The Situation and Suggestion of Diversity Actuation System Applied in China

Jing-Bin Liu, Zhong-Qiu Wang, Yun-Bo Zhang, Yan Feng, Yin-Hui Guo and Xiao-Lu Dong

Abstract Digital control system has been widely used in nuclear power plant. It brings some obvious advantages in system design and application. Meanwhile the accompanying common cause failures (CCFs) problem becomes one of the most concerned issues. To deal with this problem, many regulations and methods are proposed. NUREG 6303 describes a method for analyzing computer-based nuclear reactor protection systems to discover design vulnerabilities with common-mode failure (US NRC. NUREG/CR6303-1994 in Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems, [1]). NUREG 7007 considers that diversity in a safety system is needed for mitigating the consequences of potential CCFs and provides guidance to the staff and nuclear industry for evaluation (US NRC. NUREG/CR7007-2010 in Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems, [2]). In this paper, the diversity actuation system (DAS) has been described in detail and the functions of DAS system have been introduced. Then several representative different reactor type in China is selected (including M310 model, Second generation plus based on M310 model, AP1000 model and EPR model), and made some comparison between these

J.-B. Liu · Z.-Q. Wang · Y.-B. Zhang · Y. Feng (✉) · Y.-H. Guo · X.-L. Dong
I&C Department, Nuclear and Radiation Safety Center, Beijing, China
e-mail: fengyan@chinansc.cn

J.-B. Liu
e-mail: liujingbinjob@163.com

Z.-Q. Wang
e-mail: wangzhongqiu@chinansc.cn

Y.-B. Zhang
e-mail: zhangyunbo@chinansc.cn

Y.-H. Guo
e-mail: guoyinhui@chinansc.cn

X.-L. Dong
e-mail: dongxiaolu@chinansc.cn

Y. Xu (ed.), *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems*, Lecture Notes in Electrical Engineering 400,
DOI 10.1007/978-981-10-3361-2_19

DAS systems. At the end of this paper some suggestions are proposed to the third generation nuclear power technology in China to reduce the common cause failures and enhance the reliability.

Keywords Diversity actuation system · Common-cause failure · I&C system

1 Introduction

Currently, digital control system has been used more widely in nuclear power plants (NPPs) in CHINA and abroad. Its openness, high reliability, rapidity and operability have been gradually recognized by the industry. However, due to the application of digital technology, common cause failures become one of the factors must be considered in the design [3]. The work of diversity and common cause failures is still in research stage in our country, there are no relative specific regulations and standards. But the regulator's position is very clear: HAD 102/14 [4] points out that the possibility of common cause failures of safety-critical items must be considered; it determined where the diversity, redundancy and independence should be applied to achieve the required reliability. HAD 102/16 [5] emphasizes that software CCFs is a key issue and using the diversity strategy can reduce potential CCFs effectively and improve its reliability. CCFs problems become one of the concerned issues in safety review of digital control system design and modification [6].

Diversity actuation system provides the necessary means to alleviate the consequence when design basis accidents occur due to the CCFs of digital reactor protection system. Compared with the protection and control systems it could be based on a different platform and use diverse system design, functions driven and parameter display to provide a back-up.

2 The Functions of DAS System

Although different nuclear plants types, manufacturers and technologies of DAS system may be very different in design and implementation, the main functions of DAS system are basically the same:

- Provide diverse and backup automatic drive signals such as reactor trip (RTs) and engineered safety features (ESFs) functions. When the specified parameters exceed the setting value, automatically shutdown or drive critical ESF functions to assure the integrity of the fuel cladding, primary circuit pressure boundary and containment pressure boundary;

- Provide diverse and backup manual RT and ESF functions to assure the integrity of the fuel cladding, primary circuit pressure boundary and containment pressure boundary;
- Provide adequate information of the device status and parameters on the panel station in the main control room (such as reactivity, core residual heat removal condition, primary system coolant outlet temperature, primary circuit pressure boundary condition, Containment pressure boundary etc.) to monitor and display the safety-critical parameters.

