# Optimization measures to reduce the influence of double AP faults in DCS system of power plant

**Hou Yao**

China National Neuclear Corporation, Jiang Su Neuclear Power Corporation, Lian Yun Gang Of Jiang SU 222042, China

**Keywords:** DCS; TXP system; double AP fault; logic optimization

**Abstract:** In order to reduce or avoid the adverse impact of the DCS system in the normal operation of the nuclear power plant on the operating state of the unit in the case of double AP failure, in this paper, the control logic is sorted out according to the signal characteristics of the DCS system after double AP failure in TianWan nuclear power plant, and the corresponding optimization measures for different types of controlled equipment are formulated. After theoretical analysis and simulation, the optimized logic can effectively reduce the adverse impact of double AP faults on the unit operation state.

## 1. Introduction

The DCS (Distribute control system) of Tian Wan nuclear power plant Project Phase-1 (two sets in total) was divided into normal operation TXP(Teleperm-XP) system and safety instrument control TXS(Teleperm-XS) system. The TXP system was mainly used for the control and protection of most non-nuclear safety functional process equipment in the power station, and the TXS system was mainly used for the control and protection of nuclear safety functional equipment in power stations. In each unit there are totally 65 TXP system AP(Automation Processor, Used for logical operations and processing) cabinets, and each cabinet contains a pair of redundant AP. When the main AP fails, the TXP system will automatically switch to the slave AP to ensure the stable operation of the equipment controlled by the cabinet.

On December 13, 2015, the TXP system 2CRD11 (code of the cabinet) of unit 2 of Tian Wan nuclear power plant experienced double AP shutdown failure, which led to a large fluctuation in the level of the steam generator and triggered the shutdown protection action. In order to ensure all the equipment of the unit could maintain the pre-failure state after double AP failure, this paper would take this event as an example, with analysis of the failure consequences according to the signal characteristics after double AP failure and combing the control logic, to make corresponding optimization measures for the signal or logic that had an impact on the unit operation state.

## 2. Event introduction and cause analysis

### 2.1 Event introduction

On December 13, 2015, unit 2 of Tian Wan nuclear power plant was in full power operation. TXP cabinet 2CRD11 was shut down by double AP problem, resulting in the loss of display of all process parameters controlled by the cabinet. The liquid level of no.1 steam generator suddenly rose by 0.18m, and the corresponding feed water regulating valve began to fluctuate greatly, and the level of steam generator also fluctuated accordingly. no.1 steam generator level rise to rating above 0.3 m, triggered no.1 steam generator main water supply cut-off valve protection signal, then level began to drop, when the no.1 steam generator level reduced to less than rating of 0.5 m, the protection removed no. 1 main coolant pump, when the no.1 steam generator level continued to fall below rating of 0.65 m, triggering reactor shutdown protection signal, then the reactor the Shut

down and the unit shut down.

### 2.2 Cause analysis of liquid level fluctuation

The main regulating quantity of the evaporator level regulator was the level signal, the difference between the main steam and the main feed water flow signal was the feed forward quantity of the regulator, and the vapor pressure at the evaporator outlet was the correction quantity of the level to realize the correctness of the level measurement under different operating conditions.

Failure to halt the TXP cabinet CRD11 contained in No.1 steam generator level correction of the main steam pressure signal, when double AP fault occurred, the main steam pressure which participate in liquid level correction changed from 6.2 MPa to 0 MPa, resulting in No.1 evaporator liquid level false rose by 0.18 m, which produced a kind of step disturbance, caused the main feed water regulator and evaporator liquid level fluctuations, eventually triggered the shutdown protection signal cause of the low level.

To sum up, the direct reason for the fluctuation of liquid level was that the signal (switching quantity and analog quantity) sent by this cabinet to other cabinets through the network becomes 0 after the double AP fault occurred. Therefore, in order to ensure the stable operation of the unit after double AP failures and reserve a certain time window for troubleshooting, it is necessary to analyze the consequences of different types of controlled equipment and formulate corresponding logical optimization measures according to the changing characteristics of network signals after double AP failure.

## 3. Optimization measures

### 3.1 Types of the main controlled equipment in the first phase of Tian Wan nuclear power plant, and the control principles

The controlled equipment of the loop 1 , the loop 2 and the marine engineering system in the Tian Wan nuclear power plant phase-1 were all driven by electricity, mainly including electric pump, electric cut-off valve, electric regulating valve and electromagnetic valve.

After the electric pump receives the DCS command signal of on and off, the start and stop relay in the switch cabinet is energized, then the pump executes the start and stop command, then the start and stop auxiliary contact is used as the pump start and stop state feedback and reset the DCS start and stop command. The pump start and stop state is maintained by the self-maintaining control circuit in the switch cabinet.

Solenoid valve control principle and pump are the same.

After receiving the DCS switch command, the start and stop relay in the switch cabinet is energized. The electric stop valve performs the open and close command. When the valve is fully open or fully closed, the limit switch action resets the start and stop command of DCS, and the stop valve remains at the current position.

The control valve of the Tian Wan nuclear power plant phase-1 is pulse control valve. When the closed-loop regulator issues the open and close pulses due to the control deviation, the control valve executes the open and close instruction. When there is no open and close command pulse, the control valve maintains the current open degree. The closed loop regulator of important regulating valves is basically the synthetic signal after 3 to 2, and the mass level failure of most of the regulated signals is involved in the automatic interlock of the regulator.

