Design of Self-diagnosis for Diversity Actuation System Based on FPGA in ACPR1000 Nuclear Power Plant

Ji-Kun Wang(✉), Zhi-Hui Zhang, Gui-Lian Shi, Chang-Yu Mo, Gang Li, and Bin Wu

China Techenergy Co. Ltd., Beijing 100094, China
wangjikun@cgnpc.com.cn

Abstract. Self-diagnosis for diversity actuation systems (KDS) is essential for the safe operation of nuclear power plants (NPPs). With the development of FPGA technology, more and more KDS in NPPs are realized with FPGA technology. This paper provides a self-diagnosis solution for KDS based on FPGA, which includes fault detecting, fault handling, diagnosis information monitoring and alarm indication. After testing and verification in ACPR1000 NPPs, and this solution can effectively improve the maintainability of KDS, can be widely used in other type of NPPs, and has broad application prospects.

Keywords: Diversity actuation system · FPGA · Self-diagnosis

1 Background

According to IEC 61513 [1], the faults and errors should be fully detected, and sufficient and correct fault diagnosis information should be provided. Therefore, The self-diagnostic function is very important for the I&C system in NPPs. The design of the self-diagnostic function directly affects the maintainability of KDS, and can effectively improve the safety of NPPs [2–5].

The FitRel platform is a FPGA-based product developed by China Techenergy Co. Ltd., and has been formally applied in ACPR1000 NPP [6]. However, there is no precedent and experience to follow for KDS based on FPGA technology. Therefore, it is urgent to design a set of self-diagnostic solutions suitable for FPGA technology. Based on the practical experience in the FitRel product development, and maintainability design theory, this paper raises a self-diagnostics solution suitable for KDS in NPPs.

2 Methodology of Self-diagnosis

The system self-diagnosis function is based on the basic principles of self-diagnosis design, which includes 3 steps.

Step 1: Completeing the classification of the fault, and determining the severity of the impact of the control station function where the faulty device is located.

Step 2: Determining the fault diagnosis method based on the severity of the fault.

Y. Xu et al. (Eds.): ISNPP 2021, LNEE 883, pp. 563–571, 2022.
https://doi.org/10.1007/978-981-19-1181-1_54

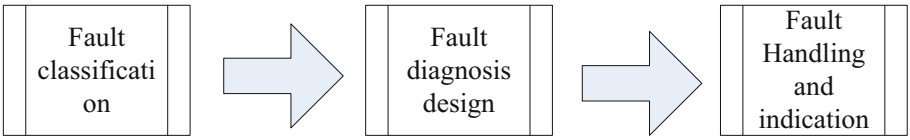

Fig. 1. Methodology of self-diagnosis diagram

Step 3: Fault indication for the operation and maintenance personnel (Fig. 1).

For the FPGA based platform, There are many fault modes that need to be defined, and for the fault diagnosis design and indication, there are some principles that need to follow.