To achieve the above functions, DAS system generally has the following devices, as described in Fig. 1:

- DAS Panel station. This Panel station includes the manual operation devices, indicating instruments and alarm devices. It is mainly used for safety-critical manual functions, provides safety-critical parameters, alarm information and other display functions.
- DAS Processor Cabinets. The cabinet is mainly used for collecting, processing and outputting the signals. In order to prevent equipment malfunction and rejection, it should be set up with architectural redundancy. Each redundant subsystem would collect signals and process, compare with the set values then generate the "local signal" for voting logic.
- Anticipated Transients without Trip (ATWT) mitigation system. ATWT event is caused by control rods that can not be inserted into the reactor core due to the CCFs and the unit failed to achieve the expected transient scram. So ATWT system uses diverse equipment to achieve reactor scram. At present most of the NPPs integrate this function into DAS systems.

In order to achieve the above functions, different instrumentation and control system uses a variety of strategies to achieve.

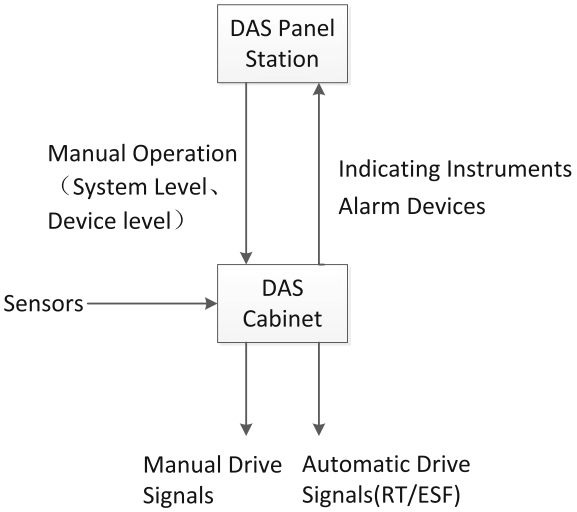

Fig. 1 The function diagram of DAS

3 The Introduction of Different Diversity Methods Used in China

3.1 M310 Model

As second-generation nuclear power technology, it is widely used in CHINA's nuclear power project, and achieved good operating performances. At present, there are still a large number of operating units. The digital technology in the nuclear power field had not been universal when this type of plants completed its design, besides consensus on diversity and common cause failures had not been agreed, therefore such models did not set up a separate DAS system.

However, to avoid common cause failures since the control rods can not be inserted into the core and the unit failed to achieve the expected transient scram, it sets ATWT mitigation system [7]. The system is mainly to monitor the SG water flow and nuclear power level. When the SG water flow is lower than the setting value and the nuclear power exceed the setting power, then the auxiliary feedwater system will be activated, the turbine will be triggered and the shut-down signal will be sent out. ATWT system uses diverse equipment to achieve reactor scram, follow the principles of diversity and independence. However because the functions are simple and there are no diverse safety-critical parameters and alarm information displayed in the main control room, in subsequent improved and new designed power plants this system is integrated to the DAS system.

3.2 Second Generation Plus Based on M310 Model

DAS system of Fangjiashan/Fuqing project is different from the safety-class digital I&C platform TRICON, it uses a non-safety digital I&C platform I/A. There are enough physical and electrical isolation between DAS system and reactor protection system. DAS system does not receive the signals processed by reactor protection system, meanwhile does not send signals to reactor protection system. As stated earlier, it integrated the functions of ATWT systems. In addition, parts of the automatic functions of reactor protection system are also selected as below [8]:

- Automatic reactor trip and turbine trip;
- Main steam(-piping) system isolation actuation;
- Safety injection actuation.

There are five reactor shutdown signals, respectively: High power range neutron fluence rate, high pressurizer pressure, low pressurizer pressure, 2 loops of low reactor coolant flow rate, low pressurizer pressure (this signal will trigger safety injection at the same time).

DAS system is not provided with system-level and device-level manual operations as well as safety-critical parameters and alarm information display. Backup

manual control and display functions are mainly achieved through safety video display unit (SVDU), network computer-video display unit (NC-VDU) and back-up disk.

As a diversity of design, the reactor trip of automatic functions is accomplished through cutting rod position indicating and rod control system (RGL) power supply, which is different from the way of protection system by opening the trip breakers. The ESF functions of DAS system are accomplished through its own cabinet which bypassing the logical processing of reactor protection system. The signals of ESF is sending to the priority logic processing module (PLM), and then sending to the relevant actuator. Furthermore, the output signals of DAS systems are initiated by energized way not de-energized way like protection system.

