Energy Engineering

Tech Science Press

http://doi.org/10.32604/ee.2026.087110

ARTICLE

Verification of Mitigation Capability for Total Loss of Feedwater Accident and Sensitivity Study on Feed-and-Bleed Cooling in a CPR1000 Nuclear Power Plant

Bo Zhang and Zhenhua Zhang*

Nuclear and Radiation Safety Center, MEE, Beijing, China
*Corresponding Author: Zhenhua Zhang. Email: zhenhuazhang05@126.com

Received: 10 June 2026; Accepted: 10 July 2026; Published: 06 August 2026

ABSTRACT: Total loss of feedwater accident is a typical transient among the design extension conditions for pressurized water reactor nuclear power plants, directly related to the loss of core cooling capability. Chinese nuclear safety regulations require in-depth analysis of such conditions, while most of the Generation II and modified Generation II units currently in operation were designed prior to the issuance of these regulatory requirements, and their mitigation capability remains to be verified. To evaluate the mitigation capability of CPR1000 nuclear power units in operation in China for this accident, an accident sequence involving main feedwater pump trip combined with complete failure of the auxiliary feedwater system under full power condition was simulated based on a high-fidelity simulation platform. By strictly following the emergency operating procedures for operator interventions, the transient responses of key safety parameters including primary coolant system pressure, coolant inventory, core outlet temperature, fuel temperature, and containment pressure were analyzed. The results show that, under the synergistic effect of automatic system actions and procedure guidance, the operator manually opened all three sets of pressurizer safety valves at about 60 min, establishing the feed-and-bleed cooling mode. The minimum reactor pressure vessel water level was 67.7%, the core remained uncovered, and both the peak fuel cladding temperature and core outlet temperature remained below the limits. At about 98 min, the residual heat removal system entry conditions were satisfied, and the core was successfully brought to a safe state. A sensitivity study on the influence of the number of opened safety valve sets was performed. The results indicate that when only two sets of safety valves were successfully opened, all acceptance criteria were still satisfied; when only one set was opened, the heat removal capacity of the safety valves was insufficient, with the pressure exhibiting saw-tooth fluctuations in the range of 2.3–3.7 MPa(a), and the residual heat removal system entry conditions could not be satisfied, thus making a smooth transition to a safe state difficult. These results provide an engineering reference for similar units in coping with total loss of feedwater accidents and for optimizing the feed-and-bleed cooling operational strategy.

KEYWORDS: Nuclear power plant; total loss of feedwater; mitigation capability verification; feed-and-bleed cooling; sensitivity study

1 Introduction

Total loss of feedwater accident is an important design extension condition for nuclear power plants [1,2]. This accident can simultaneously trigger multiple threats [3,4]: first, loss of secondary side cooling function leads to ineffective removal of core decay heat; the imbalance between heat generation and heat removal can disrupt the stability of core heat transfer and flow, thereby causing local core damage; second, the primary coolant rapidly heats up and pressurizes due to loss of heat sink, causing repeated opening of the pressurizer safety valves, resulting in continuous leakage of reactor coolant and reduction of system water inventory, which may develop into core uncovery and even fuel damage; third, the high-temperature and high-pressure coolant discharged from the pressurizer safety valves enters the containment, raising its internal pressure and temperature, threatening the integrity of the containment as the third barrier and weakening its radioactivity confinement function.

The 2011 Fukushima nuclear accident, at great cost, warned the world that utmost attention must be paid to beyond-design-basis accidents [5,6]. Following the accident, researchers worldwide have conducted extensive studies in areas such as accident diagnosis, probabilistic safety analysis, and machine learning applications, covering different technical approaches from root cause identification to rapid accident classification and diagnosis [7,8]. The "Safety Regulations for Design of Nuclear Power Plants" (HAF102-2016), revised and issued by the National Nuclear Safety Administration of China in 2016, introduced the concept of "design extension condition" for the first time and put forward clear requirements for its analysis, demonstration, and countermeasures, aiming to further enhance the capability of nuclear power plants to cope with extreme accidents. However, the nuclear power units in operation in China are mainly Generation II and modified Generation II units [9], and their original designs mostly predate this regulation. When coping with such design extension conditions, these units rely mainly on safety facilities designed for design basis accidents and post-Fukushima improvement measures; their inherent safety margins and passive safety characteristics have certain gaps compared with Generation III units such as the Hualong One [10,11]. Therefore, for the huge fleet of Generation II and modified Generation II units, their accident mitigation capability depends not only on equipment reliability, but also to a large extent on the effectiveness of the accident procedures, the operator's precise response under high stress and complex decision-making pressure, and the timing control of the accident progression [12,13].

The "Atomic Energy Law of the People's Republic of China", which came into effect in 2025, established at the national legal level the fundamental nuclear safety principles of "bottom line thinking" and "defense in depth", further strengthening the requirement for in-depth research on design extension conditions. Against this background, in-depth analysis of total loss of feedwater accidents has become a key link in implementing legal requirements and addressing realistic safety challenges.

Based on the above, this study selects a typical in-service Generation II modified unit in China as the object and uses a simulation platform to conduct full-scope simulation of the total loss of feedwater accident sequence. The research strictly follows the current accident procedures to simulate operator interventions. By analyzing the evolution of key safety parameters such as primary coolant system pressure, coolant inventory, core coolant temperature, fuel temperature, and containment pressure, the study quantitatively evaluates the accident progression characteristics and the effectiveness of existing mitigation measures, with the aim of providing theoretical basis and practical reference for improving the safe operation level of the main reactor types in operation in China.

2 Research Methodology

2.1 Simulation Platform

The simulation platform used in this study is the 'full-scope verification simulator', which is the outcome of the 'National Nuclear Safety Regulatory Technical Support System Project—Full-Scope Verification Simulator' and is the first major project of China's nuclear safety regulatory system in the nuclear energy sector [14], of which a photograph is shown in Fig. 1. The platform was constructed based on the actual design and operation data of a domestic CPR1000 unit, integrating mature modeling and simulation technologies, covering aspects such as the simulation platform itself, modeling tools, process simulation, digital instrumentation and control system simulation, system integration, configuration management, and testing. A schematic diagram of the simulation platform structure is shown in Fig. 2. The simulation platform has undergone systematic testing and plant data validation, and meets the requirements of relevant standards such as ANSI/ANS 3.5-2009 "Nuclear Power Plant Simulators for Use in Operator Training and Examination" and NB/T 20015-2010 "Simulators for Operator Training and Examination of Nuclear Power Plants." It is capable of simulating the steady-state operation and transient processes of the reference unit under all operating conditions from refueling cold shutdown to rated full power, meeting engineering analysis accuracy requirements, and also possesses the ability to simulate various operating conditions using the actual operating procedures of the reference unit. The core physics model in the platform is built upon the NESTLE code package, and the reactor thermal-hydraulic model is built upon the RELAP5 3D RT code, with the two coupled and solved together. Both of the above codes are widely recognized and thoroughly validated best-estimate codes in the international nuclear engineering community [15–17]. In the platform, the core model adopts a three-dimensional, two-energy-group, six-group delayed neutron space-time neutron diffusion kinetic model. The primary loop thermal-hydraulic model uses a six-equation model, comprising a total of 110 control volumes, covering key equipment such as the reactor pressure vessel, control rods, pressurizer, steam generators, pipelines, and related water tanks. The secondary loop system is connected to the main steam system with the steam header as the boundary, using a two-phase flow network model combined with a dedicated steam turbine module for precise simulation. The process control layer of the instrumentation and control system adopts virtual simulation, while the human-machine interface layer adopts physical simulation, which includes safety-grade and non-safety-grade control terminals, post-accident monitors, and the backup panel.

Figure 1: Photograph of the full-scope verification simulator.

