IoT-based Integrated Analysis Framework for Enhancing Nuclear Power Plant Safety in Multi-Failure Environments

Kyung Bae Jang[1*], Tae Ho Woo[2]
[1]Professor, Dept. of Electrical Engineering, Kangwon National University
[2]Professor, Dept. of Mechanical and Control Engineering, Korea Cyber University

다중 고장 환경 원자력 발전소 안전성 제고를 위한 IoT 기반 통합 분석 프레임워크

장경배[1*], 우태호[2]
[1]강원대학교 전기공학과 교수, [2]고려사이버대학교 기계제어공학과 교수

Abstract Following the stringent regulatory updates after the Fukushima accident, Multiple Failure Accident (MFA) analyses are being rigorously conducted for Nuclear Power Plants (NPPs). These analyses evaluate safety risks by integrating natural disasters with internal system malfunctions and human factors. In particular, the Internet of Things (IoT) is associated with human factors. Over the proposed 60-year operational lifespan, the final value was observed to be 2.412 times higher than the initial value (calculated as 2.05 / 0.85). To extend these MFA applications from Light Water Reactors (LWRs) to Gas-Cooled and Liquid Metal Reactors, the development of new scenarios is essential. Furthermore, it is critical to establish robust safety analysis programs and strategic improvement frameworks for MFA-related systems.

Key Words : Safety, Nuclear Power Plants, Internet of Things, Risk, System Dynamics

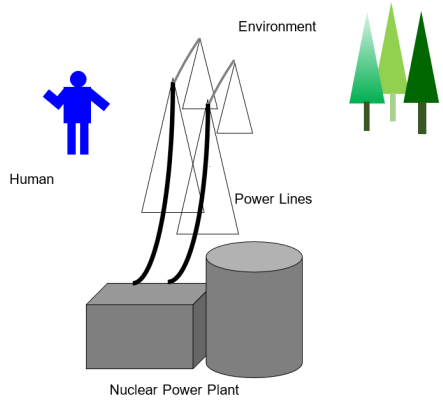
요 약 일본 후쿠시마 원전 사고 이후 강화된 규제에 따라 원자력 발전소에 대한 다중 고장 사고 분석이 활발히 진행되고 있습니다. 이러한 분석은 자연재해, 내부 시스템 오작동, 인적 요인을 통합하여 안전 위험을 평가합니다. 특히 사물인터넷은 인적 요인과 밀접하게 관련되어 있습니다. 제안된 60년의 운영 수명 동안 최종 위험도는 초기 위험도보다 2.412배 높은 것으로 나타났습니다(2.05 / 0.85로 계산). 이러한 다중 고장 사고 분석 적용 범위를 경수로에서 가스냉각로 및 액체금속로로 확장하기 위해서는 새로운 시나리오 개발이 필수적입니다. 또한 다중 고장 사고 분석 관련 시스템에 대한 견고한 안전 분석 프로그램과 전략적 개선 프레임워크를 구축하는 것이 중요합니다.

주제어 : 안전, 원자력 발전소, 사물인터넷, 위험, 시스템다이내믹스

이 논문은 2026년도 강원대학교 학술연구조성비 지원에 의하여 수행되었음
*교신저자 : 장경배(kbjang@kangwon.ac.kr)
접수일 2026년 06월 11일 수정일 2026년 07월 11일 심사완료일 2026년 08월 06일

1. Introduction

Following the Fukushima accident, nuclear regulations and standards have been significantly strengthened. This necessitates the development of enhanced nuclear system analysis methods that evaluate safety and risks associated with natural disasters, internal system malfunctions, and human factors. As shown in Fig. 1, the environments surrounding nuclear power plants (NPPs) are complex. Therefore, this study investigates multiple failure accidents (MFAs) using an analytical approach based on system dynamics (SD) algorithms. We analyze scenarios and consequences of MFAs by integrating mechanical systems and human factors, as the Fukushima meltdown resulted from a combination of these critical drivers.

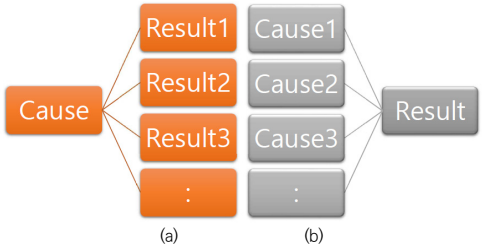


[Fig. 1] Surrounds of NPP.

