Development of Probabilistic Safety Assessment Methodology for Autonomous Micro Modular Reactor

Eun Seo So[a], Jaesun Ha[a], and Man Cheol Kim[a*]
[a] Chung-Ang university, Seoul, Korea
[*] Contact author: charleskim@cau.ac.kr

Abstract: In response to expectations for a safer reactor, many advanced reactors adopted various safety features from core design to additional safety systems including passive safety systems. Passive safety systems have been adopted to enable the reactors to enter a stable condition without continuous external power supply and operator action. However, passive systems using natural circulation are highly dependent on the plant status and the surroundings, which leads to make the performance unpredictable. Deterministic safety analysis has been performed for many examples, however there is no standardized probabilistic safety assessment method for passive systems. Recently, a conceptual autonomous micro modular reactor, which adopts passive safety systems, is proposed and its performance of the safety functions is demonstrated with thermal-hydraulic analysis. In this paper, accident sequences of the previous transient analyses are reviewed, and event trees are provided for further probabilistic safety assessment of autonomous micro modular reactor which uses supercritical carbon dioxide as coolant and working fluid. Some of other advanced reactors with similar characteristics are also investigated to get insights for probabilistic safety assessment of the autonomous micro modular reactor and initiating events are identified.

Keywords: PSA, MMR, S-CO2, advanced reactor, and passive system.

1. INTRODUCTION

After several severe accidents, advanced reactors with enhanced safety functions are gradually introduced. In order to achieve higher safety, adoption of passive systems for long term decay heat removal is widely proposed and implemented in advanced reactors. There are already several reactors with passive systems such as advanced power reactor plus (APR+), very high temperature reactors (VHTRs), and gas-cooled fast reactors (GFRs). One of GFRs, a micro modular reactor (MMR) design is suggested [1]. They selected supercritical carbon dioxide (S-CO_2) as a working fluid and enhanced the reactor design with many advantages in terms of safety as well as performance. In the previous studies done by KAIST research team, several transient analyses results showed that the system parameters do not go over the safety limit so that the strong inherent safety features were proved for several hypothetical accident scenarios [2]. However, for probabilistic safety assessment (PSA), safety analyses should be conducted for more various scenarios to calculate the reliability of the system quantitatively. In this paper, as a first stage of PSA, previous studies of other advanced reactors with similar characteristics are investigated and initiating events are identified for the autonomous micro modular reactor.

2. LITERATURE SURVEY

Before we evaluate the safety of KAIST MMR, it is necessary to investigate previous studies for reactors or safety systems with similar characteristics. The working fluid of MMR is supercritical CO_2 which might have somewhat different characteristics from other water-cooled reactors, therefore these characteristics need to be considered in the selection of initiating events for PSA. In addition, one of other features different from existing reactors, passive safety systems, has been gradually adopted in the design of advanced reactors to ensure safety even when the external power and human resources are unavailable for long term decay heat removal. The analysis on the performance of some of the similar advanced reactors in accident situations are provided in literatures. In this paper, some of the reactor

concepts with these features were surveyed while focusing on safety aspects. This survey will give insights into the PSA of MMR.

2.1. Reliability of Passive Auxiliary Feedwater System of APR+

There are many advanced reactors with passive systems and several reactors are proved their performance in some accident scenarios. Advanced power reactor plus (APR+) is an enhanced model in the safety features compared to Advanced power reactor 1400 (APR1400) which is already designed and operated in Korea. In APR1400, the auxiliary feedwater is injected by motor and turbine driven pumps to steam generators when the main feedwater flow is lost. The auxiliary feedwater system of APR1400 is replaced with the passive auxiliary feedwater system (PAFS) in APR+ to remove the decay heat in accident conditions without continuous electrical power supply. There is a passive condensate heat exchanger (PCHX) in the passive condensate cooling tank (PCCT). PCCT and PCHX are located in the outlet of the steam generator to cool down and condensate the fluids in the main steam line.