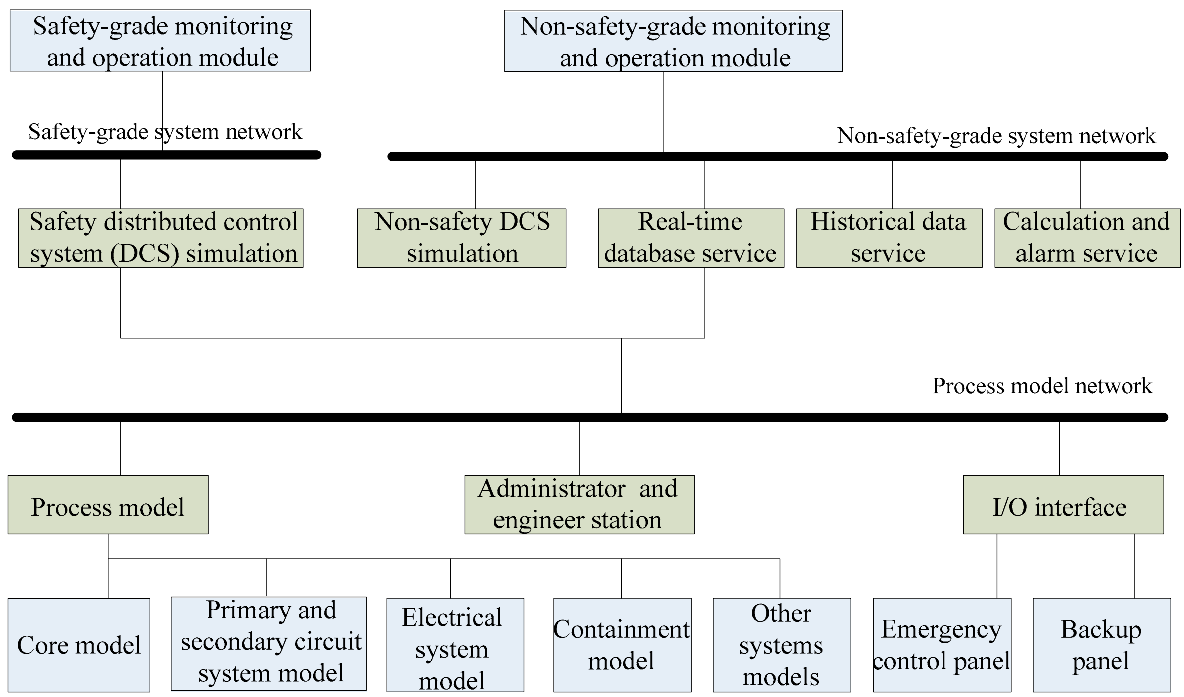

Figure 2: Schematic diagram of the simulation platform.

2.2 Initiating Event Assumptions

The initial plant state before the occurrence of the total loss of feedwater accident can cover various normal operation modes. Since full-power operation has the longest duration within the plant lifetime and, under this condition, the core decay heat to be removed after the accident is the largest, this study considers it as the most representative analysis condition.

The specific initiating event sequence set in this simulation is as follows: when the unit is operating at rated full power, an electrical fault in the main feedwater system causes the two operating main feedwater pumps to trip simultaneously, and the third pump fails to start automatically. Thereafter, the auxiliary feedwater system (including the electric-driven and turbine-driven pumps) fails to start, and thus cannot provide auxiliary feedwater to the steam generators.

2.3 Assumptions for Initial Plant Conditions

The simulation assumes that the unit is in full-power operation at the onset of the accident, and the initial values of its main parameters are shown in Table 1. Referring to common analysis methods for design extension conditions [18,19], the values of the parameters in the table are taken as design nominal values or engineering best estimates.

Table 1: Key parameters of the initial condition.

Parameter	Value Used
Core thermal power/MW	2895
Primary coolant boron concentration/ppm	775
Average primary coolant temperature/°C	310
Primary coolant system pressure/MPa(g)	15.4
Coolant flow rate/kg·s^{-1}·loop^{-1}	4718

Table 1: *Cont.*

Parameter	Value Used
Pressurizer water level/m	0
Steam generator wide-range water level/m	−0.87
Steam generator pressure/MPa(g)	6.69
Main steam flow rate/$t \cdot h^{-1} \cdot loop^{-1}$	1962

2.4 Procedures and Operator Actions

This study strictly adopts the state-oriented approach emergency operating procedures actually used for the reference unit. These procedures take the six key safety function states of the unit (subcriticality, heat removal, primary loop water inventory, steam generator integrity, secondary loop water inventory, and containment integrity) as the basis for diagnosis and decision-making, forming a closed-loop control logic. Their execution begins with state diagnosis; by identifying each safety function state and integrating their priorities, operation strategies are formulated, aiming to guide and maintain all safety functions in the optimal state.

During the simulation, the test personnel strictly follow these procedures to control the unit, simulating the various operations of actual operators as realistically as possible. In accordance with the relevant requirements of China's nuclear safety guide 'Deterministic Safety Analysis for Nuclear Power Plants' (HAD102/19-2021), and with reference to the common industry practice for design extension condition analysis assumptions in Chinese nuclear power plants, the operator no-intervention time is set to 30 min, i.e., starting from the first important signal triggered by the initiating event, the operator begins to execute the first manual operation in the main control room after 30 min.

2.5 Acceptance Criteria

The acceptance criteria adopted in this accident analysis include [20,21]: the core shall ultimately reach and remain in a subcritical state; the reactor decay heat shall be effectively removed, and a safe state shall be achieved and maintained; no significant core damage shall occur, and the coolable geometry of the core shall be preserved; the integrity of the containment shall be ensured; and the radiological consequences shall satisfy the following requirement: the effective dose received by any individual at the exclusion area boundary through cloud immersion external exposure and inhalation internal exposure during the entire duration of the accident shall be below the prescribed limits.

3 Results and Discussion

3.1 Event Sequence

Based on the initial condition settings, the simulation platform was initialized, and the initiating event was introduced at 50 s. At 59 s, the instrumentation and control system triggered a signal of "nuclear power greater than 30% and feedwater flow lower than 6%", which then triggered reactor emergency shutdown and turbine trip. This signal simultaneously directed the operator to enter the emergency operating procedures. During the period from 59 s to 1920 s, the operator diagnosed and verified the plant state based on alarm information and the emergency operating procedures. The main event sequence during the accident is detailed in Table 2.

Table 2: Key event sequence during the accident.

Time/s	Event Sequence
0	Reactor at full power operation
50	Initiating event occurs
59	Reactor trip signal triggered (nuclear power >30% and feedwater flow <6%) Turbine trip signal triggered Auxiliary feedwater pump start signal triggered (startup failure)
1929	Reactor coolant pumps trip
1981	Main steam isolation signal triggered
2784	Steam generator wide-range water level below −10 m
3660	Three sets of pressurizer safety valves opened
3696	Safety injection actuation signal triggered (low pressurizer pressure ≤ 11.9 MPa(a)) Containment phase A isolation signal triggered Main feedwater isolation signal triggered
4587	Accumulator actuated
6180	Transient simulation ends

3.2 Transient Response of Key Parameters

The plant state parameters closely related to the acceptance criteria and the integrity of the three barriers mainly include: primary coolant system pressure, coolant inventory, core coolant temperature, fuel temperature, and containment pressure. This paper focuses on the analysis of the above parameters, while also taking into account other relevant supporting parameters.

(1) Primary Coolant System Pressure and Reactor Vessel Water Level

The trends of primary coolant system pressure and reactor vessel water level are shown in Fig. 3. At full power operation, the primary coolant system pressure was stable at about 15.5 MPa(a), and the reactor vessel water level was 100%. At 50 s, the two operating main feedwater pumps tripped, causing a rapid decrease in feedwater flow. At 59 s, the instrumentation and control system triggered a signal of "nuclear power >30% and feedwater flow <6%", which then triggered a reactor trip and the control rods fell into the core. The coolant contraction caused by the trip led to a decrease in primary coolant system pressure. When the compensation differential pressure reached −0.17 MPa, the on-off electric heaters of the pressurizer automatically started to maintain pressure stability. During the trip transient, the minimum primary coolant system pressure reached 13.46 MPa(a).

