IOP Conference Series: Earth and
Environmental Science

PAPER • OPEN ACCESS

Research on Improvement of FQNPP Reactor Protection System Hardware Logic Design

To cite this article: LI Xun-Cun *et al* 2020 *IOP Conf. Ser.: Earth Environ. Sci.* **512** 012180

Research on Improvement of FQNPP Reactor Protection System Hardware Logic Design

LI Xun-Cun[*], Yang Ru-Zhen, Gong Cheng-Jun

Fujian Fuqing Nuclear Power CO.LTD, Fuqing, Fujian 350318, China

lixc@cnnp.com.cn, yangrz@cnnp.com.cn, gongcj@cnnp.com.cn

Abstract. Fuqing Nuclear Power Plant Reactor Protection System has designed emergency control panel ECP, which is used to deal with the risk of loss of digital automatic protection functions due to common software failure. ECP is designed and implemented by analogy technology, which can bypass the computerized DCS system and use buttons, indicator lights, relays and other devices to achieve system-level protection functions. In practical engineering applications, it is found that the current ECP can not meet the requirements of post-accident control in some specific circumstances. Through the analysis of system design and accident management procedures, two design improvements are listed, compared and analysed, and the optimal improvement is given in this paper.

1. Introduction

The Reactor Protection System is an important safety system for nuclear power plants. It mainly monitors important parameters related to reactor safety [1]. When these parameters reach the setting values determined by the safety analysis, emergency shutdowns are automatically triggered and necessary special safety facilities are activated to limit the development of the accident and mitigate the consequences of the accident, ensure the safety of reactors and nuclear power plant equipment and personnel, and prevent the release of radioactive materials to the surrounding environment [2].

Fuqing Nuclear Power Plant Reactor Protection System is designed and implemented with digital 1E level DCS platform (Tricon). Compared with simulation technology, digital technology has great advantages in improving the availability, reliability, maintainability, economy, and flexibility of nuclear power plants [3]. However, DCS is a software-based system. To avoid software's CCF (common cause failure), deterministic and / or CCF risk assessment combined with probabilistic safety analysis (PSA) are used to implement system diversity, application software diversity, or functional diversity. Therefore, diversified solutions are generally used in the design of reactor protection systems, including diversified equipment and diversified functions [4]. The design of the emergency control panel (hereinafter referred to as ECP) is an embodiment of equipment diversification [5]. As the backup of digital automatic protection function, ECP uses conventional control methods to design and bypass the entire computerized DCS system. When the function of the digital reactor protection system is lost due to software common mode failure and other reasons, the operator can use the emergency start button on the ECP Implement manual shutdown or start ESF system level commands.

As the last protection method after the digital protection system fails completely, ECP needs to be fully analysed and evaluated during the design. While ensuring that the protection functions required by probabilistic safety analysis are met, the negative effect on unit control caused by improper design should be avoided.

2. ECP system structure

The overall design principle of Fuqing Nuclear Power ECP is: The ECP manual control command is divided into two ways and sent to the shutdown breaker or safety-specific drive mechanism, in which one way is passed through the relay logic through the hardware line, and the other is sent to the digital protection system based on the TRICON platform. The two signals are sent to the shutdown circuit breaker and the optimized logic module at the same time. The ECP system structure is shown in Figure 1:

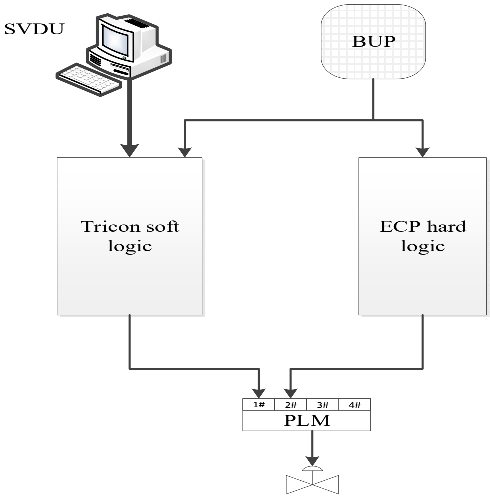

Figure 1 ECP system structure diagram

Taking the safety injection function as an example, the design and implementation of the ECP logic function are explained as follows:

1) The safety injection start command button located on the ECP sends the safety instructions to the relay logic through hard wiring all the way to the digital protection system software logic. After the two signals are processed by logical operations, the device action commands are sent separately. Enter the preferred logic module PLM corresponding to the device, and output after logic optimization.

