Nuclear Engineering and Technology 49 (2017) 1414–1422

Contents lists available at ScienceDirect

Nuclear Engineering and Technology

journal homepage: www.elsevier.com/locate/net

Original Article

A new approach to quantify safety benefits of disaster robots

Inn Seock Kim [a, *], Young Choi [b], Kyung Min Jeong [b]

[a] ISSA Technology, Inc., 21318 Seneca Crossing Drive, Germantown, MD 20876, USA
[b] Korea Atomic Energy Research Institute, 989-111 Daedeok-daero, Yuseong-gu, Deajeon 34057, Republic of Korea

ARTICLE INFO

Article history:
Received 25 July 2016
Received in revised form
30 April 2017
Accepted 4 June 2017
Available online 1 July 2017

Keywords:
Disaster Robot
PRA
Remote Response
Robot
Safety Benefit

ABSTRACT

Remote response technology has advanced to the extent that a robot system, if properly designed and deployed, may greatly help respond to beyond-design-basis accidents at nuclear power plants. Particularly in the aftermath of the Fukushima accident, there is increasing interest in developing disaster robots that can be deployed in lieu of a human operator to the field to perform mitigating actions in the harsh environment caused by extreme natural hazards. The nuclear robotics team of the Korea Atomic Energy Research Institute (KAERI) is also endeavoring to construct disaster robots and, first of all, is interested in finding out to what extent safety benefits can be achieved by such a disaster robotic system. This paper discusses a new approach based on the probabilistic risk assessment (PRA) technique, which can be used to quantify safety benefits associated with disaster robots, along with a case study for seismic-induced station blackout condition. The results indicate that to avoid core damage in this special case a robot system with reliability > 0.65 is needed because otherwise core damage is inevitable. Therefore, considerable efforts are needed to improve the reliability of disaster robots, because without assurance of high reliability, remote response techniques will not be practically used.

1. Introduction

The nuclear robotics team of the Korea Atomic Energy Research Institute (KAERI) has long been involved in robot development for a variety of applications such as remote inspection and maintenance of steam generator tubes, emergency operation of fuel exchange machines in the calandrias of pressurized heavy water reactors, and remote dismantling of radioactive equipment to support decommissioning of nuclear power plants [1]. Some of the lessons we can learn from the accident at the Fukushima Daiichi Nuclear Power Station on March 11, 2011, are, among others, that: (1) the coping capabilities of nuclear power plants against beyond-design-basis external events such as a strong earthquake or a large tsunami wave must be further enhanced; (2) nuclear disasters may create a harsh environment (e.g., radiation, heat, humidity, contamination, or darkness in the case of loss of all electric power) that will impede human mitigating actions; and (3) remote response technology is needed because of potentially hazardous environment in the field.

As there have been great advances in the capabilities of disaster robots [2–4], as demonstrated in the international competitions of the Defense Advanced Research Projects Agency (DARPA) Robotics Challenge [5], it is envisaged that robotics and remote systems, if they are properly designed and deployed to the field in accordance with an architecture for high performance, might be practically used in the near future to implement certain response actions in the harsh environment caused by an extreme event [6]. However, as Murphy [2] pointed out, development of disaster robots such as unmanned ground vehicles (UGVs) will encounter considerable challenges because disasters present extreme terrains and operating conditions that affect size, sensor performance, and general robot survivability. The use of robotic systems in the Fukushima Daiichi plant following the accident also indicates that robots may fail due to communication error, loss of power, or failure of effectors such as arms or legs. In addition to these technical challenges, significant research efforts and resources will be needed to construct practically usable robotic systems.

Therefore, as a part of efforts to make a disaster robot system, we developed a method to evaluate the potential safety benefits that successfully deployable robots could bring about. This method is based on the probabilistic risk assessment (PRA) technique [7,8], which is widely used in the nuclear power community as a standard method for quantitative evaluation of the risk associated with nuclear power generation. The selection of the

* Corresponding author.
E-mail address: isk@issatechinc.com (I.S. Kim).

http://dx.doi.org/10.1016/j.net.2017.06.008

target scenario in the PRA-based approach is built on lessons learned from a number of research and development activities in the aftermath of notable events including the September 11 terrorist attacks and the Fukushima accident, such as B.5.b mitigation strategies [9] and FLEX coping strategies [10]. This paper presents a novel approach along with a case study including risk sensitivity analysis of the safety benefits as a function of the robotic mission failure probability.

2. Basic concept of evaluating robotic safety benefits

The approach to evaluating the safety benefits that a disaster robotic system might bring about is based on the PRA technique, as mentioned earlier. Although there are many different types of PRA (e.g., internal events PRA for steam generator tube rupture or loss of coolant type events; external events PRA for earthquake or external flooding; and Levels 1, 2, or 3 PRA depending on the end state of the analysis), the risk associated with nuclear plant operation is quantified by a PRA model in terms of accident sequences that can be basically represented by:

$$IE * HW_i * SW_j * HE_k * NR_l$$

where IE, HW_i, SW_j, HE_k, and NR_l indicate initiating event, hardware failures, software (or digital component) failures, human errors, and nonrecovery events (e.g., failure to recover offsite power or failure to repair inoperable equipment), respectively. The subscripts imply that zero or any number of such events may be included in a specific sequence. In a special case in which no such events are included at all, the initiating event then directly causes the end state (e.g., core damage).

The accident sequences for a nuclear power plant can be generated by carrying out the following analyses in the case of Level 1 PRA for a nuclear reactor that is targeted for quantification of core damage frequency (CDF) [11]: (1) initiating event analysis to identify and quantify events that could lead to core damage; (2) accident sequence analysis to determine combinations of initiating events, safety functions, and system failures and successes that may lead to core damage; (3) success criteria analysis to define individual function successes; (4) systems analysis to identify and quantify the causes of system failures; (5) human reliability analysis to identify potential human failure events and estimate the associated probabilities; (6) data analysis to provide estimates of the parameters used to determine the probabilities of the basic events representing equipment failures and unavailabilities modeled in the PRA; and (7) quantification to provide an estimate of CDF based on plant-specific core damage scenarios.

A huge number of accident sequences are generated in general by quantifying a PRA model, and the total risk is obtained by summing up the frequencies of all the accident sequences above a certain truncation level. Note that an accident sequence consists of a single initiating event and any number of each of the four different types of subsequent events described above (i.e., HW, SW, HE, and NR). Therefore, robotic safety benefits can be quantified in terms of the impact of the robotic intervention on the accident sequences, and the type of the initiating event to be used should be determined up front, as will be discussed later.