At 1929 s, to maximize the limitation of heat generation in the primary coolant system, the operator manually tripped all three main coolant pumps according to the emergency operating procedures, terminating the forced core circulation. Meanwhile, due to lack of feedwater supply, the steam generator wide-range water level had gradually decreased from the initial −0.87 m to below −8.6 m, resulting in partial uncovering of the steam generator heat transfer tubes and a gradual decrease in secondary side cooling capability, which caused the primary coolant system pressure to gradually increase. At 2855 s, the primary coolant system pressure reached the opening pressure setpoint of the first set of pressurizer safety valves (16.6 MPa(a)) for the first time, causing the pressurizer safety valves to open for pressure relief, and they automatically closed when the pressure decreased to 16.0 MPa(a). During the period from 2855 s to 3660 s, the pressurizer safety valves repeatedly opened automatically, removing core decay heat by means of "overflow", and the primary coolant system pressure exhibited a saw-tooth fluctuation.

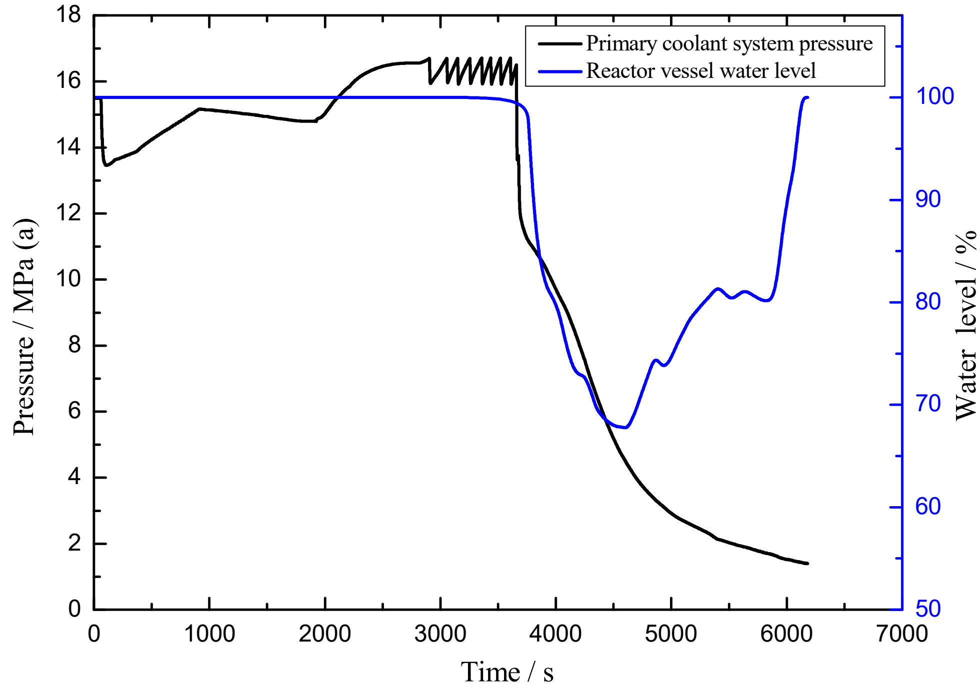

Figure 3: Trend of the primary coolant system pressure and the reactor vessel water level.

At 3660 s, the operator manually opened all three sets of pressurizer safety valves according to the emergency operating procedures, causing a sharp drop in primary coolant system pressure. The pressure decrease rate depended mainly on the heat removal capacity of the pressurizer safety valves. When the pressure decreased to 11.9 MPa(a), the safety injection system automatically started. At this point, the feed-and-bleed cooling mode was formally established. A large amount of steam-water mixture was discharged through the pressurizer safety valves to the relief tank, while the safety injection system injected high-concentration borated water from the refueling water tank into the core to compensate for the continuous coolant loss. During the pressure decrease of the primary coolant system, flashing occurred in the core coolant, causing the reactor vessel water level to continuously drop. As shown in Fig. 3, at 4620 s the reactor vessel water level reached its minimum value of 67.7%, but it remained above the top of the hot legs, and the core was not uncovered. Thereafter, under the action of continuously increasing safety injection flow, the reactor vessel water level gradually recovered. At 5941 s, the primary coolant system pressure decreased to 1.58 MPa(a), the core outlet coolant was subcooled and its temperature decreased to 171°C, satisfying the conditions for residual heat removal system entry (core outlet coolant subcooled with temperature below 172°C and primary coolant system pressure below 2.7 MPa(g)). The operator could then connect the residual heat removal system to achieve long-term controlled heat removal from the core.

After the residual heat removal system entry conditions are satisfied, the operator is required to perform a series of operations to complete the transition from feed-and-bleed cooling to residual heat removal system cooling, including: opening the residual heat removal system isolation valves, preheating the residual heat removal system, starting the residual heat removal pumps, closing the pressurizer safety valves (with only one set of safety valves kept open), and switching the safety injection system configuration to charging mode. The main operational challenges during the transition phase include: the primary coolant system pressure must be stably maintained within the allowable operating pressure range of the residual heat removal system to avoid overpressurization of the residual heat removal system due to pressure anomalies; and the residual heat removal system must be adequately preheated before entry to prevent thermal shock from adversely affecting system materials, thereby ensuring its operational reliability. The emergency operating procedures provide clear requirements for the above key steps, and the operator can effectively address the associated risks by following the procedures.

(2) Maximum Core Outlet Coolant Temperature

The trend of the maximum core outlet coolant temperature is shown in Fig. 4. During full power operation, the primary coolant system cold leg temperature was about 292°C, the hot leg temperature about 327°C, and the maximum core outlet coolant temperature about 335°C. At 59 s, the reactor tripped, terminating the fission reaction, and the core coolant temperature rapidly decreased. Thereafter, the core coolant temperature mainly depended on the core decay heat removal capability.

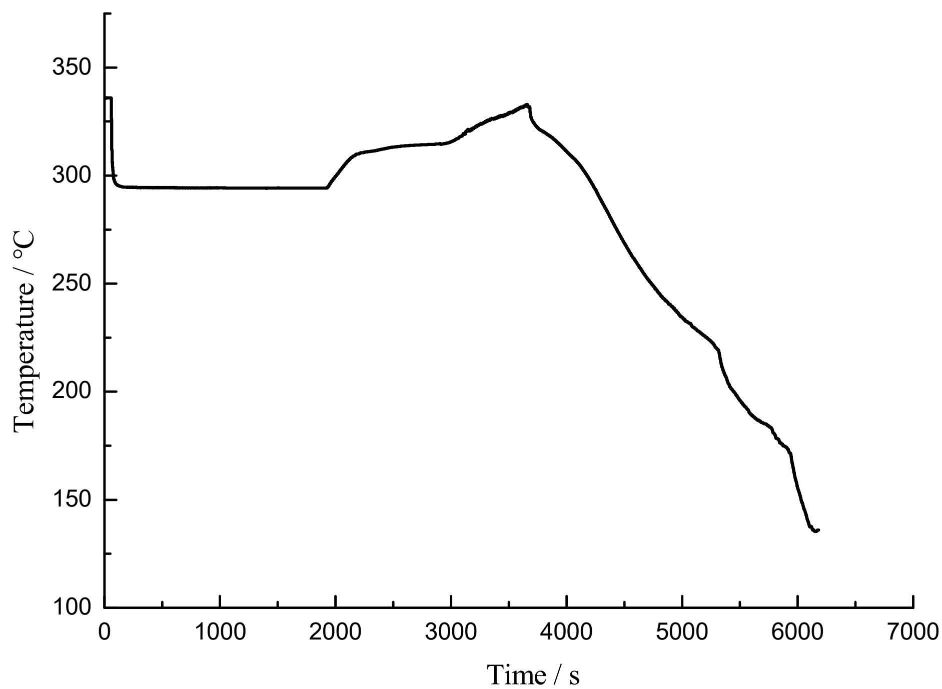

Figure 4: Trend of the maximum core outlet coolant temperature.

