



Original Article

Level 1 probabilistic safety assessment of supercritical–CO₂–cooled micro modular reactor in conceptual design phase

Eunseo So, Man Cheol Kim*

Department of Energy Systems Engineering, Chung-Ang University, 84 Heukseok-ro, Dongjak-gu, Seoul, 06974, Republic of Korea

ARTICLE INFO

Article history:

Received 28 February 2020

Received in revised form

16 June 2020

Accepted 22 July 2020

Available online 8 August 2020

Keywords:

Advanced reactor

Probabilistic safety assessment

Initiating event category

Event tree analysis

Fault tree analysis

Passive safety system

ABSTRACT

Micro reactors are increasingly being considered for utilization as distributed power sources. Hence, the probabilistic safety assessment (PSA) of a direct supercritical–CO₂–cooled fast reactor, called micro modular reactor (MMR), was performed in this study; this reactor was developed using innovative design concepts. It adopted a modular design and passive safety systems to minimize site constraints. As the MMR is in its conceptual design phase, design weaknesses and valuable safety insights could be identified during PSA. Level 1 internal event PSA was carried out involving literature survey, system characterization, identification of initiating events, transient analyses, development of event trees and fault trees, and quantification. The initiating events and scenarios significantly contributing to core damage frequency (CDF) were determined to identify design weaknesses in MMR. The most significant initiating event category contributing to CDF was the transients with the power conversion system initially available category, owing to its relatively high occurrence frequency. Further, an importance analysis revealed that the safety of MMR can be significantly improved by improving the reliability of reactor trip and passive decay heat removal system operation. The findings presented in this paper are expected to contribute toward future applications of PSA for assessing unconventional nuclear reactors in their conceptual design phases.

© 2020 Korean Nuclear Society, Published by Elsevier Korea LLC. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

1. Introduction

Recent years have witnessed growing interest in micro reactors that can be used as distributed power sources in remote areas. Kilopower [1] of National Aeronautics and Space Administration (NASA), Megapower [2] of Los Alamos National Laboratory (LANL), and eVinci™ micro reactor [3] of Westinghouse are a few examples of such reactors. In Korea, the micro modular high-temperature gas-cooled reactor (MiHTR) [4] is a micro reactor under development by Korea Atomic Energy Research Institute (KAERI). The development of MiHTR introduced several advanced concepts such as a long-life core without refueling and passive decay heat removal (PDHR) using the reactor cavity cooling system [5].

Another micro reactor under development is the micro modular reactor (MMR) [6] by the Korea Advanced Institute of Science and Technology. MMR is a direct supercritical–CO₂–(S–CO₂)–cooled fast reactor producing powers of 36 MWth and 12 MWe. As shown in Fig. 1, the entire system including the turbomachinery is

enclosed in the inner and outer containments filled with CO₂ at 5 MPa and 1 MPa, respectively [7]. It is designed to be a distributed power source in remote areas and is small and light enough for ground transportation. It has many innovative design features such as a long-life (20 years) core, autonomous load-following operations, and a PDHR system. MMR is designed to have high safety and reliability as it comprises passive safety systems and a pressurized inner containment filled with CO₂.

For design optimization and safety enhancement of MMR, several deterministic safety analyses were performed. The safety of MMR during a small loss of coolant accident (SLOCA) scenario was analyzed with different break locations, and the break at the compressor outlet was found to have the smallest safety margin [8]. The accident mitigation capability was also analyzed considering the reactivity coefficients such as the fuel temperature coefficient (FTC) and coolant temperature coefficient (CTC) under a SLOCA without scram scenario [9]. Transient analyses were performed for a loss of coolant accident without scram and loss of load without scram assuming the failure of one PDHR train [10].

Thus, PSA was performed for further enhancing safety through design improvements. It should be noted that the knowledge and

* Corresponding author.

E-mail address: charleskim@cau.ac.kr (M.C. Kim).

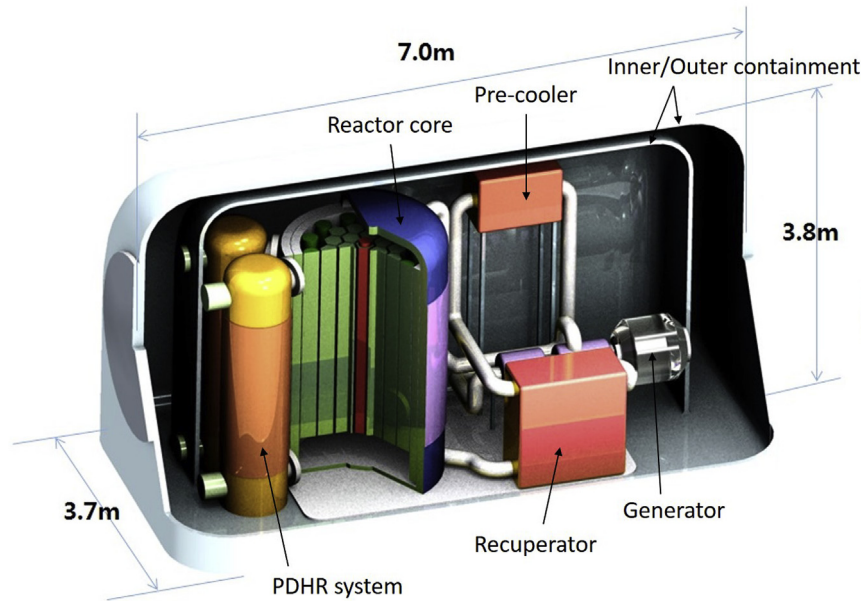


Fig. 1. Layout of MMR (concept design) [6].

experience regarding PSA are primarily based on water-cooled power reactors. Thus, this paper describes our findings during PSA of an S-CO₂-cooled micro reactor in its conceptual design phase. Level 1 PSA for internal events during full-power operations is helpful in identifying significant failure scenarios and design weaknesses. Fig. 2 shows the procedure followed for PSA of MMR. Section 2 provides a brief overview on the safety features of MMR. Section 3 describes how the initiating events were derived based on

literature survey and a comparison of the initiating or transient event list of other reactor types. Section 4 describes how event trees were developed and how success criteria were determined based on thermal-hydraulic transient analyses of the initiating events. Section 5 describes how fault tree analysis was performed. Section 6 presents the results and discussions, and Section 7 provides the conclusions drawn from the findings of this study.

