Application of the dynamic FMEA in the reliability analysis of DCS

Li Yankai[1,2]; Wang Xu[1,3]; Lin Meng,[1,3,*]

[1]Shanghai Jiao Tong University
[2]Shanghai Nuclear Reactor Simulation Technology Co.,Ltd.
[3]Shanghai Jiao Tong University Sichuan Research Institute

Abstract. Digital distributed instrumentation and control system (DCS) is critical to the safety of nuclear power plants (NPPs). Static analysis methods developed from analog control system are not applicable to DCS due to its enhanced dynamic interactions and complex structure of hardware/software/firmware. The enhanced dynamic interactions of DCS include both sequence and timing factors, which are hardly modelled in the traditional Failure Mode and Effect Analysis (FMEA). In this study, dynamic FMEA (DFMEA) method based on simulation technology is put forward for the design and review of DCS in NPP. DFMEA based on real DCS hardware and software is developed to reveal the dynamic failure paths and failure modes. The results of DFMEA can well support the establishment of the dynamic fault tree/event tree in the review of NPP DCS, which reduces the dependency on the analyst's experience significantly.

1 Introduction

FMEA (Failure Mode and Effect Analysis) plays an important role in PSA analysis in nuclear power plant (NPP). The traditional FMEA is mainly based on static analysis, which depends on the analyst's experience. However, Digital Instrument and Control System (DCS) has complex structure composed of firmware/software/hardware and interactions between components and the controlled process system [1-2]. Both failure sequence and timing should be considered in the FMEA of a DCS system. The dynamic interactions of DCS make it difficult to conduct comprehensive and accurate analysis based on the analyst's experience [3-4]. In this study, we proposed dynamic FMEA analysis that combines the simulation technology of nuclear power plant with the failure analysis of DCS, which helps to analyze the dynamic failure behavior of DCS conveniently and effectively. The main feedwater control system of NPP is analyzed in detail using this method to illustrate the dynamic FMEA method is applicable and practical for complex DCS system.

2 The FMEA method

The dynamic FMEA method uses simulation technology to describe all DCS system functions of interest, including DCS hardware, software and firmware functions, as well as the interaction between DCS and the controlled process system. Analysts can dynamically insert different DCS fault, analyze the consequence, even the respond of the entire nuclear power plant system. In this way, analyst can study the various failure modes and consequences of DCS conveniently and get rid of dependence on experience and data of the real NPP. It helps the analyst to be familiar with the functional design of the DCS system, so that it can easily explore the various dynamic failure modes of DCS, as well as the possible dynamic failure path of a certain top event. Therefore, the establishment of a dynamic fault tree could be reliable and feasible.

The development of dynamic FMEA can be divided into multiple levels, from top-level system analysis to detailed bottom-level component failure modes and consequence analysis[5]. The chosen of detailed level of dynamic FMEA depends on the needs of analysis: non-critical systems can obtain the overall failure probability through system-level failure analysis, while important systems require more detailed component-level failure analysis to obtain specific failures for targeted assessment and improvement.

Dynamic FMEA is very important for the quality and efficiency of dynamic PSA analysis. If a detailed dynamic fault tree of a real nuclear power plant DCS system is to be established, the demand for dynamic FMEA will be very urgent. In this study, the dynamic FMEA tool is developed that can truly reproduce the system operation and fault response characteristics of the DCS system and its controlled process system. The objects to be analyzed by dynamic FMEA include the DCS system itself and the controlled process system. When simulating the DCS system itself, it is required to be as consistent as possible with the real DCS system, especially the DCS software. The real DCS software should be used to simulate the behavior of the DCS as much as possible to avoid different failure modes introduced by the simulation. In this way, the dynamic failure behavior of the DCS system itself can be truly captured. When simulating the controlled process system, it is required to reflect the dynamic response behavior of the system as accurately as

* Corresponding author: linmeng@sjtu.edu.cn

possible. Usually, the best estimated mathematical physical model is used to truly reflect the response of the process system.

The content of modeling required for dynamic FMEA of a typical DCS system can be divided into the following categories[6], as shown in Table 1, and the corresponding description method is researched and proposed accordingly.