Kang et al. [3] performed a quantitative evaluation of the reliability of PAFS with several MARS code simulations. The result showed the cooling performance of the PAFS during a steam generator tube rupture (SGTR) accident and the core damage frequency (CDF) was evaluated to decrease compared to the CDF when the conventional auxiliary feedwater system was used.

In deterministic safety analysis to demonstrate the performance of APR+, small break loss of coolant accident (SBLOCA) and steam generator tube rupture (SGTR) are analyzed for various break sizes and additional conservative assumptions. The thermohydraulic analysis results showed that the system parameter is under safety limits and the CDF also decreased. This is because APR+ has a separate active component, alternate auxiliary pump (AAP), to prepare the loss of PAFS functionality. CDF would increase without AAP operation by operator when the PAFS is unavailable [4].

2.2. Reliability of Reactor Cavity Cooling System of VHTR

One of the advanced reactors, very high temperature reactor (VHTR) also adopted a passive safety system: reactivity cavity cooling system (RCCS). Han and Yang [5] conducted a quantitative reliability evaluation in the low-pressure conduction cooling (LPCC) accident to investigate the performance of RCCS. Probabilistic safety assessment framework is proposed with the stress-strength interference (SSI) model using probabilistic density functions (pdf) for the stress and strength of the system. Although the SSI model has advantages, the EP approach for the multiple states is recommended due to the unavailability of the strength model.

2.3. Reliability of Passive Decay Heat Removal System of GCR 2400MWth

One of the other advanced gas cooled reactors, GCR2400 suggested by CEA, has primary, secondary and third circuits and decay heat removal (DHR) loops using natural and forced circulation [6]. As a preliminary level 1 PSA model, LOCA and loss of offsite power (LOOP) are selected as an initiating event for transient analysis to support the design of the decay heat removal dedicated loops [7]. The insight gained in the previous study led to the design enhancements, followed by the derivation of the initiating events for final level 1 PSA model, and safety assessments were performed [8]. The initiating events were selected by the master logic diagram (MLD) approach, which is an identification method for initiating accidents. In MLD method, the determination of the top event is a starting point to identify initiating events such as loss of containment [9].

2.4. Reliability of Direct Supercritical CO_2 Cooled Fast Reactor designed by MIT

Pope [10] provided a thermal hydraulic design of a 2400 MWth supercritical CO2-cooled fast reactor and analyzed thermal hydraulic behavior during loss of external load transient (LOEL), loss of coolant accident (LOCA), and loss of flow (LOF) transient. LOEL occurs when the external power supply from the grid is not available or the turbine does not work properly as a heat sink. Two options are suggested: turbine bypass valve and power cycle bypass valve. After evaluating various options for mitigation of

an LOEL event, it was concluded that combined power cycle bypass (PCB) and turbine bypass may prevent shaft overspeed without too low or too high core flow rate and without exposing the high temperature recuperator to extreme temperature excursions.

2.5. KAIST Micro Modular Reactor

KAIST-MMR is a small modular fast reactor with supercritical CO2 cooling system [1]. It reduced the size and weight to achieve a goal to supply power to an isolated region by land transportation of the reactor. Also, it improved the performance with some additional functions in the systems, i.e., core, air cooling heat exchanger, power conversion system, and passive decay heat removal system (PDHR).

1) Safety Systems

MMR has active and passive heat removal system: intermediate CO_2 cooling loop between precooler and air fan and passive decay heat removal (PDHR) system. The active heat removal system works on normal situations and the latter works after certain set point of the pressure. In the active system, CO_2 loop takes the heat from the precooler and transfer it to the ambient air through air fan working by electricity. The passive decay heat removal system adopted shell and tube type heat exchanger and it has one more same type passive decay heat removal system for redundancy [1].

Reactivity control system and containment are also designed with priority of safety. The reactivity can be controlled by the drum-type primary reactivity control system to prevent rod rejection accident and the secondary control rod for ultimate shutdown. Moreover, due to its inherent safety features, the strong reactivity feedback maintains the system in stable states regardless of the reactor scram after the shutdown signal. In addition, there are inner and outer containments and the inner one is pressurized with 5 MPa CO_2 which makes sufficient mass flow rate even in the case of LOCA [1].

