the DCS system that cannot be self-detected. It is an important topic to analyse and identify typical faults of DCS systems and equipment, and to establish the correlation between fault modes and fault phenomena. Based on commonly used FMEA method, this study collects typical system-level and component-level fault types of DCS systems and establishes a typical fault effect model in three dimensions (severity of fault consequences, probability of the environment excitation, and scope of the fault) to describe the fault impact. Fault simulation is an effective way for fault analysis. Based on two simulation software packages, a minimised DCS simulation system is built with the capability of fault simulation, comprising Level 0 process system, Level 1 control system, and Level 2 human-machine interface (HMI). The study further performs the implantation and monitoring of several typical DCS faults based on this virtual platform, which helps to validate the fault effects and improve the fault monitoring methods.

Keywords: Fault simulation, fault monitoring, distributed control system, nuclear power plant, virtual platform.

1. Background

Nuclear safety is the cornerstone of the steady development of the nuclear power industry. The distributed control system (DCS) is regarded as the nerve centre of a nuclear power plant (NPP), and its reliability is related to the safe and reliable operation of the entire power plant, and is the basis and premise of nuclear safety.

Digital DCS of an NPP has the characteristics of complex structure and software, numerous equipment and interfaces, and high coupling of software and hardware. Although digital DCS has certain self-diagnostic functions to identify the abnormal status of some systems, equipment, interfaces or boards, it may still have latent faults that cannot be easily identified. It is necessary to study the causes, effects and monitoring methods of typical DCS faults of an NPP in order to avoid the expansion of failure effects and reduce the economic losses caused by the faults.

Zhang et al. (2018) proposed a fault diagnosis method combining hardware redundancy and discrete wavelet transform for the sensors important to safety of the NPPs. Guo et al. (2021) analysed the impact of the common cause failures for the DCS in an NPP and proposed a discrete-time Bayesian network method for the reliability analysis. Yankai, Xu, and Meng (2020) performed the reliability analysis for the DCS hardware and software with digital FMEA method. Li et al. (2022) performed the fault tree analysis for a safety level DCS in an NPP to identify and eliminate the system weaknesses. Shi, Huang, and Jia (2022) proposed a testability analysis technology of DCS in the NPP based on dependence model, which helps to detect the faults of internal components in time. Li et al. (2014) combined the actual characteristics of DCS systems in nuclear power plants and chose a consulting system type of structure to establish a basic architecture of fault diagnosis expert system.

Guo et al. (2022) proposed a three-dimensional mapping relationship between the hidden faults of the DCS and the environmental model, and the environmental mode was classified into specific application environment, specific application method and long-term dynamic operation. Guilian et al. (2022) analysed the significance of the virtual DCS, including system state detection, health assessment, and fault diagnosis. Guilian et al then proposed and built a remote intelligent operation and maintenance framework of the DCS.

The research of this paper is: firstly, to study the basic failure modes and failure effects of DCS systems and model the failure effects to facilitate the failure effects analysis. Secondly, based on the virtual PLC and virtual process system, a virtual DCS platform is established to provide verification tools for the subsequent implantation and monitoring of typical DCS faults. Thirdly, the DCS fault simulation and monitoring platform based on the virtual DCS carries out typical fault simulation and monitoring tests which helps for fault analysis. The above three parts of work are discussed in Sections 2, 3 and 4, respectively.

2. Typical Fault Modes and Effects Analysis of DCS

Determining fault modes or failure modes is the prerequisite for fault simulation and monitoring studies. It is necessary to determine the important fault modes that can occur in DCS systems and equipment based on their characteristics. The FMEA method is used in this paper to analyse the fault types, fault causes and fault effects of typical faults of DCS in NPPs, so as to establish a typical fault impact model of DCS.

2.1. *Typical fault modes of systems and electronic components*

DCS fault types are divided into two categories: random faults and systematic faults. Random faults occur at an undetermined time but follow a specific probability distribution and can be used to describe hardware and human-caused faults. Systematic faults are defined as deterministic faults under specific conditions and are further divided into three categories: hardware, software, and human-caused faults.

Table 1. Generic system-level fault modes.