3 Case study: DFMEA of the main feedwater control system

3.1The main feedwater control system

Using the above method, dynamic FMEA analysis of the main feed water control system (MFCS) of a four-loop PWR nuclear power plant is carried out. MFCS is built based on the XDC800 system(an industrial DCS system). Failures of important components are considered in the case study, including redundant power supply, redundant controller, dual-network redundant real-time control network, controller switch line, IO cards, card slots, firmware and software. The control logic of MFCS is a three-impulse level control scheme, and its simplified schematic is shown in Figure 1.

Table 1. Categories of DFMEA modeling and their modeling method

Object			Example	Required modeling method
Software	System software		XSelf	Original SW of DCS, or simulation
	Application	Configuration and logic	XCUCfg	Original SW
		Human interface	XView	Original SW of DCS, or simulation
DCS Hardware			XDC800a	Combination of real HW and simuilation
DCS Firmare			Windows CE	Depending on HW model
The controlled process system			4-loops NPP	Simulation
DCSinterface			Input from other system	Simulation

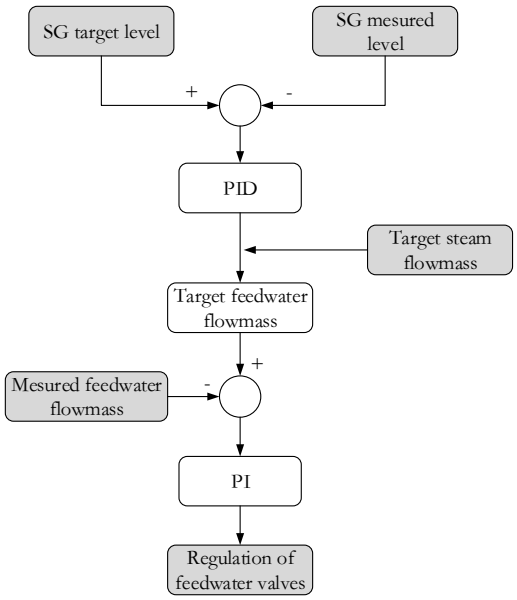


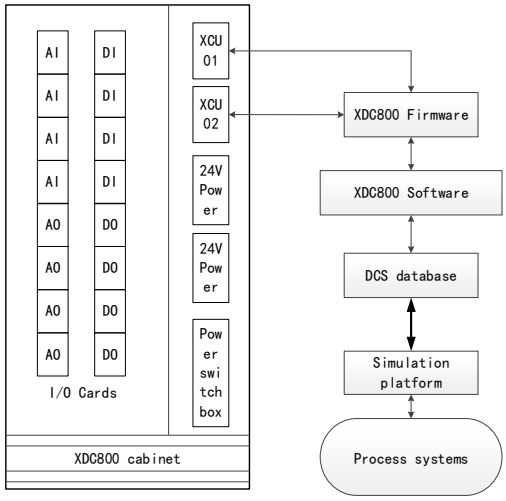
Fig. 1 Simplified schematic of MFCS logic

3.2 DFMEA With real DCS hardware

Two kind of DFMEA are implemented successively, i.e., analysis with and without real DCS hardware. The former applies to small-scale analysis, allowing analysts to carry out fault analysis on the real XDC800 cabinet to restore the structural design and fault consequences of DCS to the greatest extent. The latter is suitable for large-scale applications which describes hardware functions and various hardware failure scenarios through software simulation. In practical applications, first of all, the former is used to help analysts to form an intuitive and accurate understanding of the structural design and fault form of the DCS system. On this basis, the latter is used to carry out FMEA analysis of large-scale systems.