2) Accident Sequences

Pope [10] performed transient analysis for LOF condition for a four-loop supercritical carbon dioxide cooled fast reactor in which one of the four loops is separated from the other loops. However, the concept design of the MMR does not have any redundant loop to separate easily in the accident condition due to the compact size. Therefore, Yu et al. [11] performed a transient analysis on a small break loss of coolant accident (SBLOCA) combined with the failure of automatic reactor trip and found that reactor power gradually decreases due to negative reactivity feedback and the reactor could be cooled down by the operation of a passive decay heat removal system and the opening of the feed valve. It was concluded that fuel centerline temperature, peak cladding temperature, and maximum coolant temperature are all below safety limits during the progress of the accident.

Oh et al. [12] performed a transient analysis on a load ejection event and found that severe damage to turbine blades are possible without active control and proposed the power reduction via core inlet bypass as a solution for such a situation.

3. DEVELOPMENT OF EVENT TREES

Loss of coolant accident (LOCA) is one of the most severe accidents in nuclear power plants, and hence it is usually one of the accidents that are analyzed with priorities in deterministic safety analysis. After Fukushima event, station black out (SBO) became one of other critical accidents to be analyzed with priorities. In case of MMR, loss of load (LOL) would be a critical issue because of grid instability of the located area. For these reasons, LOCA and LOL are analyzed firstly with conservative assumptions such as failure of scram and single failure of safety features [1]. In this paper, an event tree is developed for each case as a preliminary study of the accident sequences already simulated in the previous studies.

The system is already designed to prevent turbine damage due to the change of load demand. However, in the opposite case, the reactor could rather confuse the power grid due to the variance of the output

power. Therefore, the system should disconnect the grid from the generator to protect the grid which leads to LOL of the reactor.

Both accident scenarios assumed that no reactor scram occurred which means any of the control rods are not dropped even though the reactor shutdown signal was generated. Identification of the grid connection is not considered in the event trees of both accident scenarios, because the grid disconnection is induced by the reactor shutdown signal regardless of the whether the control rods are actually dropped or not. Moreover, the failure of the grid disconnection, which means the external power source is still available, does not affect the core integrity while affecting the stability of the grid. Fortunately, the PDHR made possible the removal of thermal power steadily in any states.

Active safety features are modeled as well as passive ones such as heat exchanger between the intermediate CO_2 loop and ambient air, core bypass valve, and inventory tank. They can operate automatically when the external power is supplied continuously. If the control rods are successfully dropped, the power would decrease rapidly and other safety systems should operate in accordance with the situation differently. In addition, if the grid disconnection is not necessary in other accident scenarios, the operation of the active systems might be helpful for the mitigation of the situation and it should be considered in the event trees in that case. However, active safety features are not considered in the accident sequences as headings of the event trees in Figures 1 and 2. After more transient analyses are performed for other hypothetical accident scenarios, the event trees need to be revised. However, the current event trees are developed to reflect the current design status of the system.

Passive safety features are modeled in the event trees of the two accident scenarios considered in the previous transient analysis studies. They set up several assumptions that the scram is failed after the shutdown signal and only one train of passive decay heat removal systems is available with the assumption of the failure of the other train. Four simple trip valves are modeled as passive safety features that does not need any power supply to operate after initial opening with small power. In previous studies which evaluated the inherent safety features of the core, the trip valves are assumed to be opened at the set points of each valves. The small power source might be backup batteries even though they are not specifically mentioned. However, in terms of the probabilistic safety assessment, the failure of the valves needed to be considered for cases where the backup power supply is not available, because it would be impossible to open the valves manually due to the small size of the MMR. Therefore, the failure of the valves opening is considered in the accident sequences of both accidents. The system is assumed to maintain safe status after all the success of the safety features.

Unprotected loss of flow accident (ULOF) is one of other accidents usually included in the transient analyses of gas cooled reactors. Small loss of coolant accident (SLOCA), which is one of the critical accidents considered in design of the reactors, is previously analyzed to examine the performance of the MMR after ULOF. Small size break of 7.0715 cm^2 on the pipe located between the compressor outlet and the recuperator inlet was analyzed [11].

