Study for Reliability Analysis of Operator Response Process Under IBLOCA Accident in Nuclear Power Plant

Zhi-Hui Xu, Jie-Mei Zhang, Xue-Gang Zhang, Ming Jia, De-Song Su, and Hua-Qing Peng(✉)

State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment,
China Nuclear Power Engineering Co., Ltd., Shenzhen 518172, China

Abstract. The reliability of the operator's response process after a nuclear power plant accident has an important impact on the overall reliability of accident mitigation. The automatic diagnostic function of nuclear power plant state is designed for the advanced digital control system, by monitoring and processing the plant, it provides an initial orientation or reorientation diagnosis for the Emergency Operating Procedures (EOPs) during emergency operating conditions. Therefore, the operator response process in main control room, especially the potential human errors have some new characteristics, when compared with the traditional way. The qualitative assessment of the operator response process forms the basis for the quantification of the associated Human Error Probability (HEP). The purpose of this paper is to study the reliability of the operator actions required to establish simultaneous Hot Leg injection following an Intermediate Break Loss of Coolant Accident (IBLOCA), a typical accident condition of nuclear power plant. The accident sequence and operator's actions are given, the detail qualitative and quantitative assessment are implemented base on the foundation of SPAR-H method by a constructed fault tree. The result shows that the failure probability of operating from the Auxiliary Control Panel (ACP) is higher than operating from the Plant Computer Information & Control System (PCICS). The main recommendations are providing more training for operation from the ACP following a loss of PCICS, increase descriptive information within the EOPs and the Human Machine Interface (HMI), providing a dedicated plant status display system and then decrease the reliance placed on the knowledge and memory of the operators to understand important information about plant configuration. The reliability assessment helpful to improve the human factor suitability, provide guidance for optimize the operator's response process and effectively improve the reliability of engineering design under an IBLOCA accident scenario.

Keywords: Accident scenario · Operator Response Process · Reliability analysis · Human factor

1 Introduction

The response process of the operator after the Nuclear Power Plant (NPP) accident is an important part to mitigate the accident and limit the consequences of the accident [1].

Y. Xu et al. (Eds.): SICPNPP 2020, LNEE 779, pp. 599–609, 2021.
https://doi.org/10.1007/978-981-16-3456-7_58

Therefore, the reliability of the operator's response process after a nuclear power plant accident has an important impact on the overall reliability of accident mitigation. The purpose of this paper is to study the reliability of the operator actions required to establish Hot Leg injection following under an Intermediate Break Loss of Coolant Accident (IBLOCA). This paper is divided into four parts. The first part introduces IBLOCA accident and accident sequence, and identifies the important human actions involved. The second part gives the qualitative analysis of the reliability of the operator in the response process of the accident. The third part gives the quantitative analysis results. The final part summarizes and discusses the analysis results of this assessment.

2 Analysis of IBLOCA Accident Scenario

An IB LOCA is defined by a break size that the Safety Injection System (SIS) cannot achieve successful Residual Heat Removal mode which is required to obtain the safe state criteria. Therefore, in certain IBLOCA a scenario achieving the long-term safe state requires the operator to switch the LHSI pumps to simultaneous, a typical accident condition of nuclear power plant.

An IBLOCA occurs in the Reactor Coolant System (RCS) pipework or pipework of connected systems before the second isolation valves resulting in a decrease in RCS pressure and in the RCS water inventory. If unmitigated the core could become uncovered and fuel damage could occur. For IBLOCA accident, the operator response process is most complicated when the nuclear power plant is in operating state with full power.

At the nuclear power plant full power state, an intermediate break occurs, then medium pressure rapid cooldown (MCD) succeeds, medium pressure safety injection (MHSI) start-up succeeds, the medium pressure accumulator's injection succeeds and low pressure safety injection (LHSI) cold leg start-up succeeds. It is necessary to start up LHSI injection with hot leg manually (Fig. 1).

