A novel priority selection system for nuclear power plant

Shuo Wang and Qingwei Shi
China Nuclear Control System Engineering Co. LTD
wangshuo@cncs.bj.cn

Kelin Qi , Gang Ma and Dong Wang
China Nuclear Control System Engineering Co. LTD

ABSTRACT

The priority selection system is an important component of security level instrument control platform for nuclear power plant, the main function of which is priority processing the manual or automatic command with various security levels and driving engineering safety features and field devices, such as pump and valve. Its stability and safety plays a crucial role in the operation of the power plant.

The main objective of the present paper is to describe the new nuclear power plant-oriented priority selection system, which is developed independently by China Nuclear Control System Engineering Company. In this system, the control commands from 1E DCS, ECP and DAS systems are transmitted via hardwire, while those from NC DCS are transmitted by fieldbus. The control commands experience priority output to control the field actuators. Meanwhile, in order to control key field devices when failure of the instrument control systems occurs, the issuing interface for native instructions with permissions setting is also offered. The whole system provides collection-feedback functions for field devices, high coverage self-diagnostic functions and periodic test functions for safety systems. Moreover, the feedback information of field devices, the results of self-diagnosis and periodic test will be submitted to DCS of nuclear power plant. In addition, the core part of priority selection system, namely priority selection module, is obtained by pure FPGA technology, which is different from DCS systems and could avoid common cause failure of software effectively.

Key Words**:** Priority selection system, FPGA technology, Avoid common cause failure.

1 INTRODUCTION OF STATION

PPS(Priority Selection Station) is an important interface device of NicSys®8000N platform(1E-Class DCS). It also belongs to RPS(Reactor Protection System).

Priority Selection Station is mainly composed of Priority Logic Module(PLM), Priority Communication Module and the corresponding pinboards.

1.1 System localization

The Location of Priority Selection Station in RPS is presented in the following Fig. 1.