In the DFMEA analysis with hardware, the DCS part is completely realized by the XDC800 cabinets and the simulator provides the controlled process systems model and the supportive environment (simulation procedure control, real-time database, synchronization control, etc.) for simulation. XDC800 DCS is embedded as a special module in the simulation platform, and the development of the FMEA toolkit can be completed by using the functions of the simulation platform. Among them, the thermal power, core physics and equipment modules of the simulation platform are used to build the corresponding power plant model. The failure mode insertion for DCS is carried out on the XDC800 cabinets to simulate the behavior of DCS. By observing the behavior of the DCS itself and the response of the simulation model, various failure behaviors of the DCS can be truly reproduced and the consequences can be analyzed. The schematic diagram and physical facility of DFMEA with DCS hardware are shown in Figure 2. It provides realistic scenes that allow analysts to observe and understand of DCS behavior while they are away from the nuclear power field. However, it is only suitable for application on a small scale -due to the high cost of hardware and inconvenient implementation. On this basis,

DFMEA without DCS hardware could be carried out on large-scale.



（a）schematic diagram

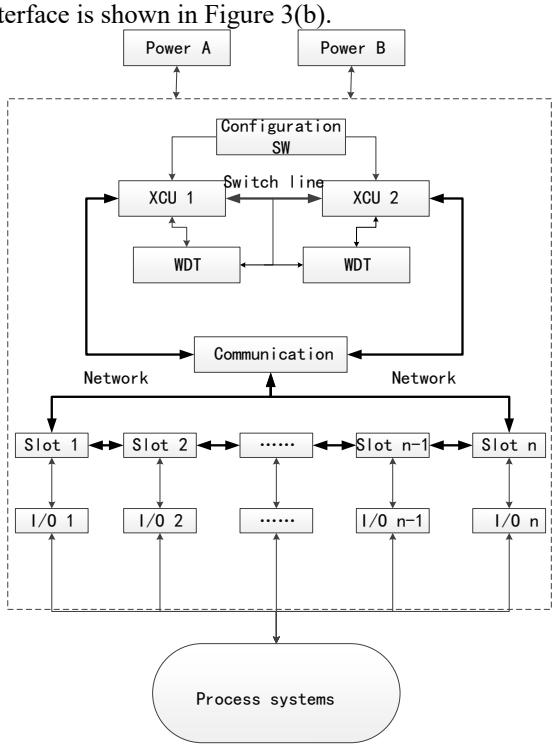
（b）physical facility

Fig. 2 DFMEA with DCS hardware

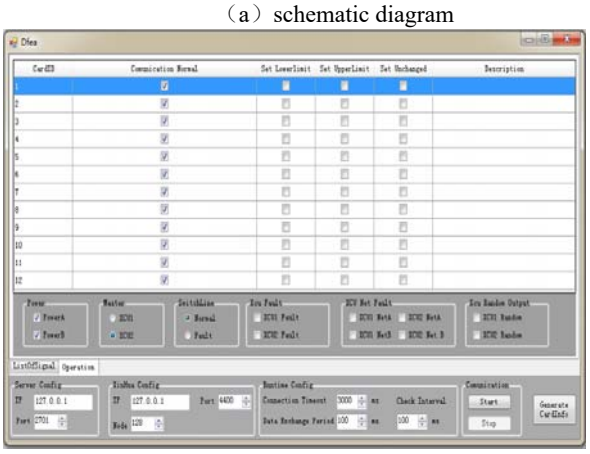
3.3 DFMEA Without real DCS hardware

Without DCS hardware, DFMEA uses the original DCS software, algorithms and hardware function simulation code to simulate the behavior of DCS. The DCS simulation module is embedded as a special module in the simulation platform. All the control logic of DCS is developed using XCUCfg (configuration software of XDC800 [7]) and runs on its virtual processor VXCU, thereby the software and algorithms of DCS are consistent with the real DCS. The power plant process system models are integrated in the simulation platform to provide the response of NPP. Schematic diagram of DFMEA Without real DCS hardware is shown in Figure 3(a).

A customized code for DCS fault insertion and failure behavior simulation is developed, based on XCUCfg and virtual controller XVCU. Two VXCUs are used to simulate the main and auxiliary control processors respectively, and the developed control logic configuration is downloaded to the two VXCUs. The hardware failure behavior is simulated based on the result of DFMEA with DCS hardware. The simulated hardware failure is shown in Table 2; the software interface is shown in Figure 3(b).