3. Quantification approach

In the case of an extreme event causing hazardous environment, various types of accident mitigation actions might be performed by disaster robots in nuclear power plants. Example robotic actions include: (1) assess the plant situation (e.g., temperature, humidity, hydrogen concentration, radiation); (2) establish emergency flow paths by opening locked closed valves; (3) operate a portable diesel generator (DG) and circuit breakers to provide emergency power; (4) provide external coolant makeup into the reactor or the spent fuel pool; and (5) conduct reconnaissance within the nuclear power plant or over the site during or following a severe accident.

The underlying assumption here is that the robotic system can be made to access the location where these actions can be performed. Because the route of the robotic system might be damaged by the extreme event (e.g., earthquake), a debris removal robot might have to be included as part of the robotic system consisting of UGVs [2]. In addition, the emergency equipment needed for accident mitigation, such as portable pumps, generators, hoses, electrical cables, or fuel should be brought to the location along with the robotic system. Because modern robotics has advanced to the extent that a robot can drive a vehicle, as seen in the 2015 DARPA Robotics Challenge (DRC) [5], development of such multi-task robotic systems in the near future looks feasible. The approach to quantify the robotic safety benefits is discussed next (Fig. 1).

3.1. Definition of risk metric

To quantify the safety benefits of the remote response technique, a risk metric that will be used for the quantification needs to be first determined. Several different types of risk metrics are typically used in analyzing risks for nuclear power plants: (1) core damage frequency (CDF); (2) large release frequency (LRF) or large early release frequency (LERF); and (3) health effects such as early fatality or late cancer fatality.

These risk metrics are quantified by Level 1, Level 2, and Level 3

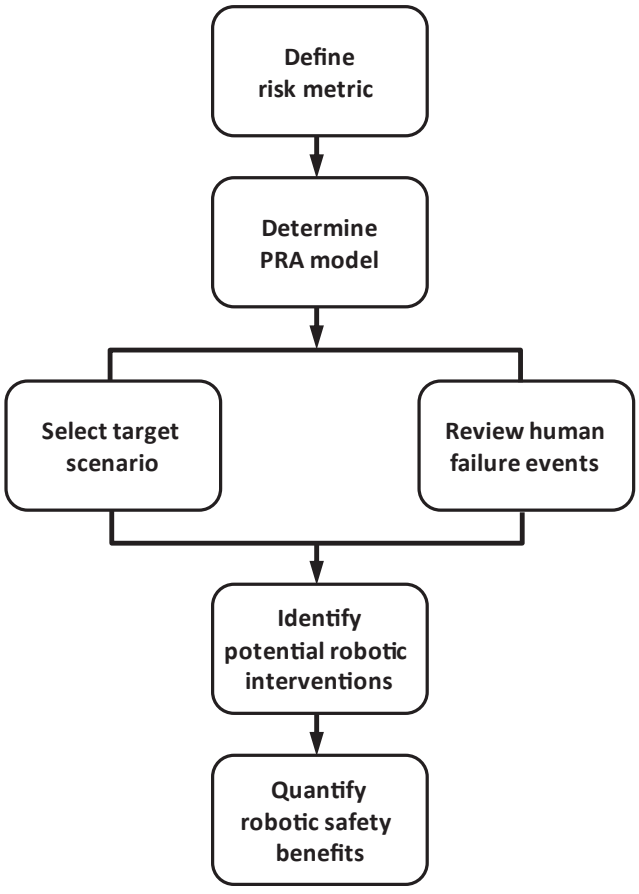

Fig. 1. Quantification approach for robotic safety benefits. PRA, probabilistic risk assessment.

PRAs, respectively. Although they are typically represented in terms of annual frequencies of occurrence, there exists similar risk metrics represented in terms of probability, such as conditional core damage probability (CCDP), conditional large release probability (CLRP), or conditional large early release probability (CLERP). These probability-based risk metrics are used to measure the risk conditional upon the occurrence of a specific initiating event. As the safety impact of robotic interventions will be assessed for a specific situation of station blackout (SBO), probability-based risk metrics will be used rather than frequency-based ones.

In this study, conditional core damage probability is used as the risk metric to quantify the robotic safety benefits. The degree of CCDP reduction by robotic intervention represents the safety impact of the accident mitigating actions performed by the robotic system. Where the risk of spent fuel pool (SFP), i.e., the risk associated with the radioactive materials stored in the pool, is concerned, the term fuel damage frequency (FDF) is oftentimes used instead of CDF. Therefore, if robot interventions are made for accident scenarios associated with the SFP, then the safety benefits will be measured in terms of conditional fuel damage probability (CFDP). Note that core damage frequency was also selected as a surrogate for risk in the state-of-the-art reactor consequence analyses (SOARCA) study [12] recently performed by the United States (US) Nuclear Regulatory Commission (NRC). SOARCA represents state-of-the-art reactor consequence analyses that involved detailed, integrated, and realistic analyses of severe accidents at nuclear power reactors based on decades of research and experience to model accident progression, mitigation, emergency response, and health effects. The accident scenarios investigated in SOARCA will be discussed later.

3.2. Determination of PRA model

Once the risk metric to be used for the safety benefit quantification is determined, the PRA model then can be chosen, as shown in Fig. 1. For instance, if either CDF or CCDP is adopted as the risk metric, then the Level 1 PRA model can be used. When LRF, LERF, CLRP, or CLERP is used, the Level 2 PRA model is needed. In this study, the Level 1 PRA model will be used because of the adoption of CCDP as the risk metric, as mentioned above. Another consideration in this regard is which will be used between internal and external event PRA models for the quantification of safety benefits. In the case where the seismic-induced SBO conditions will be used as the target scenario, the external events PRA model, more specifically the seismic PRA model, might be preferred. However, as the internal events PRA model is more readily available and the target scenario can be modified to reflect the seismic conditions, the internal events model is used in this study.

