The Several Issues in Safety Review of Digital Control System in Chinese Nuclear Power Plant

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

Abstract With the extensive application of digital control system (DCS) in Chinese nuclear power plant, the safety of DCS attracts people's attention. First of all, this paper briefly introduces the overall structure of DCS. Then it summarizes the several key issues about DCS from the perspective of nuclear safety review: the single failure criterion, testability, diversity, software verification and validation (V&V), configuration management, which are common issues in the safety review. These issues are analyzed according to the relevant regulation and standards. At last, some solutions are given to these common issues, and some suggestions are made for future review.

Keywords Nuclear power plant · DCS · Safety review

1 Introduction

Digital control system is one of the most important systems in nuclear power plant. DCS is more like the "central nervous system" of the entire nuclear power plant, and its stability is the key for the safety, reliability and economic of operation. At present, DCS technology is or will be used in most of Chinese nuclear power plants.

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

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

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

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

Y.-H. Guo
e-mail: Gyh86126@126.com

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_18

Compared with traditional analog technology, the application of DCS can improve the efficiency of the nuclear power plant, safety and reliability. With the application of DCS in nuclear power plant, the related operation event leads to widespread concern. Therefore, the review of the DCS is one of the key issues in nuclear safety review. This paper analyzes several important issues in safety review of DCS, and gives some suggestions for future review.

2 The Structure of DCS in Nuclear Power Plant

In general, DCS can be divided into 4 levels by functions: field level, automation level (individual control and measurement level), communication level, process information and control level. The field level is mainly used for detecting the parameters of process equipment, controlling the technical process according to the command, providing/controlling processing functions such as power supply equipment. The automation level is mainly used for data acquisition, signal pre-processing, logic processing, operation of control algorithm, and other functions. The communication level is mainly used for data and signal communications. The process information and control level is mainly used for information support, diagnostic, operator action and process information records, controlling unit by operating equipment and other tasks.

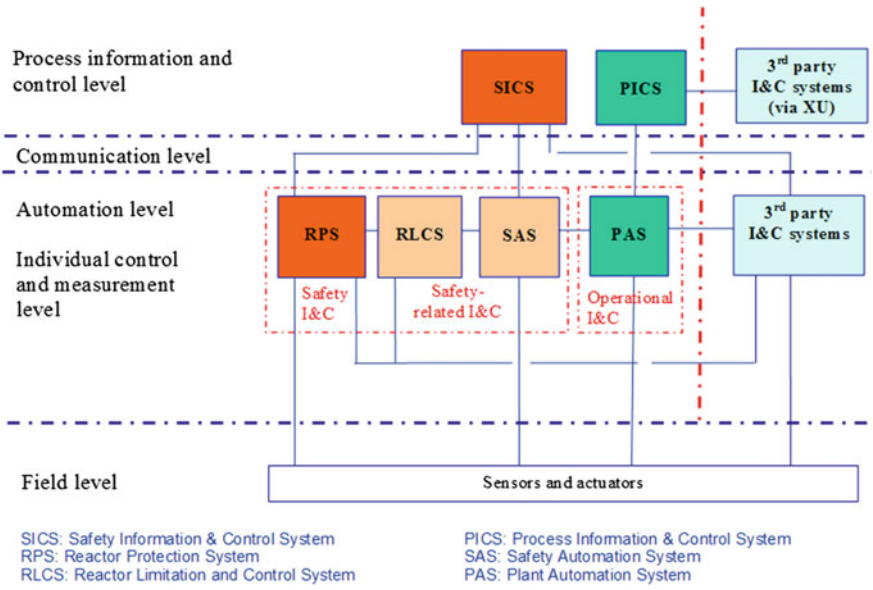

Fig. 1 DCS structure diagram

Figure 1 is the overall DCS structure diagram. Automation level, communication level, process information and control level are the focus of attention in safety review.

3 The Review Concerns

3.1 The Structure of Reactor Protection System

Reactor protection system mainly includes reactor trip (RT) system and engineered safety feature (ESF) system [1]. The RT system is made up of process measurement channel, nuclear measuring channel, acquisition and processing logic channel, reactor trip breaker, manual driving circuit and so on.

Except for adopting four redundant channels, the RT system should also adopt the principle of diversity; the protection parameters with functional diversity are assigned in different processors in order to reduce the impact of common cause failure. When a protection channel fails, if the rest of the protection channels can't meet the single failure criterion, the system will generate scram signal to achieve safe shutdown.

