Study on Reliability Improvement of Main Steam Isolation Valve Control in Nuclear Power Plants

Changxian Gan1*, Tian Wan2, Weiwei Pan3, Shengzhi Liu4, Lei Tang5, Huahuan Li6

1 Suzhou Nuclear Power Research Institute Co., Ltd., Shenzhen, Guangdong Province, 518000, China
2 Suzhou Nuclear Power Research Institute Co., Ltd., Shenzhen, Guangdong Province, 518000, China
3 Suzhou Nuclear Power Research Institute Co., Ltd., Shenzhen, Guangdong Province, 518000, China
4 Suzhou Nuclear Power Research Institute Co., Ltd., Shenzhen, Guangdong Province, 518000, China
5 Suzhou Nuclear Power Research Institute Co., Ltd., Shenzhen, Guangdong Province, 518000, China
6 Suzhou Nuclear Power Research Institute Co., Ltd., Shenzhen, Guangdong Province, 518000, China

*Corresponding author’s e-mail: Ganchangxian@cgnpc.com.cn

Abstract. There is a safety hazard in the interlock control logic of the second circuit main steam isolation valves of the CPR1000 nuclear power unit. During reactor power operation, any abnormal full-close limit switch signal of valves may lead to a reactor shutdown event or even a Safety Injection of nuclear reactor. In this Paper, the control strategy of the second circuit main steam isolation valves is analyzed and demonstrated, and after Probabilistic Safety Assessment (PSA), a feasible improvement plan is proposed, which effectively improves the control reliability of the second circuit system in nuclear power plants.

1. Introduction

The CPR1000 nuclear power unit has three evaporators, each of which has a main steam isolation valve (VVP001/002/003VV) on the corresponding second circuit. The main steam isolation valve (hereinafter referred to as MSIV) is a critical safety level device for nuclear power plant. Its primary functions are (1) after a steam line or feed line rupture at any location, the MSIV can cut off steam flow in any direction within 5s to maintain reactor coolant temperature and containment pressure within acceptable limits; (2) when the reactor is in thermal shutdown, the system is isolated to facilitate downstream servicing; and (3) the MSIV and its upstream piping are a natural extension of the containment and act as third barrier [1].
The control strategy of the MSIV of the CPR1000 unit is the same, and the control strategy has safety hazard, which can lead to unexpected closing or unintended opening of the MSIV after closing under certain conditions, affecting the safe operation of the unit.

Incident 1: During the commissioning of the 50%Pn power platform in Unit 2 of a nuclear power plant, the on-site VVP001VV full-close limit switch (hereinafter referred to as SM5) was mistakenly touched, triggering the valve to close, resulting in a decrease in steam flow, increase in pressure and decrease in water level in steam generator No.1, triggering the automatic reactor shutdown protection signal of low water level superimposed on steam-water mismatch, leading a reactor shutdown event. 

(Problem 1: When the valve is fully open, if SM5 is touched by mistake, it will trigger the valve to close and cause the reactor shutdown.)

Event 2: After the reset of VVP001/002TO button in the Emergency Control of Panel (hereinafter referred to as ECP) of Unit 4 of a nuclear power plant, the warming operation was carried out and VVP003VV was suddenly opened unexpectedly, causing the pressure of No.3 steam generator to drop rapidly to a minimum of 59.22 Bar, with a pressure difference of 6.77 Bar from No.1 steam generator, which is only 0.23 Bar away from the high pressure difference trigger ampere destined value (7 Bar). At the same time, the water level of No.3 steam generator fluctuated to -1.107m, which was only 0.15m away from the jumping water level; the lowest temperature of the first circuit reached 277.36℃, and triggered the P12 signal of the average temperature of the first circuit. (Problem 2: After the ECP button was reset, the valve opened unintentionally and the first circuit parameters fluctuated significantly)

2. Cause Analysis
Currently, the MSIV control logic is shown in Figure 1, and the control signals mainly contain.

(1) Safety level signals to perform safety functions: the main steam isolation signal (SLI) for column A/B generated by the Reactor Protection System (RPR system) and the fast-shutdown signal for column A/B of ECP panel VVP001/002TO. [2]

(2) Normal valve operation signal: the open and close signal of manual KIC (DCS operation interface) or BUP (Backup of Panel).

(3) Swing arm full-close limit switch signal SM5. SM5 full-close position signal is "1"(TURE), not in the full-close position is "0"(FALSE). There are two functions:

①SM5 is used to prevent the short command from opening the valve by mistake, and to lock the open valve self-holding command. Therefore, when the valve is opening from the full-closed position, you need to press and hold the valve open button (about 20 seconds) until the valve leaves the fully closed position, and the SM5 signal turns to '0'. The valve opening command can be maintained. It can reduce the possibility of the operator accidentally opening the valve from the perspective of preventing human factors.