3.3. Selection of target scenario

A critical step in the quantification approach (Fig. 1) is the selection of the target scenario in which the robotic intervention will be made. A challenging scenario may be preferably selected so that substantial safety benefits can be achieved. The most challenging accident type can be found in the activities of the nuclear power community following the September 11 terrorist attacks [9] and the recent Fukushima accident [10], as well as in the SOARCA of the NRC [12]. After the September 11 terrorist attacks, the NRC analyzed what might happen in the case of an aircraft attack on a nuclear power plant. The largest impact in such a case was determined to be a loss of large area, especially resulting in loss of all AC and DC power at a single unit as a consequence of an aircraft crash on the Control Room building. The Fukushima accident also involved a loss of all AC power, namely station blackout, as a result of the strong earthquake and concomitant tsunami [13].

In the SOARCA consequence study [12] the following accident scenarios were evaluated: (1) long-term station blackout (LTSBO); (2) short-term station blackout (STSBO); and (3) interfacing systems loss-of-coolant accident (ISLOCA).

LTSBO refers to an SBO event where core damage occurs relatively late, e.g., 4–8 h after loss of offsite power (LOOP), because of availability of DC control power until battery depletion, and secondary cooldown through the steam turbine-driven auxiliary feedwater (AFW) pump at a pressurized water reactor (PWR) nuclear power plant. STSBO also involves the loss of turbine-driven systems through loss of DC control power or loss of the condensate storage tank, and therefore proceeds to core damage more rapidly (hence “short term”). ISLOCA is caused by an unisolated rupture of low head safety injection piping outside the containment. Because of the rapid progression of the accident in the case of STSBO or ISLOCA, LTSBO can be selected as the target scenario for robotic interventions. Note also that the SOARCA analysis was performed assuming that those scenarios were initiated by a seismic event, because seismically induced equipment failures occur immediately following the seismic event, which produces the most severe challenge to the plant. In other studies for extreme events, e.g., the FLEX coping strategies [10] following the Fukushima accident, loss of all AC power caused by severe natural phenomena (especially, a seismic event) was also the primary focus. In view of all these developments, seismic-induced SBO condition is adopted as the target scenario to quantify the robotic safety benefits.

3.4. Review human failure events

Once the target scenario is selected, the human failure events (HFEs) modeled in the target scenario should be examined. First of all, one needs to check each top event of the SBO event tree and select those top events involving HFEs for which robotic interventions might be made. The fault trees for the selected top events can then be reviewed with special consideration given to the HFEs and the associated plant condition, along with other factors that may influence the human performance.

A number of diverse mitigation measures may be available against potential challenges to the plant, and hence should be taken into account. As a result, it is necessary to understand what kinds of mitigating measures are available at the site, especially including those new features augmented to the nuclear power plants following the Fukushima accident. Furthermore, how these measures are intended to be applied during the course of an evolving accident also needs to be understood. The ways in which the mitigating features will be employed in case of an abnormal or emergency condition are specified in the plant procedures or guidelines, such as the abnormal operating procedures (AOP), emergency operating procedures (EOP), severe accident management guidelines (SAMG), extensive damage mitigation guidelines (EDMG) [9], and FLEX support guidelines (FSG) [10].

Of these, the EDMG was developed in the aftermath of the September 11, 2001, terrorist attacks in the USA, and the FSG as a consequence of the March 11, 2011, Fukushima accident. As portable equipment, such as beyond-design-basis high capacity pumps with associated hoses and fittings, portable DGs with associated cables, connectors and switchgear, are being augmented to nuclear power stations [14] to cope with beyond-design-basis events, along with special usage guidelines, these aspects may be taken into account in reviewing human failure events.

3.5. Identification of potential robotic interventions

Following the investigation of how plant personnel will respond to extreme events in accordance with the guidelines, the mitigating

actions that might be performed by a robotic system in harsh environments can be identified. As there are a large variety of mitigation measures that might be taken to cope with an evolving extreme event and as the development of a disaster robot will require considerable efforts and resources, it is necessary to identify safety-significant mitigation measures that will be implemented by remote response technique. Potential robotic interventions can be identified by reviewing human failure events included in the dominant accident sequences of the PRA model. In particular, in consideration of the state of the art in robotics and remote systems technology, the context of the human actions associated with the HFEs needs to be examined, along with the feasibility of robotic interventions to replace human actions. It may also be mentioned that importance analysis of HFEs for the target scenarios can be performed and the selection of a risk-significant human action in terms of high importance value will generally result in a large safety benefit.

3.6. Quantification of robotic safety benefits

Once potential robotic intervention is determined in connection with a risk-significant human failure event modeled in the PRA, risk sensitivity analysis can be conducted for the target scenarios using the computerized PRA program. For the sake of clarity, let us assume that a human failure event has been identified, the action associated with which might be performed by a disaster robotic system in lieu of the human operator (e.g., due to the harmful environment caused by a strong earthquake). A sensitivity analysis of the robotic safety benefits can then be conducted to examine the effect of the robotic mission failure probabilities on the risk metric such as the CCDP, as will be illustrated below. Note here that the specific probability of the human failure event, as estimated in the human reliability analysis of the PRA, can be used as a barometer to compare the reliabilities of the human and robotic interventions.

4. Case study

4.1. Salient aspects and assumptions

In order to identify how much safety benefit can be achieved by the use of remote response technology, the safety benefits can be quantified using the aforementioned approach. The salient aspects of this quantification approach and the associated assumptions are as follows: (1) station blackout condition induced by a strong earthquake (e.g., a peak ground acceleration in the range of 0.2–0.3g) is used as the target scenario for which the robotic safety benefit will be evaluated; (2) the conditional core damage probability for LOOP and SBO conditions is used as the risk metric in this analysis. If the spent fuel pool is considered along with the reactor core as a potential radiological source that may release radioactivity in the SBO condition, the conditional fuel damage probability could be used together with CCDP. However, the condition of the spent fuel pool is not considered in this simplified approach; (3) an internal events PRA model for a PWR plant is used with an increase of all the human error probabilities (HEPs) and nonrecovery probabilities in the target scenario by an order of magnitude to reflect the seismic condition. In performing a seismic PRA based on the internal events PRA model, a variety of different adjustments are typically made to the HEPs developed for analyzing the internal events [15,16]. However, an increased factor of 10 is conservatively applied to the human error probabilities and nonrecovery probabilities in this example; (4) the earthquake might create a harsh environment (e.g., high heat, humidity, contamination, radiation) and unforeseen situations at the plant beyond the scope of expectation and imagination. Hence, it is assumed that at least 5–6 h will be needed for successful robotic interventions (i.e., deployment to the location where mitigating measures can be taken with subsequent successful execution of the mitigating actions); (5) the risk associated with a loss of offsite power depends on whether the plant is critical or shut down. It is assumed here that the plant was at power, as a loss of offsite power presents a greater challenge to the plant in general if it occurs during at-power condition as opposed to shutdown state; and (6) in modeling the SBO condition, all the DGs dedicated to the unit (i.e., DG A and DG B in the case of the nuclear power plant used in this study) are conservatively assumed to fail due to the same failure mode, i.e., failure to start, and the potentials for not only double but also triple common cause failures (CCFs) to start among the three DGs (i.e., DG A, DG B, and SBO DG) are accounted for in the risk quantification.