The ESF system consists of measurement/signal processing and logic part.

The structure of measurement/signal processing part is similar to RT system, including four redundant signal processing channels.

The logic part includes two redundant series. It receives the input signal from the signal processing channels and performs the required logic to drive the engineered safety features. Each logic series can drive minimum number of engineered safety facilities and equipment as the safety functions required. To ensure that, single failure in any redundant series will not result in the loss of protection functions.

3.2 Testability

Reactor protection system should have the ability of fault detection and testability during the reactor shutdown mode and power operation mode. The test should be conducted in several stages and each stage should be overlapped to ensure the integrity of the system test [2]. The fault detection and test of RT system should include T1 test-measuring instrument channel test, T2 test-processing unit test (digital protection system test) and T3 test-the output signal and the actuator test.

In the case of self-check failed to cover any fault, there should be specific test equipment to determine the periodic test cycle on the basis of reliability analysis.

3.3 The Diversity of ATWT and RT System

As the back-up of emergency shutdown system, anticipated transients without trip (ATWT) mitigation system should follow the principle of diversity and independence in the system design [3]. It uses the different devices (including software and hardware) to perform the functions same as RT system. For example, the functions of ATWT are implemented by the NC platform and the functions of RT are implemented by the safety platform. The diversity between different platforms are in several aspects such as design, equipment, software, human factors and so on [4].

3.4 Software Verification and Validation

In case of one nuclear power plant, its safety platform TRICON (V10.2.1) has passed the V&V conducted by the vendor itself and the independent third party. Meanwhile in the final safety evaluation report of TRICON, the NRC states that the development process of TRICON (V10.5.1) and the new/updated version of the software components meet the requirement of SRP section 7, BTP7-14, BTP7-18, EPRI TR-107330 and EPRI TR-106439, and the software modules in TRICON (V9.5.3) are also accepted due to the safety evaluation of TRICON (V9.5.3). The review conclusion requires a detailed description of the hardware and software changes from TRICON (V10.5.1) to TRICON (V10.5.3) which is used in this nuclear power plant.

For the specific TRICON application software of this nuclear power plant, the related V&V work is conducted by the independent third party. So it can effectively guarantee the independence of V&V work in management, organization and financial [5].

3.5 Configuration Management

The configuration management of DCS is used to control hardware equipment, software, and file version so as to identify the system version, help to the execution of the change, and to protect the history of configuration object and so on [6].

The following problems often exists in the configuration management work of DCS in nuclear power plant: there is no clear distinction between safety and non-safety items in the configuration state statistics; it lacks some contents such as software tool which is required in configuration management program; the naming rule of software version is unclear; the configuration state statistics can't reflect the actual situation of DCS, and so on.

A detailed and specific configuration state statistics, the naming rule of the version and the clear expression of the software version in the V&V report are

helpful to ensure the implementation of the configuration management program of DCS. The configuration management can effectively control the hardware and software version in factory test phase and site commissioning phase, and it is also helpful to the following subsequent change management and update work.

4 Conclusion and Suggestion

The structure design, testability, diversity, software V&V, configuration management of DCS should meet the requirements of relevant laws and regulations.

For future review, some suggestions should be noticed. The software configuration management of hardware and software should be enhanced and improved to ensure the effectiveness; the safety software V&V activities should be carried out strictly in the operation and maintenance phase according to the requirements of relevant laws and regulations.

In recent years, some operator workstation disable events had showed up in some nuclear power plants, and the operators had to move to the BUP panel to wait for workstation restarting. These events brought some adverse effect for the stable operation of the power plant. So it should be paid more attention to the commissioning test and operation of non-safety DCS.

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, Engineer Jing-bin Liu and Yin-hui Guo for proposed changes.

References

1. ZHENG Weizhi (2012) The Fault Analysis and Application of Reactor Protection System in Nuclear Power Plant. Nuclear Electronics & Detection Technology, Vol. 32. No. 3: 337–341.
2. GB/T5204-1994, Periodic tests and monitoring of the safety system of nuclear power plant.
3. US NRC. NUREG/CR6303-1994, Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems.
4. ZHANG Yunbo (2014) Analysis of Diversity and Independence for ATWT Mitigation System in Nuclear Power Plant. Nuclear Power Engineering, Vol. 35. No. 6: 77–79.
5. IEEE Std.1012-2012, IEEE Standard for System and Software Verification and Validation.
6. IEEE Std.828-2005, IEEE Standard for Software Configuration Management Plans.