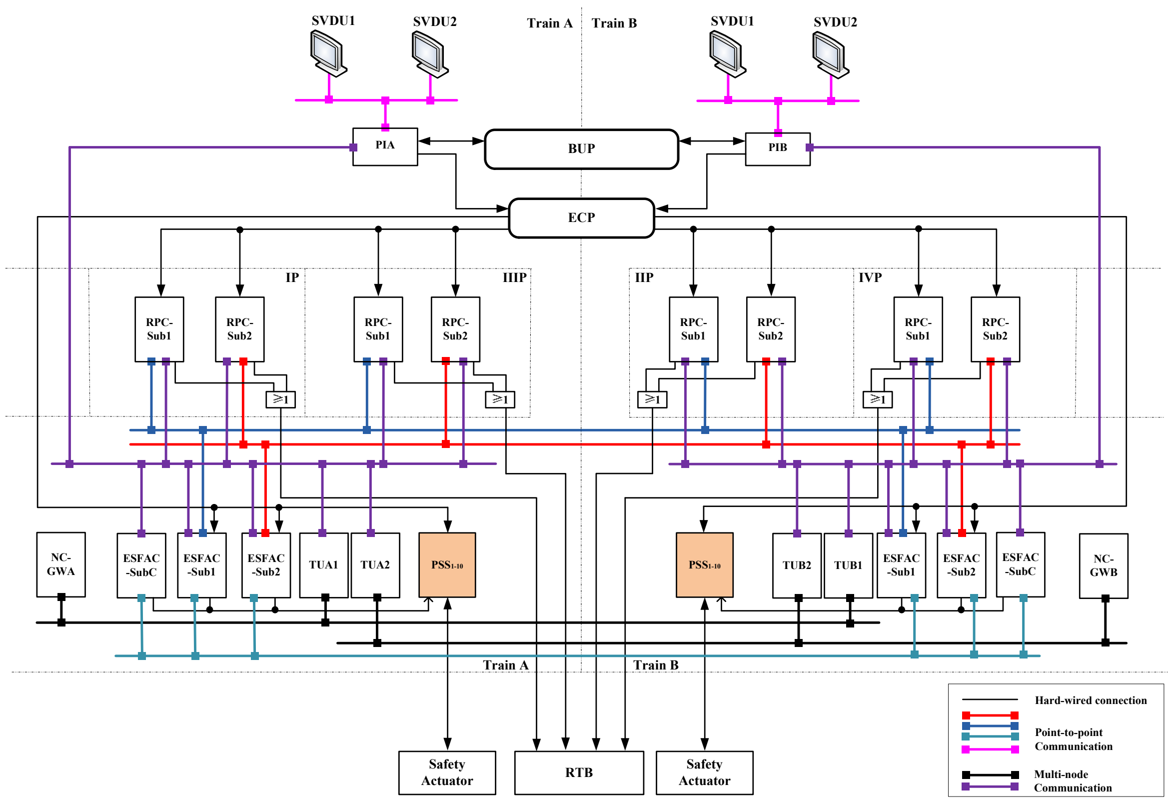

Fig. 1 System Location in RPS

1.2 System Function

The connection relation between Priority Selection Station and other system is shown in the Fig. 2.

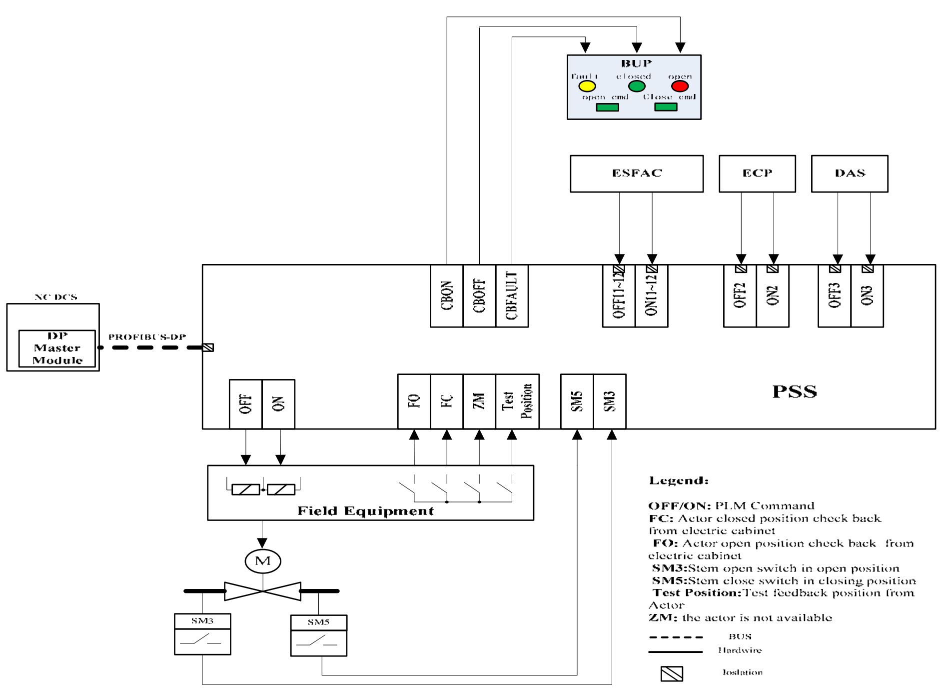

Fig. 2 System Location in RPS

The key function of Priority Selection Station(PSS) is described as follows:

- PSS receives the commands from 1E DCS(1E-Class DCS), DAS DCS(Diversity DCS), BUP(Backup Panel) in hard-wire MODE , and command from NC(None-Safety DCS) DCS in BUS MODE. Then the CPLD in PLM outputs the signal to field actuator in fixed priorities.

  The hard-wire MODE increases the instantaneity of control command and the BUS MODE from NC DCS can decrease the number of cables in industrial field (the veracity of safety can be guaranteed by the Profisafe protocol).

