SGTR Accident Analysis with Superimposed PMS Software Common Cause Failure

Authors: Liu Lixin

Date: 2025-02-25T00:00:00+00:00

Abstract

Digital instrumentation and control technology has been increasingly applied in nuclear power plants, and common-cause failures due to improper design or use may affect nuclear power plant safety. The purpose of this paper is to analyze the accident of a single steam generator heat transfer tube rupture (SGTR) in a Generation III passive nuclear power plant, superimposed with a PMS software common-cause failure. Generation III passive nuclear power plants provide a series of automatic protection measures for SGTR accidents, including: reactor trip, Core Makeup Tank (CMT) actuation, Passive Residual Heat Removal (PRHR) system actuation, and isolation of Startup Feedwater (SFW) and Chemical and Volume Control System (CVS), etc. To further demonstrate the safety of the plant, it is assumed that all the above protection measures fail due to PMS faults, to verify whether the accident can be mitigated and the plant brought to a safe steady state relying solely on DAS signals and operator actions. The analysis results show that the damaged SG will not overflow throughout the accident process, the accident consequences are not limiting, and consequently the radiological consequences will necessarily meet the limit requirements.

Full Text

Preamble

Analysis of SGTR with PMS Software Common Cause Failure Accident

Liu Lixin[1], Wang Haitao[2]
([1],[2] Shanghai Nuclear Engineering Research & Design Institute Co., Ltd., Shanghai, 200233)

Abstract

Digital instrumentation and control (I&C) technology has been increasingly applied in nuclear power plants, where common cause failures (CCFs) resulting from improper design or usage may affect plant safety. This paper aims to analyze a steam generator tube rupture (SGTR) accident combined with postulated common cause failure of the protection and safety monitoring system (PMS) software in a Generation III passive nuclear power plant. Generation III passive nuclear power plants provide a series of automatic protection measures for SGTR accidents, including reactor shutdown, core makeup tank (CMT) actuation, passive residual heat removal (PRHR) system actuation, and isolation of startup feedwater (SFW) and chemical volume control system (CVS). To further demonstrate plant safety, this analysis assumes that all these protective measures fail due to PMS failure, and verifies whether the accident can be mitigated and the plant brought to a safe steady state relying solely on diverse actuation system (DAS) signals and operator actions. The analysis results show that the ruptured steam generator will not overfill throughout the accident process, the accident consequences are not limiting, and consequently the radiological consequences will also meet regulatory limits.

Keywords: Steam Generator Tube Rupture (SGTR); SG Overfill; Single Tube Double-Ended Rupture; PMS Failure; DAS Signal

Introduction

Digital instrumentation and control technology has been increasingly deployed in nuclear power plants, where common cause failures due to design or operational deficiencies may compromise plant safety. To address digital I&C common cause failures, defense measures such as functional diversity, quality improvement, real-time monitoring, and diversity should be implemented. According to the requirements of NUREG-0800 BTP 7-19 [1], it is necessary to demonstrate the plant' s defense-in-depth design capability to mitigate accidents following postulated common cause failures in the protection and safety monitoring system (PMS) software. Generation III passive nuclear power plants are equipped with a diverse actuation system (DAS) that provides essential I&C functions to mitigate accident consequences following postulated common cause failures in the PMS. Foreign nuclear plants such as US-APWR and APR1400 have implemented defense-in-depth and diversity (D3) designs for their I&C systems and completed verification analyses. Domestic nuclear organizations have also conducted corresponding D3 analyses for HPR1000, high-temperature gas-cooled reactors, and VVER plants. This paper takes the steam generator single tube rupture (SGTR) accident—a typical initiating event from Chapter 15 of the Generation III passive nuclear power plant safety analysis report—as an example to analyze the accident combined with PMS software common cause failure, evaluating the mitigation capability of the defense-in-depth system under such conditions.

1.1 PMS System

The PMS is a safety-grade system that performs reactor trip, engineered safety features (ESF) actuation, and Class 1E data processing (QDPS) functions. The PMS equipment that executes ESF actuation and reactor trip functions, along with associated trip breakers and sensors, is mostly configured with quadruple redundancy. The PMS monitors key plant parameters and drives relevant safety functions to achieve and maintain a safe shutdown state when anomalies occur. Together with other safety systems, it provides the plant' s capability to respond to anticipated operational occurrences and postulated accidents. The PMS controls safety-grade equipment and provides equipment-level manual control in the main control room and remote shutdown room for safety-grade equipment with severe consequences. Additionally, the PMS system provides safety function monitoring for the plant during and after accidents.

1.2 DAS System

The DAS provides necessary instrumentation and control functions to reduce risks associated with postulated common cause failures in the PMS, which may include software design errors. The DAS receives signals directly from dedicated sensors and contains redundant signal processing units that employ equipment and technology different (diverse) from the PMS. The main DAS signals are detailed in Table 1 below, which includes signals for PRHR outlet valve opening and IRWST return isolation valve closing, reactor trip, turbine trip, CMT actuation, and RCP shutdown.