2) The safety reset command on the safety level display unit SVDU is sent to the TRICON software to reset the safety logic in the software. At the same time, the reset command generated is sent to the ECP relay logic through hard wiring to reset the relay logic.

3) The Anchor reset command button on the backup disk BUP is also sent to the Tricon software and ECP relay logic to reset the two Anchor memory logic. The two reset operations can be used as backups for each other.

The design characteristics of ECP relay logic are mainly reflected in the following aspects:

1) The ECP relay logic is completely independent on the TRICON soft logic except that it accepts the reset command of the protective action instruction from the TRICON soft logic. After the TRICON system fails, the protection action instruction in the ECP hard logic can also be reset directly from the backup disk BUP.

2) The protection action command from ECP hard logic is connected to the 2 # input port of PLM, and the protection action command from TRICON soft logic is connected to the 1 # input port of PLM. When the two commands conflict, the protection action command from TRICON soft logic has high priority. ECP hard logic, as a diversified protection method of TRICON soft logic, is implemented with relay circuits.

3) The ECP hard logic and the diversified protection system DAS system provide diversified protection means when the TRICON soft logic cannot issue a safe action due to a fault.

3. Analysis and Research on ECP Hard Logic Design Problems

3.1. RIS132VP valve opens by mistake during direct injection recirculation

When the Tricon soft logic and ECP are normal, if an accident that requires the activation of the safety injection function occurs, according to the accident procedure, the operator is required to press RPA058TO to start the safety injection. According to the current design of the reactor protection system, the manual injection start command will act on the Tricon system software logic and ECP hard logic at the same time. As the injection continues and the low-pressure injection flow changes, the RIS132VP action command will occur. The following changes:

1) When in the direct injection phase, when the low-pressure injection flow is lower than 300 m3/h, the RIS132VP opening instruction is sent, which is consistent with the ECP hard logic instruction;

2) When in the direct injection phase, when the low-pressure injection flow is higher than 300 m3/h， the RIS132VP shutdown instruction is sent. Although this is not consistent with the ECP hard logic instruction, its priority is higher than the ECP hard logic instruction, RIS132VP still works correctly;

3) When in the PTR isolation and subsequent safety injection recirculation stage, when the low-pressure safety injection flow is less than 300 m3/h， Tricon soft logic will send a shutdown command to RIS132VP, which is inconsistent with the ECP hard logic command, but its priority RIS132VP can still operate correctly if the instruction is higher than the ECP hard logic;

When it is in the stage of PTR isolation and safety injection recycling after that, the safety injection flow at low pressure is higher than 300 m3/h, the closing instruction of cancelling TRICON software logic is sent to RIS132VP, but since the instruction of opening RIS132VP in ECP hardware logic has been existed all the time, RIS132VP will be opened through two input ports of PLM module, and since the ECP instruction takes precedence over RIS132VP manual closing instruction on KIC in main control room, operators in main control room cannot manually close RIS132VP from KIC according to the procedure.