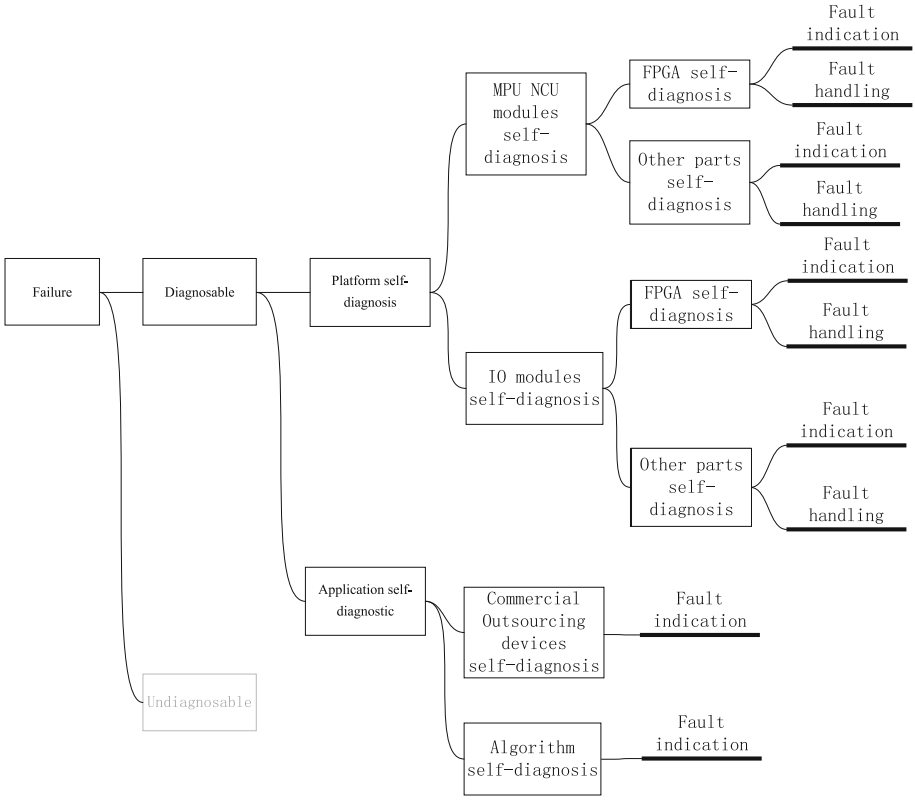

Fig. 2. Self-diagnosis diagram of KDS

3 Self-diagnosis Design

Through the failure mode effects analysis (FMEA) of KDS system [7], The diagnostic measures, handling measures and alarm indication mechanisms of the failure modes are designed based the failure mode effects.

Especially, because the FPGA is very complex, and the self-dignosis for FPGA is not easy to analysis and design, so this paper difines FPGA failure as an special part, and the self-diagnosis diagram can be shown in Fig. 2.

3.1 Fault Classification

Fault classification is to classify the fault according to the severity of the fault, and the fault level will be the basis for the fault alarm indication. In this document, the severity of the faults will be judged based on the severity of the impact of the fault modes on the function of the control station where the fault device is located.

The failure modes are shown in the following Table 1:

Table 1. List of failure modes

No.	Failure mode	Involved equipment
1	AI module channel circuit failure	AI module
2	AI module communication failure	AI module
3	AI module FPGA failure	AI module
4	DI module channel circuit failure	DI module
5	DI module communication failure	DI module
6	DI module FPGA failure	DI module
7	AO module channel circuit failure	AO module
8	AO module communication failure	AO module
9	AO module FPGA failure	AO module
10	DO module channel circuit failure	DO module
11	DO module communication failure	DO module
12	DO module FPGA failure	DO module
13	KDS Level2 equipment failure	KDS Level2 equipment
14	OPS task process failure	OPS station
15	NCU module communication with MPU failure	MPU module, NCU module
16	NCU module FPGA failure	MPU module

(*continued*)

Table 1. (*continued*)

No.	Failure mode	Involved equipment
17	NCU communication failure with other NCU module	NCU module
18	MPU module FPGA failure	MPU module
19	The power supply bus in the cabinet loses power	Power supply bus of the cabinet
20	24V power supply module failure 24V power supply module	Power supply module
21	The cabinet temperature exceeds the upper limit	Device in the cabinet
22	Fan status is abnormal	Device in the cabinet

3.2 Fault Diagnosis Design

In order to cover the faults of the KDS system to the greatest extent, the fault diagnosis design principles are as following:

1) The overall design principle follows IEC 60671 [8], self-diagnosis shall cover all diagnosable faults;
2) In order to prevent the system from spurious actuation, the fault handing shall led to fail-safe, and mainly indicate fault information in detail.

The self-diagnosis of the KDS system include two parts, the self-diagnosis function of the FitRel platform and the self-diagnosis of the engineering application. The self-diagnostic function of the FitRel platform refers to the inherent fault diagnosis measures of the FitRel product; the application self-diagnostic measures are designed according to specific engineering applications.

Platform self-diagnosis measures are shown in Table 2 For FPGA failure, this paper involes 7 self-diagnosis measures to keep all the dignosable failure mode can be detected and handled.

Application self-diagnostic measures are shown in Table 3.