- The local control command can be given by the local command interface of Station.

  Consequently, when all the DCSs fail, the engineer can control the actuator through PSS directly.

- The feedback signal of field device can be received by PLM in hard-wire MODE.
- PLM have diagnosing and alarm functions. The diagnostic information can be uploaded by Profibus-DP.
- Hot-swap function.
- Configuration by Engineer Station.
- Periodic TEST with S-VDU(Safety-Visual Display Unit).

1.3 Advantage Of FPGA Technology

All the modules in Priority Selection Station are developed by FPGA technology. And there is no “black core”, which implies that the code of the function core and operation approach are all known in FPGA, and the code for each line can be verified (the verification work is carried out by V&V team that independent of develop team).

Moreover, compared with microprocessor (in most cases with operating system), FPGA technology decreases the complexity of system and abandons some needless functions for nuclear power control station. Therefore, the higher reliability and faster responds can be achieved: the period when PSS receives the command from DCS to its outputs priority result to actuator is less than 12ms.

At last, since modules with FPGA technology are hard to be hacked, the security of nuclear power control system is guaranteed.

2 STATION COMPOSITION

PSS (generally speaking, we call a priority cabinet as a Priority Selection Station) consists of 3 priority chassis. A typical priority chassis is presented as follows.

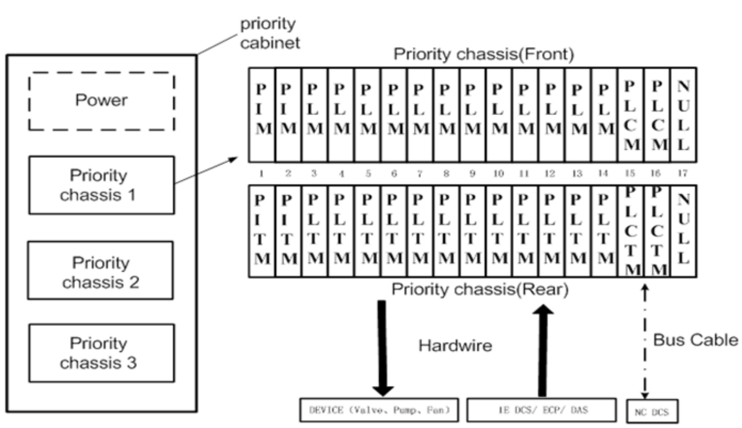

Figure 3. System composition

Each PSS can control at most 36 field actuators. The different priority chassis in one priority cabinet has no connection.(different power supply, different profibus-DP Master)

The functions of modules in PSS are described as follows:

- Priority Logic Module(PLM): complete the center priority logic function.
- Priority Logic Transfer Module(PLTM): transfer the signals from PLM to device.
- Priority Logic Communication Module(PLCM): show the state of Profibus-DP.
- Priority Logic Communication Transfer Module (PLCTM): transfer the Profibus-DP data from photon to electricity.
- Power Indication Module (PIM): detect the Over-Voltage and Under-Voltage state of the chassis power supply.
- Power Input Transfer Module(PITM): transfer the 24VDC power from cabinet to chassis.

The connection between above-mentioned modules is illustrated as follows.