While the earthquake triggered the Fukushima accident, various contributing factors influenced the final outcome. Table 1 lists the chronological sequence of events [1], highlighting the loss of coolant and the subsequent efforts to restore external cooling. By incorporating common cause failure (CCF), the MFA is analyzed through the event flow depicted in Fig. 2. The fundamental difference between these two cases lies in the total number of initiating causes and their resulting consequences. So, the meanings are opposite

〈Table 1〉 Accident sequence by time.

Sequence	Unit#1	Unit#2	Unit#3
Loss of AC power	+ 51 min	+ 54 min	+ 52 min
Loss of cooling	+ 1 hour	+ 70 hour	+ 36 hour
Water level down to top of fuel	+ 3 hours	+ 74 hours	+ 42 hours
Core damage starts	+ 4 hours	+ 77 hours	+ 44 hours
Reactor pressure vessel damage	+11 hours	Uncertain	Uncertain
Fire pumps with fresh water	+ 15 hours	-	+ 43 hours
Hydrogen explosion (not confirmed for unit 2)	+ 25 hours	+ 87 hours	+ 68 hours
Fire pumps with seawater	+ 28 hours	+ 77 hours	+ 46 hours
Off-site electrical supply	+ 11-15 days		
Fresh water cooling	+ 14-15 days		



[Fig. 2] Chain for multiple failure accident (a) Common Cause Failure (CCF) (b) Multiple Failure Accident (MFA).

characteristics each other. However, CCF and MFA have same characteristics as there are multiple components are involved. Since this reason is one of critical issues in the safety analysis, the complex algorithm is necessary in analytic as well as mathematical descriptions.

There are aspects of internal system, natural disaster and human factors. So, it is analyzed for aspect of internal system as follows,

1. Application of Design Basis Accident (DBA) to the MFAs
2. To study the effect by natural disaster
3. To study the response to the multiple failure accidents of the multiple plants in each site
4. Development of SD computer program method for quantitative analysis
5. Suggestion for the post-accident treatment

For the human factor and natural disaster,

1. To make applications for the conventional

risk analysis in human factor
2. To study and analyze the past events in geology, metrology, and sea water-related cases
3. To study the human factor and natural disaster in each nation
4. To study the international cooperation

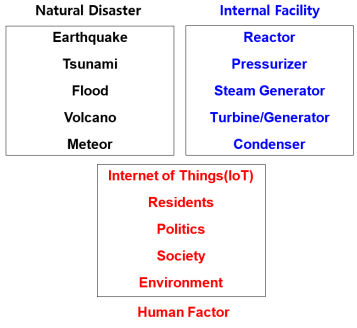
In the modeling, the SD is used for the quantifications which has been used for the social-humanity matter and some technological assessments.

Previous research has explored nuclear MFAs in various contexts. Prasad et al. investigated a hypothetical severe core damage accident in a pressurized heavy water reactor (PHWR), where multiple cooling system failures could lead to the collapse of pressure and calandria tubes, causing debris to relocate within the vessel [2]. Hassija et al. examined how multi-unit safety assessments gained global significance after the 2011 Fukushima disaster, discussing the unique challenges of multi-unit sites and developing an integrated approach to evaluate the collective risk of multiple nuclear plants at a single location [3]. Kang et al. demonstrated that, within the OECD-ATLAS project, experiments on Design Extension Conditions (DECs) such as Station Blackout (SBO) and Total Loss of Feedwater (TLOFW) were conducted to identify key thermal-hydraulic phenomena in high-risk MFAs, reflecting heightened safety concerns post-Fukushima [4]. Regarding risk analysis, Liu and Hwang determined that human reliability for Ultimate Response Guidelines (URG), analyzed via the SPAR-H method, is approximately 85%, though subject to decision-maker variability [5]. Tong et al. found that during severe accidents, zirconium-steam reactions produce hydrogen as core cooling deteriorates, though water in the calandria vessel and reactor cavity can suppress hydrogen generation for extended periods [6]. Rangel and Leveque noted that the definition of accidents involving interdependent events violates the independence assumption inherent in traditional Poisson models [7]. Functions classified as safety-critical functions that directly support reactor protection, emergency response, or critical decision-making were analyzed as Internet of Things (IoT) that complies with instrumentation and control (I&C) standards [8]. In addition, a research aimed to integrate complementary metal-oxide semiconductor technology (CMOS) and IoT applications for radioactive leakage detection methods on an industrial level [9].