After the reactor trip, the turbine bypass system (to the condenser) was the main means of core decay heat removal. This system operated automatically, adjusting the bypass valve opening based on temperature deviation to maintain the stability of the average coolant temperature. Therefore, the maximum core outlet coolant temperature remained essentially around 294°C. At 1929 s, in order to maximize the limitation of heat generation in the primary coolant system, the operator manually tripped all three main coolant pumps according to the emergency operating procedures, terminating forced core circulation, which caused a certain increase in the maximum core outlet coolant temperature. At 1981 s, the operator isolated the main steam system as per the procedures, blocked the cooling mode of the turbine bypass system (to the condenser), and switched to the turbine bypass system (to the atmosphere) to maintain the stability of the primary coolant temperature. Meanwhile, due to lack of feedwater, the steam generator wide-range water level gradually decreased, the heat transfer tubes of the steam generators became progressively uncovered, and the secondary side cooling capability gradually diminished. At 2750 s, the steam generator wide-range water level dropped below −10 m (as shown in Fig. 5), the steam generators were about to dry out and thus completely lost cooling capability. The operator marked all three steam generators as unavailable according to the procedures and set the discharge pressure setpoint of the turbine bypass system (to the atmosphere) to 7.75 MPa(g). The maximum core outlet coolant temperature gradually increased. At 3600 s, it reached 331°C, exceeding the feed-and-bleed cooling activation threshold of 330°C. At 3660 s, the operator manually opened all three sets of pressurizer safety valves, cooling the core through feed-and-bleed cooling. A large amount of steam-water mixture was discharged through the pressurizer safety valves to the relief tank, while the safety injection system injected high-concentration borated water from the refueling water tank into the core to compensate for the continuous coolant loss. As the primary coolant system pressure decreased, the maximum core outlet coolant temperature also gradually decreased. At 5941 s, the core outlet coolant was subcooled and its temperature reached 171°C, satisfying the conditions for residual heat removal system entry (core outlet coolant subcooled with temperature below 172°C and primary coolant system pressure below 2.7 MPa(g)). The operator could then connect the residual heat removal system to achieve long-term controlled heat removal from the core.

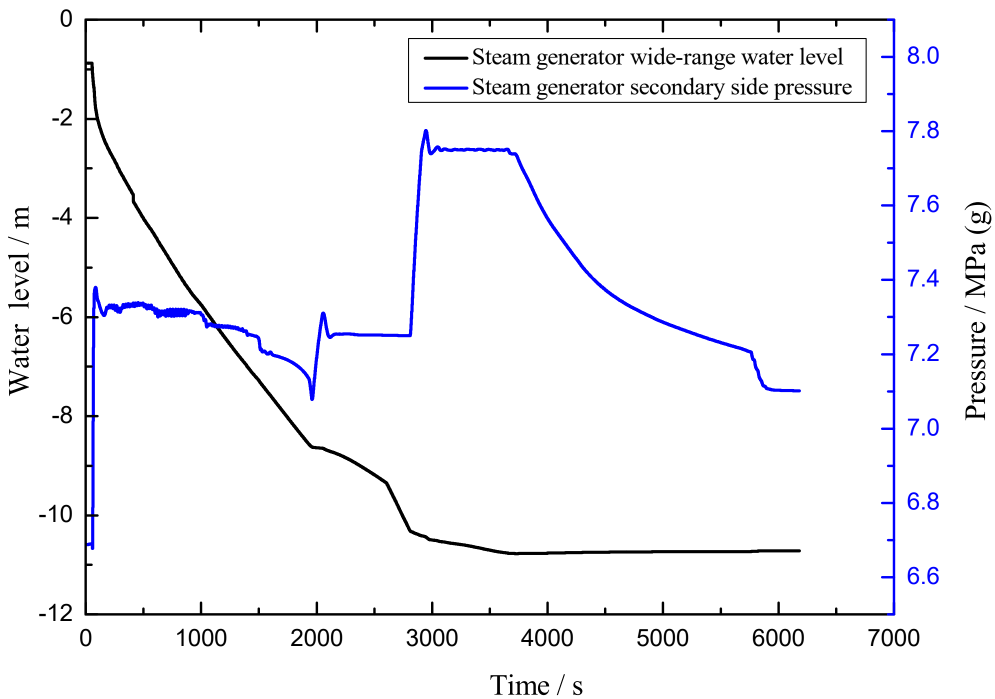

Figure 5: Trend of the steam generator wide-range water level and secondary-side pressure.

(3) Fuel Temperature

The trend of the maximum temperature on the outer surface of the fuel cladding is shown in Fig. 6. Before the accident, the maximum temperature on the outer surface of the fuel cladding was 394°C. At 59 s, the reactor tripped, and the fuel cladding temperature then dropped sharply. The variation of the fuel cladding temperature was jointly affected by core water inventory, coolant temperature, and heat transfer coefficient. At 1929 s, in order to maximize the limitation of heat generation in the primary coolant system, the operator manually tripped all three main coolant pumps according to the emergency operating procedures, terminating forced core circulation. The heat transfer coefficient between the fuel and the coolant decreased, causing a certain increase in the fuel cladding temperature. At 3660 s, the operator manually opened all three sets of pressurizer safety valves according to the procedures, establishing the feed-and-bleed cooling mode. During feed-and-bleed cooling, as the primary coolant system pressure decreased, flashing occurred in the core coolant, significantly affecting the heat transfer coefficient between the fuel and the coolant. The maximum temperature on the outer surface of the fuel cladding exhibited several step-change peaks, with the highest reaching about 610°C. A large amount of steam-water mixture was discharged through the pressurizer safety valves to the relief tank, while the safety injection system injected high-concentration borated water from the refueling water tank into the core to compensate for the continuous coolant loss. Core simulated data indicated that during the entire transient, the minimum reactor vessel water level was 67.7% (as shown in Fig. 3), always maintained above the top of the hot legs, and the core was never uncovered. As the primary coolant system pressure and temperature gradually decreased, the flashing phenomenon gradually weakened, the core heat transfer conditions progressively improved, the peak of the maximum fuel cladding outer surface temperature decreased accordingly, and the reactor vessel water level also gradually recovered.

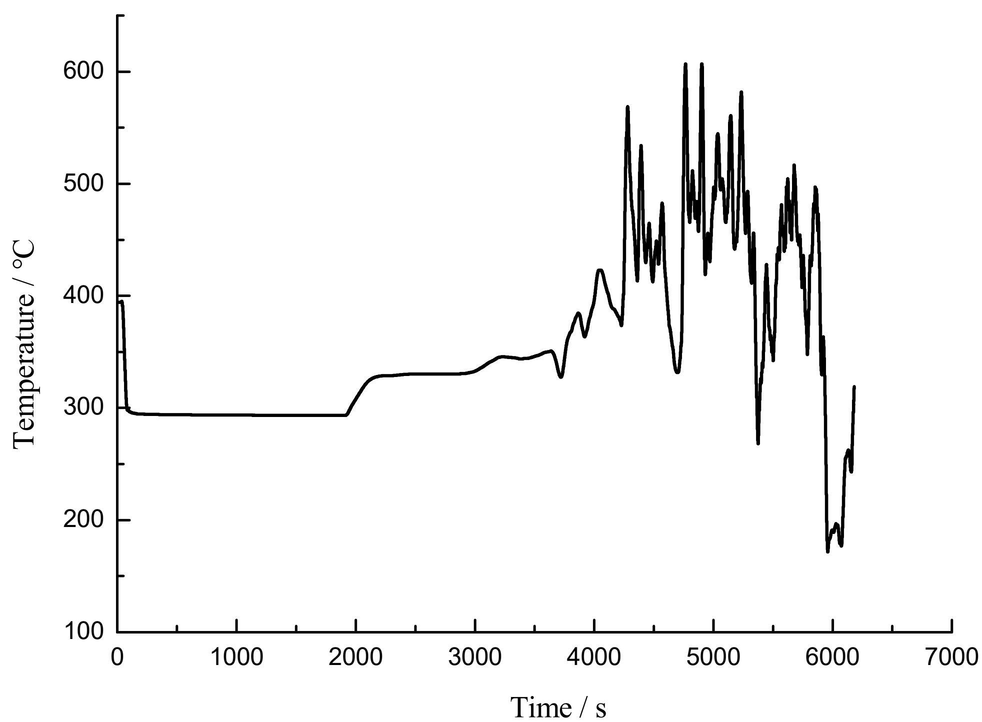

Figure 6: Trend of the maximum temperature on the outer surface of the fuel cladding.