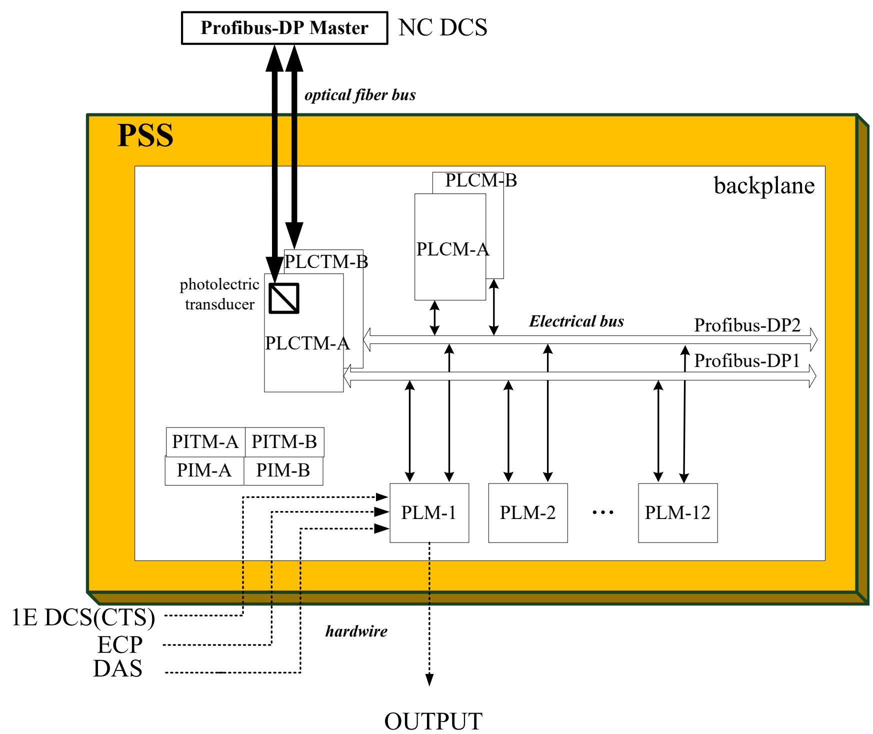

Figure 4. Modules connection in Station

3 PRIORITY LOGIC MODULE

Priority Logic Module(PLM) is the core functional module of PSS. Every PLM receives 4 kinds of DCS's command and controls one field actuator.

3.1 Function Block

The functional block diagram of PLM is shown as follows:

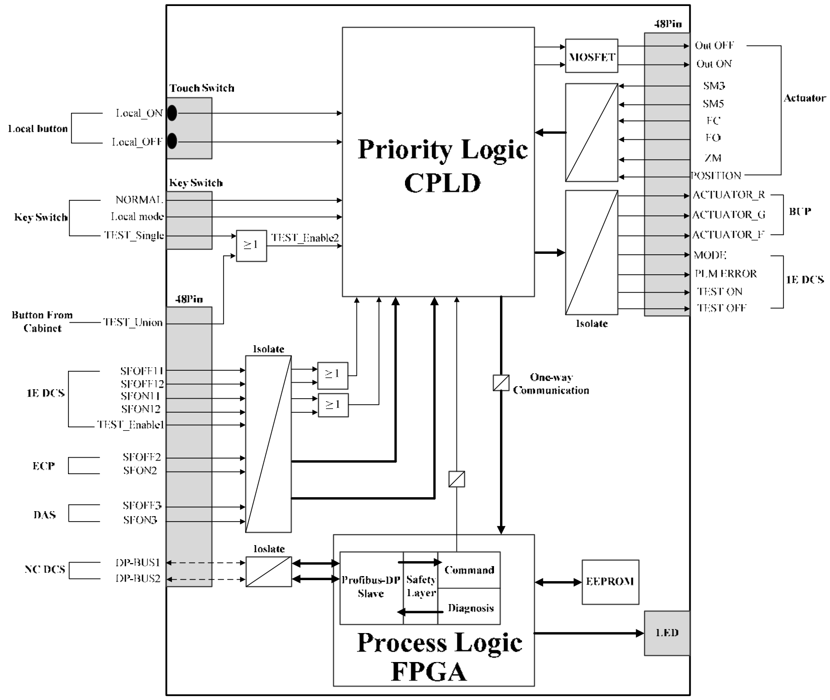

Figure 5. Block diagram of PLM

Every part of PLM will be discussed next.