3.3 AP1000 Model

As the third-generation nuclear power technology AP1000 is imported from Westinghouse. Its safety grade platform is COMMON-Q to perform the functions of the reactor protection system and its non-safety grade platform is OVATION to achieve majority control functions of nuclear island/conventional island/BOP. The safety system (PMS) uses hardware and software that is based on microprocessor and Plant Control System (PLS) is also microprocessor-based. In order to achieve diversity, the DAS system uses ALS platform that is based on Field Programmable Gate Array (FPGA).

DAS system selects parts of the automatic functions of the reactor protection system [9]:

- Automatic reactor and turbine trip;
- Automatic CMT (coolant makeup tank) valve actuation and RCP (reactor coolant pump) trip;
- Automatic PRHR (passive residual heat removal) discharge valve actuation and IRWST (in-containment refueling water storage tank) gutter isolation valve actuation;
- Automatic containment isolation valve actuation and PCS (passive containment cooling system) valve actuation.

DAS system uses independent sensors compared with PMS system, such as hot leg RTDs, containment RTDs, core exit thermocouples, steam generator level transmitters, etc.

The trip signal of automatic functions drives the generator set trip, and then CRDM (control-rod device mechanism) losing of power and dropping of control rod. This method is different from the manner of PMS that uses trip breaker to shutdown. ESF functions also uses diverse drive interface compared with PMS, and these devices can operate independently without affecting each other.

In addition, there are system-level manual operation functions in DAS Panel station and processor cabinets (partly). Its output signals are connected via hard-wired to the final load, thus can completely bypass the PMS and DAS automatic drive logic path. To support manual actuation, there are adequate instrument indications and alarms provided in the DAS Panel station and processor cabinets.

3.4 EPR Model

EPR is the third-generation nuclear power technology imported from AREVA. Due to the different strategies of diversity, EPR does not actually set up a separate DAS system strictly. It uses defense in depth strategy and adds a hard core system (HKS) to maintain the diversity. Its safety grade platform is TXS to perform the functions of the reactor protection system and its non-safety grade platform is SPPA-T2000 to achieve control functions [10].

The I&C system includes 2 levels and is made up of 9 subsystems. Level 1 layer contains process automation system (PAS), safety automation system (SAS), that are based on SPPA-T2000 platform; reactor protection system (PS), reactor control surveillance and limitation system (RCSL), severe accident I&C system (SA I&C), priority actuation and control system (PACS), hard kernel system (HKS), that are based on TXS platform. Level 2 layer contains process information and control system (PICS) and safety information and control system (SICS).

Compared with other power plant, there are a large number of F1B safety functions implemented in SPPA-T2000 SAS system, and post-accident related functions are implemented in SPPA-T2000 SAS system. Since the SPPA-T2000 is the lower safety class platform, in the event of design basis accident with SPPA-T2000 platform failure, some functions that bring the power plant into safe shutdown state will fail and lose. Therefore, the HKS functions are added into the design of I&C systems and the DEC-B functions of SAS subsystem are allocated to the dedicated cabinet. HKS system is used for the event of design basis accident with SPPA-T2000 platform failure. SAS DEC-B and SA I&C are used for DEC-B events together.

3.5 Summary

Table 1 is the situation of digital I&C system applied in CHINA. This table introduces the NPP's platform, supplier, non-1E platform and DAS/ATWT situation. It contains five types of NPP and the DAS system of Sects. 3.1–3.4 is included.