(4) Containment Pressure

The trend of containment pressure is shown in Fig. 7. Before the accident, the containment maintained a slight negative pressure of about 96.6 kPa(a). After the accident started at 50 s, since no fluid was directly discharged into the containment, the containment pressure remained stable. At 3660 s, the operator manually opened all three sets of pressurizer safety valves according to the emergency operating procedures, establishing the feed-and-bleed cooling mode. A large amount of steam-water mixture was discharged through the pressurizer safety valves to the relief tank; when the pressure in the relief tank exceeded the threshold, the rupture disc opened, causing the containment pressure to rise. The variation of containment pressure was jointly affected by the coolant discharge rate and the natural cooling rate inside the containment. During feed-and-bleed cooling, as the primary coolant system pressure and temperature continuously decreased, the energy discharge rate through the pressurizer safety valves gradually reduced. As shown in Fig. 7, at 4107 s the containment pressure reached a peak of 109.4 kPa(a), far below the containment spray system actuation pressure setpoint of 0.24 MPa(a) and the containment design pressure of 0.52 MPa(a).

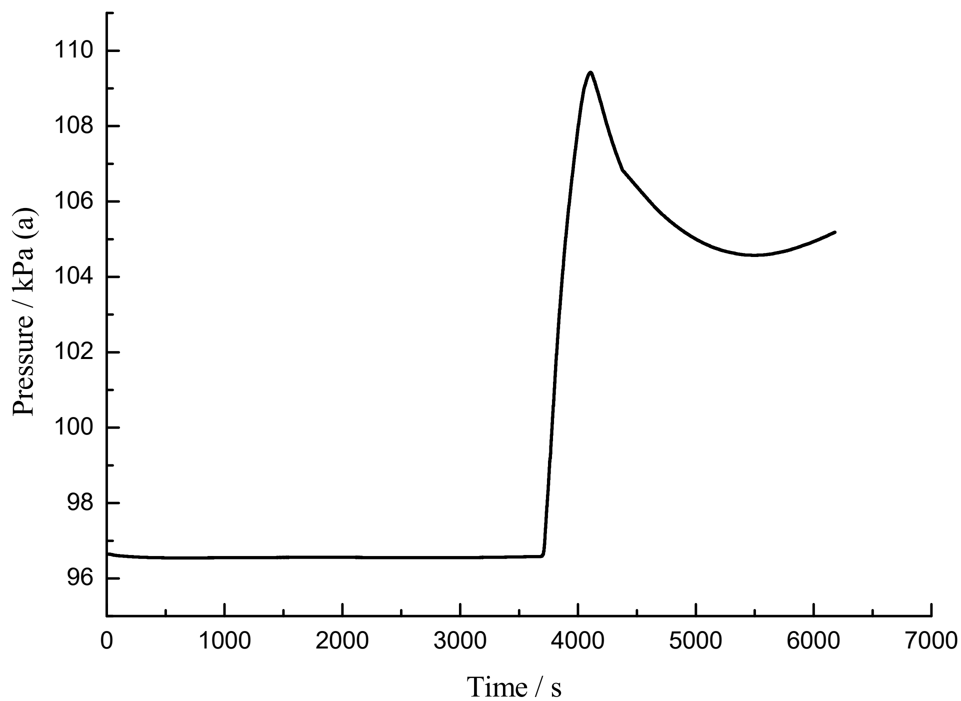

Figure 7: Trend of the containment pressure.

During feed-and-bleed cooling, the pressurizer relief tank pressure trend is shown in Fig. 8. The pressurizer relief tank design pressure is 0.7 MPa(g), the design temperature is 170°C, the rupture disc release pressure setpoint is 0.7 MPa(g), and the discharge capacity is 560 t/h, which is greater than the total discharge capacity of all three sets of pressurizer safety valves. The simulation results show that during the entire transient process, the pressurizer relief tank pressure did not exceed the design pressure, the rupture disc opened as expected, and the integrity of the pressurizer relief tank was not affected.

In the later phase of the accident, when the core conditions satisfied the residual heat removal system entry conditions (5941 s), the operator could connect the residual heat removal system to achieve long-term controlled heat removal from the core. Therefore, the integrity of the containment was not compromised during the entire accident transient.

The above data analysis shows that, under the synergistic intervention of automatic system actions and procedure guidance, the operator successfully brought the core to a safe state by initiating the feed-and-bleed cooling mode. Core safety is ensured: the core ultimately reached and maintained a subcritical shutdown state; about 98 min after the accident, the core state parameters satisfied the conditions for residual heat removal system entry (core outlet coolant subcooled with temperature below 172°C and primary coolant system pressure below 2.7 MPa(g)), the reactor decay heat could be continuously and effectively removed, and the core was able to maintain a safe state; the maximum fuel cladding temperature was about 610°C, far below the safety limit of 1204°C; the minimum reactor vessel water level was about 67.7%, and the core was never uncovered during the entire transient; the maximum core outlet coolant temperature was about 332°C, also below the threshold for severe accident management guideline entry (650°C), thus effectively preventing the accident progression to a severe accident; no significant core damage occurred, no radiological consequences were produced, and the coolable geometry of the core remained intact; the containment pressure peak was 109.4 kPa(a), far below the containment spray system actuation pressure setpoint of 0.24 MPa(a) and the containment design pressure of 0.52 MPa(a), and the containment integrity was not threatened. In summary, all acceptance criteria listed in Section 2.5 were satisfied.

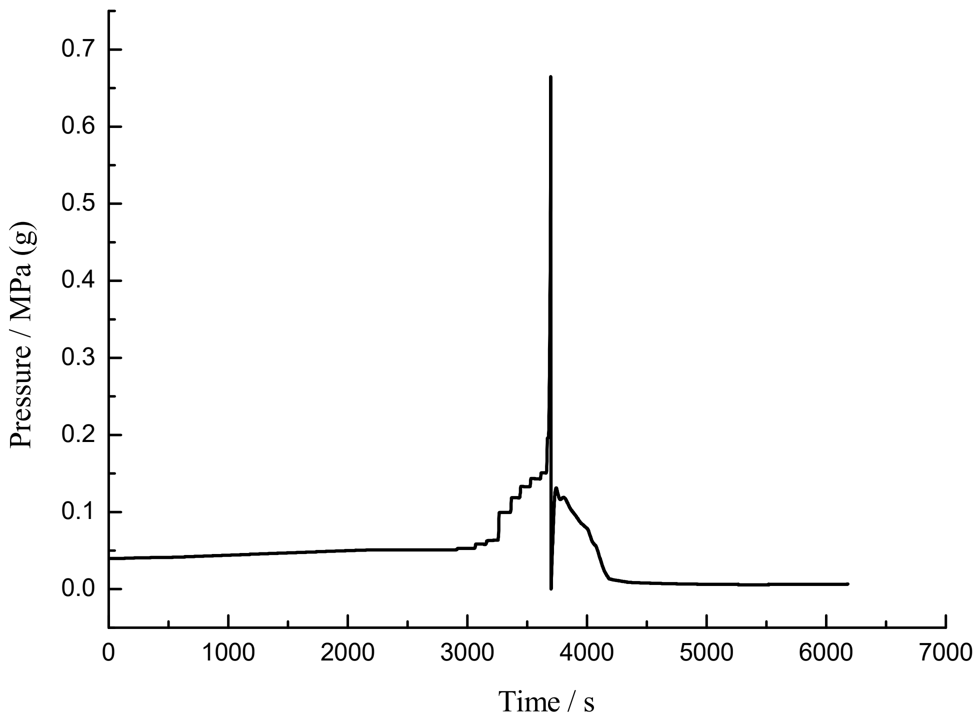

Figure 8: Trend of the pressurizer relief tank pressure.