The controlled state is achieved when:

- SIS and Atmospheric Steam Dump System (ASDS) are removing RCS heat; and
- Core sub-criticality is ensured; and
- RCS inventory stabilised by SIS.

The key event sequence can be drive from the above description, the key operator action success only in the following preceding events:

a) Medium pressure rapid cooldown.
b) Medium pressure safety injection.
c) Medium pressure accumulator injection.
d) Low pressure safety injection.
e) Simultaneous hot leg and cold leg injection.

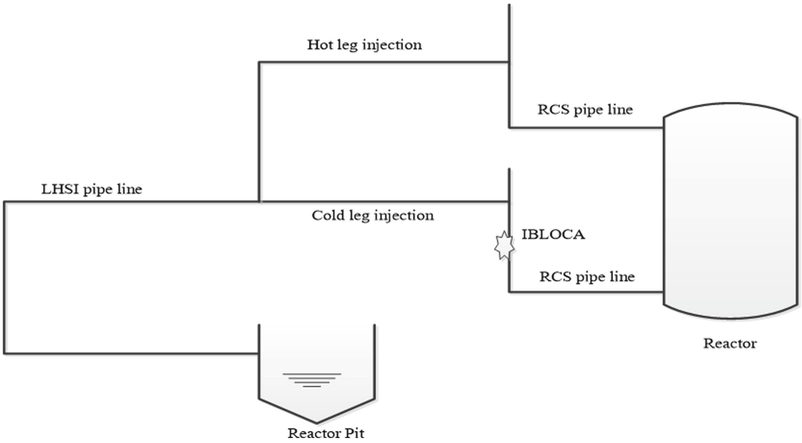

Fig. 1. The general flow diagram of IBLOCA

3 Overview of Operator Response Process

3.1 Required Operator Actions

The key operator action to initiate simultaneous injection to the Hot Leg is specified in the Emergency Operating Procedure (EOP) of NPP for restoring primary loop inventory. The requirement for the operator to enter the EOP for restoring primary loop inventory is indicated by the presence of the permissive signal (P signal). The permissive signal is actuated when the conditions are all met. Therefore, the operator will not be directed to enter the EOP for restoring primary loop inventory that containing instructions to establish simultaneous hot leg injection after the IBLOCA occurs.

Based on the above event scenario description, the following auxiliary operator actions are also required to achieve the safe state following an IBLOCA:

- MCD manually: The RCS is cooldown by steam generators in medium pressure via the secondary side using ASDS.
- Stop MHSI: The MHSI pumps are manually stopped when the core outlet temperature is reduced to the threshold and the hot leg saturation margin and hot leg water level are sufficiently high.
- Isolate medium pressure accumulators: Manual isolation when RCS pressure is below the defined threshold.
- Establish hot leg injection: For the SIS is unable to achieve residual heat removal mode in this scenarios to establish long term heat removal mode, then the operator must establish simultaneous LHSI injection to the hot and cold legs.

3.2 Overview of Operator Response Process in Main Control Room (MCR)

The automatic diagnostic function of NPP state is designed for the advanced digital control system, which is installed on the Plant Computer Information & Control System

(PCICS). By monitoring and processing the plant, it provides an initial orientation or reorientation diagnosis for the EOPs during emergency operating conditions.

The initial annunciation of the automatic diagnostic function of NPP state, which occurs almost immediately following the IBLOCA, directs the operator to implement the EOP for cold shutdown with safety injection (SI) signal. The operator will be implementing the EOP until re-directed to another EOP by the re-annunciation of the Automatic diagnostic function of nuclear power plant system, when the automatic diagnostic function of NPP state re-annunciates.

The main control room contains PCICS and Auxiliary Control Panel (ACP), ACP is a backup of PCICS, if there has a PCICS failure, and the operator can transfer to the ACP to continue the control and monitoring required by the accident procedure (Fig. 2).