2. Methods

2.1 Strategy for multiple failure accident (MFA)

To facilitate this analysis, Fig. 3 categorizes the MFA factors into three modeling frameworks. These are classified as natural disasters, internal facility malfunctions, and human factors. Natural disasters involve broad phenomena, with earthquakes representing one of the most critical examples. Meanwhile, the internal facility category encompasses various essential equipment systems within the NPPs. The human factors are composed of the social matters including human behaviors.



[Fig. 3] Factors for MFA.

In particular, human relationships are considered in the human factor because they are connected through internet-based networking.

2.1.1 Internet of Things (IoT) based Human Factor

IoT is included in the human factor. During the Fukushima nuclear accident, power outages caused by the earthquake and tsunami rendered all sensors monitoring the inside of the reactors inoperable. Consequently, radiation leaked without an accurate assessment of the internal situation, and the inability to track the level of risk workers were exposed to in real time caused serious setbacks in ensuring the safety of on-site personnel.

To overcome these critical limitations, advanced IoTs technologies are being actively introduced into the nuclear power sector today. First, robots and drones equipped with radiation-resistant IoT sensors and communication modules capable of withstanding strong radiation have been developed for deployment in high-radiation environments inaccessible to humans, ensuring the safe collection of on-site data.

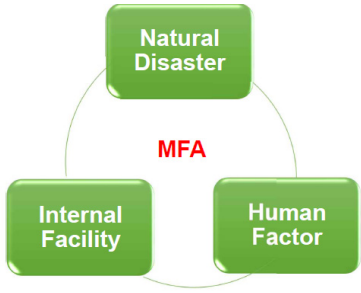
At the same time, on-site workers are provided with sensor-embedded wearable IoT devices, such as smart gas masks or smart suits. Through this, the central control room monitors key vital signs—such as workers' real-time location, cumulative radiation exposure, and heart rate—in real time. By issuing immediate evacuation orders before dangerous levels are reached, the system protects the lives of the workers.

2.1.2 Chain for MFA

Fig. 4 shows the relationship of MFA related with the natural disaster, internal facility, and human factor. There were some preventions of core damage due to multiple failures as follows [10],

- Common cause related loss of safety functions
- Some measures to prevent core damage
  - Opening of a safety-relief valve with mobile battery and/or compressor
  - Injection of the water into RPV with mobile pumping unit
  - Supplying the power from ground power unit(GPU) during SBO

In addition, the natural disaster has produced the turmoil in Fukushima site form 2011 East-Japan



[Fig. 4] Chain of MFA.

earthquake event. So, it is needed to consider the unexpected natural disasters like the flood, volcano, or even meteoroid. Although the design of plant had been made for preparing of the natural happenings, it is not imagined exactly about the scale of the natural damage. Pau Gunter said that a natural disaster can make the on-site emergency generators fail the operations and in U.S. Nuclear Regulatory Commission (NRC) report, Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants, where the core damage was estimated to begin in approximately 1 hour in the event of station blackout at the Surry and Peach Bottom NPPs for the case of the safety injection systems failures [11]. He insisted that the plant ageing, inspection/maintenance cost, safety margin, and defense-in-depth should be considered for the natural disaster related nuclear accident [11]. The analysis of the human factor is considered by the task, personal management, training/education, procedures, control room feature, reporting, and maintenance/testing [12]. The purpose of the human factor is to make the integral to the safe operation of the NPPs where

U.S. NRC had focused on both protecting and ensuring adequate training of plant staff to take the tasks [13]. So, it is considered that the operator performance should enhance the operations of the plants [13].