3.3 Sensitivity Analysis of Feed-and-Bleed Cooling under Different Numbers of Opened Safety Valve Sets

After a total loss of feedwater accident, the secondary side cooling function of the steam generators is gradually lost, the core decay heat cannot be effectively removed, the primary coolant temperature and pressure continuously increase, and the core faces the risk of damage. Initiating feed-and-bleed cooling is the most important mitigation measure under this design extension condition. Its basic principle is to actively discharge the primary coolant by manually opening the pressurizer safety valves, while simultaneously injecting borated water through the safety injection system, forming a "discharge-injection" cycle to remove the core decay heat. The previous verification shows that under automatic system actions and procedure guidance, the operator can successfully avoid core damage by manually opening all three sets of safety valves. However, the pressurizer safety valves may have reduced reliability due to repeated opening and closing during the accident, posing a risk of failing to open. Therefore, this section further investigates the influence of the number of opened safety valve sets (i.e., only two sets or only one set successfully opened) on the accident consequences.

(1) Safety Valve Structure and Reliability Issues

The pressurizer safety valves consist of three sets, each with the same discharge capacity. Their downstream piping converges into a single annular pipe connected to the relief tank. Each set is composed of one pilot valve and one isolation valve in series, both of which are provided with opening and closing pressure setpoints. During normal operation, the pilot valve is closed and the isolation valve is open. The pilot valve is an automatic pilot-operated valve, consisting of a pilot and a main valve. In automatic mode, the pressurizer pressure is transmitted to the pilot, and the upward and downward movement of the pilot piston rod controls the opening and closing of the main valve. In manual mode, the operator can directly control the solenoid coil below the piston rod to operate the main valve; the initiation of feed-and-bleed cooling is an example of this manual mode.

It should be noted that before the operator initiates feed-and-bleed cooling (from 2855 s to 3660 s), the primary coolant system pressure had repeatedly reached the safety valve opening setpoint, causing the safety valves to automatically open and reseat repeatedly, discharging part of the steam-water mixture by means of "overflow" and temporarily relieving the pressure rise. As shown in Fig. 3, the pressure during this stage exhibited a saw-tooth fluctuation, and each safety valve action experienced a process of rapid opening, pressure relief, and reseating. Operating experience at nuclear power plants indicates that after multiple automatic opening and closing cycles, pilot-operated safety valves may experience failure modes such as setpoint drift of the opening pressure, scoring or sticking of the pilot valve sealing surfaces. The failure of the main valve to open in time after the pilot valve opens, and the failure of the main valve to reseat properly after opening, are typical problems encountered in the actual operation of pilot-operated safety valves. Therefore, at the critical moment of initiating feed-and-bleed cooling, it is realistically possible that some safety valve sets may fail to open.

(2) Simulation Setup for Different Numbers of Opened Safety Valve Sets

To investigate the sensitivity of accident consequences to the number of opened safety valve sets, two additional simulations were performed under the same initial conditions: only two sets successfully opened (i.e., one set fails to open), and only one set successfully opened (i.e., two sets fail to open). More complex failure modes, such as partial opening of a valve, were not considered in the simulation, focusing only on the most critical failure form of "whether the valve set can be successfully opened".

(3) Fuel Cladding Temperature Response

The trends of the maximum temperature on the outer surface of the fuel cladding under different numbers of opened safety valve sets are shown in Fig. 9. During feed-and-bleed cooling, regardless of how many safety valve sets are successfully opened, as the primary coolant system pressure rapidly decreases, the local pressure of the core coolant drops below the saturation pressure, and flashing occurs. Vapor bubbles generated by flashing attach to the fuel rod surface, forming a vapor film, which significantly deteriorates the heat transfer coefficient between the fuel and the coolant, causing multiple step-change peaks in the cladding temperature. This temperature oscillation is a typical manifestation of two-phase flow instability.

The fewer the number of opened safety valve sets, the slower the primary coolant system pressure decreases, meaning that the pressure range over which flashing occurs is extended, and the duration of bubble generation and collapse is correspondingly prolonged, thus making the step-change fluctuations of the cladding temperature more persistent. Nevertheless, with only two or one set of safety valves opened, the maximum cladding temperature remains in the range of 600°C–700°C, far below the safety limit of

1204°C for zirconium alloy cladding. This indicates that, in terms of cladding integrity, sufficient safety margin is retained under both of the above conditions.

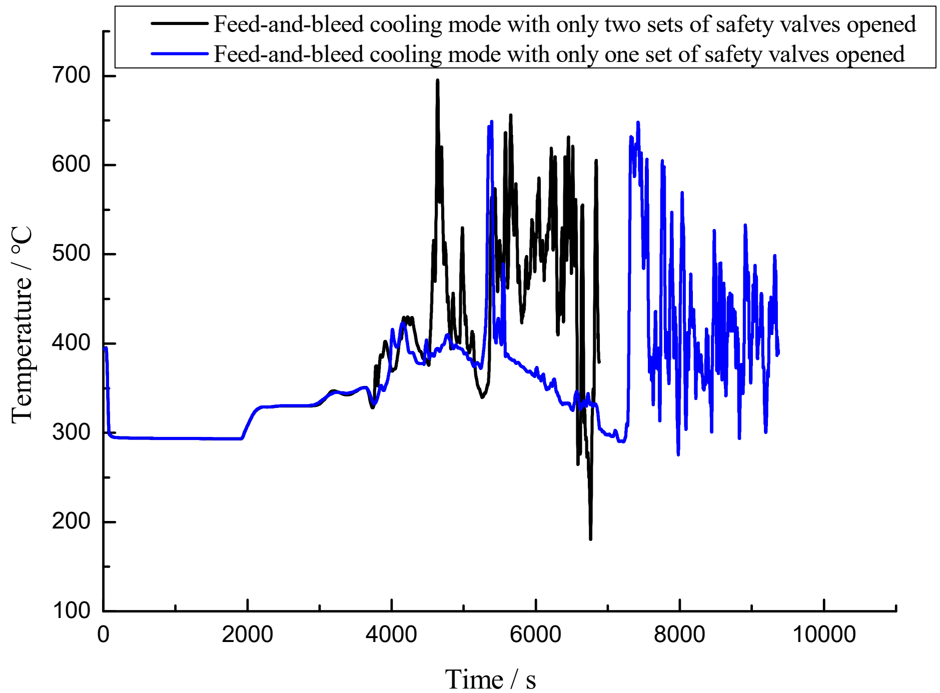

Figure 9: Trend of the maximum temperature on the outer surface of the fuel cladding with different sets of safety valves opened.

(4) Reactor Vessel Water Level and Core Uncovery Risk

Fig. 10 shows the variation of reactor vessel water level under different numbers of opened safety valve sets. Intuitively, the fewer the safety valve sets opened, the smaller the mass flow rate of coolant discharge. With the injection flow characteristics of the safety injection system unchanged, the net loss rate of primary coolant decreases, and consequently the minimum water level in the reactor vessel becomes higher. Specifically, when only two sets of safety valves are opened, the minimum water level is 70.2%; when only one set is opened, the minimum water level is 80.6%, both higher than the 67.7% when all three sets are opened. In all three cases, the water level remains above the top of the hot legs, and the active core region never becomes uncovered during the entire transient. This indicates that when only one set of safety valves is opened, the reactor vessel water level is highest and the core uncovery risk is lowest; however, this advantage comes at the cost of reduced discharge flow, which directly leads to a slower decrease in primary coolant system pressure and thereby affects the timely entry of the residual heat removal system.