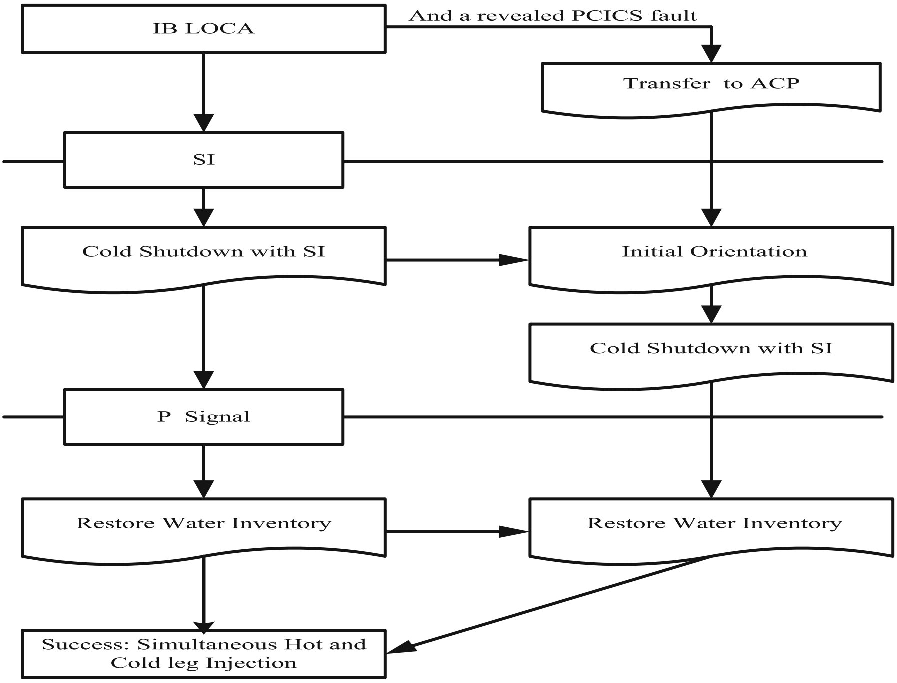

Fig. 2. Overview of operator response process in MCR

4 Analysis of Potential Errors in Operator Response Process

Task Analysis is used to conduct a qualitative assessment of the operator actions required in response to an IBLOCA and to determine the key task steps and relevant PSFs. A Task Analysis was completed of the required operator response to an IBLOCA scenario using the two main operating systems within the MCR; the PCICS and the ACP. The qualitative assessment forms the basis for the quantification of the associated HEPs [2].

4.1 Task Analysis

The task analysis provides a graphical illustration of the individual task steps that constitute the required operator response and the relationships between the individual task steps. The task analysis is based on a generic structure containing three high level tasks; detect, diagnose and implement (Fig. 3).

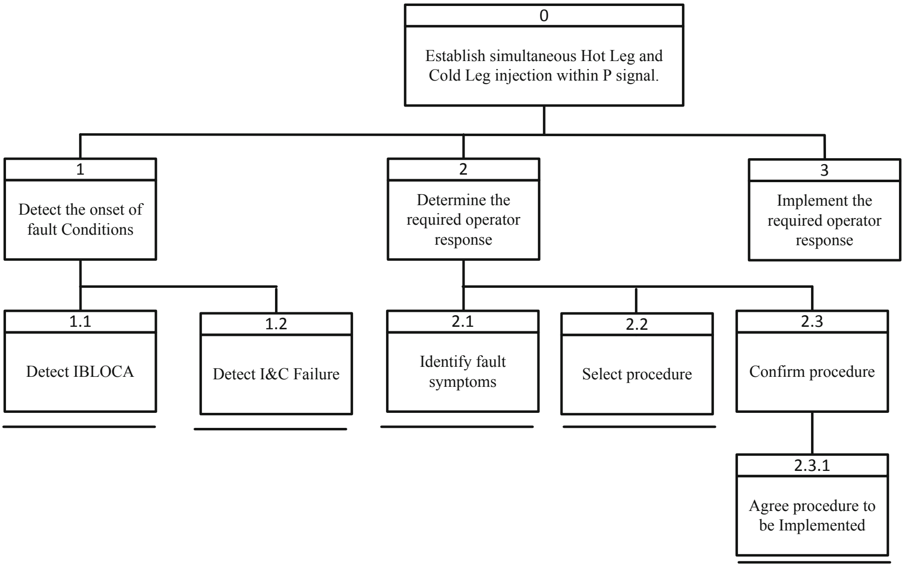
0
Establish simultaneous Hot Leg and Cold Leg injection within P signal.
1
Detect the onset of fault Conditions
2
Determine the required operator response
3
Implement the required operator response
1.1
Detect IBLOCA
1.2
Detect I&C Failure
2.1
Identify fault symptoms
2.2
Select procedure
2.3
Confirm procedure
2.3.1
Agree procedure to be Implemented