No.	Fault modes
1	Failure in operation
2	Cannot run at the specified time
3	Cannot stop running at the specified moment
4	Run ahead of schedule

Table 1 lists common system-level fault modes, which provide the basic direction for subsequent specific FMEA. By extending Table 1, the classification of fault modes can be made more specific, which in turn leads to typical failure modes and mechanisms of equipment components according to the type of equipment component.

Table 2. Some typical fault modes and mechanisms of DCS components.

Components	Fault modes
Transistor	Disconnection High Ice B-C junction short circuit
Relay	Open contact Open coil High contact resistance
Transformer	Open winding Shorted winding
Resistor	Open Circuit Short circuit Drift
Capacitor	Short circuit Open circuit Leakage
Connector	Misalignment Corrosion

For common components and parts, their fault modes can be determined from relevant standards and manuals. According to the types of equipment components, some typical fault modes and mechanisms are given in Table 2.

2.2. *Typical Fault Effect Model of DCS*

According to multiple judgment bases such as the occurrence probability of environmental excitation, the impact range of defect faults, and the comprehensive evaluation of the severity of defect consequences, the impact of typical faults is analysed, and the three-dimensional mapping relationship of fault impact is established, as shown in Fig. 1.

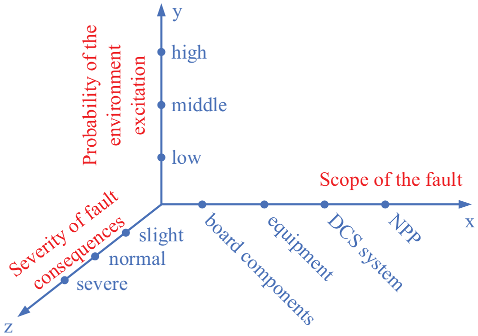


Fig. 1. DCS Typical Fault Effect Model.

The model shown in Fig. 1 can be regarded as a simplified model of Risk Priority Number (RPN) method, which can be used in situations where neither the probability of occurrence nor the severity can be easily quantified. The three dimensions of the model correspond to the severity level and probability level of the RPN method respectively. The model only roughly estimates the probability of fault, and the specific fault probability needs to be determined in combination with the manufacturer's data, operation and maintenance data of the actual equipment.

3. DCS Fault Simulation and Monitoring Platform Construction

Fault simulation is an effective way for fault research. Based on conventional DCS system, the virtual software-based fault simulation DCS platform can be used to realize the implantation for hardware and software faults in typical DCS systems of NPPs, i.e., the fault scenarios to be simulated are set in the simulation platform through the network. At the same time, the feedback data of the embedded faults can be collected through the network and reflected visually through the human-machine interface (HMI).

The virtual software-based DCS fault simulation and monitoring platform consists of 3 parts, namely: Level 0 process system, Level 1 control system, and Level 2 HMI. The architecture of the platform based on virtual software is shown in Fig. 2, where the process system is designed as a water level single-loop control system.