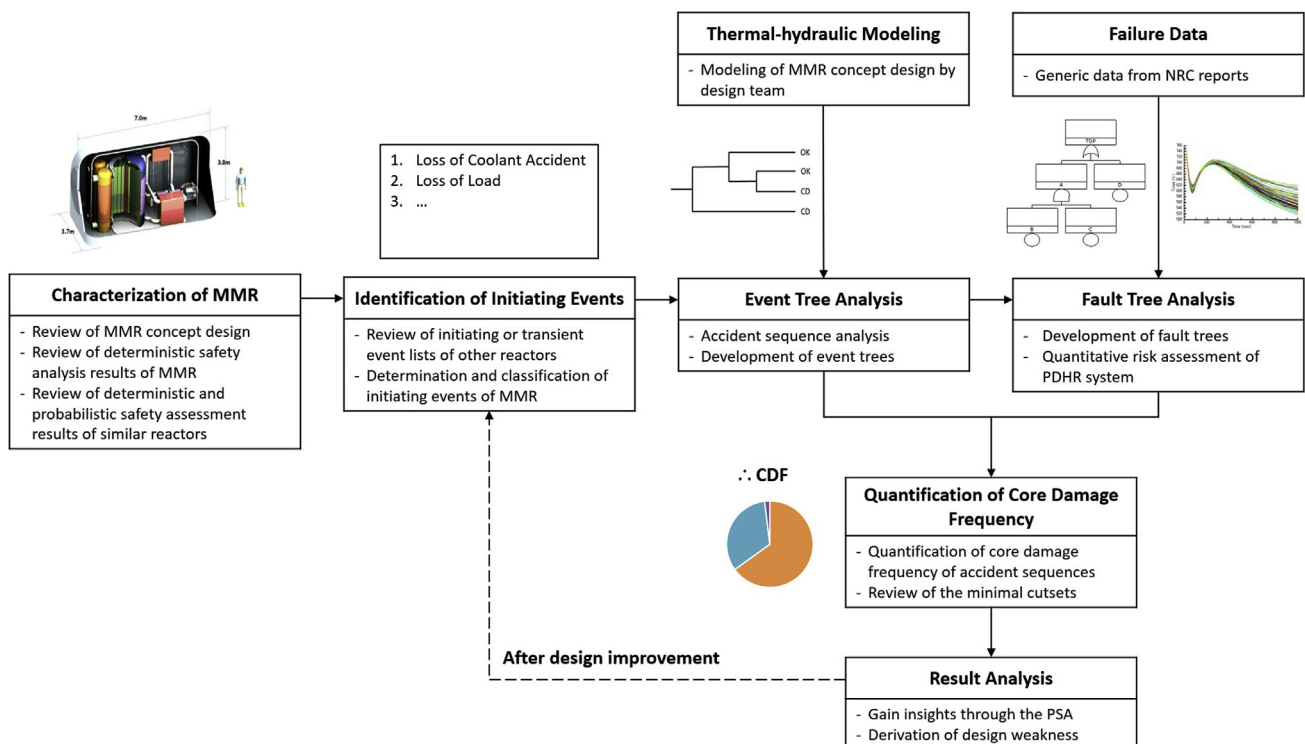


Fig. 2. PSA procedure for MMR.

2. Safety features of MMR

When electrical power is available in normal operation, MMR can control the reactor power autonomously for load-following operations, and electrically driven air fans can remove heat to the ambient air through the precooler [10]. If electrical power is not available, the load-following operations cannot be performed and the active cooling system cannot operate; thus, only the four safety features presented in Table 1 are available for mitigating accidents or transient situations. The safety features of MMR are based on only conceptual designs and detailed designs have not been developed yet.

Reactor trip means the insertion of negative reactivity to shut down the reactor. It has two activation signals: high pressure and low pressure of the primary system. The highest pressure in the primary system can be measured at the compressor outlet. The reactor trip signal also disconnects the generator from the external grid to protect the vulnerable grid system in remote areas from unstable turbine rotational speeds [10]. After grid disconnection, the air fans and CO₂ circulator in the active cooling system will be unavailable owing to the loss of electrical power.

The remaining three safety features are the opening of valves (the green dotted lines in Fig. 3). Once opened, the valves in the safety features remain open and the valve opening fractions are not controlled. For the inventory makeup of the primary system with CO₂ in the inner containment, the feed valve passively opens when the pressure at the compressor inlet, where the feed valve is located, becomes lower than the containment pressure. The venting valve opens to protect the primary system from overpressure. For long-term decay heat removal, the PDHR system removes decay heat from the core and delivers it to the ambient air via natural circulation. The PDHR system consists of two redundant trains, each of which has 100% decay heat removal capability.

Activation signal and power supply by small batteries are required to activate some of the safety features such as the venting valve and PDHR valves. The activation setpoint and functions of the four safety features considered in the accident mitigation process are presented in Table 1.

As MMR might be located in remote areas, we excluded the recovery of the external power source and human actions for accident mitigation. During transient analyses to develop event trees, described in Section 4, we assumed that the four safety features may fail to operate during accident mitigation. The success and failure of safety features were considered during the thermal-hydraulic transient analysis and development of the event trees.

3. Initiating event categories

One of challenges in the PSA for a reactor in its conceptual design phase like MMR is the identification of initiating events. Even though the review of such events considered in the safety analysis and PSA for light water reactors (LWRs) and in the safety analysis of plants with similar designs [11–13] are helpful, the lack of experience in performing PSA of new reactor types makes it difficult for PSA analysts to derive a detailed list of initiating events.

Therefore, initiating event categories were first roughly established and then the severest initiating event was selected as

the representative one in each initiating event category. Furthermore, the initiating events in the same category are reviewed, and the frequencies of initiating events relevant to the MMR are summed and used as the frequency of the representative initiating event for the category. For example, a large LOCA with a break size of 100 in² is selected as the representative initiating event for the LOCA category, and the frequencies of small, medium, and large LOCAs are summed and used as the frequency for this LOCA. This approach produce more conservative results compared to the approach with detailed initiating events; however, the approach adopted in this study is more appropriate under situations where information on the reactor design and possible accident sequences is limited.

Referring to IAEA-TECDOC-719 [12] and WASH-1400 [14], initiating event categories were derived as follows:

- Loss of coolant accidents (LOCAs)
- Reactor vessel rupture (RVR)
- Transients involving loss of load (LOL)
- Transients involving loss of the power conversion system (PCS)
- Transients with the PCS initially available.

Fig. 4 presents the classification scheme for initiating events. Initiating event categories are approximately grouped into LOCA and transient categories. The difference between LOCAs and RVR lies in the effectiveness of the safety features in mitigating the accident. As shown in Fig. 3, pipe lines of the reactor coolant (supercritical-CO₂) originate from the reactor; pass through the turbine, recuperator, precooler, and compressor; and finally end back at the reactor. A break in any of these pipe lines may lead to a LOCA. Transients were divided into three categories depending on whether offsite power and PCS are available. The five initiating event categories are expected to exhaustively cover all relevant internal initiating events considered in PSA studies.

4. Event tree analysis

To identify success criteria for the branches in the event trees, transient analyses are necessary. For MMR, transient analyses were performed using GAMMA + [15] code. GAMMA + code was initially developed by KAERI for the design and safety analysis of very-high-temperature gas-cooled reactors (VHTRs). The MMR design team modified the GAMMA + code by introducing S–CO₂ properties. For event tree analysis, event trees were developed using AIMS-PSA [16] code.

Event trees describe accident mitigation using the safety features of MMR. Event trees were developed based on transient analyses performed considering the success and failure of safety features. Safety limits were assigned for four plant parameters and are presented in Table 2. We analyzed the results and identified whether the properties exceeded the safety limits or not. If one of the four plant parameters exceeded its associated safety limit, we conservatively assumed that the core or system of MMR might be damaged.

Table 1
Safety features of MMR.