It was assumed that the primary and secondary shutdown system does not work properly after the generation of shutdown signal. Redundant safety features such as inherent safety feature of the core and the passive safety features including passive decay heat removal system (PDHR) and feed valve contributed to maintain the safety of the reactor. At the open signal setpoint pressure 13.46 MPa of PDHR valve, the decay heat starts to be removed from the system due to the natural circulation between the core and the air. Soon after the grid is disconnected, any active control systems are assumed to be inoperable to remove the decay heat. Another passive system in the conceptual design, feed valve, is opened and the pressure of the compressor inlet becomes higher than the pressure of the containment even after the loss of power. The inner containment is pressurized with 5 MPa CO2, and hence the pressure of the compressor inlet can be easily lowered compared to the containment of typical LWRs. After the valve opens, the system pressure in the inner containment maintains slightly above the 5 MPa. Consequently, the system parameters maintain stable states under the safety limit due to various safety features of MMR.

Reactor trip and reactivity control is considered before the passive system operation. The current accident scenarios assumed that the control rods fail to drop. The red lines in the event trees show that the reactor trip is failed. In previous studies, MMR is designed to maintain stable conditions due to reactivity feedback even after the failure of the reactor trip. However, in the event tree of anticipated transient without scram (ATWS), typical pressurized water reactor (PWR) considers the unfavorable exposure time (UET) in the case of turbine trip failure by ATWS mitigation systems. In MMR, if the turbine is not tripped in the accident condition, there might be positive reactivity feedback like UET of PWR, and the reactor power might not decrease with the inherent safety feature.

Figure 1: Event Tree of LOCA-WS-SF

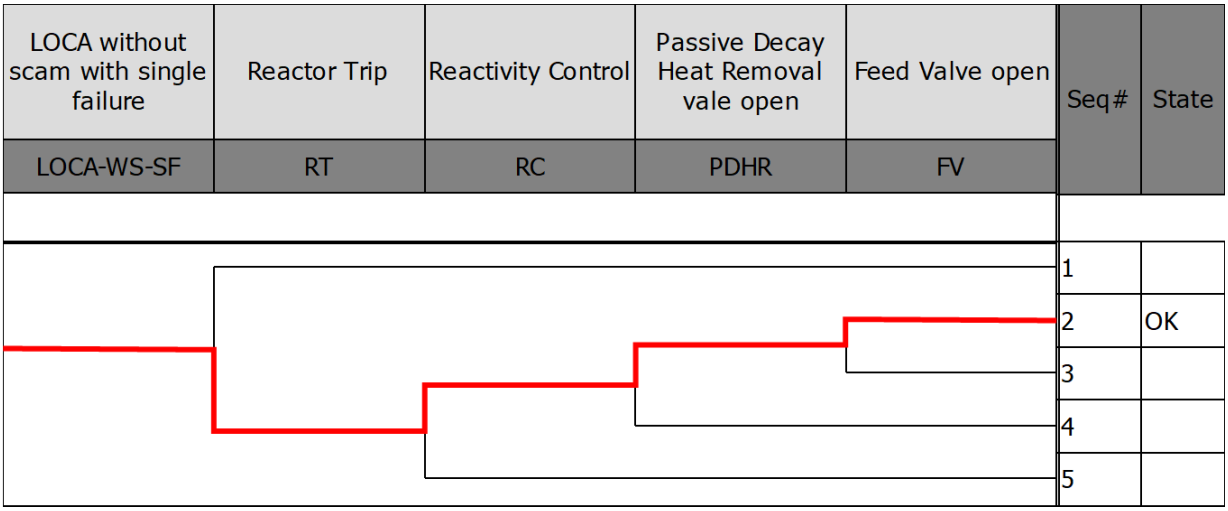
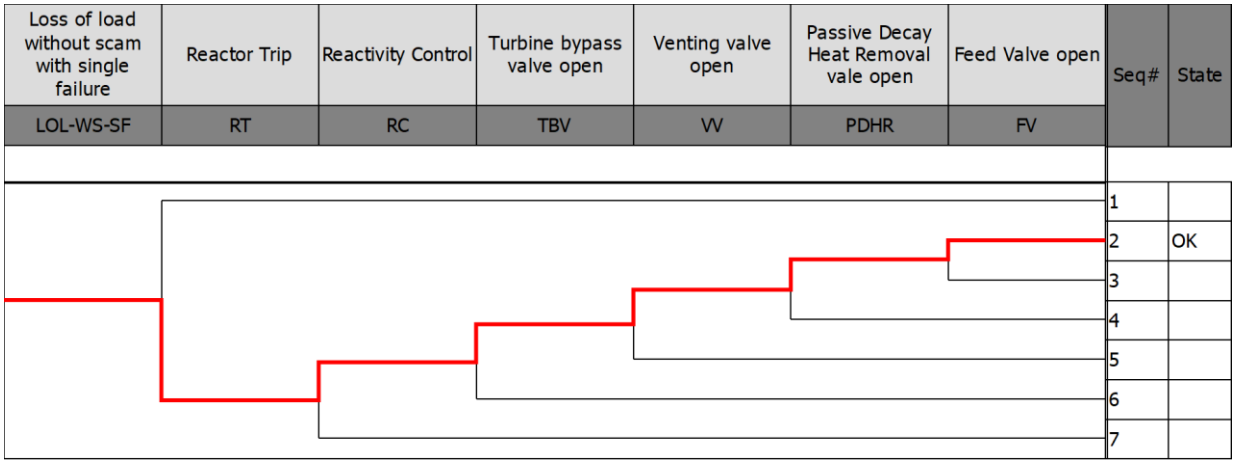