Fig. 3. Task analysis of operator response process

4.2 Potential Error Identification

Potential errors are safety significant if their consequence is a failure to achieve the required operator response (simultaneous LHSI to the hot and cold Legs) within the time available. The general error mode of the situational awareness and workload has a high-level nature that the detailed insights into potential error modes that support the development of error mitigation strategies are more difficult to obtain. Therefore, this paper combines the SPAR-H with these general concepts of human performance [3].

4.2.1 Situational Awareness

The factors that influence situational awareness are predominantly a function of the HMI, which is one of the eight PSFs of SPAR-H. Therefore, the consideration of relevant HMI design features (i.e. the provision of appropriate cues, indications and feedback) is used to identify (where practicable from the information currently available) any potential for insufficient and/or ambiguous information to be detrimental to the operator's ability to maintain an appropriate level of situational awareness [4].

A good level of operator situational awareness is a manifestation of the validity of a number of the fundamental assumptions that are necessary to conduct Human Reliability Assessment (HRA); Fit for duty individuals operating in accordance with well-designed procedures from well-designed HMIs.

The key cues and necessary feedback is provided for the operator and the purpose of the monitoring and re-orientation phases of the EOPs is to maintain operator situational awareness by regularly checking the relevant parameters. No reliance is placed on the knowledge and memory of the operators to understand the plant state.

4.2.2 Workload

The factors that influence workload are predominately a function of task design. Therefore, the consideration of the task design related PSFs such as stress, time-pressure, unfamiliarity and complexity, is used to identify any potential for a high workload to be detrimental to operator reliability [5].

Manually determining the correct post fault strategy, as is required when operating from the ACP following a loss of the PCICS, increases the workload associated with the required operator response and introduces an additional opportunity for a potential error to occur.

4.2.3 Potential Errors

The following safety significant potential errors have been identified for the scenarios that are considered within the scope of this paper:

When operating from the PCICS with automatic diagnostic function of nuclear power plant state to get the required post fault strategy:

Operator fails to detect the requirement to implement the procedure for restoring water inventory; Operator fails to establish hot leg injection within some minutes after the P signal.

When operating from the ACP following failure of the PCICS system (and therefore no automatic diagnostic function of NPP state is available):

Operator fails to detect the P signal; Operator fails to determine the requirement to implement the procedure for restoring water inventory; Operator fails to establish hot leg injection within some minutes after the P signal.

5 Human Reliability Assessment

The reliability of the required operator actions associated with establishing hot leg injection following an IBLOCA is quantified using the SPAR-H methodology. The time to complete the actions necessary to establish simultaneous hot leg injection following an IBLOCA are considered in the following sub-sections for the two variants that are operate from the PCICS and operating from the ACP. If PCICS failure occurs and is detected by the operators, then operations are conducted from the ACP. However, when operating from the ACP, there is no automatic diagnostic function of NPP state and therefore the operator must manually determine the requirement procedure [6–8].