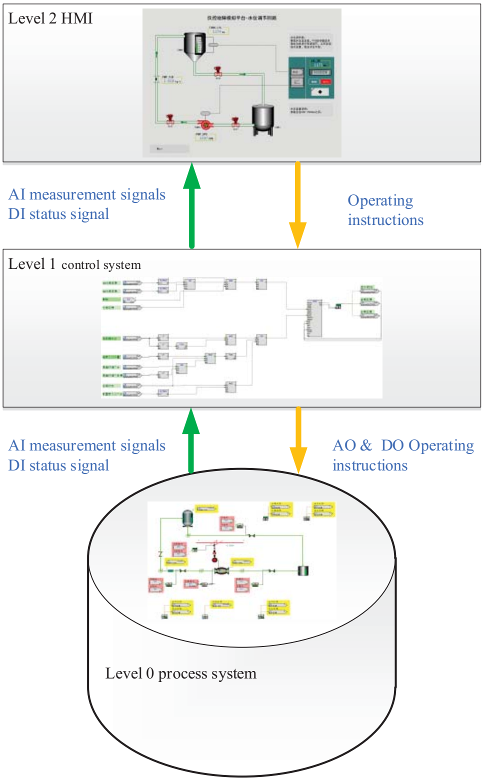


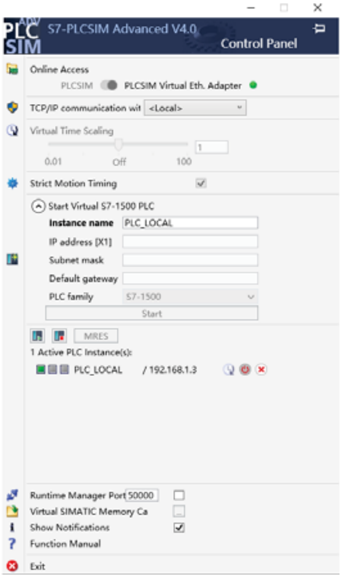
Fig. 2. Architecture of virtual fault simulation platform for DCS systems.

3.1. *Level 0 process system model*

The simulation model of the process system built in this study is a water circulation system: the tank can be filled with water by a pump, and the tank has a drainage pipe to discharge the water to the storage tank; the water level of the tank is controlled by a single-loop control loop, and when the water level of the tank is set, the PID module adjusts the speed of the pump according to the actual water level deviation, thus regulating the water inlet flow of the tank, so that the water level reaches the set value. The Level 0 process system model is built by vPower simulation software developed by Neoswise company (http://www.neoswise.com.cn/).

3.2. *Level 1 control system model*

The virtual fault simulation platform employed a set of virtual PLC to realise the control functions of the Level 1 layer of DCS. Specifically, this study uses Siemens S7-PLCSIM Advanced V3.0 simulation software to realise the functional simulation of the PLCs and Siemens TIA Portal V17 to realise the control logic configuration of DCS Level 1 (https://support.industry.siemens.com/). Level 1 enables communication with Level 0 via the OPC-UA protocol. The virtual PLC start-up screen is shown in Fig. 3.



TCP/IP communication wit <Local>

Virtual Time Scaling 0.01 Off 100 1

Strict Motion Timing ☑

Instance name PLC_LOCAL

IP address [X1]

Subnet mask

Default gateway

PLC family S7-1500

1 Active PLC Instance(s):

PLC_LOCAL / 192.168.1.3

Runtime Manager Port 50000 ☐

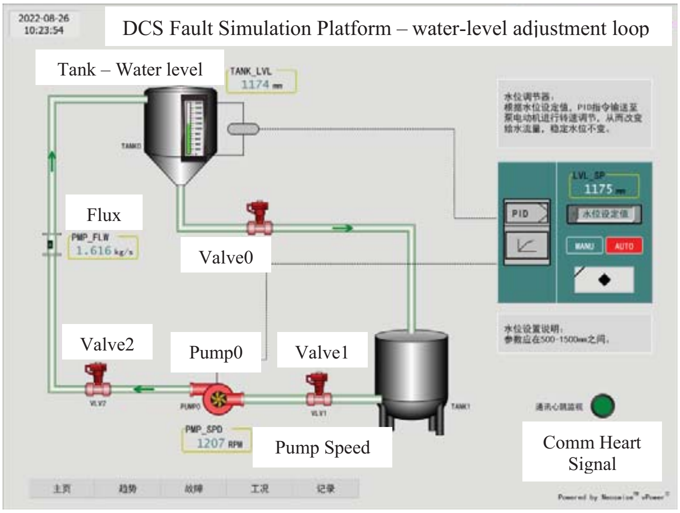
Virtual SIMATIC Memory Ca ☐

Show Notifications ☑

Fig. 3. Front panel of virtual PLC.

3.3. *Level 2 human-machine interface*

The Level 2 HMI of the virtual fault simulation platform implements the control and monitoring of the water level regulation loop, and the main monitoring screen of which is shown in Fig. 4. The HMI is implemented by the vPower software. Level 2 also communicates with Level 1 via the OPC-UA protocol.