2 Analysis Methods and Assumptions

Steam generator tube rupture (SGTR) causes primary coolant to leak into the secondary side of the steam generator through the break. The break leads to primary pressure reduction and contaminates the secondary side via fluid passing through the heat transfer tubes. The primary consequence is the potential radiological release to the atmosphere through the power-operated relief valves (PORVs), mainly on the ruptured SG side. For SGTR accidents, two acceptance criteria must be satisfied simultaneously: the ruptured SG must not overfill, and the radiological steam release to the atmosphere must not exceed limits [2]. This paper assumes that various automatic protection measures for SGTR mitigation fail due to PMS failure, including PRHR and CMT actuation as well as CVS and SFW isolation based on SG narrow-range "high-2 level" signals. Accident mitigation relies solely on DAS signals and operator actions.

2.1 Analysis Method

Following a steam generator tube rupture, radioactive coolant flows into the secondary side through the break, causing the ruptured SG water level to rise and secondary system radioactivity to increase. Reactor trip triggered by the pressurizer low-level DAS signal, PRHR actuation, and SG feedwater isolation require consideration of operator intervention actions.

The accident is analyzed using a thermal-hydraulic system code. Written in FORTRAN, this code has been enhanced to simulate PRHR heat exchangers, CMTs, and related protection and safety monitoring system trigger logic, as well as operator action sequences, making it suitable for analyzing SGTR accidents in advanced pressurized water reactor nuclear power plants.

The radiation monitoring system (RMS) provides radioactive measurement data to the plant control system (PLS) (via the data display and processing system, DDS) and the PMS. Through PLS analysis, it provides trigger signals to plant equipment in both non-safety-related and safety-related systems to actuate plant control facilities and terminate radioactive material release to the environment. The radioactive N-16 signal is transmitted directly to the DDS and is not affected by PMS failure. Therefore, when the PMS fails, the N-16 signal remains valid, allowing operators to identify the SGTR accident and directly implement the "Steam Generator Tube Rupture" emergency operating procedure [3] to mitigate the accident.

According to DAS signal design, DAS automatic protection functions include: opening PRHR outlet valves and closing in-containment refueling water storage tank (IRWST) return isolation valves, reactor trip, turbine trip, CMT actuation, and reactor coolant pump (RCP) shutdown. The analysis considers reactor trip, main pump coastdown, turbine trip, and CMT actuation triggered by the pressurizer low-level DAS signal. Actions that cannot be automatically triggered by DAS signals (including main feedwater and startup feedwater isolation, electric heater isolation, CVS isolation, and PRHR actuation) are assumed to be manually triggered by operators following emergency operating procedures with appropriate time delays.

2.2 Assumptions

The assumptions for the SGTR with PMS software common cause failure accident analysis are as follows [4]:

Since the break flow would be larger initially if located on the cold leg side than on the hot leg side, a single heat transfer tube double-ended rupture is postulated at the tube outlet on top of the steam generator tube sheet. The accident is assumed to occur with the plant at full power operation. The initial pressurizer level is taken as the nominal value for rated power operation. The steam dump system is not simulated; steam is discharged directly to the atmosphere through the atmospheric relief valves. Decay heat is taken from the 1979+2sigma decay heat curve. PRHR and CMT are assumed at their nominal capacities. When the pressurizer low-level DAS signal is reached, reactor trip and pump shutdown are triggered with a 2-second delay, turbine trip with a 7-second delay, and CMT actuation with a 12-second delay.

When the PMS system fails, main feedwater control remains functional. However, the analysis conservatively assumes that main feedwater continues at constant nominal flow until reactor trip. According to emergency operating procedures, operators must isolate main feedwater and startup feedwater to the ruptured loop and inject startup feedwater to the intact SG loops. The analysis conservatively assumes that operators isolate all main feedwater 30 minutes after the accident and simultaneously inject constant nominal flow startup feedwater to both loops; operators later isolate startup feedwater according to emergency operating procedures.

When the PMS system fails, automatic CVS makeup pump start signals and automatic CVS letdown open signals are blocked, and automatic CVS makeup pump stop signals are triggered. Operators can manually control the CVS makeup pump to maintain pressurizer level according to emergency operating procedures. Therefore, the analysis conservatively assumes CVS injects at maximum flow at the beginning of the accident, and operators later isolate CVS per emergency operating procedures.

Pressurizer electric heaters are assumed to be in service. Higher pressurizer electric heater power results in greater primary-to-secondary pressure differential and larger break flow. Based on emergency operating procedure steps and pressurizer drain time, operators are conservatively assumed to manually isolate pressurizer electric heaters 10 minutes after manually isolating main feedwater. According to emergency operating procedures, operators must manually actuate PRHR. The analysis conservatively assumes operators manually actuate PRHR 10 minutes after manually isolating pressurizer electric heaters.