(5) Primary Coolant System Pressure Evolution and Residual Heat Removal System Entry Capability

The trends of primary coolant system pressure under different numbers of opened safety valve sets are shown in Fig. 11. Before the initiation of feed-and-bleed cooling, the pressure trend was essentially consistent with that in Fig. 3; after 3660 s, the pressure decrease trends exhibited different patterns. The fewer the safety valve sets opened, the slower the primary coolant system pressure decreased, which is attributed to the gradual reduction in the heat removal capacity of the pressurizer safety valves. When all three sets of safety valves were opened, about 98 min after the accident, the core state parameters satisfied the residual heat removal system entry conditions (core outlet coolant subcooled with temperature below 172°C and primary coolant system pressure below 2.7 MPa(g)). When only two sets of safety valves were opened, the primary coolant system pressure decreased to 1.86 MPa(a) at 6721 s, and the core outlet coolant was subcooled with a temperature of 171°C, satisfying the residual heat removal system entry conditions. Compared with the case with all three sets opened, the time to satisfy the conditions was extended by about 780 s. When only one set of safety valves was opened, the pressure decreased to about 3.58 MPa(a) and then could not steadily decrease further, instead exhibiting a saw-tooth fluctuation in the range of 2.3 MPa(a)–3.7 MPa(a).

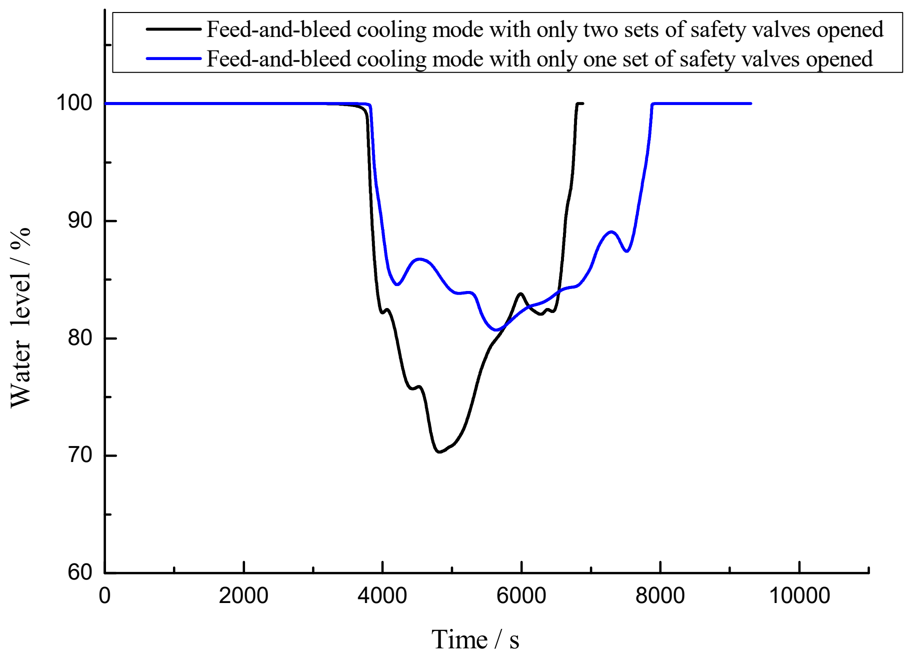

Figure 10: Trend of the reactor vessel water level with different sets of safety valves opened.

Analysis of the cause of the saw-tooth fluctuation: At the initial stage of feed-and-bleed cooling, the primary coolant system pressure was high, the discharge flow rate of a single safety valve set was large, and its heat removal capacity was significantly higher than the core decay heat power, so the pressure decreased continuously and rapidly. As the pressure gradually decreased, the discharge flow rate dropped substantially, and the heat removal capacity decreased accordingly. When the pressure decreased to about 3.58 MPa(a), the heat removal capacity of a single safety valve set tended toward a dynamic balance with the core decay heat power. Owing to the inherent instability of two-phase flow, the phase state and flow rate of the discharged medium continuously fluctuated around the equilibrium point, causing the heat removal capacity to vary, which in turn led the primary coolant system pressure to oscillate above and below the equilibrium point, forming a saw-tooth waveform. This self-sustained oscillation state prevented the primary coolant system pressure from being stably reduced below 2.7 MPa(g).

According to the emergency operating procedures, entry into the residual heat removal system must simultaneously satisfy three conditions: primary coolant system pressure below 2.7 MPa(g), core outlet coolant subcooled, and its temperature below 172°C. When only one set of safety valves was opened, the saw-tooth fluctuation meant that the pressure repeatedly crossed the threshold but could not be stably maintained, and the operator could not safely connect the residual heat removal system. The fundamental goal of the procedures is to bring the unit to a shutdown state under the conditions of residual heat removal system operation—in this state, the primary coolant system pressure is low, core decay heat removal is controllable, and safety margins are sufficient, which is the basis for achieving long-term stable safety. Therefore, when only one set of safety valves was opened, a smooth transition to a safe state during the later phase of the accident was difficult to achieve.

In summary, under this design extension condition, feed-and-bleed cooling permits a single failure of one safety valve set to open (i.e., at least two sets successfully open), but does not permit failure of two sets to open (i.e., only one set successfully open). This conclusion provides a quantitative basis for operator decisions in the event of partial failure of safety valves.

It should be noted that the sensitivity analysis in this paper focuses on the number of opened safety valve sets as the key variable; the uncertainties introduced by factors affecting simulation model accuracy (such as thermal-hydraulic model parameters and boundary conditions) as well as operator action time have not been systematically quantified in this paper. Meanwhile, the simulation results are obtained based on a given platform and specific accident conditions, and the numerical values are affected by model assumptions and other factors. The engineering reference value of this paper is mainly reflected in the revelation of the physical laws of accident evolution and the trends of key parameter responses. The systematic quantification of the above uncertainty factors can serve as a direction for future research.

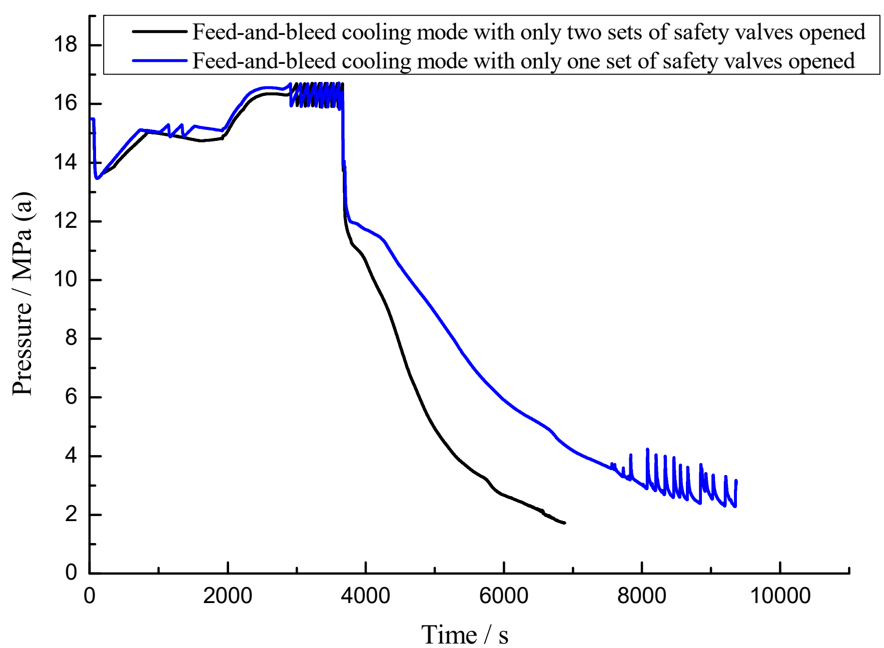

Figure 11: Trend of the primary coolant system pressure with different sets of safety valves opened.