Safety features	Setpoints of activation	Functions
Reactor trip	$P_{\text{comp,out}} > 21.13 \text{ MPa}$; $P_{\text{comp,out}} < 16.08 \text{ MPa}$	Protection from excess core power
Venting valve opening	$P_{\text{comp,out}} > 21.13 \text{ MPa}$	Protection from primary system overpressurization
Feed valve opening	$P_{\text{comp,in}} < P_{\text{cmt}}$	Inventory makeup of primary system
PDHR system operation	$P_{\text{comp,out}} < 16.08 \text{ MPa}$	Long-term decay heat removal

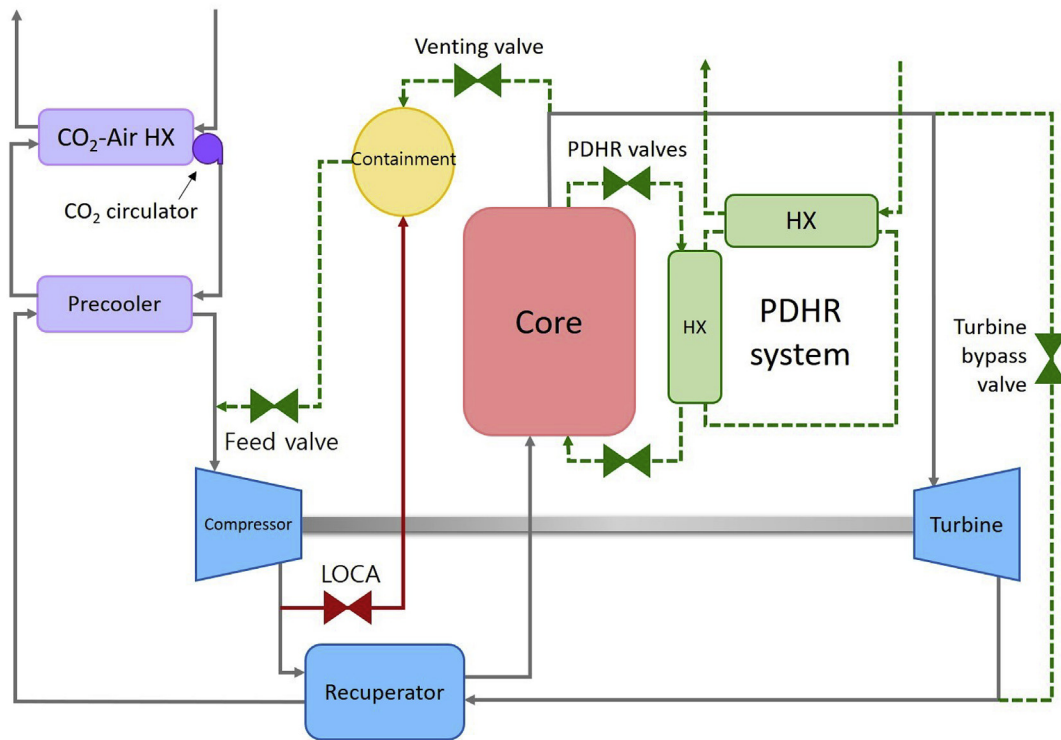


Fig. 3. Schematic of MMR

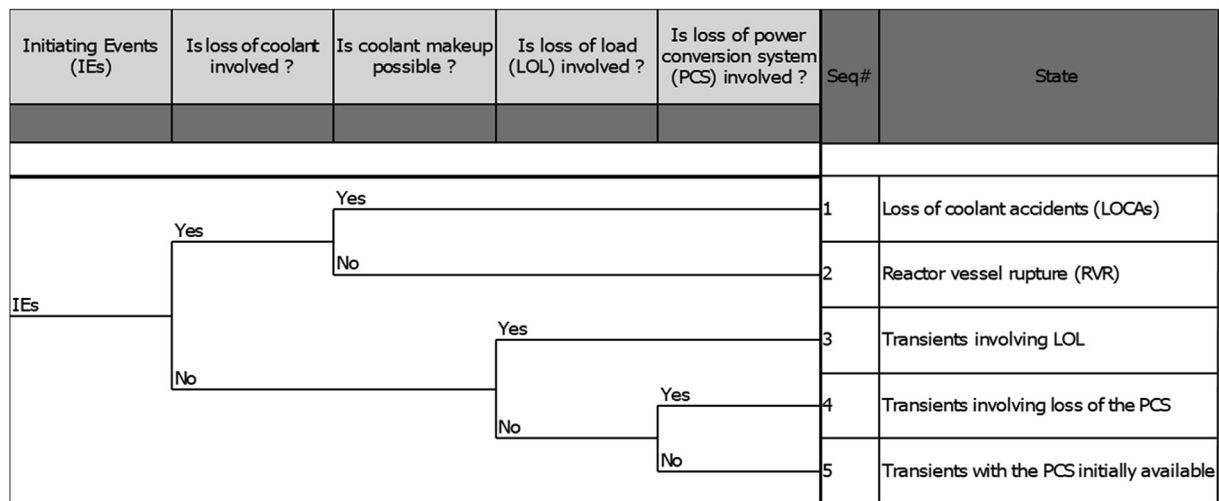


Fig. 4. Classification scheme for initiating events.

Table 2
Safety limits considered in transient analysis [10].

Properties	Safety limits
Fuel centerline temperature	2507 °C
Cladding temperature	1200 °C
Primary system coolant temperature	676 °C
Primary system pressure	24 MPa

4.1. LOCAs

A LOCA induces rapid loss of inventory, and it is generally included in the safety analyses of most reactor types. MMR has a

feed valve and CO₂-filled containment to passively make up the inventory of the primary system without any electrical power.

During PSA for LWRs, LOCAs are grouped into three to five categories depending on break sizes. In determining such different break size categories, different success criteria for inventory makeup by the safety injection system or emergency core cooling system play important roles. During PSA for MMR, the success criterion for inventory makeup was the opening of the feed valve regardless of break sizes. Therefore, LOCAs with different break sizes can be grouped into a single category. This conclusion is consistent with previous transient analysis results involving different break sizes 0.064516 m² and 0.00064516 m² (100 in² and 1 in²) [7].

A large LOCA with a break size of 100 in^2 was selected as the representative initiating event of the LOCA category. This break size of 100 in^2 has also been adopted for conservation analyses in previous studies [7,10]. Additionally, the break size of 100 in^2 is more conservative than the large LOCA break size of APR1400, which is equal to 71.3 in^2 (0.046 m^2). Fig. 5 shows the change in the compressor inlet pressure, compressor outlet pressure, and containment pressure after the large LOCA occurred at 10 s. We assumed that the LOCA occurred at the compressor outlet where the pressure is the highest in the primary system. As the coolant leaks out from the primary system, the pressure at the compressor outlet decreases rapidly; then the reactor trip signal is generated and the PDHR system is activated by opening the PDHR valves at 16.08 MPa. The generator would be decoupled from the grid, and the air fans and CO_2 circulator would stop working owing to the loss of electrical power. If the compressor outlet pressure drops below the containment pressure, the feed valve opens for inventory makeup of the primary system. The activation signals were generated in less than 10 s after the large LOCA occurred owing to rapid changes in the primary system pressure. Fig. 6 depicts the change in the temperatures of the fuel centerline, cladding, and coolant.

In LOCA scenarios, three safety features contribute to the accident mitigation process: reactor trip, feed valve, and PDHR system. We performed transient analyses using combinations of the safety feature failures. Fig. 7 shows the event tree for LOCA developed based on the results of the transient analyses. In Fig. 7, OK means that no safety limit is exceeded and CD means that any of the safety limits such as the peak cladding temperature (PCT) limit and coolant temperature limit is exceeded.

When the reactor trip failed, we observed that the coolant temperature limit was exceeded and hence conservatively assumed core damage. In addition, when the feed valve failed to open, we conservatively assumed core damage because no other safety features were provided for inventory makeup of the primary system. When both trains of the PDHR system are not available, PCT exceeds the safety limit, and hence core damage can be expected.

4.2. RVR

As a special case of LOCA, RVR needs to be considered. As in most PSA studies, we assumed that RVR directly results in core damage without considering any accident mitigation process.