3.1.1 Key Switch in Front Panel

The Key Switch can set PLM into 3 modes:

- Normal mode(default): PLM controls the field actuator normally.
- Local mode: when all the DCSs fail, local mode can set the command from local (see chapter 3.1.4) to the highest level, so engineer can control the actuator through PSS directly.
- TEST_Single mode: Output TEST_Single signal(One of the conditions which sets PLM into periodical TEST mode).

The key guarantees only the engineer with corresponding level can changes the PLM's mode.

3.1.2 Hardwire Command from DCS

The hardwire command from DCS includes:

- Command from 1E DCS: SFOFF11/SFON11, SFOFF12/SFON12. Two "OFF" will do OR operation in CPLD to produce SFOFF1 and two "On" will do OR operation in CPLD to produce SFON1. Two same commands can decrease rejection rate of system.
- Command from ECP(Emergency Control Panel):SFOFF2/SFON2. In some emergency situation (such as1E DCS fails), engineer can control the actuator through ECP manually.
- Command from DAS(Diversity Control System): SFOFF2/SFON2.To avoid the CCF(Common Cause Failure) in Reactor Protection System, we introduce a Diversity Control System, whose design and architecture is different from 1E DCS.

3.1.3 Bus Command from NC DCS

PLM receives redundancy NC DCS(None-Safety DCS) command through Profibus-DP BUS. To improve security of command from DC DCS, we design a Safety Layer in standard Profibus-DP Data Unit, which avoids the communication errors (such as Corruption, Unintended repetition, Incorrect sequence, Unacceptable Delay and so on.) and describes in IEC 61784-3. When the message fails to pass the check of Profibus-DP protocol or Safety Layer, the command will be abandoned.

Redundant Bus design can decrease the rejection rate of system with the assurance of Safety.

The whole protocol process is shown in Figure 5.

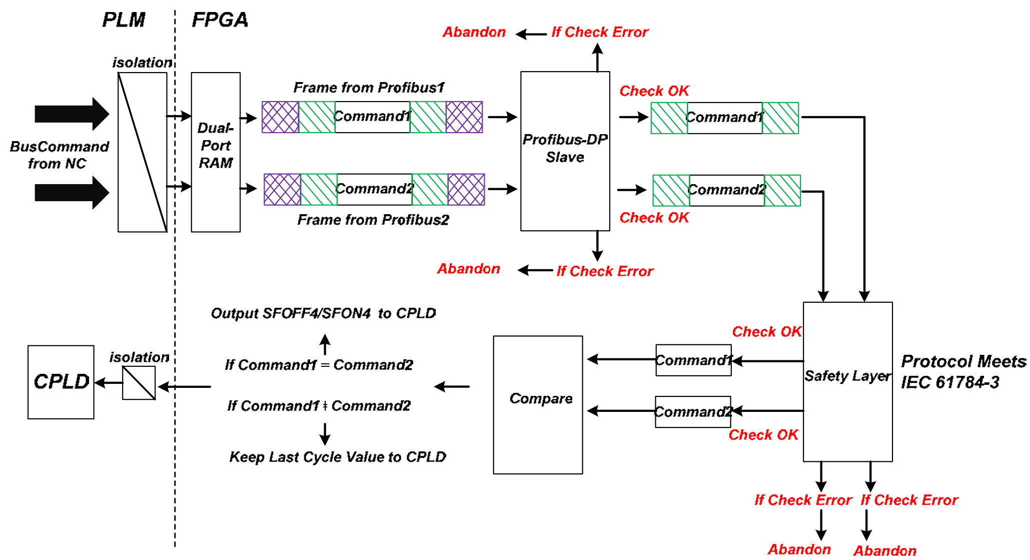

Figure 5. Process to message from NC DCS

3.1.4 Command from Local

When all DCSs (1EDCS,ECP,DAS,NC DCS) fail, PLM provides a local control interface for engineer to control the field actuator in emergency situation. To complete the local control function, Local_ON/Local_OFF from local control interface have the highest priority than other DCSs. (Local_ON/Local_OFF are only effective when the Key Switch is set to Local mode using corresponding key).