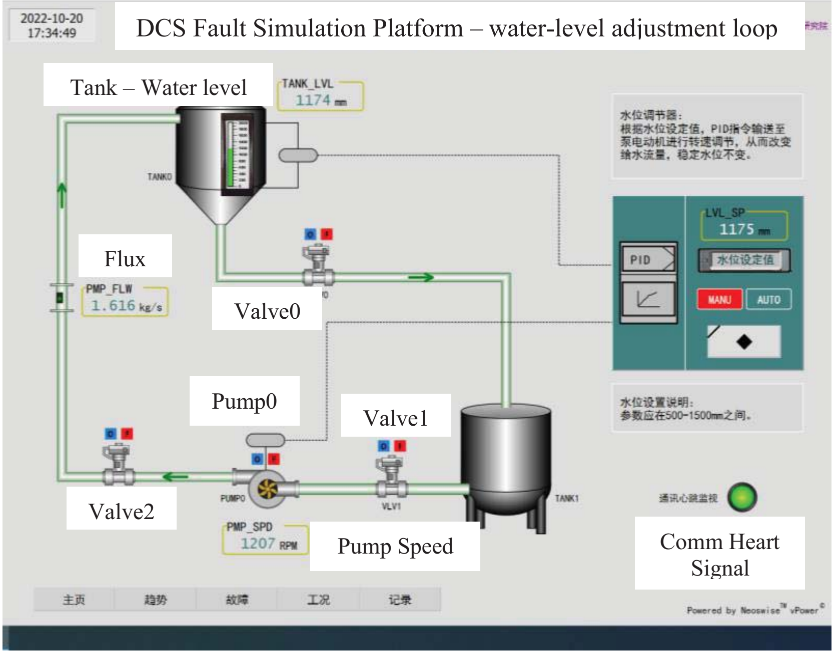
水位调节器：
根据水位设定值，PID指令输送至泵电动机进行转速调节，从而改变给水流量，稳定水位不变。

水位设置说明：
参数应在500-1500mm之间。

Fig. 4. Virtual fault simulation platform Level 2 monitoring interface.

Table 3. Faults implanted by virtual fault simulation platform.

No.	Fault location	Fault mode	Expected fault phenomenon	Implantation method
1	Level 0	Analogue signal drift	Observes analogue signal drift at Level 2	Adds random error simulation signal drift at Level 0
2	Level 0	Switching signal disconnection	Observes a change in the state of the switching signal and alarms at Level 2	Forced switch signal change at Level 0
3	Level 0	Drive relay malfunction	Pump/valve malfunction observed at Level 2	Forced switching signal change at Level 0
4	Level 0	Analogue signal drift	Observes a drift in the analogue signal with no significant change in other signals at Level 2	Sets the trend of the analogue signal at Level 2
5	Level 1	Power supply/CPU module failure	Observed at Level 2 heartbeat signal stopped, display not refreshed, control commands not issued, PLC status change observed at Level 1	PLC set to standby at Level 1
6	Level 1	DI module failure	Pump and valve status abnormal at Level 2, double 0 fault reported	Force all DI module input signals to 0 at Level 1
7	Level 1	AI module failure	Abnormal analogue display and alarm at Level 2	Force AI module to collect 0mA at Level 1
8	Level 1	PLC software failure	Analogue display stuttering at Level 2	Add analog delay at Level 1
9	Level 2	HMI software failure	No display at Level 2, abnormal screen display	Design the Level 2 software as an exception
10	Level 2	HMI misconfiguration	Tank inlet valve closed when tank outlet valve is closed at Level 2	Misconfigured HMI at Level 2



TANK_LVL 1174 mm

PMP_FLW 1.616 kg/s

PMP_SPD 1207 RPM

LVL_SP 1175 mm

水位调节器：
根据水位设定值，PID指令输送至泵电动机进行转速调节，从而改变给水流量，稳定水位不变。

水位设置说明：
参数应在500-1500mm之间。

Fig. 5. Level 2 HMI with implanted DI module failure.