4.3. Transients involving LOL

Transients involving LOL are those transients in which the NPP loses the connection between the generating unit and the grid and

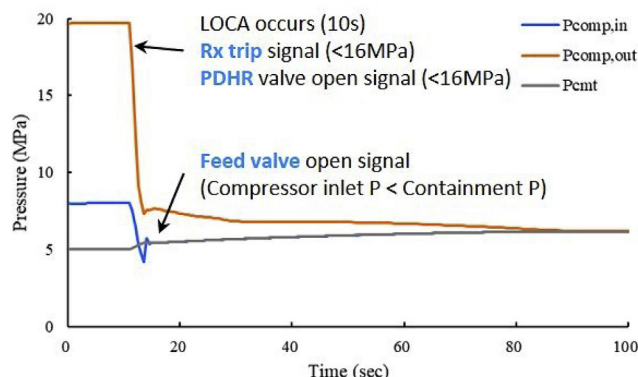


Fig. 5. Pressures and accident mitigation process during LOCA.

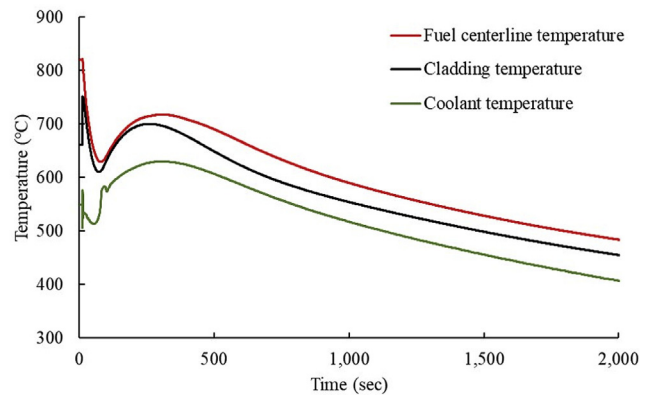


Fig. 6. Temperature change during LOCA.

the NPP is not able to transmit power to the grid [17]. In a remote area where the grid is not able to provide electrical power to the NPP, LOL is synonymous with loss of offsite power (LOOP). In PSA for LWRs, LOOP is one of most widely applied common cause initiators; it not only induces reactor shutdown but also simultaneously disables one or more safety features for accident mitigation.

LOL was selected as the representative initiating event for the transients involving LOL category. LOL is an important initiating event for MMR because MMR is likely to be installed in remote areas where the electrical power grid may not be stable. LOL causes disconnection of the generator from the grid, and hence the air fans and CO_2 circulator would lose electrical power. Thus, operation of the PDHR system is required for decay heat removal.

Fig. 8 shows the changes in the compressor inlet pressure, compressor outlet pressure, and containment pressure after an LOL occurs. After the generator is disconnected from the grid, the turbine rotational speed may increase; hence, the compressor, which is on the same shaft as the turbine, may rotate faster, resulting in higher pressure at the compressor outlet. The reactor trip signal and venting valve opening signal were generated at 21.13 MPa, and then the primary system pressure decreased rapidly owing to the opened venting valve. The PDHR valve opening signal was generated when the primary system pressure decreased below 16.08 MPa. The turbine bypass valve also opened if the turbine rotational speed exceeded 110% of its nominal speed. Moreover, we found that the activation signals were generated in less than 10 s after the occurrence of the LOL owing to rapid changes in the primary system pressure.

In LOL scenarios, all the following four safety features contribute to the accident mitigation process: reactor trip, venting valve, feed valve, and PDHR system. Transient analyses were performed considering the combinations of their failures. Fig. 9 shows the event tree for LOL developed based on the results of the transient analyses. The MMR features drum-type control elements for reducing the core height by eliminating axial movement and a secondary (shutdown) control rod, which is passively inserted into the core via gravity for reactor shutdown. Although reactor shutdown achieved via the secondary control rod is expected to be highly reliable, a failure in the reactor trip is considered in the event tree in order to account for possible mechanical failures in the secondary (shutdown) control rod.

When the reactor trip is successfully performed, the operation of at least one train of the PDHR system is required to successfully mitigate the accident. However, when the reactor trip fails, three safety features are required to successfully operate to avoid exceeding the safety limits and hence successfully mitigate the

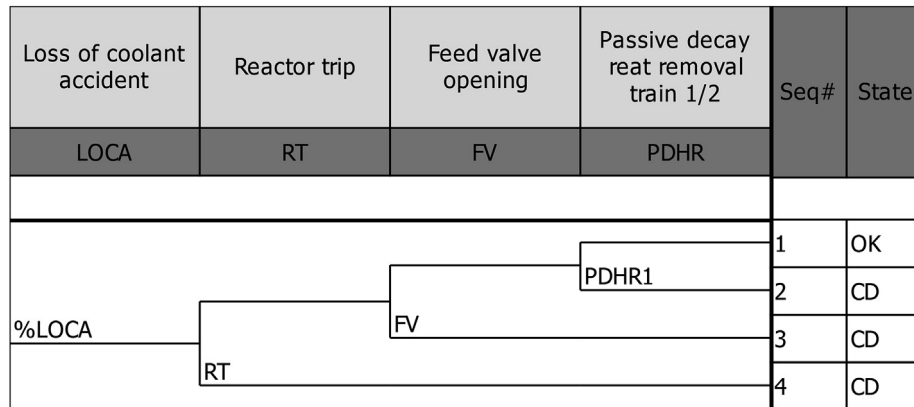


Fig. 7. Event tree for LOCA.

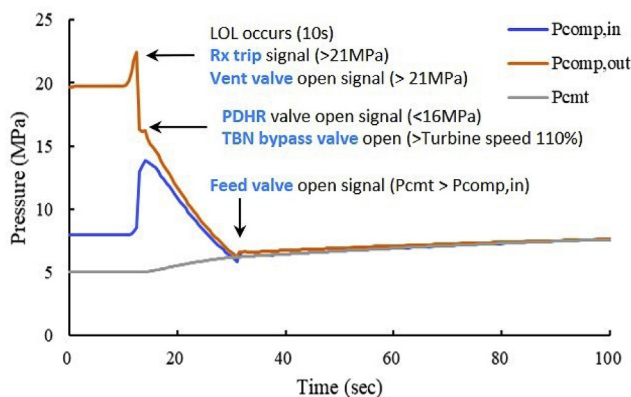


Fig. 8. Pressures and accident mitigation process during LOL.

accident. When the failure of venting valve opening was accompanied by the reactor trip failure, the coolant temperature and primary system pressure exceeded the safety limits. When the failure of feed valve opening was accompanied by the reactor trip failure, the coolant temperature exceeded the safety limit. Failure of the PDHR train system accompanied by the reactor trip failure would also result in core damage.

4.4. Transients involving loss of the PCS

Transients involving loss of the PCS are those in which the power generated in the core cannot be transported to normal heat sink. In PSA for LWRs, the loss of the PCS may include closure of the main steam isolation valves or loss of condenser vacuum.

Loss of heat sink (LOHS) was selected as the representative initiating event for transients involving loss of the PCS category. If electrical power is available in MMR, residual heat can be removed to the ambient air by the active cooling system including the pre-cooler, CO₂ circulator, and CO₂–air heat exchanger. LOHS can result from the malfunction of mechanical components or insufficient heat transfer in the pre-cooler or CO₂–air heat exchanger.

Fig. 10 shows the event tree for LOHS developed based on the results of the transient analyses. When LOHS occurs, reactor trip and PDHR system operation are required. We conservatively assumed that failure of either the reactor trip or PDHR system operation could result in core damage.

4.5. Transients with the PCS initially available

Transients with the PCS initially available are those transients in which both the load and PCS are available. Such events are normally called general transients (GTRNs). When a GTRN occurs, reactor trip followed by PDHR system operation is needed to mitigate the accident. Failure in any of the two could result in core damage. Fig. 11 shows the event tree for GTRNs.