4 Conclusions

(1) Based on a high-fidelity simulation platform, this study performed a full-scope simulation of the design extension condition of "total loss of feedwater" occurring in a CPR1000 unit under full power condition, with operator interventions strictly following the emergency operating procedures. The results show that, under the synergistic effect of automatic system actions and procedure guidance, the operator manually opened all three sets of pressurizer safety valves about 60 min after accident initiation, triggering the safety injection system and establishing the feed-and-bleed cooling mode. About 98 min

after the accident, the core state parameters satisfied the residual heat removal system entry conditions (core outlet coolant subcooled with temperature below 172°C and primary coolant system pressure below 2.7 MPa(g)), and the core was successfully brought to a safe state. All key safety parameters met the acceptance criteria: the maximum fuel cladding temperature was about 610°C, far below the safety limit of 1204°C; the normalized minimum water level in the reactor pressure vessel was 67.7%, and the core was never uncovered during the entire transient; the maximum core outlet coolant temperature was about 332°C, below the severe accident management guideline entry threshold of 650°C; and the containment pressure peak was 109.4 kPa(a), far below the containment spray system actuation pressure setpoint of 0.24 MPa(a) and the containment design pressure of 0.52 MPa(a). The above results verify that the operating CPR1000 units in China possess effective mitigation capability for this design extension condition.

(2) A sensitivity study was performed on the influence of the number of opened safety valve sets during feed-and-bleed cooling. Under the same accident sequence, two additional simulations were conducted assuming that only two sets or only one set of safety valves were successfully opened. When only two sets of safety valves were opened, the time to satisfy the residual heat removal system entry conditions was extended by about 780 s compared with the case with three sets opened, the minimum reactor vessel water level increased to 70.2%, and all safety acceptance criteria were still met. When only one set of safety valves was opened, the heat removal capacity of a single set was insufficient to steadily decrease the primary coolant system pressure below 2.7 MPa(g); the pressure exhibited a saw-tooth fluctuation in the range of 2.3 MPa(a)–3.7 MPa(a), failing to satisfy the residual heat removal system entry conditions and making a smooth transition to a safe state difficult. Therefore, under this design extension condition, when the operator initiates feed-and-bleed cooling, a single failure of one safety valve set to open is permissible (i.e., at least two sets successfully open), but failure of two sets to open is not.

(3) This study quantitatively verifies the inherent safety mitigation capability of similar Generation II and modified Generation II units in China for total loss of feedwater accidents, and provides an engineering reference for optimizing the feed-and-bleed cooling operational strategy. It should be noted that the conclusions of this paper are drawn based on a given simulation platform and specific operating conditions, and their engineering reference value is mainly reflected in the revelation of physical laws and parameter response trends; the systematic quantification of uncertainty factors requires further investigation in future research.

Acknowledgement: None.

Funding Statement: The authors received no specific funding for this study.

Author Contributions: The authors confirm contribution to the paper as follows: Bo Zhang was responsible for experimental analysis, data processing, and content writing. Zhenhua Zhang was responsible for the overall planning and design of the study, literature investigation, and manuscript revision. All authors reviewed and approved the final version of the manuscript.

Availability of Data and Materials: The data that support the findings of this study are available from the corresponding author upon reasonable request and with the permission of the data owner.

Ethics Approval: The study did not involve any human participants, human biological samples, or animal experiments. No sensitive personal privacy data and no ethical-related risky behaviors were involved in the whole process of experimental modeling and data collection. Therefore, ethical approval and informed consent are not required for this research work.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. International Atomic Energy Agency. Design extension conditions and the concept of practical elimination in the design of nuclear power plants. Vienna, Austria: International Atomic Energy Agency; 2024. [CrossRef].
2. International Atomic Energy Agency. Safety of nuclear power plants: design. Vienna, Austria: International Atomic Energy Agency; 2016.
3. Ramezani A, Nazari T, Rabiee A. Total loss of feedwater accident for VVER-1000/V446 NPP with operator action. Int J Nucl Energy Sci Technol. 2018;12(4):351. [CrossRef].
4. Wang G, Zheng C, Zhang Y, Wu P, Chen F. Simulated safety analysis of a total loss of feedwater accident in the steam generator of CPR1000 nuclear power plant. Front Energy Res. 2024;12:1252320. [CrossRef].
5. International Atomic Energy Agency. The fukushima daiichi accident: report by the director general. Vienna, Austria: International Atomic Energy Agency; 2015. [CrossRef].
6. Xu H, Zhang B. Diverse and flexible coping strategy for nuclear safety: opportunities and challenges. Energies. 2022;15(17):6275. [CrossRef].
7. Zubair M. Investigation of loss of feedwater (LOFW) accident in the APR-1400 using fault tree analysis. Sci Technol Nucl Install. 2022;2022:4666161. [CrossRef].
8. Zubair M, Samir Abushady M, Hussain Alzarooni A. Classification of LOCA events in pressurized water reactors using neural networks. Ann Nucl Energy. 2026;227:111909. [CrossRef].
9. World Nuclear Industry Status Report. The WNISR interactive dataviz—world nuclear power reactors 1951–2026: 75 years of nuclear power (as of 4 July 2026) [Internet]. Rome, Italy: World Nuclear Industry Status Report; 2026 [cited 2026 Jul 8]. Available from: https://dv.worldnuclearreport.org/.
10. Chen XM, Nie JG, Qu J, Yuan MC, Zhao MM. Analysis of the development status of third generation nuclear power technology. Dev Innov Mach Electr Prod. 2025;38(5):214–8. (In Chinese). [CrossRef].
11. Xing J, Song D, Wu Y. HPR1000: advanced pressurized water reactor with active and passive safety. Engineering. 2016;2(1):79–87. [CrossRef].
12. Qing T, Liu Z, Zhang L, Tang Y, Hu H, Chen S. Cognitive behavioral model of an operation crew in the main control room of a nuclear power plant based on a state-oriented procedure. Processes. 2022;10(2):182. [CrossRef].
13. Bae YK. An evaluation of operator's action time for core cooling recovery operation in nuclear power plant. J Korean Soc Saf. 2012;27(5):229–34. [CrossRef].
14. China Atomic Energy Authority. Nuclear power full-scope verification simulator project completes final acceptance. Beijing, China: China Energy News; 2016. (In Chinese).
15. Lorusso P, Polidori M, Del Nevo A, Lombardo C, Martelli D, Meloni P, et al. State-of-the-art review of the T/H system codes RELAP5 for HLM applications. Nucl Eng Des. 2023;414:112627. [CrossRef].
16. Ringane TP. Developing a full core model of the North Anna Reactor using SCALE 6.2.3, NESTLE and MCNP 6.2 [master's thesis]. Potchefstroom, South Africa: North-West University; 2022.
17. WSC, Inc. Accuracy enhancement of nuclear power plant simulators utilizing high accuracy simulation predictions: Phase II-A. Frederick, MD, USA: WSC, Inc.; 2024. Report No.: DOE-WSC-18915. [CrossRef].
18. International Atomic Energy Agency. Deterministic safety analysis for nuclear power plants. Vienna, Austria: International Atomic Energy Agency; 2019.
19. Kral P. Evolution and implementation of the design extension conditions (DEC) concept: assessment of selected events. In: Proceedings of the 2018 26th International Conference on Nuclear Engineering (ICONE26); 2018 Jul 22–26; London, England. [CrossRef].
20. GB/T 40860-2021. Analysis requirements for design extension conditions of pressurized water reactor nuclear power plants. Beijing, China: State Administration for Market Regulation; 2021. (In Chinese).
21. Zhang J, Havet M, Zheng J, Bousbia Salah A, Ševeček M, Kral P, et al. Analyses of design extension conditions without significant fuel degradation for operating nuclear power plants: an OECD/NEA review. Nucl Eng Des. 2024;425:113320. [CrossRef].