4.2. LOOP and SBO models

A typical event tree for loss of offsite power at a PWR is shown in Fig. 2, in which the LOOP scenarios are modeled in terms of 13 top events representing safety functions and recovery of AC power [17]. The first top event is “Reactor trip”. The upper branch under this top event represents a successful reactor trip (i.e., insertion of the control rods into the core), although the lower branch is a failure of the reactor trip, i.e., an anticipated transient without scram (ATWS). The ATWS scenarios are modeled in another subsequent event tree (i.e., transfer to ATWS event tree). The second top event in the event tree is “Emergency power”, and the lower branch under it represents an SBO condition because of failures of all unit-dedicated DGs (i.e., DG A and DG B in the PRA model used in this study) given a LOOP. The SBO scenarios are modeled in the separate event tree shown in Fig. 3. Other top events in Fig. 2 can be interpreted in a similar manner. Another thing to note in Fig. 2 is the end state represented at the end of the event tree structure. Other than LOOP-1 (an event tree to model reactor coolant pump seal cooling scenarios), SBO (an event tree to model SBO scenarios), and ATWS (an event tree to model ATWS scenarios), the end state is either OK (no core damage) or CD (core damage). It is the SBO scenarios in which the robotic system might help to intervene so as to avoid core damage.

In Fig. 3, the SBO scenarios are modeled as a link to the LOOP event tree given failure of the emergency power system. If both offsite and onsite emergency power are unavailable, secondary cooling is required. The steam turbine-driven AFW pump is the only equipment available for secondary cooling to remove decay heat from the reactor core in a station blackout condition at a PWR plant. Once secondary cooling has been established, the reactor coolant system (RCS) pressure is questioned to determine if a power-operated relief valve (PORV) has been challenged. If the PORVs have been challenged, then the PORVs must reclose. In addition to the PORVs, the integrity of the RCP seals will also be challenged during the SBO condition. If the RCP seals are still intact, then secondary cooling can place the plant in a stable condition once AC power is recovered. AC power recovery is required prior to battery depletion. Once the batteries are depleted, no pump control will be available. The turbine-driven AFW pump is thus assumed to fail if the AC power is not recovered before battery depletion (i.e., within 8 h in the case of the PWR plant used in this analysis). In view of the SBO event tree, the robotic system could be developed to assist in mitigation of those SBO scenarios where: (1) a turbine-driven AFW pump successfully functions with control power provided from the batteries; (2) PORVs do not open or, if opened, are successfully reclosed; and (3) RCP seals do not fail. In these scenarios, 8 h will be available to recover AC power in the sample PWR plant. In the case of other scenarios such as those involving the turbine-driven AFW pump failure or RCP seals failure, robotic