Figure 2: Event Tree of LOL-WS-SF



4. IDENTIFICATION OF INITIATING EVENTS

As a starting point of PSA, selectin of initiating events should take into account every possible accident. Usually, the following are considered in this process.

- Initiating event lists given for the reactor type (e.g. EPRI lists)
- Initiating events considered in other reactors with similar characteristics
- Thermal hydraulic analysis based on the engineering judgement
- Logical methodology (e.g. master logic diagram)
- Previous operating experience

The previous operating experience is not applicable in the design stage of reactors. Therefore, it is necessary to reflect properly the rest of the methods. The results from thermal hydraulic analyses performed in the previous studies are reflected in section 3. More thermal hydraulic analyses on different situation will be helpful to update the event trees and initiating event lists. It will be possible to structuralize the logical method such as master logic diagram (MLD).

4.1. Pressurized water reactor

As an example of initiating event list for other reactor types, the classification of events presented in the safety analysis report of typical PWR as follows.

1) Increase in heat removal by the secondary system
2) Decrease in heat removal by the secondary system
3) Decrease in reactor coolant flow rate
4) Reactivity and power distribution anomalies
5) Increase in reactor coolant inventory
6) Decrease in reactor coolant inventory
7) Radioactive release from a subsystem or components
8) Anticipated transient without scram (ATWS)

There is no steam generator connected to power conversion system, therefore secondary system does not exist in the design of MMR. The heat exchanger between the precooler and air can be regarded as circulating system in PWRs. Kim et al. [1] suggested two methods for active safety system: air fan and dry cooling tower. Although the CO_2 circulator produces a constant flow rate for cooling, it is expected that the heat removal performance will change depending on the air condition, which is the final heat sink of the active safety system. After the final design is established, it will be clear whether the relevant initiating events are reflected.

Among the initiating events normally included in the CDF calculation of PWRs, the initiating events in LOCA group are as follows.

1) Loss of coolant accident (LOCA) by break size
2) Steam generator tube rupture (SGTR)
3) Interfacing system loss of coolant accident (ISLOCA)
4) Reactor vessel rupture (RVR)

The safety analysis results performed in the previous studies are reflected as LOCA initiating events. SGTR and ISLOCA cannot be reflected due to the design difference between typical PWRs and MMR. RVR can be considered after the definition of the event is determined.