（a）schematic diagram



（b）graphical interface of the analysis code

Fig. 3 DFMEA without DCS hardware

Table 2. The simulated hardware failure

HW object		Simulation function
Power	Power A	Power supply,faults
	Power B	Power supply,faults
Controller	XCU 1	Works,faults, random output
	XCU 2	Works,faults, random output
	Switch	Normal,faults
Networks	Switch line	Normal,faults
	XCU1 NET A	Works,faults
	XCU1 NET B	Works,faults
	XCU2 NET A	Works,faults
	XCU2 NET B	Works,faults
Cards	Slots	Works,faults
	AO	Normal output, upper

	AI	output fault, lower output fault, remain unchanged output for n cards
	DO	
	DI	
	PT100	
	RTD	
	AO-MV	
	PO	

4 Result analysis

Various failure modes of MFCS were studied in detail using DFMEA toolkit. The main analysis failures are shown in Table 3. A comprehensive dynamic FMEA will be a huge process, combined by kinds of failures in Table 2 and Table 3 considering sequence and timing. In this paper, parts of typical failures are selected as examples to show the result of DFMEA.

It is found that although most failure modes and paths are consistent with the analyst's expected results, some failure modes with a high degree of coupling and strong dynamic interaction are beyond

Table 3. Main analysis content of DFMEA of MFCS

Object	Content	Typical example
Hardware	Shown in Table 2	-
Software	Output failure of the main calculation module	Output of Level deviation PID is the upper limit
	Memory misalignment	random output
	Abnormal operation caused by SW	The setup box of the display unit cannot be popped up
	Abnormal communication	Input and output of SW remain unchanged
	Software crash	Output of the configuration SW remain unchanged
Firmware	Communication error caused by firmware	The configuration SW reads the database abnormally
	Firmware crash	Controller failure status due to firmware crash

the analyst's expectations and difficult to judge by empirical knowledge. DFMEA can help to discover this part of the failure mode and path, and confirm its specific consequences. It has great significance to ensure the comprehensiveness and accuracy of the model of dynamic fault tree and enhance the confidence in the analysis results. Here are some typical dynamic failure scenarios:

1）Main controller fails after the dual-controller switching line failure. At this case, backup controller cannot take charge although it works. However, it could be activated manually by operator through the engineering station. Ignoring the former will underestimate the failure probability of DCS, while ignoring the latter will overestimate its failure probability.

2）Software running in main controller fails. It mains that the watchdog fails at the same time so that the system status cannot be detected. Although the software and hardware of the backup controller are all normal, it cannot be activated and the output value is wrong. This shows that although DCS has self-detection and redundant protection functions, the failure of software may lead to the failure of redundant functions.

3）DCS output fault leads to the valve maintained at current position. In this case, it shows the timing effect of the failures. At different fault time, the SG level could reduce or increase under different valve regulation. The responses of the NPP system could be totally different due to the same failure in different time.

Acknowledgments

Supported by Sichuan Science and Technology Program(2020YFSY0063).

References

1. Aldemir T, Miller D W, Stovsky M, et al. Current state of reliability modeling methodologies for digital systems and their acceptance criteria for nuclear power plant assessments[J]. NUREG0CR-6901, US Nuclear Regulatory Commission. 2006.
2. Aldemir T, Stovsky M P, Kirschenbaum J, et al. Dynamic reliability modeling of digital instrumentation and control systems for nuclear reactor probabilistic risk assessments[J]. Nureg/Cr-6942. Washington, DC: US Nuclear Regulatory Commission. 2007.
3. Kirschenbaum J, Bucci P, Stovsky M, et al. A benchmark system for comparing reliability modeling approaches for digital instrumentation and control systems[J]. Nuclear Technology. 2009, 165(1): 53-95.
4. Ieee B E. IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations - Redline[J]. 2010: 1-82.
5. Chu T L, Yue M, Martinez-Guridi G, et al. Modeling a Digital Feedwater Control System Using Traditional Probabilistic Risk Assessment Methods[J]. US Nuclear Regulatory Commission. Washington, DC. 2009.
6. Li Yankai. Research on Dynamic Analysis Methods Based on Simulation Technology for Nuclear Power Plant Digital Instrument and Control system [D]. 2017.
7. Xinhua control technology Technology Co.,Ltd. OnXDC user manual[M]. 2013.