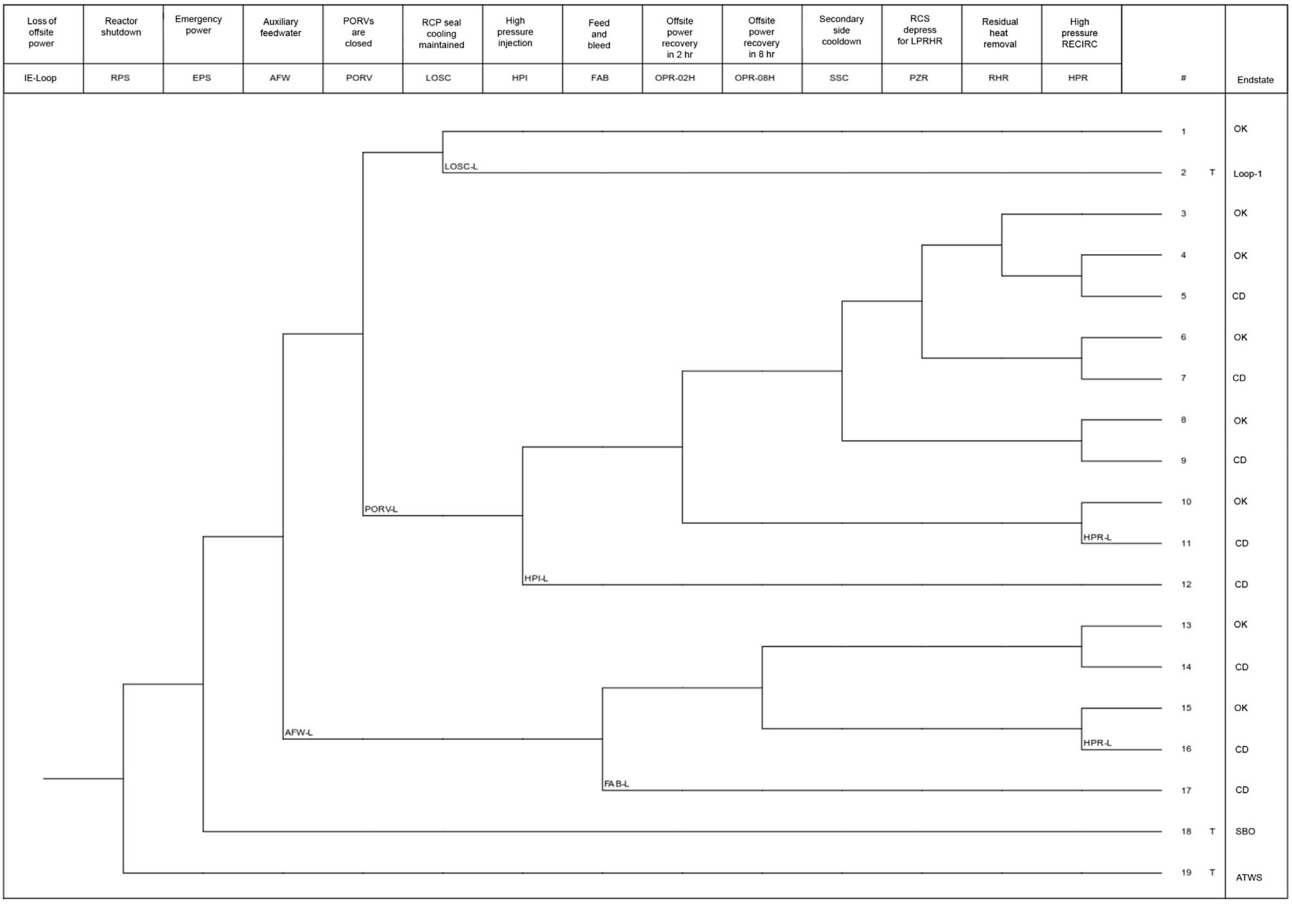

Fig. 2. Loss of offsite power event tree. AFW, auxiliary feed water; ATWS, anticipated transient without scram; CD, core damage; EPS, emergency power; FAB, feed and bleed; HPI, high pressure injection; HPR, high pressure recirculation; LOOP, loss of offsite power; LOSC, loss of seal cooling; OPR-O2H, offsite power recovery in 2 h; OPR-O6H, offsite power recovery in 6 h; PORV, power-operated relief valve; RHR, residual heat removal; RPS, reactor shutdown; SBO, station blackout; SSC, secondary side cooldown.

systems would not be able to intervene in those fast-evolving events in such a short mission time of 1 h.

A fault tree is used to model each top event shown in the LOOP and SBO event trees. One of the most important fault trees modeling the SBO condition is the fault tree for the emergency power system (EPS), which is connected to the top event EPS of the LOOP event tree (Fig. 2). Given a LOOP event, onsite emergency DGs are required to start and supply emergency power to the division buses for the safety equipment. If the emergency DGs fail, then a station blackout occurs. The SBO condition exists at the plant until the SBO DG is successfully connected to either of the safety buses, or until the offsite power or one of the emergency DGs is recovered. The various failure modes of the two unit-dedicated DGs and the SBO DG are modeled in terms of the EPS fault tree depicted in Fig. 4, where the triangle symbol indicates that the event is modeled by a subtree. It is the basic event included in this figure, i.e., ACP-XHE-XM-ALT (Operator fails to start and align SBO DG), that is used to model the robotic intervention. A risk sensitivity analysis for the robotic intervention was also performed by evaluating the CCDP as a function of the probability of this basic event.

4.3. Data modifications

A strong earthquake (i.e., in the range of 0.2–0.3*g* seismic intensity) is assumed to have occurred, with the reactor tripped but the offsite power lost due to the seismic impact. Because an internal events PRA model is used to quantify the safety benefit of the robotic intervention, the probabilities of human failure events and nonrecovery events are increased by a factor of 10 or to the maximum probability of 1.0 to reflect the seismic condition. As indicated in Table 1, the probabilities for AFW-XHE-XM-TDP, ACP-XHE-XM-ALT and OEP-XHE-XL-NR08H were increased by a factor of 10. However, the probabilities for EPS-XHE-XL-SBORMC, OEP-XHE-XL-NR02H, and EPS-XHE-XL-NR08H were increased to the maximum probability of 1.0. Some of the SBO scenarios include offsite power or emergency diesel nonrecovery events for different time intervals (e.g., OEP-XHE-XL-NR04H for 4 h and EPS-XHE-XL-NR06H for 6 h), and the probabilities for all these events were also modified in a similar manner.

Note that the modification of the human error probabilities (HEPs) in this way is consistent with the approach taken in the seismic PRA of the Kewaunee nuclear power plant [16] where, given a seismic intensity between 0.12*g* and 0.36*g*, a factor of 10 was applied to the HEPs; however, the maximum HEP of 1.0 was assumed for the intensity larger than 0.36*g*. In addition, it is also notable that in the internal events PRA model adopted in this study, the failure probability of the human mitigating action selected for robot intervention, i.e., ACP-XHE-XM-ALT, was originally estimated at 0.02 in consideration of the following: (1) this human failure event is associated with only action because little diagnosis is needed; (2) the operators have just enough available time to start and align the SBO DG given that dedicated diesels are unavailable; and (3) the stress level is greater than nominal due to the failure of the dedicated DGs.