Table 2. Platform self-diagnosis measures

Classification	Failure mode	Self-diagnosis measures	Fault handling and indication
FPGA failure in MPU\NCI\IO modules	FPGA failure	Digital power diagnosis	Fault indication
		Clock diagnosis	FPGA reset, Fault indication

(*continued*)

Table 2. (*continued*)

Classification	Failure mode	Self-diagnosis measures	Fault handling and indication
		State machine self-diagnosis	FPGA reset for five times, then Lock-down, Fault indication
		Watchdog	FPGA reset, Fault indication
		Module in-position diagnosis	Fault indication
		Interface diagnosis	FPGA reset, Fault indication
		EEPROM CRC check	FPGA reset for five times, then Lock-down, Fault indication
Other failures in MPU\NCU\IO modules	Data communication failure	Data frame serial number detection	Output AS-IS, Fault indication
		Communication cycle detection	
		Source address and destination address detection	
		CRC check	
	Analog signal drift failure	AI dynamic self-check	Fault indication
	Fixed failure of analog acquisition signal		
	Analog acquisition signal over-range fault	AI over-range self-checking	Fault indication
	Digital acquisition signal is always a fixed value	DI redundant hardware acquisition and comparison	Fault indication
	Analog output signal drift failure	AO output end sampling and readback	Fault indication
	No output for analog output signal		
	Digital output signal fixed failure	DO channel readback	Fault indication

Application self-diagnostic measures: Application self-diagnostic measures are aimed at failure modes related to the application, and are a supplement to platform self-diagnostic measures. The application self-diagnostic measures of KDS system in ACPR1000 NPP are as follows.

Table 3. Application self-diagnostic measures

Classification	Failure mode	Self-diagnosis measures	Fault handling and indication
Commercial Outsourcing Device failures	The cabinet temperature exceeds the upper limit	Temperature sensor	Fault indication
	Fan status is abnormal	Fan monitoring	Fault indication
	The cabinet door status is abnormal	The travel switch check	Fault indication
	24 V power supply module failure	Power supply voltage monitoring	Fault indication
	KDS Level2 equipment failure	Level2 equipment self-diagnosis	Fault indication
	Power failure	Monitoring of power supply bus in the cabinet	Fault indication
Algorithm failures	Redundant channel deviation	Real-time comparison of the deviation of the collected value, calculated value and output value of the redundant channel	Fault indication

3.3 Fault Indication

Principles of alarm indication:

1) Indicate fault information on the human-machine interface;
2) The failure information display needs to be consistency with different human-machine interface.

After the fault is diagnosed, each cabinet of the KDS system will give an alarm indication in the following three ways:

Main control room alarm indication: alert the operator and maintenance personnel of KDS failure in the first time;

Local display alarm indication: the fault diagnosis information is transmitted to the LOC-VDU through the network to indicate the faulty equipment;

Local cabinet indication: process the fault information with turning off the cabinet lamp and other module lamps, and help maintenance personnel locate the faulty cabinet (Fig. 3).