2.2 System dynamics (SD) algorithm

The SD was developed at MIT Sloan by Prof. Emeritus Jay W. Forrester, beginning in the 1950s [14] in which a lots of tasks like risk management, safety assessment, climate change issue, public health, and economic matters have been studied. The method is based on the non-linear complex algorithm incorporated with the random number generations. The skills are including the stock, flows, and feedback of the event where the event values are accumulated, weighting, and backward direction of event, respectively [15]. In the case of stock, it appears as follows,

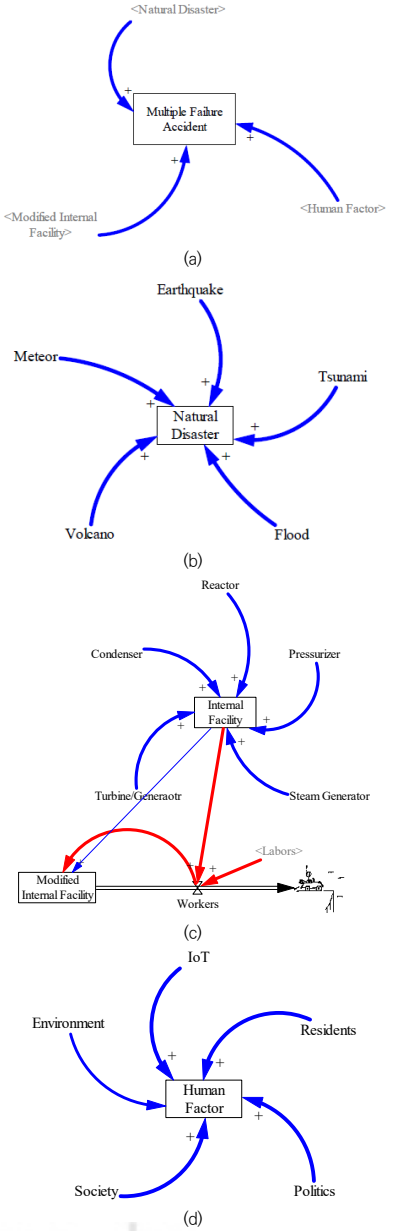
$$Stock(t) = Stock(t_o) + \int_{t_o}^{t} [Inflow(h) - Outflow(h)]dh \quad (1)$$

Stock accumulates inflows and subtracts outflows. Mathematically, the value of stock at time t is the integral of net inflows from the initial time t_o to the present plus the initial value. In addition, the equation representing feedback is as follows,

$$\frac{dN}{dt} = k \cdot N \quad (2)$$

Here, N is a variable representing the cause, and k represents the weight. This feedback loop refers to a cyclical structure where a cause reinforces an effect, and that effect, in turn, further amplifies the cause, causing the system to lose equilibrium and lead to exponential growth or destruction.

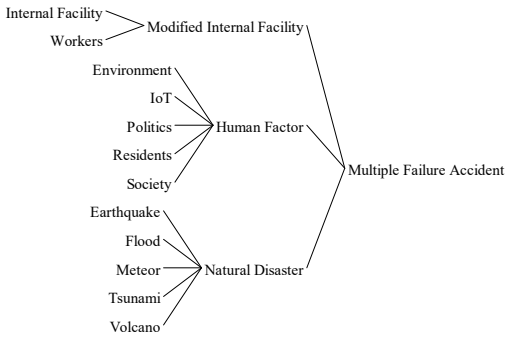
In the SD method, the procedure is very flexible and non-linear progress trend which focuses on the goal of the modeling in the designed topic. In addition, the linear modeling does not describe the complex algorithm where the feedback algorithm of the event flows. However, SD can make the arbitrary event flows. From Fig. 5, the models are shown where MFA, Disaster, Internal Facility, and Human Factor are described respectively. Here, modeling is performed using Vensim code [16].



[Fig. 5] SD Modeling (a) MFA, (b) Natural Disaster, (c) Internal Facility and (d) Human Factor.

3. Results

This study utilizes several models where the MFA is primarily composed of natural disasters, modified internal facilities, and human factors. The modified internal facility incorporates a feedback loop integrated with labor-related causal lines, meaning it is directly influenced by the worker-centric loop. Fig. 6 presents the MFA cause tree, illustrating the event connections across the scenarios of interest, while Fig. 7 displays the simulation results. The variables for Natural Disaster, Modified Internal Facility, and Human Factor are normalized to a maximum value of 1.0. Furthermore, each basic event is quantified using random numbers derived from expert judgment within specific stochastic generation frameworks. For example, in Table 2, the Earthquake value has the random number of 0 or 1 where the random number between 0 and 1 is lower than 0.3, the value is 0. Otherwise, it is 1. Consequently, the basic elements have the values and they are calculated by arithmetic operations as addition, subtraction, multiplication, or division. If there is any mathematical equation made by the operator, it could be used. In Fig. 7 (d), the value increased gradually which means that the MFA possibility could be increased as the time goes on. The quantity is compared as the relative value. The calculation was repeated 121 times at time intervals over the 60-year lifespan of the proposed NPP, and the difference between the initial value and the final value was 2.412 (= 2.05/0.85), which means that the final value is 2.412 times higher than the initial value. In addition, the sensitivity analysis is shown in Table 3, with a standard deviation of 0.4390. Compared to the mean value, it is 30% (=0.4390/1.4262).