3.1.5 Signals of the Actuator

PLM provides 6 digital input channels to collect field actuator's feedback signals(SM3/SM5/FC/FO/ZM/TEST POSITION).

3.1.6 Signals to BUP

PLM has 3 digital output channels to control the lights in BUP(Backup Panel). Thus, the state(open/close/error) of the actuator controlled by PLM through the 3 lights is known for the engineer.(For more details, see Fig. 2)

3.1.7 Signals to 1E DCS

To indicate the state of PLM to 1E DCS(1E-Class DCS) fast and reliably , we design a digital output channel to show ERR_STATE to 1E DCS.

3.1.8 Processor in PLM

There exist a FPGA and a CPLD in one PLM. We use Verilog HDL to complete the logic and there is no Integrated IP Core in FPGA(Every line of the code can be tested).

The functions of FPGA are described as follows:

- Profibus-DP Slave station can receive command from NC DCS. The protocol is accorded with IEC61784-3 to ensure safe communication.
- Configuration information in EEPROM(Save configuration information).
- Communication with Management Module through M-BUS(Complete configuration function).

- Control LED in front panel.

The functions of CPLD are as follows:

- Receive dual command signals from DCS(SFOFF1、SFON1、SFOFF2、SFON2、SFOFF3、SFON3、SFOFF4、SFON4) and do priority logic function(see Chapter3.2).
- Output dual priority command to field actuator.
- Acquire feedback signals from actuator.
- Control the lights in BUP(Backup Panel).
- Complete Periodic TEST(see Chapter3.3)

In order to eliminate the influence between CPLD and FPGA, we design a dual port ram to complete the communication work between them.

3.2 Priority Output

To deal with several level commands from DCS (1EDCS,ECP,DAS,NC DCS), we design a priority logic function in CPLD, which is determined by the safety level of different DCS. The priority logic is shown as follows.

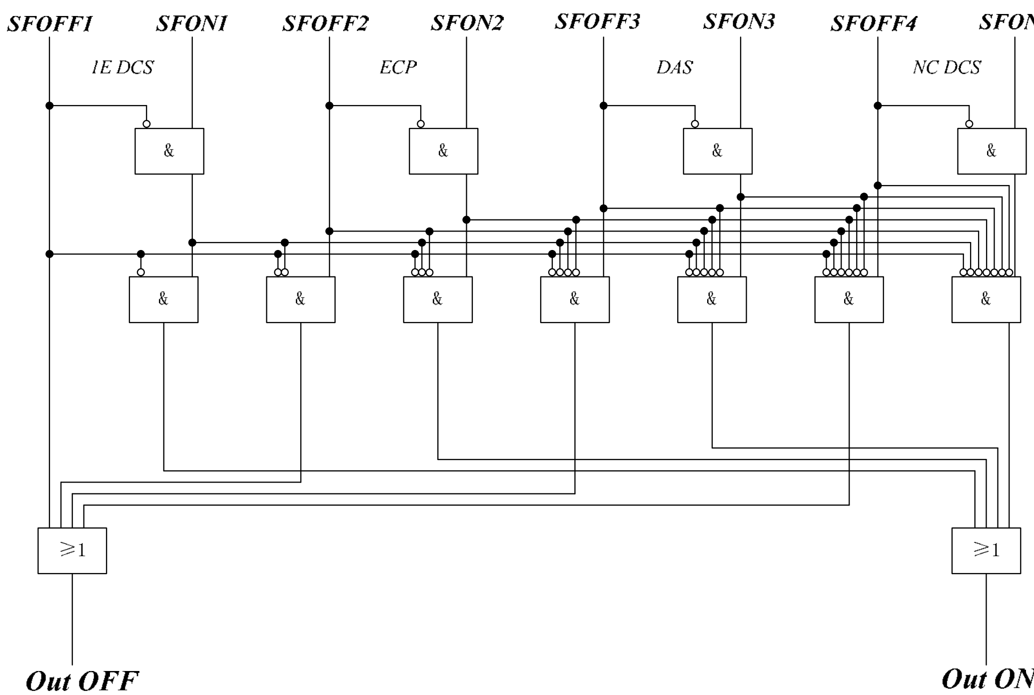

Figure 6. Priority Logic in CPLD

We use synchronization logic in CPLD. Every input and output signal in logic gate has a trigger by use of the same clock, which guarantees that every signal changes synchronously.