5.1 Fault Tree Structure of Operator Response Process

The automatic diagnostic function of NPP state automates Step 2 in the task analysis. Therefore, when the automatic diagnostic function of NPP state functions correctly there are no credible potential operator errors associated with determining the required response. If the automatic diagnostic function of NPP state where to fail, then the operator must manually determine the required response which will introduces the potential for error to occur during Step 2. The fault tree structure proposed for use in these scenarios is provided by Figure 4. Note, in this fault tree structure the veracity checks provide a genuine recovery opportunity for all potential failure modes of the automatic diagnostic function of NPP state. This fault tree structure also provides an appropriate model for the scenarios that include a loss of the PCICS.

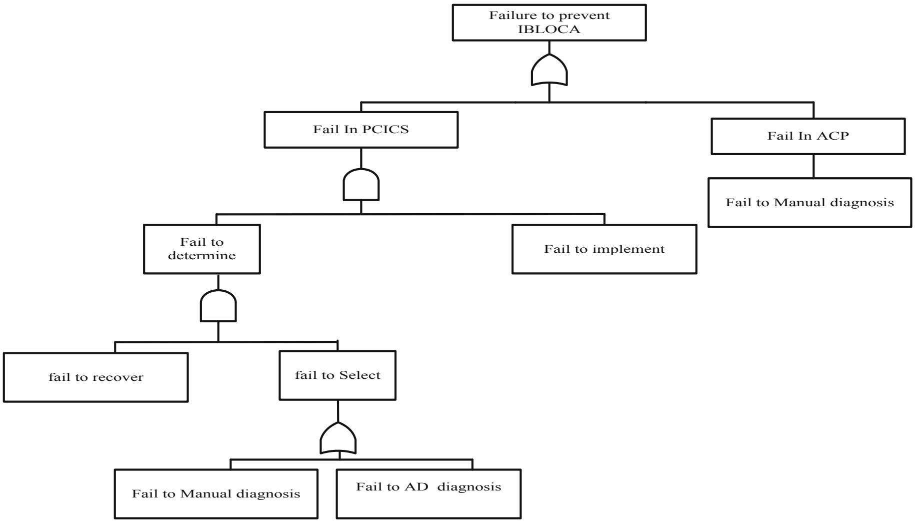

Fig. 4. Fault tree structure (automatic diagnostic function of NPP State /PCICS failure)

5.2 Recovery Opportunities

A MCR crew contains OP1, OP2, Unit Supervisor (US), Shift Supervisor (SS), Safety Engineer (SE), OP1 is responsible for the Nuclear Island and OP2 is responsible for the Conventional Island. In accident conditions, OP1 is responsible for operator of the Nuclear Steam Supply System (NSSS) and engineered safety features, whilst OP2 takes charge of the operating of the steam generator, turbine generator, water supply system and other auxiliary systems.

The opportunities for self-recovery of errors by the MCR crew of OP1, OP2 and the US are provided by the monitoring (and, if operating from the ACP, also the re-orientation) phase of the EOPs are noted.

The SE, who can arrive in the MCR a dozen minutes after the onset of the fault conditions and will be conducting their veracity checks from ACP. The SS fulfills the

SE role until he arrives in the MCR. Therefore, it is reasonable to consider the available recovery opportunity.

5.3 Dependency Analysis

No consideration is made on the US recovering errors made by OP1, which is equivalent to modelling complete dependency between these members of the MCR crew.

The potential for dependency to affect the reliability that can be considered for the recovery opportunity provided by the SE is assessed, due to their increased level of independence from the other members of the MCR crew.

Figure 5 illustrates the logic employed to derive a moderate level of dependency for the recovery opportunity when operating from the PCICS and ACP (scenario 1 and 2).