[Fig. 6] Causes tree for MFA.

〈Table 2〉 Basic elements of MFA

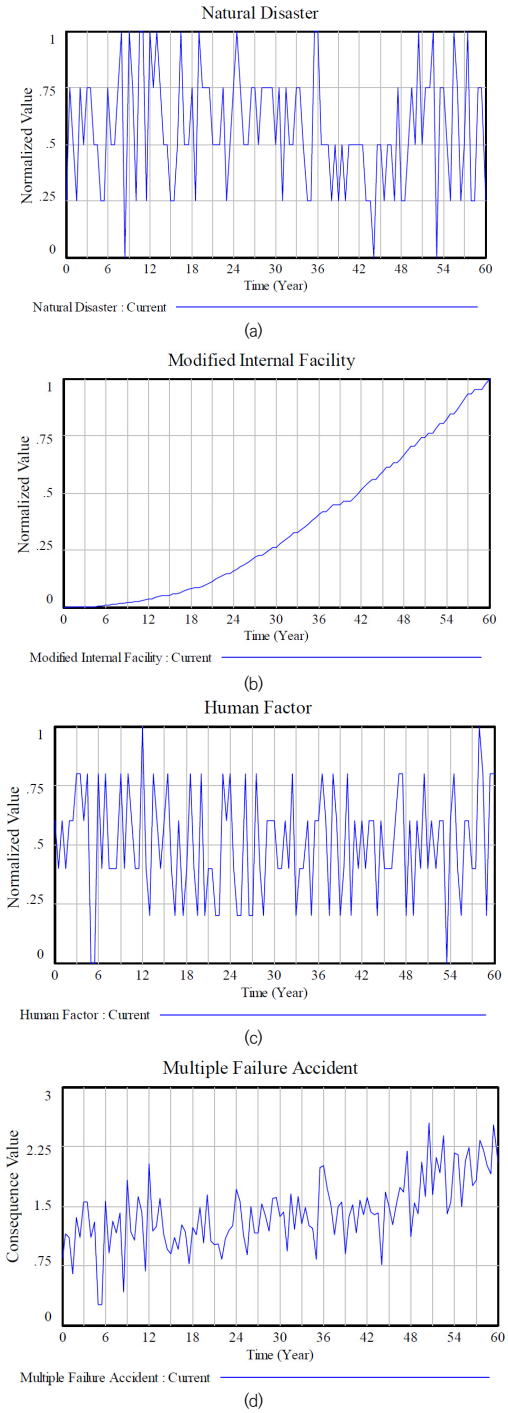
Parameter	Value
Earthquake	if then else(random 0 1 () < 0.3, 0, 1)
Tsunami	if then else(random 0 1 () < 0.4, 0, 1)
Flood	if then else(random 0 1 () < 0.3, 0, 1)
Volcano	if then else(random 0 1 () < 0.7, 0, 1)
Meteor	if then else(random 0 1 () < 0.9, 0, 1)
Reactor	if then else(random 0 1 () < 0.3, 0, 1)
Pressurizer	if then else(random 0 1 () < 0.2, 0, 1)
Steam Generator	if then else(random 0 1 () < 0.2, 0, 1)
Turbine/Generator	if then else(random 0 1 () < 0.1, 0, 1)
Condenser	if then else(random 0 1 () < 0.2, 0, 1)
IoT	if then else(random 0 1 () < 0.7, 0, 1)
Residents	if then else(random 0 1 () < 0.5, 0, 1)
Politics	if then else(random 0 1 () < 0.6, 0, 1)
Society	if then else(random 0 1 () < 0.4, 0, 1)
Environment	if then else(random 0 1 () < 0.3, 0, 1)

4. Conclusions

Since the Fukushima disaster, MFAs have been prioritized for severe accident prevention. This paper aims to enhance safety measures within nuclear power plants. Consequently, a robust protocol for preventing nuclear accidents involving

MFAs can be effectively established. There are some important points of this study as follows,

- The MFA is investigated.
- The Fukushima case is exampled.
- Advanced safety assessment is introduced.
- MFA is controlled by new strategy.