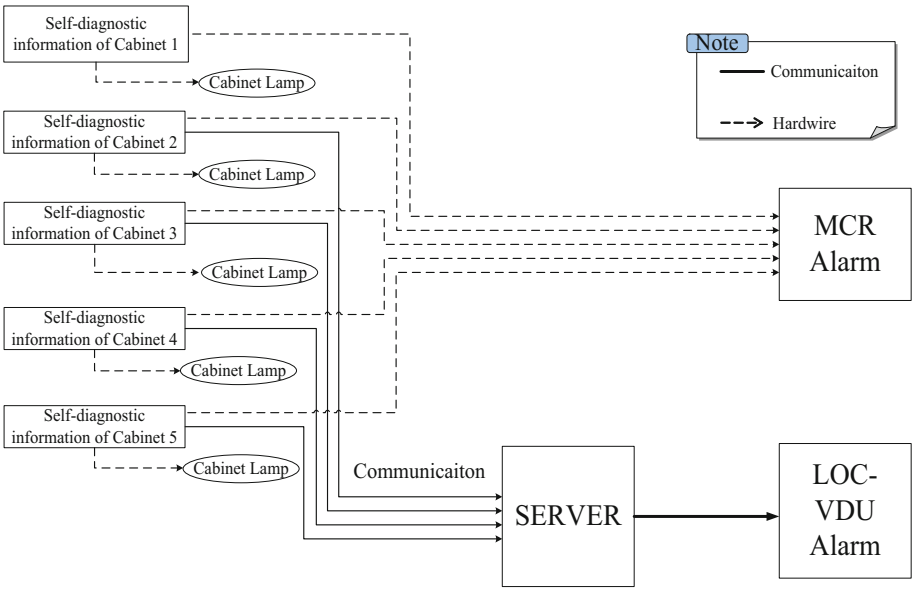

Fig. 3. Fault indication flow diagram

4 Test

The test results are shown as follow in KDS in Yangjiang 5&6 NPP and engineering prototype. All the failure mode of KDS can be detected and indicated, and if the FPGA failure, the output of failure module can be set as fail-safe. There is no spurious trip in KDS (Table 4).

Table 4. Test results

Fault classification	Requirement	Result
AI module channel circuit failure	Warning in real time	√
AI module communication failure	Warning in real time, fail-safe	√
AI module FPGA failure	Warning in real time, fail-safe	√

(*continued*)

Table 4. (*continued*)

Fault classification	Requirement	Result
DI module channel circuit failure	Warning in real time	√
DI module communication failure	Warning in real time, fail-safe	√
DI module FPGA failure	Warning in real time, fail-safe	√
AO module channel circuit failure	Warning in real time	√
AO module communication failure	Warning in real time, fail-safe	√
AO module FPGA failure	Warning in real time, fail-safe	√
DO module channel circuit failure	Warning in real time	√
DO module communication failure	Warning in real time, fail-safe	√
DO module FPGA failure	Warning in real time, fail-safe	√
The cabinet temperature exceeds the upper limit	Warning in real time	√
Fan status is abnormal	Warning in real time	√
KDS Level2 equipment failure	Warning in real time	√
OPS task process failure	Warning in real time	√
NCU module communication with MPU failure	Warning in real time, fail-safe	√
NCU module FPGA failure	Warning in real time, fail-safe	√
NCU communication failure with other NCU module	Warning in real time, fail-safe	√
MPU module FPGA failure	Warning in real time, fail-safe	√
The power supply bus in the cabinet loses power	Warning in real time Warning in real time	√ √
24 V power supply module failure 24 V power supply module	Warning in real time Warning in real time	√ √

5 Conclusion

This paper presents a self-diagnostic solution for the KDS in ACPR1000 NPP. The self-diagnostic solution draws on the best practical experience in the field safety I&C. At present, the self-diagnostic solution has been applied in Yangjiang 5&6, The Hongyanhe 5&6 project, and has undergone testing and verification, including R&D testing, in-plant testing, owner's factory commissioning. The results show that the solution can cover all diagnosable faults of the FitRel platform based on FPGA technology, can indicate the diagnosis information in real-time, and can provide sufficient information for the daily maintenance of nuclear power plants. After adaptive adjustment, it can meets the requirements of AP1000, EPR reactor-type NPP, and has broad application prospects.

References

1. IEC: IEC 61513 Nuclear power plants - Instrumentation and control important to safety - General requirements for systems. IEC, Geneva (2011)
2. NUREG/CR-7006: Review Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems. NRC (2010)
3. Naser, J.: Guidelines on the Use of Field Programmable Gate Arrays (FPGAs) in Nuclear Power Plant I&C Systems. TR-1019181 EPRI 2009, pp. 41– 59 (2009)
4. Ranta, J.: The current state of FPGA technology in the nuclear domain. VTT (2012)
5. Bobrek, M., Bouldin, D., Holcomb, D.: Survey of field programmable gate array design guides and experience relevant to nuclear power plant applications, pp. 5– 9. ORNL (2007)
6. Shi, G., Wang, J.: The design of diverse actuation system device in ACPR1000 PWR nuclear power plant. Nucl. Saf. **15**(1), 61–65 (2016)
7. IEC: IEC 60880 Nuclear power plants - Instrumentation and control important to safety - Software aspects for computer-based systems performing category a functions. IEC, Geneva (2006)
8. IEC: IEC 60671 Nuclear power plants - Instrumentation and control important to safety - Surveillance testing. IEC, Geneva (2007)