②The opening command can be reset when the valve is closed to avoid unexpected automatic reopening after the valve is closed. For example, after quickly closing the valve through the button VVP001ITO in column A of the ECP, the valve opening self-holding command can be reset through the SM5 signal.

In addition, if there isn’t close command but the valve is closed due to equipment failure (e.g. oil leakage, air pump failure, etc.), the valve open self-holding command can also be reset through the SM5 signal.

In event 1, the valve is in the fully open position due to the presence of the open self-holding command.SM5 is mistakenly touched will reset the open self-holding command, causing the valve to close, resulting in a reactor shutdown. In event 2,If SM5 is not triggered after fast-shutdown the valve via the ECP button, the open self-hold command is not reset and when the ECP fast-shutdown button is reset, the MSIV will open unintended.

In addition to events 1&2, a nuclear power plant has also experienced an internal failure of SM5 resulting in valve closed and shutdown of the reactor. At the same time, there is also a risk that the SM5 signal is mistakenly touched to jump the reactor when the MSIV online maintenance limit
switches and other sensors. In summary, the design of the MSIV control logic has the risk of a single failure of the SM5, which is a safety hazard and needs to be studied for reliability improvement.

Figure 1 Main steam isolation valve control logic

3. Improvement schemes

3.1 Scheme 1: Add RS flip-flop to original logic (R-side first)

SM3 is the MSIV full-open limit switch, the introduction of "SM3 non-" participation logic, SM3 non- and SM5 to take “and” logic characterize the valve in the full-close position; through the RS flip-flop to achieve the open command set hold and reset[3]. At the same time, the introduction of the ECP fast-shutdown signal to the R terminal to reset the open self-holding command (see Figure 2 for details). SM3 non- plays an auxiliary role to confirm the valve position and prevent false action. SM3 non- and SM5 set 5s before the delay time is to prevent the valve from partially closing the test or limit switch online maintenance, accidentally touching another limit switch to close the valve.

Figure 2 Improvement scheme 1 - Add RS trigger logic schematic
The improvement solves the safety hazard in events 1&2 without changing the original control function. When MSIV is opening from full-close position, press and hold the valve open button to open the valve; when the valve leaves the full-close position, the SM5 signal changes from "1" to "0", the RS trigger S terminal is set to 1 and the R terminal is "0". When the open valve button is released, the S terminal changes to "0" and the output maintains the open command of the previous cycle until there is a reset signal. After the valve is fully open, if SM5 is touched by mistake, the state of valve will unchanged (solve problem 1). When the ECP VVP001/002TO button is pressed, while MSIV is fast shutdown, the R terminal is 1 reset and open the self-holding command (solve problem 2).

Summarizing the input conditions in Figure 2 into 6, there are 64 kind of combinations. The exhaustive method is used to compare the output results before and after the improvement of all working conditions [4]. The truth table is shown in Figure 3 below (① manual open command, ② SM5 non-, ③ SM5&SM3 non-, ④ manual close command, ⑤ RPR close command, ⑥ ECP close command, ⑧ Final valve command). The final results show that among 64 combinations of states, 62 combinations remain unchanged, 2 combinations have differences before and after improvement, and the differences show that the results are better than before, solving problems 1&2. Combination 1 is improved to solve the problem of valve closing caused by SM5 mistaken touch. The output valve command of combination 17 corresponds to three working conditions: ① The valve is fully open; ② The valve fails to close under irrelevant commands and SM5 does not trigger the working condition (open self-holding do not reset); ③ The valve is closed by ECP but SM5 is not triggered, the working condition at the time when ECP is reset. Working conditions ① and ② after the model is improved, the result is the same as the result before the improvement, and the valve opening command still exists. Working condition ③, after the improvement, the R terminal will reset the self-holding command, and the valve will not open unexpectedly. Therefore it solves problem 2.

