# Analysis of SGTR Accident with PMS Software Failure

**Authors:** Ms. Liu Lixin, Lixin, Miss Liu

**Date:** 2025-02-06T00:00:00+00:00

## Abstract

Digital instrumentation and control technology has gradually been applied in nuclear power plants (NPPs), and common cause failures (CCFs) due to improper design and/or use may affect NPP safety. The purpose of this paper is to analyze steam generator tube rupture (SGTR) combined with PMS software common cause failure in third-generation passive nuclear power plants. Third-generation passive nuclear power plants provide automatic protection measures for SGTR accidents, including reactor shutdown, core makeup tank initiation, passive residual heat removal heat exchanger actuation, isolation of startup feedwater, and chemical and volume control system operation. To further demonstrate plant safety, it is assumed that all the above protective measures have failed due to a PMS failure, and that only DAS signals and operator actions can mitigate the accident and bring the plant to a safe steady state. The analysis results show that the ruptured SG will not overfill during the entire accident process, the accident consequences are limited, and the radioactive consequences meet regulatory limits.

## Full Text

## Analysis of SGTR with PMS Software Failure Accident

**Liu Lixin, Wang Haitao**
Shanghai Nuclear Engineering Research & Design Institute Co., Ltd., Shanghai, 200233, China

### Abstract

Digital instrument and control technology has been gradually applied in nuclear power plants (NPPs). Common cause failure (CCF) due to improper design and/or use may affect NPP safety. This paper analyzes steam generator tube rupture (SGTR) combined with PMS software common cause failure in third-generation passive nuclear power plants. These plants provide automatic protection measures for SGTR accidents, including reactor shutdown, core makeup tank initiation, passive residual heat removal system heat exchanger action, and isolation of startup feedwater and chemical volume control system. To further demonstrate plant safety, it is assumed that all these protective measures fail due to PMS failure, and that only DAS signals and operator actions can mitigate the accident and bring the plant to a safe steady state. The analysis results show that the ruptured SG will not overfill throughout the accident process, the accident consequences are limited, and the radioactive consequences meet limit requirements.

**Keywords:** Steam generator tube rupture (SGTR), SG overfill, Single tube double-ended, PMS failure, DAS signal

**Introduction**

Digital instrument and control systems have been increasingly applied in nuclear power plants. Common cause failure caused by improper design or use may affect nuclear power plant safety. To address CCF in digital instrumentation and control, defense measures such as functional decentralization, quality improvement, real-time monitoring, and diversity should be adopted. According to NUREG 0800 BTP 7-19 [1], it is necessary to demonstrate the defense-in-depth design capability of the plant after PMS software CCF. The diverse actuation system (DAS) in third-generation passive nuclear power plants provides necessary instrumentation and control functions to mitigate consequences of assumed CCFs in the PMS.

Overseas nuclear power plants such as US-APWR and APR1400 have implemented defense-in-depth and diversity (D3) design for instrumentation and control systems and completed relevant analysis and verification. This paper takes the steam generator tube rupture (SGTR) event from Chapter 15 of the safety analysis report for third-generation passive nuclear power plants as an example to analyze the superimposed PMS software CCF and evaluate the mitigation capability of the defense-in-depth system under this accident.

## Instrument and Control Design Defense-in-Depth Analysis

### 1.1 PMS System

The PMS is a safety-class system that performs reactor emergency shutdown, ESF actuation, and qualified data processing system (QDPS) functions. The PMS equipment that performs ESF actuation functions, reactor emergency shutdown, as well as related shutdown breakers and sensors, are mostly configured with quadruple redundancy. The PMS monitors key plant parameters and drives safety functions when abnormalities occur to achieve and maintain safe shutdown state. Together with other safety systems, it provides capability to respond to expected operational events and assumed accidents. The PMS controls safety-class equipment and also provides manual control in the main control room and remote shutdown room. In addition, the PMS provides safety function monitoring during and after accidents.

### 1.2 DAS System

The DAS provides necessary instrumentation and control functions to reduce risks associated with assumed CCFs in the PMS system. Possible CCFs include software design errors, etc. The DAS directly receives signals from dedicated sensors, contains redundant signal processing units, and uses different (diverse) equipment and technologies from the PMS. The main DAS signals are detailed in Table 1 .