When PLM is in Normal Mode, the command from 1E DCS(1E-Class DCS) has the highest priority among all the DCSs ("OFF" has a higher priority than "ON"). For instance, when SFOFF1 = 1, no matter other input changes, Out OFF = 1 Out ON = 1 means that the controlled field actuator should be closed.

3.3 Periodic TEST

In the period of nuclear power operation, in order to ensure the availability of nuclear power control system (Each PLM can be tested independently), engineer can do periodical TEST. But the test signal cannot be sent to field actuator (the actuator should not act), so it should be locked.

So we design a MOSFET circuit as the digital output channel, which has a fast open and close time. When PLM is in periodical TEST mode, engineer provides a test signal through input channel (SFOFF1~SFON4), then CPLD in PLM will generate a short pulse to MOSFET circuit. The MOSFET will act for a short time, then the feedback circuit can detect the short pulse, which proves that the MOSFET is OK. Because the MOSFET act time is very short, field actuator will not act.

As is shown in Fig.7, we choose SFOFF1 channel as an example. Several steps are required to complete the Periodic TEST:

- Engineer use S-VDU(Safety-Visual Display Unit) to control 1E DCS generates Test_Enable1. Then in PLS field engineer will see the Test_Enable1 through LED in front of PLM, he will generates Test_Enable1 from local. So PLM will output MODE to 1E DCS to indicate PLM is in periodic TEST mode.(This method can decrease the possibility of misoperation)

  Meanwhile the ① and ② will break, ④ and ② will connect.(In Normal mode,① and② connect, ④ and ② break).

  So in Periodic TEST mode, PLM can still respond the command from NC DCS.

- The MODE signal will be transmitted from 1E DCS to S-VDU. Thus, engineer realizes that the corresponding PLM is ready for Periodic TEST.
- Then engineer will use S-VDU to control 1E DCS makes SFOFF1 enable.
- When PLM receives SOFOFF1, the Priority Logic will output OUT_OFF.
- And then ② will generate a short pulse to MOSFET. After MOSFET act for a short time, the Pulse Detect Circuit will detect the signal and outputs Test_PulseA.
- At last, PLM will output Test_OutputA enable to 1E DCS to indicate the SFOFF1 channel is OK.
- When the engineer knows the message from S-VDU, he will know SFOFF1 channel is OK and disable SFOFF1(then he can do next channel test).

  When all the channels are tested, engineer will disable Test_Enable1 and puts PLM into Normal mode.