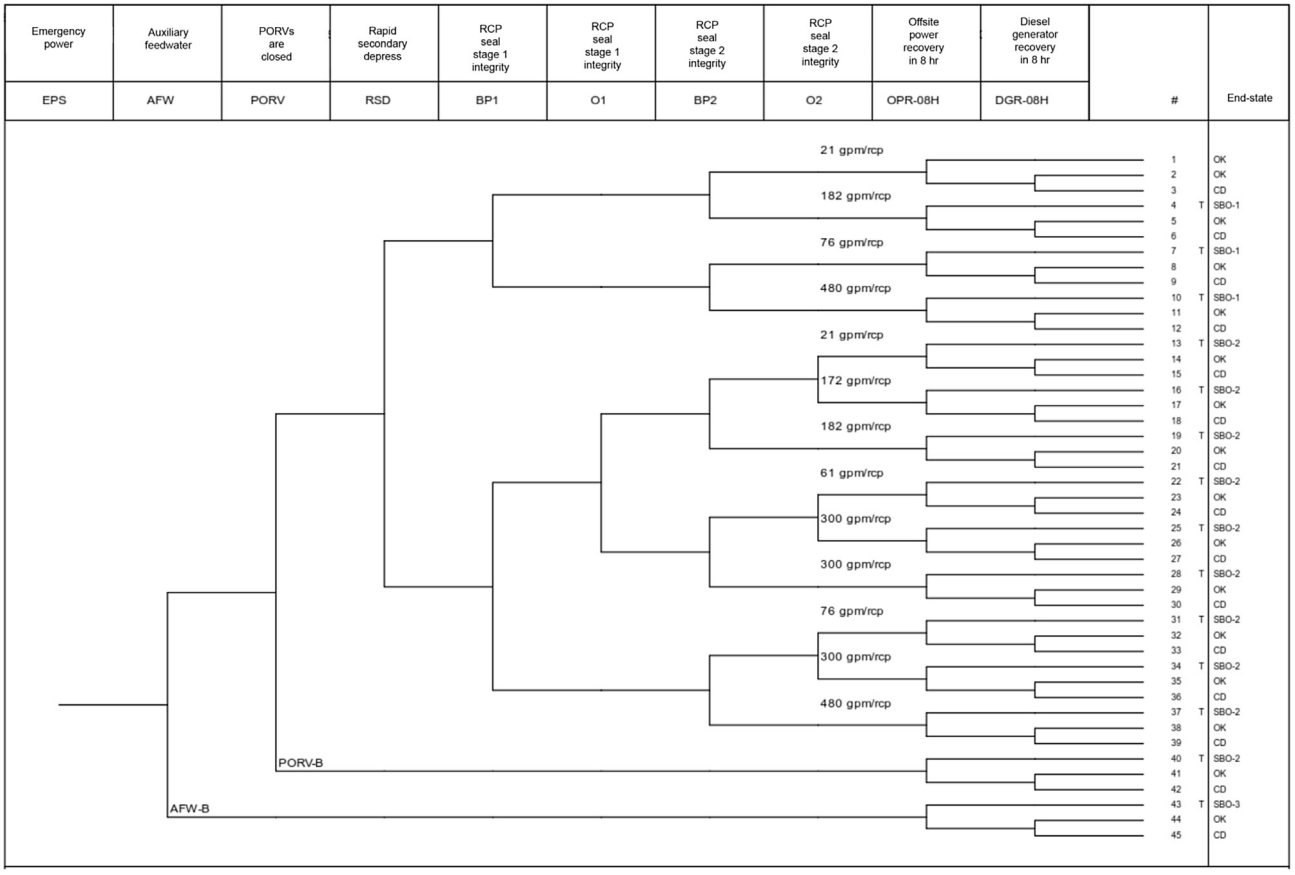

Fig. 3. Station blackout event tree. AFW, auxiliary feed water; CD, core damage; EPS, emergency power; OPR-08H, offsite power recovery in 8 h; PORV, power-operated relief valve; RSD, rapid secondary depressurization; DGR-08H, diesel generator recovery in 8 h.

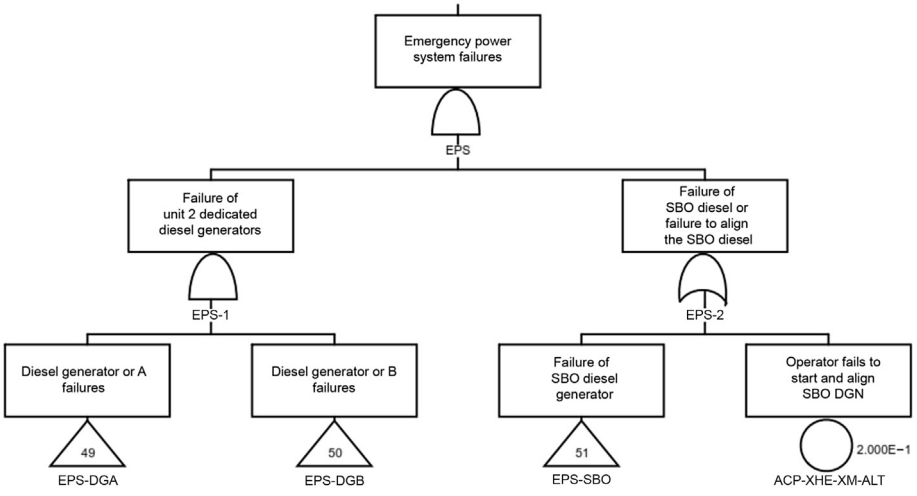

Fig. 4. Emergency power system fault tree. DGN, diesel generator; EPS, emergency power system; SBO, station blackout.

Table 1 also shows changes made to the PRA model such that: (1) the LOOP initiating event is set to TRUE to model the occurrence of a loss of offsite power; (2) the basic event for DG A to fail to start and the basic event for DG B to fail to start are each set to TRUE in order to model the SBO condition and also the potential common cause failures between two DGs or among three DGs; and (3) the SBO DG basic event for test or maintenance unavailability, i.e., EPS-DGN-TM-SBO, is set to FALSE so that robotic safety benefits can be quantified in connection with the SBO DG.

4.4. Importance analysis

In order to evaluate what human actions are risk-significant in the seismic-induced SBO condition, importance analysis [18] was carried out and the result is shown in Table 2 in terms of decreasing Fussell-Vesely importance measure (FV). Other importance measures represent risk achievement worth (RAW) and risk reduction worth (RRW). FV importance can be regarded as the fractional contribution to the total risk level of all sequences containing the

Table 1
Data modifications to reflect the seismic SBO condition.

Basic event	Description	Nominal probability	New probability	Remarks
AFW-XHE-XM-TDP	Operator fails to locally start TDP	4.00E−03	4.00E−02	Increased by an order of magnitude to reflect the seismic condition.
ACP-XHE-XM-ALT	Operator fails to start and align SBO DG	2.00E−02	2.00E−01	Increased by an order of magnitude to reflect the seismic condition.
EPS-XHE-XL-SBORMC	Operator fails to recover room cooling to SBO DG	1.30E−01	1.00E+00	Increased to 1.0 to reflect the seismic condition.
OEP-XHE-XL-NR02H	Operator fails to recover offsite power in 2 hr	3.18E−01	1.00E+00	Increased to 1.0 to reflect the seismic condition.
OEP-XHE-XL-NR08H	Operator fails to recover offsite power in 8 hr	6.72E−02	6.72E−01	Increased by an order of magnitude to reflect the seismic condition.
EPS-XHE-XL-NR08H	Operator fails to recover DG in 8 hr	2.96E−01	1.00E+00	Increased to 1.0 to reflect the seismic condition.
IE-LOOP	Loss of offsite power initiating event	1.30E−01	1.00E+00	Set to TRUE to model loss of offsite power.
EPS-DGN-FS-DGA	DG A fails to start	5.00E−03	1.00E+00	Set to TRUE to model SBO condition and potential CCF.
EPS-DGN-FS-DGB	DG B fails to start	5.00E−03	1.00E+00	Set to TRUE to model SBO condition and potential CCF.
EPS-DGN-TM-SBO	SBO DG unavailable due to test or maintenance	9.00E−03	0.00E+00	Set to FALSE To analyze robotic intervention in connection with the SBO DG.

AFW, auxiliary feedwater; CCF, common cause failure; DG, diesel generator; DGA, diesel generator A; DGB, diesel generator B; EPS, emergency power system; LOOP, loss of offsite power; SBO, station blackout; TDP, turbine-driven pump.