**Table 1 DAS Signals**

Protection Function: Reactor trip/Turbine trip
Monitored Variables: Both RCS hot leg high temperature signals simultaneously reach setpoint; Both SG wide range low level signals simultaneously reach setpoint; Pressurizer low level signal; Manual reactor trip signal

Protection Function: CMT start
Monitored Variables: Both SG wide range low level signals simultaneously reach setpoint; Pressurizer low level signal; Manual CMT start signal

Protection Function: RCP shutdown
Monitored Variables: Both SG wide range low level signals simultaneously reach setpoint; Pressurizer low level signal; Manual CMT start signal

## 2 Analysis Methods and Assumptions

A steam generator tube rupture (SGTR) causes primary side coolant to leak into the secondary side through the ruptured tubes. The break leads to primary pressure drop and contamination of the secondary side. The main consequence is possible radioactive release to atmosphere through the power-operated relief valve (PORV). For SGTR accidents, acceptance criteria require no overfill of the faulted SG and radioactive steam release to atmosphere not exceeding limits [2]. This paper assumes all automatic protection measures for mitigating SGTR, including PRHR and CMT activation and isolation of CVS and SFW, fail due to PMS failure. Only DAS signals and operator actions are used to mitigate the accident.

### 2.1 Analysis Method

After SGTR, radioactive coolant flows into the secondary side through the break, causing increased water level in the faulted SG and increased radioactivity in the secondary side. Reactor trip initiated by DAS, PRHR initiation, and SG feedwater isolation require operator intervention.

The accident is analyzed using a thermal-hydraulic system program. This program can simulate PRHR heat exchangers, safety logic, monitoring system triggers, and operator action sequences. It can analyze SGTR accidents in advanced pressurized water reactor (PWR) nuclear power plants.

The radioactive N-16 signal is directly sent to the data display and processing system (DDS) and is not affected by PMS failure. Therefore, when PMS fails, the N-16 signal remains valid, and operators can determine SGTR occurrence based on this signal and directly execute the "Steam Generator Tube Rupture" emergency operating procedure [3] to mitigate the accident.

According to DAS signal design, reactor shutdown, main pump coastdown, turbine trip, and CMT activation are initiated by the DAS signal for pressurizer low water level. Actions that cannot be automatically initiated by DAS signals (including main feedwater and startup feedwater isolation, CVS isolation, pressurizer heater isolation, etc.) and PRHR activation are assumed to be initiated by operators according to emergency operating procedures with certain delay times.

### 2.2 Assumptions

The assumptions for SGTR with PMS software failure accident analysis, which differ from DBA conditions, are as follows [4]:

- PRHR and CMT operate at nominal capacities. When the pressurizer low water level DAS signal is reached, reactor trip and pump coastdown, turbine trip, and CMT activation occur.
- When PMS fails, main feedwater regulation remains effective. However, it is conservatively assumed that main feedwater is continuously supplied at constant nominal flow rate before reactor trip.
- According to emergency operating procedures, operators need to isolate main feedwater and startup feedwater of the faulted SG and supply startup feedwater to the intact SG. In the analysis, it is conservatively assumed that operators isolate all main feedwater 30 minutes after accident initiation and simultaneously supply constant nominal startup feedwater flow to both loops. Later, operators isolate startup feedwater according to emergency operating procedures.
- Operators can manually operate CVS charging pumps to maintain pressurizer level. Therefore, it is conservatively assumed that CVS injects at maximum injection flow rate at accident beginning.
- According to emergency operating procedures, operators need to manually start PRHR. In the analysis, it is conservatively assumed that operators manually start PRHR 10 minutes after manually isolating pressurizer heaters.

## 3 Results Analysis

At time zero, a double-ended break of a single SG tube occurred. The operator manually activated CVS to provide makeup water flow, and pressurizer heaters were put into operation. The break caused reactor coolant leakage from primary to secondary side (as shown in Figure 1 [Figure 1: see original paper]), leading to temperature and pressure drop in the reactor coolant system primary side and pressurizer level decrease.