| Combination | S side: ① AND ② | R side: ③ OR ④ OR ⑤ OR ⑥ | Before improve ⑦ | After improve ⑧ | Comparison of results | Better after improvement, solve problem 1 | Better after improvement, solve problem 2 |
|-------------|------------------|------------------|------------------|------------------|------------------|---------------------------------|---------------------------------|
| 1           | 0                | 0                | 0                | 0                | 0                | Qn-1                            | 1 | 0                           |
| 2           | 0                | 0                | 0                | 0                | 0                | Unchanged                       | 1 | 0                           |
| 3           | 0                | 0                | 0                | 0                | 0                | Unchanged                       | 0 | 0                           |
| 4           | 0                | 0                | 0                | 0                | 1                | Unchanged                       | 0 | 1                           |
| 5           | 0                | 0                | 0                | 1                | 0                | Unchanged                       | 0 | 1                           |
| 6           | 0                | 0                | 0                | 1                | 0                | Unchanged                       | 0 | 1                           |
| 7           | 0                | 0                | 0                | 1                | 1                | Unchanged                       | 0 | 1                           |
| 8           | 0                | 0                | 0                | 1                | 1                | Unchanged                       | 0 | 1                           |
| 9           | 0                | 0                | 1                | 0                | 0                | Unchanged                       | 0 | 1                           |
| 10          | 0                | 0                | 1                | 0                | 0                | Unchanged                       | 0 | 1                           |
| 11          | 0                | 0                | 1                | 0                | 0                | Unchanged                       | 0 | 1                           |
| 12          | 0                | 0                | 1                | 0                | 0                | Unchanged                       | 0 | 1                           |
| 13          | 0                | 0                | 1                | 0                | 0                | Unchanged                       | 0 | 1                           |
| 14          | 0                | 0                | 1                | 0                | 0                | Unchanged                       | 0 | 1                           |
| 15          | 0                | 0                | 1                | 0                | 0                | Unchanged                       | 0 | 1                           |
| 16          | 0                | 0                | 1                | 0                | 1                | Unchanged                       | 0 | 1                           |
| 17          | 0                | 1                | 0                | 0                | 0                | Unchanged                       | 1 | 1                           |
| 18          | 0                | 1                | 0                | 0                | 0                | Unchanged                       | 1 | 1                           |
| 19          | 0                | 1                | 0                | 0                | 0                | Unchanged                       | 1 | 1                           |
| 20          | 0                | 1                | 0                | 0                | 0                | Unchanged                       | 1 | 1                           |
| 21          | 0                | 1                | 0                | 0                | 0                | Unchanged                       | 1 | 1                           |
| 22          | 0                | 1                | 0                | 0                | 0                | Unchanged                       | 1 | 1                           |
| 23          | 0                | 1                | 0                | 0                | 0                | Unchanged                       | 1 | 1                           |
| 24          | 0                | 1                | 0                | 0                | 0                | Unchanged                       | 1 | 1                           |

Figure 3 Improvement scheme 1——truth table diagram

Remark: 1) When the output ⑧ is "1" (TRUE), the valve will open; when the output ⑧ is "0" (FALSE), the valve will close. 2) Qn-1 means the state value of the previous moment. 3) After improved, it is impossible for both ② and ③ to be "1" at the same time, therefore no need to compare from state combinations 25~32, 57~64.
3.2 Improvement Scheme 2: Non-RS Trigger Scheme

Added "SM3 non-" logic (SM3 is the valve full-open limit switch, "SM3 non-" means the valve is not in the fully open position), SM3 non- and SM5 are set 5s before the time delay, both take "AND" logic to replace the original SM5, and the introduction of the ECP fast-shutdown signal to reset the self-holding circuit open command (see Figure 4 for details).

The improvement solves the safety hazards in events 1&2 without changing the original control function. When MSIV is opening from the closed position, press and hold the valve open button to open the valve. And when the valve leaves the fully closed position, the SM5 signal changes from 1 to 0 and the open command self-hold circuit takes effect. At this time, the open valve button can be released, the valve opens and remains fully open under the action of open self-holding command. After the valve is fully open, if SM5 is touched by mistake, the valve state will not change (problem solving 1). When the ECP button triggers the fast-shutdown signal, the MSIV fast-shutdown while the newly introduced ECP signal will reset the open self-holding command (problem solving 2). A comparison of 64 state combination truth table is performed in the same way as the improved scheme 1, and scheme 2 has the same results as scheme 1.

Figure 4 Improvement Scheme 2 - Non-RS Trigger Scheme

3.3 Risk analysis of two improvement schemes

After the improvement, on the basis of not changing the original control function, the hidden safety hazard in incident 1&2 is solved. And greatly reduces the probability of false activation. The improvement schemes have a small increase in the probability of rejection over the original design. PSA is carried out by establishing a model. According to the analysis results, the possibility is negligible, and has controllable measures. The specific analysis is as follows 3.3.2.