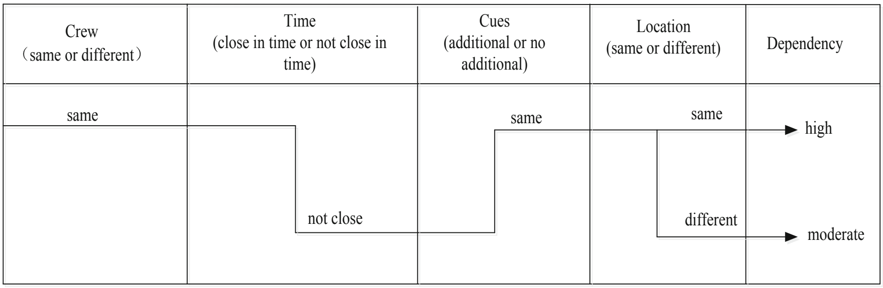

Fig. 5. Recovery opportunity dependency assessment

5.4 Human Error Probability of Operator Response Process

According to the qualitative analysis, The PSFs for determining and implement the requirement of procedures for restoring the water inventory from the PCICS and ACP are assessed using the SPAR-H method. Moreover, according to the above analysis, three different sub-scenarios are evaluated in order to make a comparison

Scenario 1: Operating from the PCICS with automatic diagnostic function of nuclear power plant state.
Scenario 2: Operating from the ACP.
Scenario 3: Operating from the PCICS and manually determining the post-fault procedure.

The assessment of scenarios 1 and 2 provides a model that can be used to bound the assessment of scenario 3, so the Table 1 below only give the PSFs for Scenario 1 and 2. And for Scenario 1, when the automatic diagnostic function of nuclear power plant state correctly, there is no opportunity for operator error when determining the correct strategy. So just need analysis the PSFs for actions [9].

SPAR-H has two basic HEPs 0.01 for diagnosis and 0.001 for actions. These can be modified using the 8 PSFs given in Table 1. Human error probability $P = P_d + P_a$,

Table 1. PSFs for operator response process

PSF for diagnosis (Scenario 2)	Multiplier	PSF for action (Scenario 1 and 2)	Multiplier
Available Time	1	Available Time	1
Stress	2	Stress	2
Complexity	2	Complexity	2
Experience/Training	1	Experience/Training	1
Procedures	0.5	Procedures	0.5
HMI	1	HMI	1
Fitness for Duty	1	Fitness for Duty	1
Work Processes	1	Work Processes	1

where P_d refers to diagnosis error probability and P_a refers to action error probability. P_d and P_a are calculated according to the following equations respectively:

$$P_d = 0.01 \times \prod_{i=1}^{8} PSF_i \tag{1}$$

$$P_a = 0.001 \times \prod_{i=1}^{8} PSF_i \tag{2}$$

The HEPs for establishing Hot Leg injection following an IBLOCA during full power state from both the PCICS and the ACP are summarised below, and the recovery of safety engineer also considered [10].

Scenario 1: Operator fails to establish hot leg injection (from the PCICS, with Automatic diagnostic function of nuclear power plant state)

$$P_a = 1.0E\text{-}3 \times 1 \times 2 \times 2 \times 1 \times 0.5 \times 1 \times 1 \times 1 = 2.0E\text{-}3 \tag{3}$$

HEP = 2.0E-03 × 0.15 = 3.0E-4.

Scenario 2: Operator fails to establish hot leg injection (from the ACP)

$$P_d = 1.0E\text{-}2 \times 1 \times 2 \times 2 \times 1 \times 0.5 \times 1 \times 1 \times 1 = 2.0E\text{-}2 \tag{4}$$

$$P_a = 1.0E\text{-}3 \times 1 \times 2 \times 2 \times 1 \times 0.5 \times 1 \times 1 \times 1 = 2.0E\text{-}3 \tag{5}$$

HEP = (2.2E-2 + 2.0E-3) × 0.5 = 1.1E-2.

Note that the overall figure for Scenario 2 does not include the contribution from the HEP associated with detecting I&C failure.