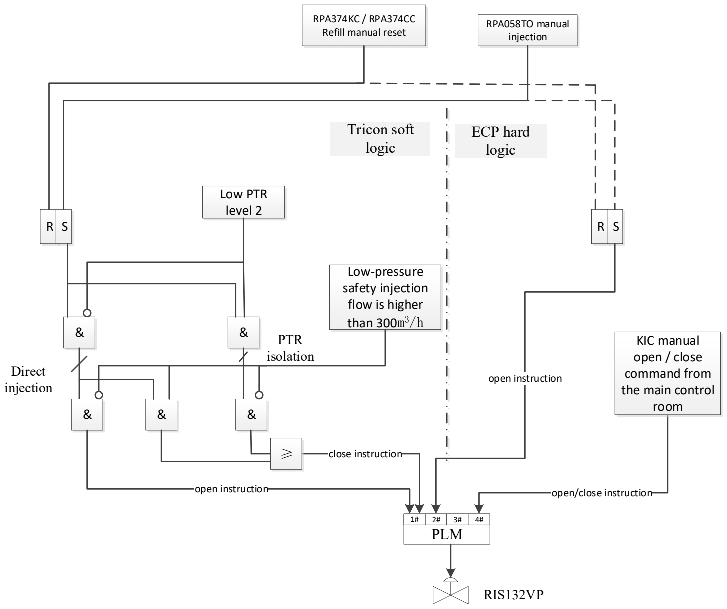

Figure 2 RIS132VP logic diagram

Table 1 RIS132VP operation under different conditions

Working condition	Tricon soft logic command	ECP hard logic command	RIS132VP expected action	RIS132VP actual action
Direct injection + low pressure injection with a flow rate below 300 m^3/h	open	open	open	open
Direct injection + low pressure injection with a flow rate above 300 m^3/h	close	open	close	close
Safety injection recirculation + low pressure safety injection flow below 300 m^3/h	close	open	close	close
Safety injection recirculation + low pressure safety injection flow above 300 m^3/h	close → command disappears	open	close	open

From the above analysis, it can be known that 4）will cause the RIS132VP to open by mistake.

Based on the above analysis, the problem is shown as follows: when the logic of TRICON software and ECP are normal, if there is an accident that needs to start the safety injection function, when it is in the PTR isolation and the subsequent safety injection recycling stage and the low-pressure safety injection flow is higher than 300 m3/h, RIS132VP will malfunction.

3.2. RIS132VP cannot be operated manually after Tricon system failure

According to the current design, the instructions to opening the RIS132VP in the ECP hard logic are issued after the safety injection recirculation memory. When the Tricon software logic fails to properly control the RIS132VP due to a failure, the direct safety injection instructions in the ECP cannot be used to control the RIS132VP. The reason is as follows.

When in the direct injection phase, when the low-pressure injection flow is higher than 300 m3/h, the RIS132VP needs to be closed, but this logic is not set in the ECP hard logic. In the ECP hard logic, there is only the continuous RIS132VP open instruction. The priority is higher than the RIS132VP shutdown command on the KIC. Therefore, the operator in the main control room cannot shut down the RIS132VP from the KIC when the outlet flow of the low-pressure safety injection pump is higher than 300 m3/h.

3.3. The Tricon system cannot be manually recirculated after a failure

Taking safety injection as an example, if a safety accident occurs when a system operation accident that requires safety injection occurs, and a common action of the Tricon software cannot be issued (Tricon software common mode failure may have occurred, but because it cannot be detected, The Tricon function can be restored in time.) The Tricon software logic of columns A and B will fail. At this time, it is necessary to rely on the diversified protection system DAS system and ECP to manually activate the injection function. However, neither the DAS system nor the ECP hard logic is provided with PTR isolation and safety injection recirculation functions (at the beginning of the design, it takes a long time to consider the safety trigger to transition to PTR isolation, and the transition process can be manually completed by the operator). After the direct injection phase, the operator needs to manually bring the injection into the recirculation.

However, as described in question 3.1, because the manual injection instruction in the ECP hard logic is memorized by the recirculation memory, according to the existing accident procedures, the recirculation memory can only be reset after it has been confirmed to switch to the injection recirculation. Therefore, before manually switching to safe injection recirculation, ECP hard logic will always send control instructions to the relevant valves, such as the "ECP control command" in Table 2. When it is necessary to switch to safe injection recirculation, these valve drivers should Operate according to the "Control command during recirculation" in Table 2.

Table 2 Valve operation before and after recirculation switching

valve	ECP control commands	Control command during recycling
RIS012VP	open	close
RIS167VP	close	adjust according to the injection flow
RIS132VP	open	close
RIS144VP	open	close
RIS075VB	open	close
RIS051VP	close	open

However, at this time, the Tricon system is unable to issue a control instruction due to a failure, and the control instructions that have not been reset in the ECP hard logic take precedence over the control instructions of the above valves on KIC and BUP, resulting in the operator not being able to manually inject the safety instructions from KIC or BUP Transfer to recycle. This problem also exists for safety jet recycling.