Table 2
Importance analysis for human actions in seismic-induced SBO.

Basic event	Description	FV	RAW	RRW
OEP-XHE-XL-NR08H	Operator fails to recover offsite power in 8 hr	9.92E−01	1.07E+00	8.96E+00
EPS-XHE-XL-NR08H	Operator fails to recover emergency diesel in 8 hr	9.92E−01	1.00E+00	8.96E+00
ACP-XHE-XM-ALT	Operator fails to start and align SBO DG	2.92E−01	1.06E+00	1.03E+00
OEP-XHE-XL-NR02H	Operator fails to recover offsite power in 2 hr	1.07E−01	1.01E+00	1.01E+00
EPS-XHE-XL-NR02H	Operator fails to recover emergency diesel in 2 hr	1.07E−01	1.00E+00	1.01E+00
AFW-XHE-XM-TDP	Operator fails to locally start TDP	4.61E−02	1.05E+00	1.00E+00
EPS-XHE-XL-SBORMC	Operator fails to recover room cooling to SBO DG	4.30E−03	1.00E+00	1.00E+00

DG, diesel generator; EPS, emergency power system; FV, Fussell-Vesely importance measure; RAW, risk achievement worth; RRW, risk reduction worth; SBO, station blackout; TDP, turbine-driven pump.

specific feature (in this case, human action). RAW is the increase in risk if the feature is assumed to fail at all times, although RRW is the decrease in risk if the feature is assumed to be perfectly reliable. Because these importance measures are interrelated somehow (e.g., FV $= 1 - 1/$RRW), one can primarily focus on FV, with some consideration of RAW if deemed necessary.

Table 2 indicates that the recovery of an emergency DG and offsite power is very important from a standpoint of FV importance (i.e., 9.92×10^{-1} for the 8-hour cases and 1.07×10^{-1} for the 2-hour cases). However, these were not selected in this study as candidate actions that would be replaced by a robotic system, because they are likely to involve intricate failure diagnosis and repair/recovery actions that cannot be readily carried out by robotic intervention alone. Out of the remaining three human actions, namely, ACP-XHE-XM-ALT, AFW-XHE-XM-TDP, and EPS-XHE-XL-SBORMC, the first and the third actions could be performed by a robot. However, the second action would be hard to conduct by a robot because it necessitates delicate manipulations to maintain the adequate steam generator level and involves monitoring various indicators and controlling the speed of the turbine-driven pump (TDP).

Therefore, the final selection of the human action to be replaced by robotic intervention can be made from several alternative actions, i.e., ACP-XHE-XM-ALT and EPS-XHE-XL-SBORMC. A comparison of the FV importance for these two actions indicates that the former is more important from a risk standpoint than the latter (i.e., 67.9 times larger in FV importance). Note that the RAW values are very small in Table 2 for all the human actions, the reason being that the CCDP in this seismic SBO is already extremely high, approaching the maximum value of 1.0 (9.36×10^{-1}); as a result, RAW is not a good measure to rely on in comparing the risk significance among the human actions. Therefore, in this study, ACP-XHE-XM-ALT was chosen as the target human action against which robotic intervention would be made. Note that the FV importance of this human action itself, namely 0.292, is also high, in view of the fact that an FV importance > 0.05 at system level or 0.005 at component level is generally considered as significant importance in the decision criteria for the evaluation of risk [19].

4.5. Quantification results

A risk sensitivity analysis was carried out using Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) code [20] for the robotic intervention (i.e., the robotic system starts and aligns SBO DG) by evaluating the effects of varying the failure probability of the ACP-XHE-XM-ALT basic event on the CCDP risk metric. The conditional core damage probability is plotted as a function of the robotic mission failure probability in Fig. 5. As can be seen in this figure, the CCDP almost linearly increases as the robotic mission failure probability increases because the survivability of the SBO DG in the station blackout condition (i.e., failure of both dedicated DGs) predominantly drives the conditional risk.

From Fig. 5 one can observe the following, among others: (1) the failure probability of robotic intervention in the seismic SBO condition should be < 0.35; in other words, a robotic reliability of at least 0.65 is needed, because otherwise core damage is inevitable (namely, CCDP = 1.0) according to the PRA model. This is based on the presumption that a decision has been made to deploy a disaster robotic system to perform the mitigating action (e.g., due to harmful environments in the location where the mitigating measure needs

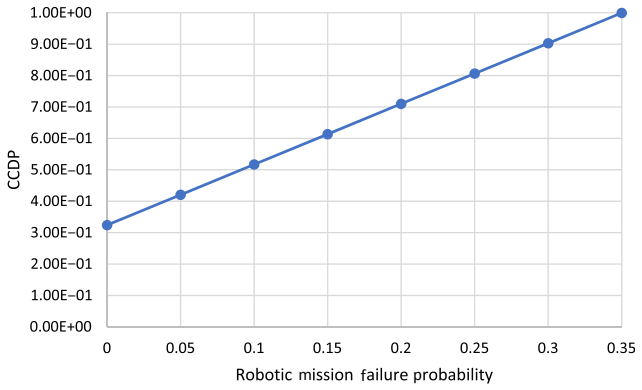

Fig. 5. Risk sensitivity analysis of robotic intervention. CCDP, conditional core damage probability.

to be taken); (2) in the case where a human operator tries to execute the mitigating action in the harsh environment, the CCDP is estimated to be 9.36×10^{-1}, because the human error probability in the seismic SBO condition is estimated to be as high as 0.2 due to the limited time available and high stress; (3) if the robotic system successfully performs the mitigating action (i.e., starting and aligning the SBO DG) in time, then the CCDP is reduced to 3.24×10^{-1} which is the CCDP value corresponding to the zero failure probability of robotic intervention, shown in Fig. 5; (4) note that failure of support systems (e.g., service water, DC power, DG room cooling) to the SBO DG, and all other potential failure mechanisms, are accounted for in the CCDP evaluation by the seismic PRA model; and (5) given that the accident situation is so serious that the human operator cannot access the area to execute the mitigating action (i.e., a human error probability of ACP-XHE-XM-ALT is 1.0), then the PRA model yields a CCDP of 1.0, implying that core damage is certain to occur under such circumstances. One can see the benefit of remote response techniques in this case, because the possibility of core damage can be reduced to some extent if a robotic system is available to carry out the mitigating action.