Scenario 3: Operator fails to establish hot leg injection (from the PCICS, without automatic diagnostic function of NPP state)

$$P_d = 1.0E\text{-}2 \times 1 \times 2 \times 2 \times 1 \times 0.5 \times 1 \times 1 \times 1 = 2.0E\text{-}2 \tag{6}$$

$$P_a = 1.0\text{E-3} \times 1 \times 2 \times 2 \times 1 \times 0.5 \times 1 \times 1 \times 1 = 2.0\text{E-3} \quad (7)$$

HEP = (2.2E-02 + 2E-03) × 0.15 = 3.3E-03.

6 Conclusions

Usually, operator is often passively adapted to the characteristics of the design finished product, which is not conducive to the ascension of the reliability of operator. At the same time, it also may cause unnecessary human error.

This paper has carried out a qualitative and quantitative human reliability assessment of the operator's response process after a nuclear power plant IBLOCA accident. For IBLOCA accident, the time window is ample and the accident process is not urgent, however the failure probability of operating from the ACP is higher than operating from the PCICS. This is because detect I&C failure, transfer to the ACP and reorientation in ACP will consume extra time, weakens the available time window. In order to improve the reliability of operator's response process, the recommendations are as follows:

Provide training for operating from the ACP following a loss of PCICS. Increase descriptive information within the EOPs and the HMI, and providing a dedicated plant status display system. Then decrease the reliance placed on the knowledge and memory of the operators to understand important information about plant configuration.

This paper is only a rough and conservative assessment and further detailed analysis can help to carry out more accurate evaluation and find more useful recommendations, so as to effectively improve the reliability of engineering design.

References

1. Boring, R., Boring, L., Gertman, D.I.: Atomistic and holistic approaches to human reliability analysis in the US Nuclear Power Industry. Safety Reliab. **25**(2), 21–37 (2005)
2. Lee, S.W., Kim, A.R., Ha, J.S., Seong, P.H.: Development of a qualitative evaluation framework for performance shaping factors (PSFs) in advanced MCR HRA. Ann. Nucl. Energy **38**, 1751–1759 (2011)
3. Lee, S.J., Kim, J., Jang, S.C.: Human error mode identification for NPP main control room operation using soft controls. J. Nucl. Sci. Technol. **48**(20), 902–910 (2011)
4. Taylor, R.M.: Situational awareness rating technique (SART): the development of a tool for aircrew systems design. In: Situational Awareness. Routledge, New York, pp. 111–128 (2017)
5. Moray, N.: Mental Workload: Its Theory and Measurement. Springer Science & Business Media, Boston (2013). https://doi.org/10.1007/978-1-4757-0884-4
6. Jang, I., Kim, A.R., Jung, W., Seong, P.H.: A framework of human reliability analysis method considering soft control in digital main control rooms. In: Proceedings of 16th International Conference on Human Interface and the Management of Information: Information and Knowledge Design and Evaluation, Heraklion, Grete, Greece (2014)
7. Ma, Z., Yoshikawa, H., Nawaz, A., Yang, M.: A human–machine interaction design and evaluation method by combination of scenario simulation and knowledge base. J. Nucl. Sci. Technol. **55**(5), 516–529 (2018)
8. Jun, Y., Bowen, Z., Ming, Y.: Bidirectional implementation of Markov/CCMT for dynamic reliability analysis with application to digital I&C systems. Reliab. Eng. Syst. Safety **185**, 278–290 (2019)

9. Gertman, D., Blackman, H., Marble, J., Byers, C., Smith C.: The SPAR-H Human Reliability Analysis Method, NUREG/CR-6883. Idaho National Laboratory. USNRC, Washington D.C. (2004)
10. Jang, I., Jung, W., Seong, P.H.: Human error and the associated recovery probabilities for soft control being used in the advanced MCRs of NPPs. Ann. Nucl. Energy **87**(2), 290–298 (2016)