4. ECP hard logic design improvement scheme

4.1. Simplify ECP hard logic design

ECP hard logic is a design measure against common cause failures of Tricon software (including hardware that allows the software to run). It only exists as a backup for automatic protection. Therefore, it can be considered as a part of a diverse protection system. For the following reasons:

1) Because all manual safety level trigger instructions on the ECP are designed with two paths, in which one path is directly sent to Tricon software and automatic instructions for OR operation and then sent out, and the other path is sent to the ECP hard logic in order to It can provide a variety of manual accident mitigation methods when an accident occurs and the fault of the Tricon soft logic circuit is superimposed.

2) When an accident occurs and the fault of the Tricon system is superimposed, the design of the ECP hard logic should provide the necessary safety action start function on the one hand, and on the other hand, it should not deal with the manual intervention that the plant operator may implement according to the operating procedures during the accident handling Cause negative effects;

3) The purpose of setting the injection and injection recirculation memory is to ensure that when the PTR water level is low 2 and the PTR water level is low 3, the PTR can be isolated or the injection/safety injection is brought into the recirculation. However, in fact, the PTR isolation and the injection / safety recirculation logic are not implemented in the ECP hard logic. Therefore, setting the injection/safety recirculation memory in the ECP hard logic has no substantial meaning.

Taking logic series A as an example, for the direct injection signal in ECP hard logic, the simplified scheme of ECP hard logic is as follows: Retain the refill memory in the ECP hard logic. Because the switchgear corresponding to the relevant electric valve has a holding function, other than RCV033VP and RCV376VP, the opening or closing instructions of the electric valve related to direct injection are directly connected to the manual injection button RPA058TO. After that, not only the control command after the hold can be sent to the valve through the TRICON soft logic (in the case of the Tricon system without failure). And, as a backup of diversity, short-level control commands will also be sent to the electrical switchgear through ECP hard logic (in the event of a fault in the Tricon system, these commands are memorized by the electrical switchgear). Since this command is a short-level type, other subsequent safety-related operations performed from the KIC can be implemented.

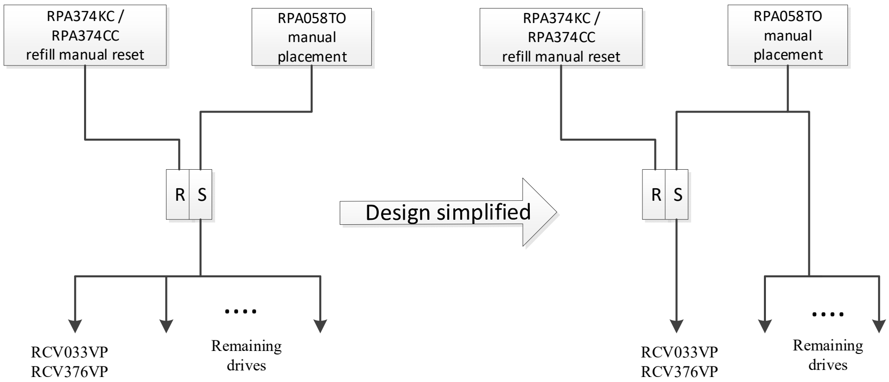
RPA374KC / RPA374CC refill manual reset
RPA058TO manual placement
R
S
Design simplified
RCV033VP
RCV376VP
....
Remaining drives
RPA374KC / RPA374CC refill manual reset
RPA058TO manual placement
R
S
RCV033VP
RCV376VP
....
Remaining drives

Figure 3 ECP safety injection recycling hard logic simplified scheme

For the direct injection signal in ECP hard logic, the modification scheme is as follows: Cancel the safe recirculation memory in the ECP hard logic. Directly connect the opening and closing instructions of the electric valve related to direct injection to the manual injection buttons RPA285TO and 286TO. After the RPA285TO and 286TO are pressed, not only can the Tricon soft logic send the remaining control instructions to the valve in the case that the Tricon system has no faults), and as a diverse backup, it will also send short-level control commands to the electrical switch cabinet through ECP hard logic (in the case of a fault in the Tricon system, these commands are provided by Electrical switch cabinet for memory). Because this command is a short-level type, other subsequent security-related operations performed from the KIC can be implemented.