[Fig. 7] Results for MFA (a) Natural Disaster, (b) Modified Internal Facility, (c) Human Factor, and (d) MFA.

〈Table 3〉 Sensitivity of MFA

	Min.	Max.	Mean	Median	St. Dev.
MFA	0.2547	2.5425	1.4162	1.4040	0.4390

Furthermore, developing nuclear safety analysis programs for NPPs remains essential. This paper's SD program demonstrates flexible algorithmic applications for complex, simultaneous accidents like an MFA. The SD feedback logic quantifies how future events influence prior ones, providing operators with dynamic numerical data.

Consequently, operators can prepare for unexpected disasters using relative metrics, comparing current values against historical data. This allows operators to assess disaster probabilities where human factors, natural hazards, and plant systems interact. It is needed to make the safety improvement strategy in MFA-related systems. For the safety regulation, it is considered for the new regulation to include the MFA matters. It has been witnessed that the nuclear accident happened by several kinds of the events with inter-correlations, especially for the Fukushima case. Although the plant design focuses on a single event, the accident has the tendency to be produced by the complex multiple consequences. So, the SD based modeling could be a regulation of the nuclear related protocols.

For the applications of nuclear MFAs by gas cooled reactor and liquid metal reactor as well as light water reactor, new scenarios are needed. In the case of the gas cooled reactor, the gas leak accident could produce the MFA with the combinational accident in the plant systems. The nuclear fuel matter could make the hydrogen explosion where the water should be isolated from the primary loop in the helium coolants of the high temperature gas cooled reactor (HTGR). However, the leak of the secondary pipe could make the explosion of the hydrogen. Furthermore, the blocking of the piping can make the unexpected explosion of the hydrogen due to the failure of heat cooling. In the case of the liquid metal

reactor, the sodium is very easy to make the explosion in the accident of the leak to atmosphere where the moisture exists. Although the highly cautious system of the liquid metal coolant is performed, the leak accident could be happened. So, it is necessary to prepare of the coolant leak accident should be estimated.

Unlike conventional Probabilistic Safety Assessment (PSA) or CCF analysis, in this study, SD views the risks of complex systems not as fixed snapshots, but as dynamic processes that change over time. Unlike existing methods that rely on linear causality, SD models feedback loops and non-linear interactions to capture phenomena where safety measures produce unintended side effects. Furthermore, unlike Human Reliability Analysis (HRA), it does not isolate human error but addresses technology, organizational culture, and economic pressures within a single integrated socio-technical system.

In the analysis of the Fukushima nuclear accident, SD clearly identifies 'Inter-unit interference' and 'Risk amplification over time,' which were overlooked by existing expert assessments or safety analysis tools (such as PSA). While existing tools treated each reactor and emergency generator as independent entities and thus failed to predict simultaneous failures, SD is capable of dynamically capturing feedback loops where power loss, high pressure conditions, and radioactive contamination exacerbate one another. Consequently, SD demonstrates a distinctiveness by going beyond the probability of individual component failure to prove, through organic causal relationships, how the entire safety system collapsed like a domino effect due to the combination of organizational response delays and physical risk factors.

It is suggested for international co-work related to the International Atomic Energy Agency (IAEA). The NPPs have similar systems in the worldwide market. So, the preparations for the MFA could be done by cooperation about multinational tasks where the IAEA has a role of the management of the cooperation. Regular meeting and conference can improve the quality of constructing the MFA regulations. In addition, another study of close cooperation for natural disaster is necessary. Especially, the earthquake and volcano around the Pacific-Rim region should be investigated for the exact and rapid information exchange. There are many NPPs and the increasing rates are higher where the Japan and China are closely located.

REFERENCES

[1] WNA. Fukushima Accident, World Nuclear Association, London, UK, 2015.

[2] S.V.Prasad, A.K.Nayak, P.P.Kulkarni, P.K.Vijayan and K.K.Vaze, "Study on heat removal capability of calandria vault water frommolten corium in calandria vessel during severe accident of a PHWR," Nuclear Engineering and Design. Vol. 284, pp.130-142, 2015.