The proposed scheme of classifying initiating events into five categories is expected to be applicable to all reactor types, including the advanced non-LWRs in their conceptual design phase. As the design of the MMR results in identical accident sequences, the same event tree is applicable to transients both with and without the PCS; however, this does not necessarily imply that the initiating event categories should be merged together. In the PSA models of LWRs, different initiating events, especially transients, frequently exhibit similar accident sequences; therefore, these initiating events are modeled using identical event trees.

5. Fault tree analysis and quantification

For quantifying the core damage frequency (CDF), the initiating event frequencies and component reliability data need to be reflected. Limited initiating event frequency and component reliability data pertaining to the MMR are available in literature. The most similar available initiating event frequency and component reliability data applicable to the MMR are the generic data for LWRs such as NUREG-1829 [18], NUREG/CR-5750 [19], and NUREG/CR-6928 [20], although the types of components or operating conditions may differ. Table 3 and Table 4 present the initiating event frequency data and the important component reliability data used for the PSA of the MMR, respectively. The component reliability data from NUREG/CR-6928 (2015 update) are used. For fault tree development and quantification, we used AIMS-PSA [16] and FTREX [21] codes.

As mentioned in Section 4, four safety features are available during accident mitigation processes of MMR. With no safety-grade electrical power system, the small batteries are the only electrical power source after grid disconnection. Each safety feature consists of simple operating mechanisms. For example, the feed valve is a check valve that does not need any power supply or activation signal. Therefore, the failure of the feed valve was modeled as a basic event. Reactor trip requires an activation signal, and therefore, failure of the reactor trip was modeled with three basic events, namely mechanical failure, signal failure, and power supply failure for signal generation. If a detailed design for the reactor protection

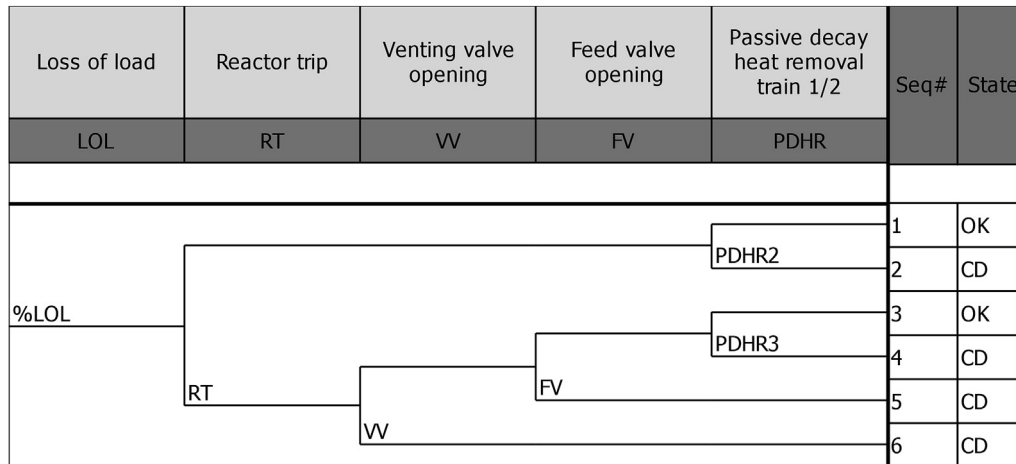


Fig. 9. Event tree for LOL.

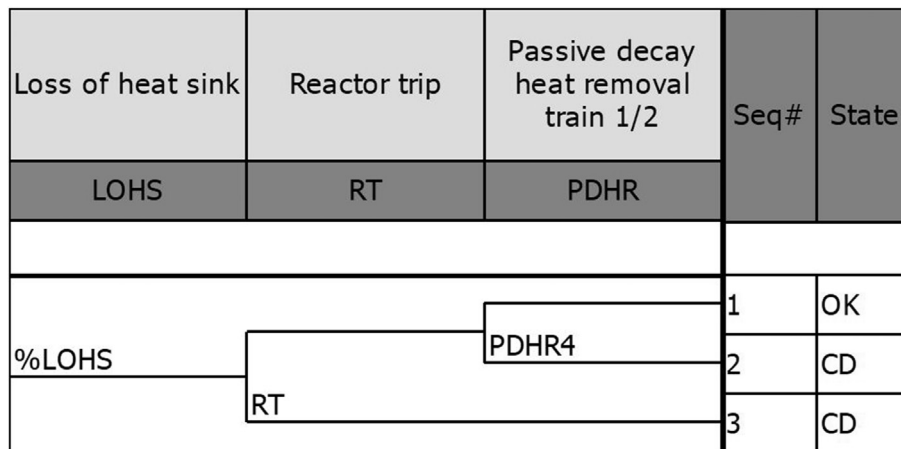


Fig. 10. Event tree for LOHS.

Table 3

Initiating event frequency data used for PSA of MMR.

Initiating event category	Frequency	Source
LOCA	1.9E-3	NUREG-1829
RVR	2.9E-8	NUREG-1829
Transients involving LOL	1.10E-2	NUREG/CR-6928 (2015 update)
Transients involving loss of the PCS	4.82E-2	NUREG/CR-6928 (2015 update)
Transients with the PCS initially available	6.49E-01	NUREG/CR-6928 (2015 update)

Table 4

Important component reliability data used for PSA of MMR.

Event	Failure probability/rate	Unit
Feed valve fails to open	9.25E-06	
Venting valve fails to open	4.21E-04	
PDHR valve fails to open	4.21E-04	
Sensor/Transmitter (pressure) fails to operate on demand	1.17E-04	
PDHR heat exchanger plugging/heat transfer	3.85E-07	h ⁻¹
Shutdown rod drive fails to operate/insert rod	1.54E-07	h ⁻¹
Battery (DC) fails to operate	3.72E-07	h ⁻¹

system is developed, a more detailed fault tree for analyzing signal failure can also be developed.

Fig. 12 shows the fault tree for the PDHR system. The PDHR system has two redundant trains and each one has two PDHR valves and two heat exchangers. Common cause failures (CCFs) were considered for the valves and heat exchangers under the same operating condition. The alpha factor model was used for the CCF analysis, with common cause component groups (CCCGs) comprising two components (CCCG = 2). Failure of natural circulation in the PDHR system due to weak driving forces was also modeled in the fault tree; the failure probability was estimated by considering uncertainties in plant and environmental parameters such as the inlet air temperature and pressure of the PDHR system (see Table 5).

Based on the review of existing methods for reliability analysis of passive systems such as reliability evaluation of passive safety system (REPAS) [22], reliability methods for passive safety functions (RMPS) [23], and assessment of passive system reliability (APSRA) methodology [24], we developed a procedure for reliability analysis of passive systems and applied it for risk assessment of the PDHR system. The failure probability of the natural circulation of PDHR was determined from the probability distributions of PCT and CET, which were determined through the probability distributions of physical parameters (such as the inlet air temperature and the pressure of the PDHR system) and thermal-hydraulic models. The probability distributions of physical parameters were determined from literature survey, and one-hundred samples were generated by MOSAIQUE [25] code using the Latin-hypercube sampling (LHS) [26] method. None of the thermal-hydraulic analyses results exceeded the safety limits of PCT and core exit temperature (CET) of coolants, as shown in Fig. 13; hence, we applied

the exceedance probability model [27] assuming that the thermal-hydraulic analyses results of the PCT or and CET follow normal distributions. Based on the thermal-hydraulic analyses results for one-hundred samples, the distributions of PCT and CET for the LOCA were expressed as

$$\text{PCT} \sim N(751.6, 3.0) \quad (1)$$

$$\text{CET} \sim N(631.4, 8.5) \quad (2)$$

The limiting case was determined from the CET, whose safety limit is 676 °C. By calculating the probability that the CET exceeds the safety limit, i.e., $\Pr(\text{CET} > 676^\circ\text{C})$, the failure probability of the natural circulation of PDHR was estimated to be 6.14E-08 for the LOCA. Similarly, the failure probabilities of the natural circulation of PDHR for other initiating events could also be estimated.