3 Results Analysis

At time zero, a single steam generator heat transfer tube double-ended rupture occurs. Operators manually actuate CVS to provide makeup flow while pressurizer electric heaters are in service. The tube rupture causes reactor coolant to leak from the primary side to the secondary side [Figure 1: see original paper], resulting in primary system cooldown and depressurization and pressurizer level drop. Reactor trip, pump shutdown, turbine trip, and CMT actuation are triggered at 2 seconds, 7 seconds, and 12 seconds respectively after the pressurizer low-level DAS signal.

Following reactor trip, pressurizer level and primary pressure drop rapidly [Figure 2: see original paper]–[Figure 3: see original paper], steam generator water volume increases rapidly [Figure 4: see original paper], causing secondary side pressure to rise quickly [Figure 5: see original paper] until reaching the opening setpoint of the atmospheric relief valves, which open to discharge steam [Figure 6: see original paper].

According to emergency operating procedures, operators must isolate main feedwater and startup feedwater to the ruptured SG and inject startup feedwater to the intact SG. The analysis conservatively assumes operators isolate all main feedwater 30 minutes after the accident and simultaneously inject constant nominal flow startup feedwater to both loops, which results in larger water inventory in the ruptured SG. Based on emergency operating procedures and pressurizer drain time, operators are conservatively assumed to manually isolate pressurizer electric heaters 10 minutes after manually isolating main feedwater, eliminating an additional heat source to the primary system. Per procedures, operators must actuate PRHR for heat removal; the analysis conservatively assumes operators manually actuate PRHR 10 minutes after manually isolating pressurizer electric heaters.

The break flow causes continuous rise of the SG secondary side water level. According to emergency operating procedures, when any SG reaches narrow-range high level, CVS makeup line isolation valves and startup feedwater isolation valves are closed. The analysis conservatively assumes operators isolate CVS and startup feedwater 30 minutes after the ruptured SG reaches narrow-range high level. After the passive residual heat removal system is placed in service, RCS primary side temperature and pressure drop rapidly, and pressurizer level continues to decrease. The primary-to-secondary pressure differential gradually diminishes, causing break flow to approach zero [Figure 1: see original paper] and steam generator water volume to stabilize [Figure 4: see original paper]. Eventually, pressures on the primary and secondary sides of the steam generator essentially equalize, and break leakage flow terminates.

During the SGTR with PMS software common cause failure accident, primary coolant leakage through the ruptured SG heat transfer tube causes reactor coolant system depressurization before reactor trip, which would reduce the core departure from nucleate boiling ratio (DNBR). However, pressurizer electric heaters effectively limit primary pressure reduction [Figure 3: see original paper], and the depressurization caused by SGTR with PMS software common cause failure is much slower than that from pressurizer safety valve or automatic depressurization system (ADS) inadvertent opening accidents. After reactor trip, core DNBR increases rapidly. Therefore, DNB does not occur during the SGTR with PMS software common cause failure accident.

Table 2 SGTR with PMS Software Common Cause Failure Accident Sequence

Figure Captions:
Fig. 1 [Figure 1: see original paper] Break Flowrate
Fig. 2 [Figure 2: see original paper] Pressurizer Level
Fig. 3 [Figure 3: see original paper] Pressurizer Pressure
Fig. 4 [Figure 4: see original paper] Rupture SG Water Volume
Fig. 5 [Figure 5: see original paper] SG Steam Pressure
Fig. 6 [Figure 6: see original paper] Rupture SG Steam Flow

4 Conclusions

(1) The SGTR accident combined with PMS software common cause failure can be effectively mitigated through DAS signals and manual operator

interventions. The maximum steam generator water inventory during the accident is 295.8 m^3, with an SG overfill margin of 48.0 m^3. The ruptured SG does not overfill throughout the accident, the accident consequences are not limiting, and consequently the radiological consequences will meet regulatory limits.

(2) This analysis represents the first evaluation of an SGTR accident combined with PMS software common cause failure, mitigated solely by DAS signals and operator actions. It further verifies the plant' s capability to mitigate accidents involving common cause failures, making the SGTR analysis more comprehensive and the accident analysis system more complete.

(3) The analysis further demonstrates that the current Generation III passive nuclear power plant design possesses the capability to cope with accidents more severe than design basis accidents involving multiple common cause failures, thereby further validating 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] 刘立欣, 刘展. SGTR 事故 SG 满溢分析扩展研究 [J]. 核动力工程, 2020, 41(3): 81-85.
[3] 刘立欣, 王喆. 核电厂 SGTR 规程优化研究 [J]. 核动力工程, 2022, 43(4): 126-130.
[4] 柯晓. CAP1000 核电厂全功率范围 SGTR 事故研究 [J]. 原子能科学技术, 2014, 48(6): 1031-1037.

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