Initiating events in the transient group are as follows.

1) General transients
2) Loss of main feedwater (LOMF)
3) Loss of condenser vacuum (LOCV)
4) Loss of offsite power (LOOP)
5) Station blackout (SBO)
6) Main steam line break (MLSB)
7) Anticipated transient without scram (ATWS)

LOMF and MSLB cannot be applied to the initiating event lists due to the design difference. LOCV is considered to reflect the situation of loss of ultimate heat sink, and hence break of the U-shaped tubes

in MMR design or failure of circulating pump can be included in the initiating event lists. LOOP and SBO are included as loss of load in section 3. General transients can be included after definition is made for MMR. ATWS suggests unfavorable exposure time (UET) that the plant cannot be shutdown at a small probability after the failure of control rods insertion. PWRs reflected 1% for UET, and definition of UET and analysis of probability is required for MMR.

In addition, the following events might be considered.

1) Loss of component cooling water (LOCCW)
2) Loss of DC bus or AC bus
3) Loss of instrument air (LOIA)

There are various safety systems in typical PWRs, however CCW system is not mentioned in the current design. Therefore, it is necessary to analyze whether the component cooling is possible only with the CO_2 in the internal containment. LOIA is not considered, because there are no air operated valves in MMR.

4.2. CEA GFR 2400

In order to calculate the reliability of the reactor, other initiating events need to be considered. The following initiating events are those that are analyzed in the safety assessment of the GFR 2400 developed by CEA [7]:

1) Loss of feed water (LOFW)
2) Reactor or turbine trip
3) Generator trip or fault (secondary and tertiary)
4) Loss of primary flow (LOF, partial and total)
5) SB-LOCA on secondary circuit
6) LOCAs on reactor cooling system
7) Steam generator tube rupture
8) Turbo-machinery trip or fault
9) Main steam line break
10) CRA withdrawal
11) DHR HX interfacing LOCA (gas-water HX)
12) LOOP (short and long-term duration)
13) Loss of one electrical train
14) Main IHX interfacing LOCA (gas-gas HX)

The GFR 2400 is also gas cooled fast reactor like MMR, which can give insights to the selection of the initiating events that need to be analysed. However, MMR is designed as a distributed power in isolated region, the size and capacity of the system is significantly different from the GFR 2400. Some of the initiating event lists might be included in the initiating event lists of MMR, and hence specific comparison should be conducted between GFR 2400 and MMR.

4.3. Initiating event list for MMR

Based on the current stage, initiating events need to be analyzed in future studies are selected as follows.

1) Loss of coolant accident (LOCA)
2) Reactor vessel rupture (RVR)
3) General transients
4) Loss of ultimate heat sink
5) Loss of load (LOL)
6) Anticipated transient without scram (ATWS)

These will be the first targets of the safety analysis in the future.

5. FUTURE STUDIES

Several transient analyses showed the performance of the MMR in hypothetical situations. Nevertheless, there are still critical issues left to be considered. The system parameters such as pressure and

temperature showed lower value below the safety limit, even though the accidents are postulated with conservative assumptions. However, to evaluate the safety features probabilistically, other accidents, that considered to be less or more severe, should also be analyzed. For example, the break location might occur on the loop the PID controllers are located or one of the valves might be opened and fail to reclose, so that it can make the situation more unpredictable. In addition, the passive safety features such as turbine bypass valve, venting valve, feed valve, and PDHR valve might fail due to failure of small power supply for opening. These hypothetical accident scenarios will be reflected properly after safety analysis in the future.

Typical reactors are mainly composed of active components like pumps and valves and hence it is rather straightforward to determine the successive operation of the system or component and failure rate databases are also available to be used to determine their reliabilities. In case of passive systems, however, it is necessary to consider various status of the reactor and the ultimate heat sink such as ambient air, because the performance of passive systems is highly dependent on the operating conditions including surrounding environmental situation. Consequently, a lot of transient analysis are needed to be performed including other initiating events, accident scenarios, and various conditions affecting the passive systems. In order to evaluate the passive systems, many thermohydraulic code runs are needed with PSA methodologies for passive system such as reliability evaluation of passive safety system (REPAS), reliability methods for safety functions (RMPS), and analysis of passive system reliability (APSRA). Safety analysis will define new initiating events and update the accident scenarios. It will help to obtain CDF for each event and derive improvements for MMR.