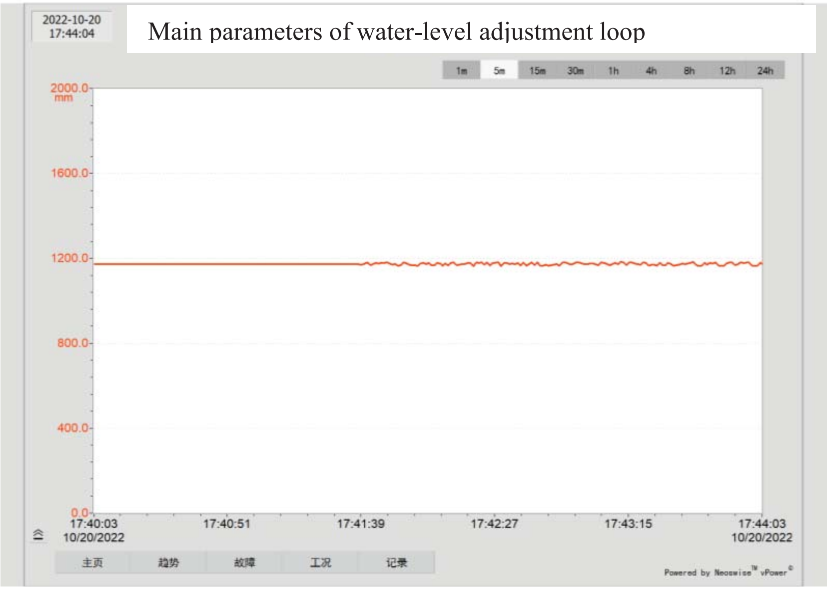
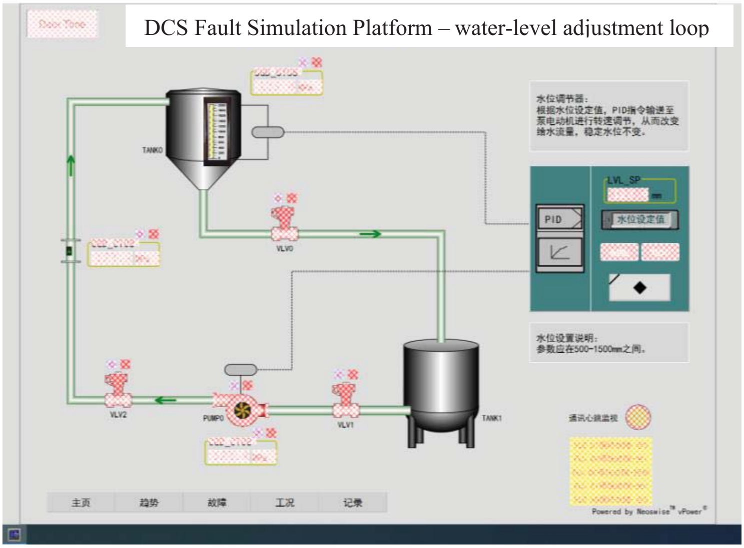


Fig. 6. Level 2 HMI with embedded analogue signal drift faults.



DCS Fault Simulation Platform – water-level adjustment loop

水位调节器：
根据水位设定值，PID指令输送至泵电动机进行转速调节，从而改变给水流量，稳定水位不变。

水位设置说明：
参数应在500-1500mm之间。

Fig. 7. Level 2 HMI after HMI software failure implantation at Level 2.

4. Experiments and Discussions

In this study, a set of fault modes of typical DCS systems and equipment is selected and the virtual fault simulation platform is used for fault implantation and monitoring. Based on the location of the faults, the implanted faults are classified into Level 0, Level 1 and Level 2. The typical faults implanted are shown in the Table 3.

Fig. 5 shows the fault mode "DI module failure" in Table 3. In the experiment, after pressing the corresponding button in the fault implantation page, the values of the DI signals collected by the Level 1 virtual PLC are forced to 0. The HMI flow chart page of the pump and valve both show double 0 abnormal alarms ("O" and "F" alarms), i.e. no "open in place" and "close in place" signals are received. This state is as expected for the fault phenomenon.

Fig. 6 shows the phenomenon after the fault mode "Analogue signal drift" has been implanted in the simulation platform. After pressing the corresponding button on the fault implantation page, the output tank level signal is forced to drift at Level 0. This fault mode can be identified from the variable trend graph at Level 2.

Fig. 7 shows the phenomenon after the implantation of the "HMI software failure". After pressing the corresponding button on the fault implantation page, the Level 2 HMI does not display the screen normally, so the device status, the parameters, and the heartbeat signal are not displayed, which makes it easy to identify the fault from the HMI.