[3] V.Hassija, C.S.Kumar and K.Velusamy, " Probabilistic safety assessment of multi-unit nuclear power plant sites - An integrated approach," J. Loss Prev. Proc. Ind. Vol.32, pp.52-62, 2024.

[4] K.H.Kang, B.U.Bae, J.R.Kim, Y.S.Park, S.W.Lee, C.H.Song and K.Y. Choi, "Development of a phenomena identification ranking table for simulating a station blackout transient of a pressurized water reactor with a thermal-hydraulic integral effect test facility," Annals of Nuclear Energy. Vol.75, pp.72-78, 2015.

[5] The procedures of ultimate response guideline for nuclear power plants," Nuclear Engineering and Design. Vol.273, pp.234-240, 2014.

[6] L.Tong, J.Zou and X.Cao, "Analysis on hydrogen risk mitigation in severe accidents for Pressurized Heavy Water Reactor," Progress in Nuclear Energy. Vol.80, pp.28-135, 2015.

[7] L.E.Rangel and F.Leveque, "How Fukushima Dai-ichi core meltdown changed the probability of nuclear accidents?" Safety Science. Vol. 64, pp.90-98, 2014.

[8] F.E.Arhouni, M.A.S.Abdo, S.Ouakkas, A.Boukhair, "Digital twins in nuclear science and Engineering: Bridging AI, Real-Time Data, and physical systems," Annals of Nuclear Energy. vol.237, p.112469, 2026.

[9] S.Patel, S.Sutaria, R.Daga, M.Shah, M.Prajapati, "A systematic study on complementary metal-oxide semiconductor technology (CMOS) and Internet of Things (IOT) for radioactive leakage detection in

nuclear plant," Nuclear Analysisnce. Vol. 2, p.100080, 2023.

[10] T.Fuketa, "Lessons Learned from the Fukushima Dai-ichi Accident and Responses in New Regulatory Requirements," International Experts' Meeting on Severe Accident Management in the Light of the Accident at the Fukushima Daiichi Nuclear Power Plant, Vienna, Austria March 17, 2014.

[11] P. Gunter, "Natural Disasters and Safety Risks at Nuclear Power Stations, Nuclear Information and Resource Service," Washington, DC, USA, 2004.

[12] NEA, NEA Issue Brief: An analysis of principal nuclear issues, OECD Nuclear Energy Agency (NEA), Issy-les-Moulineaux, France, 1988.

[13] NRC, Human Factors, U.S. Nuclear Regulatory Commission (NRC) Washington, DC, USA, 2014.

[14] MIT, System dynamics, MIT Sloan School of Management, MA, USA, 2022,

[15] SDS. What is System Dynamics? System Dynamics Society (SDS), Albany, NY, USA, 2022.

[16] Ventana, Vensim, Ventana Systems, Inc. Harvard, USA, 2016.

장 경 배(Kyung-Bae Jang) [종신회원]

- 1995년 2월 : 광주과학기술원 기전공학과(공학석사)
- 2006년 8월 : 고려대학교 전기공학과(공학박사)
- 1997년 2월 ~ 2000년 3월 : SK 하이닉스 주임연구원
- 2000년 4월 ~ 2008년 8월 : 현대모비스 선임연구원
- 2008년 12월 ~ 2013년 5월 보건복지부 국립재활원 공업연구관
- 2014년 3월 ~ 2025년 2월 : 고려사이버대학교 기계제어공학과 교수
- 2025년 3월 ~ 현재 : 강원대학교 전기공학과 교수

〈관심분야〉
사물인터넷, 제어시스템, 로봇

우 태 호(Tae-Ho Woo) [정회원]

- 1991년 2월 : 경희대학교 원자력공학과 (공학사)
- 1993년 2월 : 서울대학교 원자핵공학과 (공학석사)
- 1999년 8월 : 미시간대학교 원자핵 및 방사선공학과 (공학석사)
- 2013년 2월 : 서울대학교 에너지시스템공학부 (공학박사)
- 2007년 3월 ~ 2013년 2월 : 서울대학교 에너지시스템공학부 BK21연구원
- 2015년 9월 ~ 현재 : 고려사이버대학교 기계제어공학과 교수

〈관심분야〉
사물인터넷, 에너지, 원자력, 정책