The underlying assumptions in the risk sensitivity analysis are that all these actions will be performed within 8 h: (1) the robotic system along with the SBO DG can be brought to the connection point of the SBO DG to the plant electrical distribution system in order to provide emergency AC power; (2) if there is debris on the route, the debris will be removed by a debris-removal robot; (3) the robot for mitigation action will enter one of the electrical rooms and operate circuit breakers to strip unnecessary DC bus loads; and (4) fuel continues to be provided to the SBO DG until the emergency power from this equipment is not needed any longer.

5. Conclusion

As part of fundamental research in the robotics development program of KAERI, a new approach to quantify the safety benefits associated with mitigation actions to be implemented by disaster robots in cases of extreme nuclear accidents has been developed. This approach is based on a PRA technique, and seismic-induced station blackout condition was used as the target scenario. A case study was accordingly conducted with a risk sensitivity analysis to evaluate the effect of robotic mission failure probability on the risk metric. When a decision has to be made to select the most appropriate robotic mitigating measure out of several alternatives, the approach can also be applied to evaluate the safety benefits of each alternative, so that the evaluation results may be used as an input to the decision making process, together with other factors (e.g., development costs, technical feasibility).

Although remote response technology was assumed to be applied only for a single mitigating measure (i.e., start and align the SBO DG) in this study, it could also be used for many other purposes during an extreme event. For instance, a robotic system may be used in providing an external injection to the reactor or spent fuel pool if plant personnel cannot easily perform the action due to certain reasons (e.g., harmful environment, potential danger of hydrogen explosion). Alternatively, unmanned aerial vehicles, sometimes called drones or unmanned aircraft systems, might be used for reconnaissance purposes [2] to identify the site condition following a site-wide extreme event such as one caused by a strong earthquake or typhoon. Information on the site condition could be valuably used in the decision making process to determine how to cope with the evolving accident. Finally, note that the result of the case study performed indicates that a robot system with reliability > 0.65 is needed in this special case to avoid core damage because otherwise core damage is inevitable. Therefore, considerable efforts are needed to improve the reliability of disaster robots because, without the assurance of high reliability, the remote response technique cannot be practically used.

Conflicts of interest

The authors have no conflict of interest to declare.

Acknowledgments

This work was supported by the National Research Foundation of Korea (NRF 2016M2A8A4952316) grant funded by the Korea Government (Ministry of Science, ICT, and Future Planning). We thank the anonymous reviewers for their many insightful comments that greatly helped improve the quality of this manuscript.

References

[1] S.H. Kim, K.M. Jung, S.U. Lee, H.C. Shin, C.H. Kim, Y.C. Seo, Y.G. Bae, Innovative robot technologies for nuclear power plant inspection and maintenance, in: ICONE22, Int. Conf. Nucl. Engr., July 7–11, 2014. Prague.
[2] R.R. Murphy, Disaster Robotics, The MIT Press, Cambridge, MA, 2014.
[3] B. Siciliano, O. Khatib (Eds.), Springer Handbook of Robotics, Springer-Verlag, Berlin, 2008.
[4] B.S. Dhillon, Robot Reliability and Safety, Springer-Verlag, New York, 1991.
[5] DARPA Robotics Challenge (DRC), [Internet]. 2015. Available from: www.darpa.mil/program/darpa-robotics-challenge. [Accessed June 23, 2017]
[6] Y. Choi, K.M. Jeong, I.S. Kim, Strategy to Enhance Applicability of the KAERI's Remote Response Technology, Trans Am Nucl Soc, San Antonio, TX, June 7–11, 2015.
[7] M. Modarres, What Every Engineer Should Know About Reliability and Risk Analysis, Marcel Dekker, New York, 1993.
[8] M. Modarres, I.S. Kim, Deterministic and probabilistic safety analysis, in: D.G. Cacuci (Ed.), Handbook of Nuclear Engineering, Springer Science, New York, 2010, pp. 1742–1812.
[9] Nuclear Energy Institute, B.5.b Phase 2 & 3 Submittal Guideline, NEI-06-12, Rev. 3, Nuclear Energy Institute, Washington, DC, 2009.
[10] Nuclear Energy Institute, Diverse and Flexible Coping Strategies (FLEX) Implementation Guide, NEI-12-06, Nuclear Energy Institute, Washington, DC, 2012.
[11] ASME/ANS RA-Sa-2009, Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, American Society of Mechanical Engineers, New York, 2009.
[12] U.S. Nuclear Regulatory Commission, State-of-the-Art Reactor Consequence Analyses (SOARCA) Report, NUREG-1935, U.S. Nuclear Regulatory Commission, Washington, DC, 2012.
[13] Institute of Nuclear Power Operations (INPO), Special Report on the Nuclear Accident at the Fukushima Daiichi Nuclear Power Station, INPO 11–1005, INPO, Atlanta (GA), 2011.
[14] Arizona Public Service Company, APS Overall Integrated Plan in Response to March 12, 2012 Commission Order Modifying Licenses with Regard to Requirements for Mitigation Strategies for Beyond-design-basis External Events, Arizona Public Service Company, Phoenix (AZ), February 28, 2013.
[15] J.A. Julius, J. Grobbelaar, K. Kohlhepp, Advancing human reliability analysis methods for external events with a focus on seismic, in: Probabilistic Safety Assessment and Management, PSAM12, June 22–27, 2014. Hawaii.

[16] J.H. Kim, I.-K. Choi, Modeling of human error probability dependent on seismic intensity, Trans. Kr. Nucl. Soc., Gyeongju, Korea, October 25–26, 2012.
[17] U.S. Nuclear Regulatory Commission, Reevaluation of Station Blackout Risk at Nuclear Power Plants, Analysis of Loss of Power Events: 1986–2004, NUREG/CR-6890, U.S. Nuclear Regulatory Commission, Washington, DC, 2005.
[18] M.V.D. Borst, H. Schoonakker, An overview of PSA importance measures, Rel. Engr. Sys. Saf. 72 (2001) 241–245.
[19] J.-E. Holmberg, U. Pulkkinen, T. Rosqvist, K. Simola, Decision Criteria in PSA Applications, VTT Automation, Finland, 2001.
[20] U.S. Nuclear Regulatory Commission, Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 8, NUREG/CR-7039, U.S. Nuclear Regulatory Commission, Washington, DC, 2011.