When the DAS signal for pressurizer low water level was reached, the reactor tripped, pumps coasted down, turbine tripped, and CMT activated. After reactor trip, pressurizer water level and primary side pressure dropped rapidly (as shown in Figures 2 and 3), and steam generator water volume increased rapidly (as shown in Figure 4 [Figure 4: see original paper]), causing secondary side pressure to rise rapidly (as shown in Figure 5 [Figure 5: see original paper]) until reaching PORV opening pressure to release steam.

According to emergency operating procedures, operators need to isolate main feedwater and startup feedwater of the faulted SG and supply startup feedwater to the intact SG. In the analysis, it is conservatively assumed that operators isolated all main feedwater 30 minutes after accident initiation and simultaneously supplied constant startup feedwater flow to both loops. According to pressurizer empty time, it is conservatively assumed that operators manually isolated pressurizer heaters 10 minutes after manually isolating main feedwater. According to procedures, operators need to activate PRHR to remove heat. In the analysis, it is conservatively assumed that operators manually activated PRHR 10 minutes after manually isolating pressurizer heaters.

The break flow caused continuous rise in SG secondary side water level. According to operating procedures, when narrow-range high liquid level of any SG is reached, CVS isolation valves and startup feedwater isolation valve should be closed. In the analysis, it is conservatively assumed that operator action to isolate CVS and startup feedwater is delayed 30 minutes after the faulted SG reaches narrow-range high liquid level setpoint.

After PRHR operation, RCS primary side temperature and pressure dropped rapidly, and pressurizer level continued to drop. The pressure difference between primary and secondary sides gradually decreased, causing break flow to gradually approach zero (as shown in Figure 1), and steam generator water volume began to gradually stabilize (as shown in Figure 4). Finally, primary and secondary side pressures of the steam generator basically reached equilibrium, and break flow terminated.

**Table 2 SGTR with PMS Software Common Cause Failure Accident Sequence**

Event: Double-ended break of steam generator tubes
Time (s): [Not specified]

Event: Pressurizer low water level signal (DAS signal)
Time (s): [Not specified]

Event: Reactor trip (DAS signal)
Time (s): [Not specified]

Event: CMT initiated (DAS signal)
Time (s): [Not specified]

Event: Main feedwater isolation and startup feedwater operated (operator action)
Time (s): [Not specified]

Event: PRHR put into operation (operator action)
Time (s): [Not specified]

Event: Isolation of CVS charging flow (operator action)
Time (s): [Not specified]

Event: Isolation of startup feedwater (operator action)
Time (s): [Not specified]

**Figure Captions:** Fig. 1 Break Flowrate
Fig. 2 [Figure 2: see original paper] Pressurizer Level
Fig. 3 [Figure 3: see original paper] Pressurizer Pressure
Fig. 4 Faulted SG Water Volume
Fig. 5 SG Steam Pressure

## 4 Conclusion

(1) The SGTR with PMS software failure accident can be effectively mitigated through DAS signals and operator manual intervention. During the accident, the maximum water volume of the SG is 295.8 $m^3$, and the SG overfill margin is 48.0 $m^3$. Throughout the accident, the faulted SG will not overfill. The radioactive consequences must also meet limit requirements.

(2) This is the first analysis of SGTR with PMS software failure accident relying only on DAS signals and operator actions to mitigate the accident, which further verifies that the nuclear power plant has the ability to mitigate common cause failures.

(3) The analysis further proves that current third-generation passive nuclear power plant design can cope with more severe accidents than design basis accidents, including multiple failures, further verifying nuclear power plant safety.

### References

[1] Anon. Final revision to branch technical position 7-19 guidance for evaluation of defense in depth and diversity to address common-cause failure due to

latent design defects in digital safety systems[J]. The Federal Register / FIND, 2021, 86(18): 7577.

[2] Liu Lixin, Liu Zhan. Extended research on SGTR accident SG overflow analysis[J]. Nuclear Power Engineering, 2020, 41(3): 81-85.

[3] Liu Lixin, Wang Zhe. Research on optimization of SGTR procedures in nuclear power plants[J]. Nuclear Power Engineering, 2022, 43(4).

[4] Ke Xiao. Research on SGTR accident in full power range of CAP1000 nuclear power plant[J]. Atomic Energy Science and Technology, 2014, 48(6): 1031-1037.

*Note: Figure translations are in progress. See original paper for figures.*