With the above modifications, whether the Tricon system is normal or fails to send out a safe action signal, the instructions in the ECP hard logic will not affect the possibility of manual intervention by the operator from KIC and BUP.

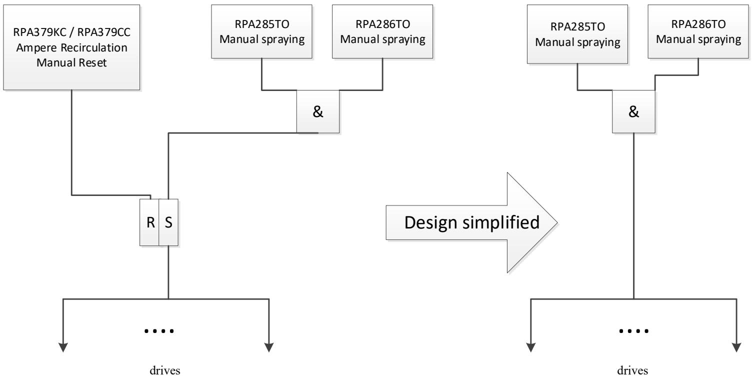

Figure 4 Simplified scheme of ECP safety jet recirculation hard logic

4.2. Add PTR water level signal and low-pressure safety injection pump flow signal

According to the analysis in Chapter 3, the root of problems 3.1-3.3 is that the PTR isolation function is not considered in the ECP design. Therefore, by introducing the PTR water level signal and the low-pressure safety injection pump flow signal into the ECP hard logic, the same PTR isolation, safety injection, and safety injection recirculation functions as Tricon soft logic can be achieved. To prevent the ECP from receiving signals from the Tricon soft logic and being affected by the Tricon common cause failure, the following solutions can be adopted to implement the signal introduction.

The PTR water level simulation signal and the low-pressure safety injection pump flow simulation signal are imported from the Tricon cabinet into the ECP hard logic through the simulation isolation distributor. After setting the threshold comparison relay in the ECP hard logic, the corresponding PTR low water level 2 signal. After the high-pressure signal of the low-pressure safety injection pump is interlocked with the direct safety injection and safety injection logic in the ECP.

5. Conclusion

Through in-depth analysis of the ECP hard logic, combined with the requirements of the unit state control after the accident, the existing problems of the existing ECP hard logic design were simulated and studied in detail. After analysis, the existing ECP hard logic cannot meet the unit control requirements under certain specific operating conditions. From the perspective of ECP design, this paper proposes two design improvement schemes, and conducts a comparative analysis from the aspects of scheme complexity, impact scope, reconstruction project volume, and economy. Based on the comprehensive analysis results, the scheme that simplifies the ECP hard logic is the optimal scheme.

Acknowledgments:

The study is supported by the Nuclear Power Institute of China and FuQing Nuclear Power Plant.

References

[1] Yu Bing, Gong Chengjun, Li Suncun. Optimization of T2 test scheme for reactor protection system of Fuqing nuclear power plant [J]. China nuclear power, 2016,9 (3): 267-266

[2] Yang Ruzhen, Wang Wumei. Regular test scheme and feasibility analysis of digital protection system in Fuqing nuclear power plant [J]. Automation Expo, 2012,08:54-57

[3] Su Junhai, Yang Meng, Li Ying. Diversity analysis of safety level DCS Based on TRICON platform [J]. Instrument users, 2019,04:25-27

[4] JUNBEOM YOO, JONG-HOON LEE, & JANG-SOO LEE. . A research on seamless platform change of reactor protection system from plc to fpga. Nuclear Engineering & Technology, 45(4), 477-488.

[5] Cong Cui, Duo Li, Chao Guo. A preliminary research on software reliability model of Reactor Protection System of High Temperature Gas-Cooled Reactor-Pebble bed Module[C]// 2015 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD). IEEE, 2015.