Sensitivity analysis was also performed using the MOSAIQUE code by comparing the values of normalized slope. The normalized slope was calculated as follows:

$$\text{normalized slope} = \frac{n \sum xy - (\sum x)(\sum y)}{n \sum x^2 - (\sum x)^2} \times (\max(x) - \min(x)) \quad (3)$$

where x = value of the uncertainty parameter and y = result value (e.g. CET).

The normalized slope provides the slope of the linear regression line. The sensitivity analysis result indicates that the ambient air condition has a relatively high impact on the coolant temperature in LOCA scenarios.

Table 5

Probability distributions of physical parameters for estimating the failure probability of the natural circulation of the PDHR system.

	Uncertainty parameter	current value	Distribution	Nominal value	Range	Standard deviation
1	Fuel thermal conductivity	Dependent on T	Normal	1.0	0.8–1.2	0.102043
2	Fuel heat capacity	Dependent on T	Normal	1.0	0.8–1.2	0.102043
3	Cladding thermal conductivity	Dependent on T	Normal	1.0	0.8–1.2	0.102043
4	Cladding heat capacity	Dependent on T	Normal	1.0	0.8–1.2	0.102043
5	Fuel temperature coefficient	−0.457 pcm/K, BOL	Normal	1.0	0.8–1.2	0.102043
6	Coolant density coefficient	2.063 pcm/(kg/m ³)	Normal	1.0	0.8–1.2	0.102043
7	PDHR inlet air temperature	25 °C	Uniform	25.0	5.0–45.0	
8	PDHR inlet air pressure	102.4 kPa	Uniform	102.4	102.35–102.45	
9	PDHR outlet air pressure	102.3 kPa	Uniform	102.3	102.25–102.35	

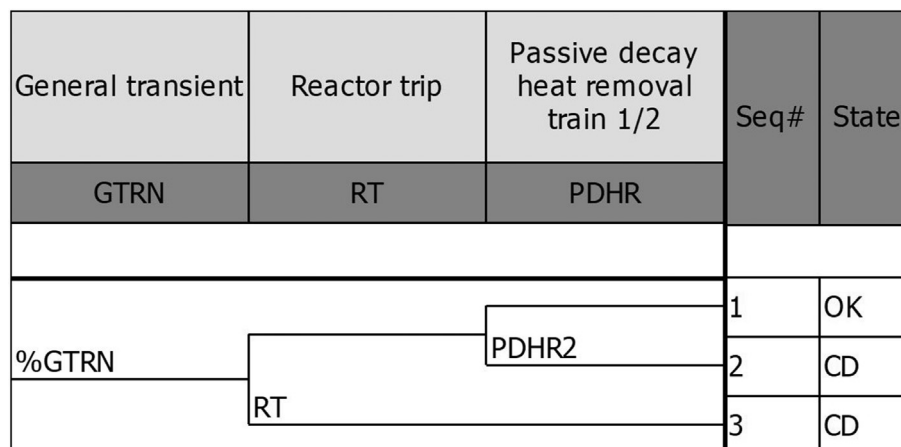


Fig. 11. Event tree for GTRN.

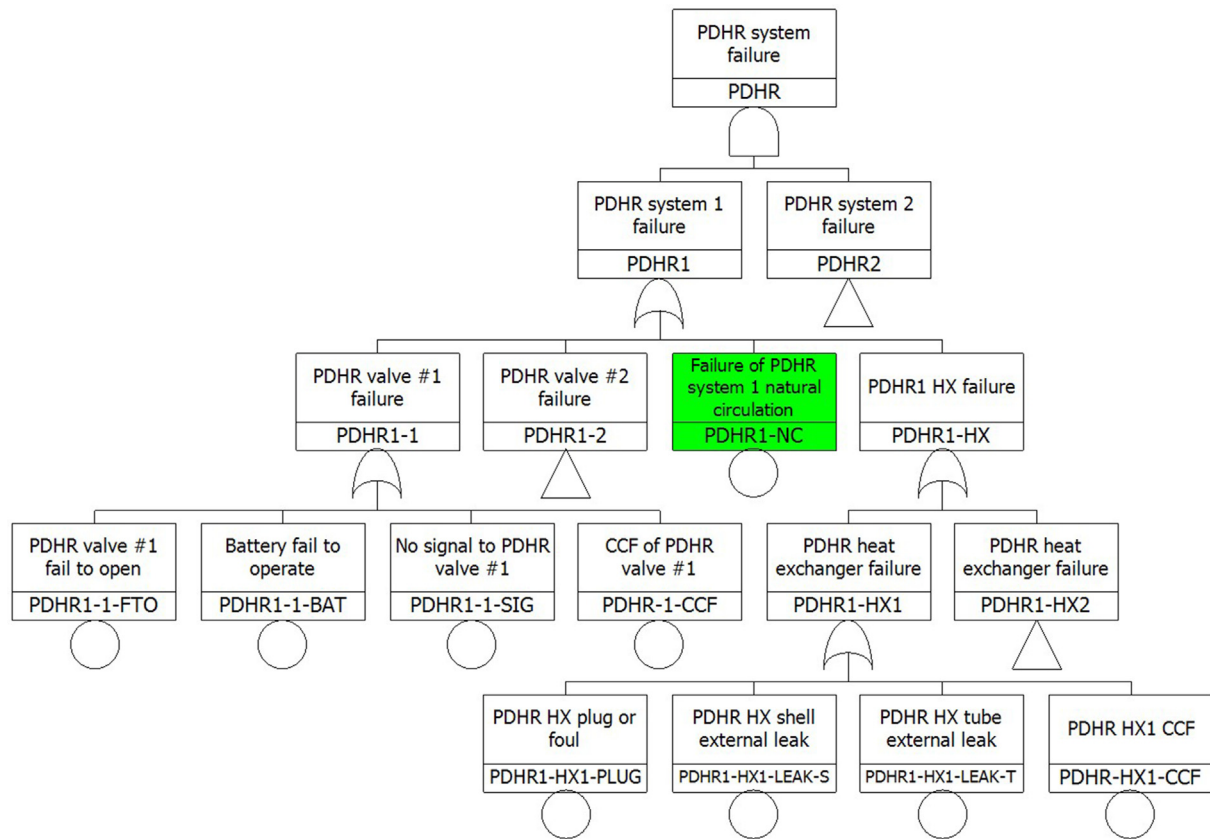


Fig. 12. Fault tree for the PDHR system.

6. Results and discussions

Following level 1 PSA of MMR considering internal events at full power, we could estimate CDF by integrating the results of the event tree and fault tree analyses. It should be noted that the PSA model for the MMR was developed with many conservative assumptions. The CDF is estimated to be less than 10^{-4} per year; hence, it meets the quantitative health objective, which is one of the safety goals for nuclear reactors in Korea [28], by satisfying the CDF performance objective. Fig. 14 shows the CDF contributions of the initiating event categories. The transients with the PCS initially available category is the most significant contributor to CDF, mainly because of its relatively high initiating event frequency compared to other categories. The occurrence of transients with the PCS initially available combined with the failure in the reactor trip, i.e., Sequence 3 in Fig. 11, is identified as the most significant failure scenario. The low contribution of the LOCA category can be attributed to the design features implemented to protect the reactor from LOCAs, such as the pressurized inner containment filled with CO_2 , which supplies the coolant (CO_2) to the primary system during design basis accidents.