Table 1 Digital I&C system situation applied in China

NPP	1E platform	Supplier	Non-1E platform	DAS/ATWT situation
Tianwan1,2	TXS	AREVA	TXP	Only ATWT system (Seismic)
Lingao3,4	TXS	AREVA	TXP	
Tianwan3,4	TXS	AREVA	SPPA-T2000	
Taishan1,2	TXS	AREVA	SPPA-T2000	ATWT+HKS, same with Sect. 3.4 introduction (Seismic)
Hongyanhe1–4	Meltac	Mitsubishi	Hollias	Only ATWT system (Seismic)
Ningde1–4	Meltac	Mitsubishi	Hollias	
Yangjiang1–4	Meltac	Mitsubishi	Hollias	
Fangchenggang1,2	Meltac	Mitsubishi	Hollias	
Fuqing1–4	TRICON	INVENSYS	FOXBORO I/A	DAS system is based on non-1E platform, same with Sect. 3.2 introduction (Seismic)
Fangjiashan1,2	TRICON	INVENSYS	FOXBORO I/A	
Changjiang1,2	TRICON	INVENSYS	FOXBORO I/A	
Sanmen1,2	Common Q	Westinghouse	Ovation	DAS system is based on FPGA technology, same with Sect. 3.3 introduction (Non-seismic)
Haiyang1,2	Common Q	Westinghouse	Ovation	
Yangjiang5,6	FirmSys	CTEC	HOLLiAS-N	DAS system is based on diverse platform compared with protection system. It is like Sect. 3.2, but added some functions such as system-level and device-level manual functions, instrument indications and alarms (the final solution is not confirmed yet) (Seismic)

4 Conclusions

We can make a thinking and conclusion from the introduction and comparison of the different DAS system.

The DAS system of AP1000 has the most comprehensive and deepest diverse means in design. It uses a different I&C platform compared with protection system (especially different from control system and its digital technology is based on FPGA). Besides it uses a different shutdown strategy and has part of automatic functions of the reactor protection system and manual functions. There are adequate

instrument indications and alarms provided in the DAS Panel station and processor cabinets. DAS system also uses a different dedicated driver interface and sensor. The only drawback is that the DAS system is not designed to be ant seismic, just not caused an inadvertent actuation of a squib valve.

M310 and EPR model does not set up a separate DAS system strictly. Though EPR adds HKS system to ensure safe shutdown when the event of design basis accident with SPPA-T2000 platform failure. However it does not set up automatic functions in response of design basis accidents with failure of TXS safety platform. There is still much room for improvement.

M310 plus model takes many effective measures in diversity design such as automatic trip and ESF functions of DAS system. But it does not contain system-level and device-level manual functions, independent parameters display, sensors and driver interfaces are shared with protection system, so there is also much room for improvement. Table 1 has shown that subsequent Yangjiang5,6 and Hongyanhe5,6 units have some improvements in these aspects, but the final solution is not determined.

HPR1000 (Hua-long Pressurized Reactor) project has reached the international advanced level of third generation nuclear power technology in safety indicators and technical performance. Its instrumentation and control system design can draw on the above diversity strategy of DAS system, enhance advantages and avoid disadvantages, to implement the principle of defense in depth and diversity.

Acknowledgements This work is supported by the soft subject "Research and standard development of cyber security about digital I&C system in nuclear power plant". Many people have offered me valuable help in this work. I thank professor Zhong-Qiu WANG for helpful conversation, Senior Engineer Yun-Bo ZHANG for assistance with the information material.

References

1. US NRC. NUREG/CR6303-1994, Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems.
2. US NRC. NUREG/CR7007-2010, Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems.
3. US NRC. NUREG 0800 Chapter 7-2007, Guidance for evaluation of diversity and defense in-depth in digital computer-based instrumentation and control systems.
4. HAD 102/14-1988, Safety related instrument and control system in nuclear power plant.
5. HAD 102/16-2004, The important safety system based on computer software in nuclear power plant.
6. Mao Congji, Wu qi (2012) Discussing the Design of Digitized I&C for NPP from the Perspective of Safety Review. PROCESS AUTOMATION INSTRUMENTATION, vol. 7:39–42.
7. Zhang Yunbo, Zhang Mi, Huang Weijie, Mao Congji, Li Shixin, Yin Baojuan (2014) Analysis of Diversity and Independence for ATWT Mitigation System in Nuclear Power Plant. Nuclear Power Engineering, Vol. 35. No. 6:77–79.

8. Xiao Peng, Liu Hongchun, Zhou Jixiang, Guan Zhonghua (2014) Design of Diverse Actuation System in Nuclear Power Plant. Nuclear Power Engineering, Vol. 35. No. 2:90–93.
9. YU Jinbo (2008) The diversity analysis of AP1000 drive system. Heilongjiang science and technology information, Vol. 33:53–54.
10. JIN Si-qi, PENG Jin, PENG Hua-qing, ZHOU Wei-hua (2012) Research on the strategy coping with DCS platform failure of EPR. Nuclear Science and Engineering, Vol. 32 s2:105–110.