6. CONCLUSION

To evaluate the safety of MMR, literature survey was conducted for other advanced reactor types with similar characteristics. LOCA and LOL were performed in most previous studies for transient analysis of new and advanced reactors. MMR safety system is also analyzed in LOCA and LOL with conservative assumptions. The accident sequences are provided in event trees which will be updated in future studies. Besides, other initiating events are selected through review of initiating event lists for other reactor types. The initiating events will be first objective to be analyzed and the accident sequences will be updated for various hypothetical accident scenarios. Event trees and fault trees will also be developed to calculate the CDF of MMR, and therefore design improvements will be derived.

Acknowledgements

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (2017M2B2B1071973).

References

[1] S. G. Kim, H. Yu, J. Moon, S. Baik, Y. Kim, Y. H. Jeong, and J. I. Lee, "*A concept design of supercritical CO_2 cooled SMR operating at isolated microgrid region*", International Journal of Energy Research, 41, pp. 512-525, (2017).

[2] 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 CO_2 cooled micro modular reactor*", Annals of Nuclear Energy, 110, pp. 1202-1216, (2017).

[3] S. H. Kang and H. G. Kim, "*Performance Analysis of APR+ PAFS for CDF evaluation"*, Transactions of the Korean Nuclear Society Spring Meeting, pp.26-27, (2011).

[4] H. Moon and H. G. Kim, "*A study on the probabilistic safety assessment and sensitivity analysis of success criteria of large LOCA for APR+*", Journal of the Korean Society of Safety, Vol. 31, No. 6, pp.129-134, (2016).

[5] S. J. Han and J. E. Yang, "*A quantitative evaluation of reliability of passive systems within probabilistic safety assessment framework for VHTR*", Annals of Nuclear Energy 37, pp. 345–358, (2010).

[6] M. Marques, C. Bassi, and F. Bentivoglio, "*Reliability analysis of 2400 MWth gas-cooled fast reactor natural circulation decay heat removal system*", Workshop on PSA for New and Advanced Reactors, NEA/CSNI/R(2012)2, pp. 173-196, (2012).

[7] C. Bassi, P. Azria, and M. Balmain, "*Level 1 probabilistic safety assessment to support the design of the CEA 2400MWth gas-cooled fast reactor*", Nuclear Engineering and Design 240, pp. 3758-3780, (2010).

[8] M. Balmain, C. Bassi, and P. Azria, "*Achievement of the level 1 PSA in support to the CEA 2400 MWth gas-cooled fast reactor*", NEA/CSNI/R(2012)2, (2012).

[9] I.A. Papazoglou, and O.N. Aneziris, "*Master logic diagram: method for hazard and initiating event identification in process plants*", Journal of Hazardous Materials A97, pp. 11-30, (2003).

[10] Michael A. Pope, "*Thermal hydraulic design of a 2400 MWth direct supercritival CO_2 cooled fast reactor*", Massachusetts Institute of Technology, Department of Nuclear Science and Engineering, (2006).

[11] H. Yu, D. Hartanto, B. S. Oh, J. I. Lee, and Y. Kim, "*Neutronics and Transient Analyses of a Supercritical CO2-cooled Micro Modular Reactor (MMR)*", Annals of Nuclear Energy, Energy Procedia 131, pp. 21-28, (2017).

[12] B. S. Oh, Y. H. Ahn, S. G. Kim, S. J. Bae, S. K. Cho, and J. I. Lee, "*Transient analyses of S-CO2 cooled KAIST Micro Modular Reactor with GAMMA+ code*", Proceedings of the 5th International Symposium – Supercritical CO2 Power Cycles, San Antonio, Texas, March 28-31, 2016.