Table 6 presents the results of the importance analysis of events with high Fussell–Vesely (F–V) importance. The risk reduction worth (RRW) and the risk achievement worth (RAW) importance measures are also provided with the F–V importance. The lack of redundancy or diversity in the signal generation of the reactor trip is identified as the most significant design weakness, with F–V importance of 0.895. Because reactor trip and PDHR system operation are essential for accident mitigation in four out of the five initiating event categories (the remaining one is RVR, which

directly results in core damage), reactor trip failure and CCFs of the PDHR system valves have high importance. Therefore, the safety of MMR can be significantly improved if the reliability of reactor trip and PDHR system operation can be improved.

As mentioned previously, the generic data for LWRs were inevitably applied to the MMR owing to the insufficient MMR-specific data. The authors believe that applying the event frequency and component reliability data of LWRs to newly developed non-LWRs is an important topic for future research; reaching a consensus on this topic is expected to require a significant amount of discussion. In this study, the authors focused on applying PSAs to newly developed reactors with limited operation and reliability data, while utilizing existing generic data to quantify PSA models and derive essential safety insights for these reactors.

Additional design considerations were also identified while performing the PSAs; these considerations benefited the design team of the MMR. The current conceptual design of MMR does not sufficiently consider the supporting functions of the reactor. In addition to existing small batteries, reliable electrical power supply for the actuation of safety features designed with redundancy and diversity would be necessary to improve the safety of MMR. Details on the instrumentation and control (I&C) system design such as signal cabling and electrical power supply need to be considered in addition to their functions of sensing and actuation signal generation for activating safety features (reactor trip, PDHR valve opening, and venting valve opening) and turbine protection (turbine bypass valve opening). Methods for testing and maintenance (T&M) of the safety features and major components inside the containment need to be developed to ensure safe operation of MMR.

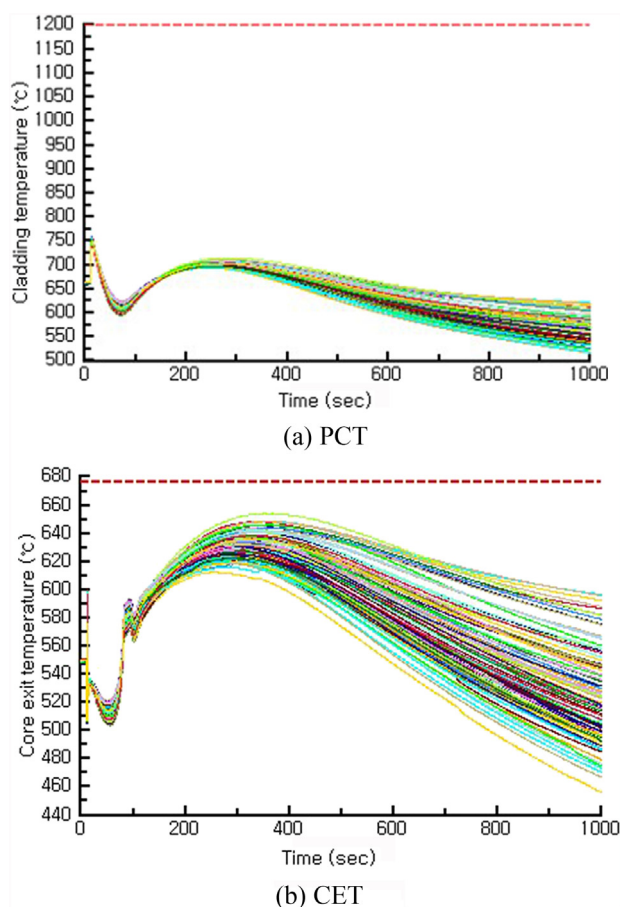


Fig. 13. Variation in PCT and CET for one-hundred samples of LOCA scenarios.

7. Conclusions

The S-CO₂ cooled MMR has many innovative design features including modular design and passive safety features. For quantitative safety assessment and identifying design weaknesses, we carried out PSA starting from the selection of initiating events to the quantification of CDF.

Based on our literature review, we grouped the initiating events into five initiating event categories and representative initiating events were selected from these categories. The selected representative initiating events were large LOCA, RVR, LOL, LOHS, and

Table 6

Results of the importance analysis.

Event	Description	F–V	RRW	RAW
RT-SIG	Reactor trip failure due to signal failure	0.895	9.558	7.65E + 03
PDHR-V1-CCF	PDHR valve #1 common cause failure	0.041	1.042	7.77E + 03
PDHR-V2-CCF	PDHR valve #2 common cause failure	0.041	1.042	7.77E + 03
PDHR4-NC	PDHR failure in natural circulation under LOHS	0.005	1.005	5.29E + 02
PDHR-T2-V1-FTO	PDHR train #2 valve #1 fails to open	0.004	1.004	9.747
PDHR-T2-V2-FTO	PDHR train #2 valve #2 fails to open	0.004	1.004	9.747
PDHR-T1-V1-FTO	PDHR train #1 valve #1 fails to open	0.004	1.004	9.609
PDHR-T1-V2-FTO	PDHR train #1 valve #2 fails to open	0.004	1.004	9.609
BAT-FTO	Battery (DC) fails to operate	0.003	1.003	7.77E + 03
PDHR-HX1-CCF	PDHR heat exchanger #1 common cause failure	0.002	1.002	7.77E + 03
PDHR-HX2-CCF	PDHR heat exchanger #2 common cause failure	0.002	1.002	7.77E + 03
RT-FTO	Shutdown rod drive fails to operate	0.001	1.001	7.66E + 03

GTRN. Transient analyses were performed to develop event trees and associated success criteria. Moreover, conservative assumptions were introduced in developing event trees. Fault trees were developed and generic failure data for mechanical components were used. Failure probability of natural circulation was also estimated considering the uncertainties in physical parameters. CDF was quantified by combining event trees, fault trees, generic failure data, and reliability of passive system.

The most significant initiating event category contributing to CDF was the transients with the PCS initially available category, owing to its relatively high occurrence frequency. Importance analysis revealed that the safety of MMR can be significantly improved by improving the reliability of reactor trip and PDHR system operation. Several design considerations regarding the redundancy and diversity of the electrical power supply, I&C systems, and T&M of the safety features and major components could be identified during PSA.

The CDF quantification results, importance analysis results, and design considerations are expected to contribute toward enhancing the safety of MMR as well as the development of its detailed design. In addition, the findings described in this paper, especially regarding the selection of initiating event categories, and the basic assumptions and lessons learned, are expected to contribute toward future applications of PSA to other types of nuclear reactors in their conceptual design phases.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

This research was supported by the Chung-Ang University Graduate Research Scholarship in 2018. This work was also supported by the National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIT), Republic of Korea (2017M2B2B1071973). We thank Professor Jung Ik Lee and Mr. Bong Seong Oh of Korea Advanced Institute of Science and Technology for sharing the input model for MMR used in the transient analysis.