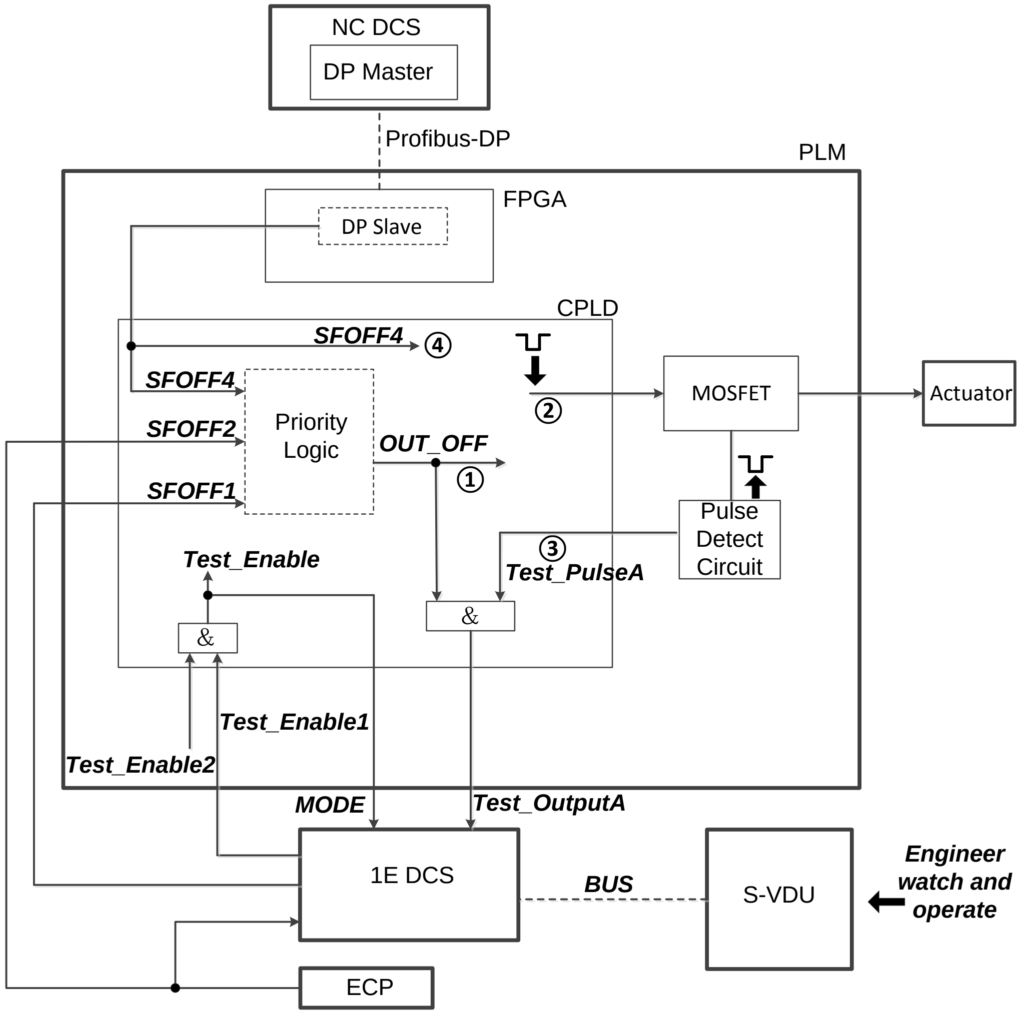

Figure 7. Periodical TEST

4 CONCLUSIONS

Nowadays, the Priority Selection Station designed by us is successfully applied to Reactor Protection System, which achieves fast response time and high realiability. By means of the FPGA/CPLD technology, not only the code can be identified line by line by the V&V team, but also avoiding Common Cause Failure from other DCS by use of microprocessor technology.

5 REFERENCES

1. WEI Zhi-kang, LIANG Jia-lin, “Analysis of advantage and limitation of FPGA technology in nuclear power plant” , Instrumentation Customer, **Vol. 6**,pp90-93 (2013).
2. J.Naser, “Guidelines on the Use of Field Programmable Gate Arrays(FPGAs)in Nuclear Power Plant I&C Systems” **TR-1019181 EPRI**,pp41-59(2009).
3. Chen Yinjie, Zhang Chunlei Qi Min, “Research on the Application of FPGA in Diversity System of Nuclear Power Plants”, Process Automation Instrumentation , **Vol.35(2)**, pp46-49(2014).

4. Liu Zhen, Jiang Guojin, Sun Yongbin"The V&V activities and techniques for safety-class I&C system in the nuclear power plant", Chinese Journal of Nuclear Science and Engineering, **Vol.31**,pp45-50(2011).
5. Luo Pan, "The System Design and Implement between Safety and non-Safety Communication Gateway in Nuclear Power Plant" , Electronic Component & Device Applications, **Vol.9**, pp35-37(2011).