3.3.1 Probability Safety Assessment

Probability Safety Assessment (PSA) is a method used in the operation of complex process systems to determine the frequency and consequences of a set of potential accidents. It consists of a set of logical models that determine the undesired consequences of plant functions, systems, component states, and human-caused failure events following an initiating event. Probabilistic safety analysis integrates all aspects of plant design and operation, logically incorporating various correlations such as equipment co-factor failures, support system failures, operational and personnel correlations, and spatial and
physical phenomenon correlations. A probabilistic safety analysis was performed for this improvement, and the specific analysis process is not detailed here [5].

### 3.3.2 Risk analysis and countermeasures

In terms of design risk, the two improvement schemes both have the risk of “the valve is closed by failure and the open command is not reset” in the combined 17 working condition ② described in section 3.1. After the improvement, the introduction of the "SM3 non-" signal assists in judging that the valve is closed, so the probability of occurrence of this risk is greater than before the improvement. PSA is carried out by establishing a model. According to the analysis results, the possibility of such mechanical failure and malfunction of the valve is extremely low (2.51E-07). It is calculated that the probability of occurrence of this risk before the improvement of working condition ② is 2.76E-11, and after the improvement is 5.52E-11, which is much lower than the probability of functional failure caused by the failure of the valve equipment itself (level E-04). At the same time, through the PSA, it is concluded that the influence and contribution of the control signal of the improvement plan to the overall plant-wide safety target stack melting probability CDF is almost negligible. When the valve close by self-fault(hydraulic oil circuit leakage, starting pump failure, etc.), it will generate low oil pressure alarm and other alarms to indicate that the valve is abnormal, at this time the operator can be manually reset the open self-hold command and perform related isolation operations for immediate troubleshooting. Therefore, the risk is acceptable after the transformation [5].

The improvement scheme 1 completely retains the original design of SM5 anti-error opening function, and the improvement plan 2 has a certain weakening of the anti-error opening function. In scheme 2, if the SM3 fault makes signal "1" (for example, jam fault and do not reset), when the operator clicks the open button, the open self-holding signal is established immediately, and the valve will open directly (that is, click the open button, the valve will open directly). SM3 fault superimposed on human error operation will lead to a low probability of valve opening by mistake. If the improvement plan 2 is adopted, in order to reduce this kind of human error, an alarm of abnormal valve status feedback can be added to the DCS logic, and the limit switch should be checked when the alarm exists, and the valve can be opened after the status is confirmed [6].

In terms of implementation risk, both solutions require the introduction of signals that are already present in the original system and do not require changes to the safety level DCS hardware circuit, the amount of change is not significant and a complete functional re-qualification can be performed.

### 4. Conclusion

In this paper, two schemes for improving the reliability of the control logic of the second circuit main steam isolation valve (MSIV) of a CPR1000 nuclear power plant are studied. Through the demonstration and PSA quantitative analysis of the above two improvement schemes for various operating conditions, it is concluded that both improvement schemes are feasible and can solve the safety hazard of the current control strategy of MSIV, and Scheme 2 has been implemented in a nuclear power plant site, which has improved the reliability of the main feed water isolation valve control, the stability of the system and the safety status when the valve control is abnormal. In addition, the CPR1000 nuclear power unit equipped with the secondary circuit main feed water isolation valve also adopts the same control strategy as the main steam isolation valve, which also has the potential safety hazards described in this article. In the process of improving the reliability of the main steam isolation valve control strategy, has also conducted an in-depth study on the main feed water isolation valve control strategy. Schemes 1&2 are also applicable to the main feed water isolation valve (ARE043/044/045VL), which will not be described in detail in this paper.

### References

[1] Hu,W.S.(2019) Normal Problems and Countermeasures of the Main Steam Isolation Valve. China Nuclear Power,12:177-181.
[2] Li, Y.H. (2018) Design Of Inter Row Signal Transmission Function Of Main Steam Isolation Valve Actuator. Industrial & Science Tribune, 8:101-103.

[3] Zhou, J.Z. (2018) Eliminating X BLEED MAN CTL Maintenance Message of A320s Based on the Theory of RS FLIP-FLOP. AVIATION MAINTENANCE & ENGINEERING, 1:64-65.

[4] Cao, X.D. (2003) The Application Of Exhaustive Method In Determining The Parameters Of Dynamic Standard Target Devices. Opto-Electronic Engineering, 30:29-32.

[5] Liu, C.Y. (2010) Analysis On Modification Of Main Feed Water Isolation Measures Of CPR1000. Chinese Journal of Nuclear Science and Engineering, 30:224-233.

[6] Zhu, L.X. (2020) Risks and Coping Strategies of Initially Opening Main Steam Isolation Valves Before Criticality of Nuclear Power Unit. Electric Engineering, 6:44-46.