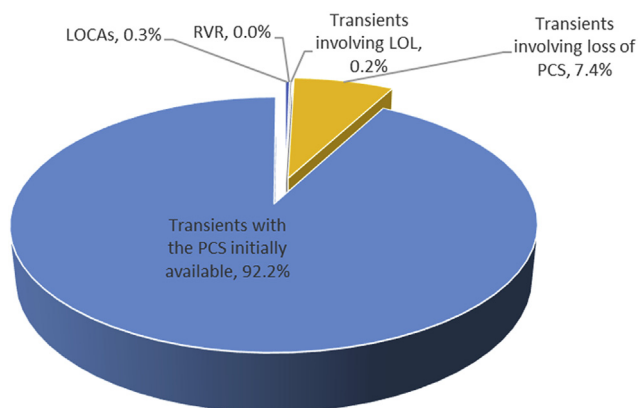


Fig. 14. CDF contributions of the initiating event categories.

References

- [1] M.A. Gibson, S.R. Oleson, D.I. Poston, P. McClure, NASA's Kilopower reactor development and the path to higher power missions, in: *Proceedings of the 2017 IEEE Aerospace Conference*, Big Sky, MT, 2017, pp. 1–14.
- [2] P. McClure, D. Poston, D.V. Rao, R. Reid, "Design of Megawatt Power Level Heat Pipe Reactors," LA-UR-15-28840, Los Alamos National Laboratory, 2015.
- [3] A. Levinsky, J. van Wyk, Y. Arafat, M.C. Smith, Westinghouse eVinci™ Reactor for Off-Grid Markets, American Nuclear Society Winter Meeting, Orlando, Florida, Nov, 2018, pp. 11–15, 2018.
- [4] C.K. Jo, Core Nuclear Design of a Micro Modular High Temperature Gas-Cooled Reactor, Transactions of the 2018 Korean Nuclear Society Autumn Meeting, Yeosu, Korea, 2018, October 25–26.
- [5] J.S. Jun, C.K. Jo, Design Considerations of the Air-Cooled RCCS on the Very Small-Size HTGR, Transactions of the 2018 Korean Nuclear Society Autumn Meeting, Yeosu, Korea, 2018, October 25–26.
- [6] S.G. Kim, H. Yu, J. Moon, S. Baik, Y. Kim, Y.H. Jeong, J.I. Lee, A concept design of supercritical CO₂ cooled SMR operating at isolated microgrid region, *Int. J. Energy Res.* 41 (4) (2017) 512–525.
- [7] B.S. Oh, Safety Analysis and Development of Control Logic of KAIST Micro Modular Reactor with GAMMA+ Code, MS Thesis, Korea Advanced Institute of Science and Technology, Department of Nuclear and Quantum Engineering, 2016.
- [8] B.S. Oh, Y.H. Ahn, S.G. Kim, S.J. Bae, S.K. Cho, J.I. Lee, Transient analyses of S-CO₂ cooled KAIST micro modular reactor with GAMMA+ code, in: *Proceedings of the 11th International Topical Meeting on Nuclear Reactor Thermal Hydraulics, Operation and Safety*, Korean Nuclear Society, October 9–13, 2016, Gyeongju, Korea.
- [9] H. Yu, D. Hartanto, B.S. Oh, J.I. Lee, Y. Kim, Neutronics and transient analyses of a supercritical CO₂-cooled micro modular reactor (MMR), *Energy Procedia* 131 (2017) 21–28.
- [10] B.S. Oh, Y.H. Ahn, H. Yu, J. Moon, S.G. Kim, S.K. Cho, Y. Kim, Y.H. Jeong, J.I. Lee, Safety evaluation of supercritical CO₂ cooled micro modular reactor, *Ann. Nucl. Energy* 110 (2017) 1202–1216.
- [11] KEPCO and KHNP, "Probabilistic Risk Assessment Summary Report," APR1400-E-P-NR-13001-NP, Rev. 0, Korea Electric Power, Corporation & Korea Hydro & Nuclear Power Co., Ltd, 2013.
- [12] IAEA, "Defining Initiating Events for Purposes of Probabilistic Safety Assessment," IAEA-TECDOC-719, International Atomic Energy Agency, Vienna, September 1993.
- [13] M.A. Pope, "Thermal Hydraulic Design of a 2400MWth Direct Supercritical CO₂ Cooled Fast Reactor", Ph.D. Thesis, Massachusetts Institute of Technology, Department of Nuclear Science and Engineering, 2006.
- [14] USNRC, "Reactor Safety Study, An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," WASH-1400, United States Nuclear Regulatory Commission, October 1975. Washington, D.C.
- [15] H.S. Lim, "GAMMA+1.0 Vol. 2: Theory Manual," KAERI/TR-5728/2014, Korea Atomic Energy Research Institute, Daejeon, Korea, 2014.
- [16] S.H. Han, et al., "AIMS-PSA: a software for integrated PSA. Proceedings of the 13th International Conference on Probabilistic Safety Assessment and Management (PSAM 13), October 2–7, 2016, Seoul, Korea.
- [17] IAEA, "Electric Grid Reliability and Interface with Nuclear Power Plants," IAEA Nuclear Energy Series No. NG-T-3.8, International Atomic Energy Agency, Vienna, 2012.
- [18] R. Tregoning, L. Abramson, P. Scott, Estimating Loss-of-Coolant Accident (LOCA) Frequencies through the Elicitation Process, NUREG-1829, United States Nuclear Regulatory Commission, Washington, D.C., 2008.
- [19] USNRC, "Rates of Initiating Events at U.S. Nuclear Power Plants: 1987–1995, NUREG/CR-5750, United States Nuclear Regulatory Commission, Washington, D.C., 1998.
- [20] USNRC, "Industry-Averaged Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants," NUREG/CR-6928, United States Nuclear Regulatory Commission, Washington, D.C., 2007.
- [21] W.S. Jung, S.H. Han, J. Ha, A fast BDD algorithm for large coherent fault trees analysis, *Reliab. Eng. Syst. Safe.* 83 (Suppl. 3) (2004) 369–374.
- [22] J. Jafaria, F. D'Auria, H. Kazeminejad, H. Davilu, Reliability evaluation of a natural circulation system, *Nucl. Eng. Des.* 224 (Suppl. 1) (2003) 79–104.
- [23] M. Marqués, J.F. Pignatelli, P. Saignes, F. D'Auria, L. Burgazzi, C. Müller, R. Bolado-Lavin, C. Kirchsteiger, V. La Lumia, I. Ivanov, Methodology for the reliability evaluation of a passive system and its integration into a probabilistic safety assessment, *Nucl. Eng. Des.* 235 (Suppl. 24) (2005) 2612–2631.
- [24] A.K. Nayak, M.R. Gartia, A. Antony, G. Vinod, R.K. Sinha, Passive system reliability analysis using the APSRA methodology, *Nucl. Eng. Des.* 238 (Suppl. 6) (2008) 1430–1440.
- [25] H.G. Lim, S.-H. Han, J.J. Jeong, Mosaique – a network based software for probabilistic uncertainty analysis of computerized simulation models, *Nucl. Eng. Des.* 241 (Suppl. 5) (2011) 1776–1784.
- [26] J.C. Helton, F.J. Davis, Latin hypercube sampling and the propagation of uncertainty in analyses of complex systems, *Reliab. Eng. System Reliab.* 81 (Issue. 1) (2003) 23–69.
- [27] S.-J. Han, J.-E. Yang, A quantitative evaluation of reliability of passive systems within probabilistic safety assessment framework for VHTR, *Ann. Nucl. Energy* 37 (Suppl. 3) (2010) 345–358.
- [28] J.S. Kim, M.C. Kim, Consistency issues in quantitative safety goals of nuclear power plants in Korea, *Nuclear Eng. Technol.* 51 (Suppl. 7) (2019) 1758–1764.