### 3.2 Influence of the double AP faults

In order to prevent the DCS double AP fault from causing disturbance to the unit state, the control logic analysis and optimization should be carried out according to the signal characteristics after double AP fault combined with the controlled equipment.

When double AP failure occurs in the cabinet where the control signal is located, there are no obvious influences on the stable operation state of the unit in the following situations:

When the control device and control signal are in the same AP, as the double AP fails, DCS loses logic control function, and the device remains in the current state;

When the output signals of the control device and the switch quantity are not in the same AP, the double AP fails and the output signals to other AP are 0.

If the mass level of the regulated value (Analog signals or Analog synthetic signals)of the closed-loop regulator fails to interlock the auto-deactivation function of the closed-loop regulator and the regulator and the regulated value are not in the same AP. If the transferred amount of AP occur double P-stop failures, automatic regulator will exit (closed loop) control mode, keep for refund automatically adjust valve before opening.

When double AP failure occurs in the cabinet where the control signal is located, the following situation will affect the stable operation state of the unit:

"Analog signals or analog synthesis signals and regulator or correction algorithm are not the same AP, if analog signal or analog synthesis of AP double-stop fault occurs, the output analog signals to other AP is 0, a modification of the analog signal control object or cause disturbance feed-forward operation control circuit".

When the mass level failure signal of the closed loop regulator regulated (analog signal or analog synthetic signal) does not have the interlock regulator back automatic function and the regulator is not in the same AP with the regulated, if the AP in which the regulated is located has a double-stop fault, the regulator will be out of control because the regulated becomes 0.

If the output signal of the controlled device and the digital quantity are not the same AP, when the AP fails, the output signal to other AP will be 0. If the above zero signal is inverted in the interlock protection logic of other AP, the interlock protection function of the controlled device will be triggered by mistake.

### 3.3 Optimization measures

In view of the "analog signal or analog synthesis and regulator or correction algorithm is not the same AP, if analog signals or analog synthesis signals of AP double-stop fault occurs, the output analog signals to other AP is changed to 0, Then the disturbance will be caused to the control loop in which the analog signal participates in the control object correction or feed forward operation “:

1. It is suggested to move the logic of the analog synthesis signals involved in the closed-loop regulator deviation operation or the modulator correction to the AP of the closed-loop regulator deviation operation logic or actuator driven logic;

2. For the analog signals participating in the feed-forward operation of the controlled object, it is suggested to control the influence on the control object by controlling the smoothing time of the signal quality bit failure signal, or by blocking the feed-forward function of the signal quality bit failure signal;

3. For the temperature signals directly involved in flow signal correction, there is no need to make rectification due to the control of signal quality level failure signal in logic (when the signal is invalid, the temperature correction value will be cut into the set value reference value), which has little influence;

In view of "the mass level failure signal of the closed loop regulator regulated (analog signals or analog synthetic signals) has no interlock regulator back automatic function and the regulator and the regulated are not the same AP, if the AP in which the regulated is located has a double stop fault, the regulator will be 0 out of control due to the regulated":

The quality position failure signal interlock regulator of the synthetic signal is automatically deactivated, which means the valve is automatically cut when the synthetic signal is invalid.

In view of "if the output signals of the controlled device and the digital quantity are not the same AP, if the AP fails, the output signal to other AP will be 0. If the above zero signal is inverted in the interlock protection logic of other AP, the interlock protection function of the controlled device will be triggered by mistake":

The logic to reverse the interlock protection in other AP can be moved forward into the AP generated by the switching signal, which can ensure that even after the failure of double AP, the signal output to other AP is still 0, and the interlock protection function of the device will not be triggered by mistake.

## 4. Optimization implementation

Based on double AP fault impact on normal operation of the Tian Wan nuclear power plant phase-1 DCS system in all of the control logic for the comb, and the cabinet in the double influential to the unit state after failure of AP signal and logic is optimized, primarily concerned with logic: evaporator liquid level correction and control logic, the reactor pressure vessel under pressure control logic, and back filling discharge logic, voltage regulator level correction and control logic, ii plus liquid level control logic, high and low level control logic, etc.

The simulation results show that the optimized logic can effectively avoid the disturbance caused by double AP faults.

## 5. Conclusion

Normal operation of the instrument control system cabinet involves the collection and control of some important process parameters of the unit. If a cabinet fails to operate, it may cause great disturbance to the state of the unit and even lead to the occurrence of shutdown. According to the signal characteristics of double AP faults, combined with the logical analysis of the controlled equipment, the fault consequences were analyzed in the paper, and the corresponding optimization measures were formulated for the signals or logic that have an impact on the operation state of the unit, which can effectively reduce or avoid the adverse impact on the operation state of the unit. The methods and measures mentioned in this paper could also be used for reference to the peer power station and design institute.

## References

[1] Xu Xiajun, TXP Control System Optimization and Improvement in Tianwan Nuclear Power Station, 1st China (International) Nuclear Power Instrument and Control Technology Conference, 2011.
[2] Intermediate Report Concerning the analysis of the Unit2 AP106 failure, SIEMENS, 2016.
[3] Teleperm XP Manuals, SIEMENS, 2003.