By establishing a software-based virtual DCS platform, this research has enabled the implantation and monitoring of typical faults in the DCS.

It should be noted that all the typical faults shown in Table 3 have been simulated in the research. Due to space limitation, only three examples are given in this paper to prove the effectiveness of the fault simulation method for fault research. This research is based on the simulation of fault phenomena and effects, and it is not yet possible to realize fault simulation from the perspective of fault generation mechanism.

5. Conclusion

Reliable operation of DCS is an important guarantee for the economy and safety of nuclear power plants. Due to the complexity of functions and structures, the diversity of equipment and interfaces, DCS systems cannot achieve a high fault self-test rate. It is an important research problem to identify the faults of typical DCS systems and equipment, and to establish the correlation between fault modes and fault phenomena.

Based on commonly used FMEA method, this study collects typical system-level and component-level fault types of DCS systems and establishes a typical fault effect model in three dimensions to qualitatively describe the fault impact. Based on two simulation software packages, a minimised DCS system is built, comprising Level 0 process system, Level 1 control system, and Level 2 HMI. The study further implements the implantation and monitoring of more than ten typical DCS faults based on this virtual platform.

This study has practical engineering implications for verifying and improving the fault monitoring of DCS systems and equipment, and improving system reliability.

Acknowledgement

This research was supported by National Natural Science Foundation of China (Grant No. 71801141), LingChuang Research Project of China National Nuclear Corporation, and Nuclear Energy Development Research Project (20204601007).

References

Guilian, Shi, Huang Xiaojin, Zhao Xiaopeng, and Wang Lei. 2022. "Research and Application of Remote Intelligent Operation and Maintenance System for Digital Instrument and Control Equipment in Nuclear Power Plant." 2022 29th International Conference on Nuclear Engineering, ICONE 2022, August 8, 2022 - August 12, 2022, Virtual, Online.

Guo, Chao, Shuqiao Zhou, Duo Li, and Xiaojin Huang. 2022. "Analysis of Hidden Fault in Digital Instrumentation and Control System of Nuclear Power Plant Based on Environmental Model." 2022 29th International Conference on Nuclear Engineering, ICONE 2022, August 8, 2022 - August 12, 2022, Virtual, Online.

Guo, Y. J., M. J. Zhong, C. Gao, H. D. Wang, X. F. Liang, and H. Yi. 2021. "A discrete-time Bayesian network approach for reliability analysis of dynamic systems with common cause failures." *Reliability Engineering and System Safety* 216:1-11.

Li, Su, Jianming Lou, Xiju Zong, and Songxiang Ma. 2022. "Application of Fault Tree Analysis to the DCS Reliability of Nuclear Power Plants." 5th IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference, IMCEC 2022, December 16, 2022 - December 18, 2022, Chongqing, China.

Li, You-Ran, Ai-Guo Liu, Wei Sun, and Zhi-Wu Guo. 2014. "Study on structure of fault diagnosis expert system for DCS of nuclear power plant." *Yuanzineng Kexue Jishu/Atomic Energy Science and Technology* 48:1048-1053. doi: 10.7538/yzk.2014.48.S1.1048.

Shi, Gui-Lian, Xiao-Jin Huang, and Hu-Jun Jia. 2022. "Research on Testability Analysis Technology of Nuclear Safety Level DCS System Based on Dependence Model." 6th International Symposium on Software Reliability, Industrial Safety, Cyber Security and Physical Protection of Nuclear Power Plant, ISNPP 2021, October 22, 2021 - October 22, 2021, Zhuji, China.

Yankai, Li, Wang Xu, and Lin Meng. 2020. "Application of the dynamic FMEA in the reliability analysis of DCS." 2020 5th International Conference on Advances in Energy and Environment Research, ICAEER 2020, September 18, 2020 - September 20, 2020, Virtual, Online, China.

Zhang, Liangliang, Ji Shi, Jijing Wang, and Huifeng Chen. 2018. "Research of Online Fault Diagnosis for Sensors Important to Safety in Nuclear Power Plants." 2018 International Conference on Power System Technology, POWERCON 2018, November 6, 2018 - November 9, 2018, Guangzhou, China.