Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference
Edited by Eirik Bjorheim Abrahamsen, Terje Aven, Frederic Bouder, Roger Flage, Marja Ylönen
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P4627-cd

Human performance and reliability in a complex seismic accident scenario at a nuclear power plant

Ilkka Karanta

Nuclear Safety research area, VTT Technology Research Centre of Finland Ltd, Finland.
E-mail: Ilkka.Karanta@vtt.fi

Rasmus Hotakainen

Fortum E&P, Finland. E-mail: Rasmus.Hotakainen@fortum.com

A scenario, where a nuclear power plant has experienced an earthquake, and lost its automation systems and main control room, is improbable but exceptionally severe. Then, the mission of the operators is to steer the plant to a safe and as stable as possible state, and secure residual heat removal. In this paper, the scenario is described. Factors affecting operator performance in the scenario are considered. A human reliability analysis model for the scenario is proposed, and its main features outlined. The model consists of treatment of timings and of human errors. Concerning timings, an activity network model is proposed. Concerning human errors, special features of the scenario are treated in performance shaping factors (PSF); central PSFs are identified and factors affecting them are described.

Keywords: human reliability analysis, human performance, seismic, earthquakes, scenario, performance shaping factors, timings, loss of main control room, loss of automation.

1. Introduction

Earthquakes are a major hazard to nuclear power plants (NPP). As hazards, they are nonspecific: almost any system, structure or component (SSC) may fail when subjected to an earthquake. After an earthquake, the crew of an NPP may face several challenges: the plant has to be steered to a safe stable state (usually shut down). Initially there is no reliable information on whether some SSCs of the plant are damaged, and if so, which ones and to what extent.

In this paper, we consider crew actions in a particular seismic scenario, where scram has been successful but the main control room of the plant unit, as well as its automation, have been lost. Then, the crew's task is to manually secure residual heat removal. The scenario is improbable, but its consequences may be serious, and the crew plays an even more essential role than in more conventional incidents. Although there is a considerable amount of research published in seismic human reliability analysis (SHRA) (e.g.)Park et al. (2015)), it seems that this scenario has not attracted any attention to it.

We consider the question of how likely the crew's actions are to succeed in the framework of SHRA, a subfield of human reliability analysis (HRA). We aim to shed light on the following questions. How to model this scenario? What factors influence the execution of the actions? How should it be taken into account that the task is executed in the aftermath of a seismic event? How to take earthquake strength into account in a meaningful way?

2. The scenario

The following scenario has been identified at Loviisa NPP as a potential threat to plant safety, and one to which the HRA methods currently in use at the plant are not necessarily applicable.

We consider a pressurized water reactor unit that is subjected to an earthquake. The plant's safety automation performs a scram successfully. The primary circuit remains intact. However, the main control room and automation racks in I&C cabinet rooms are lost.

The MCR crew moves to field. The necessary safety function at this phase is securing residual heat removal (RHR). According to operating instructions, RHR is to be performed by utilizing an additional emergency feedwater system (AEFW) that should pump water to operational steam generators (SG). AEFW consists of 2 pumps, 2 diesel generators that run the pumps, a water tank, and associated valves and pipes. Thus, this human action consists of deploying AEFW (and configuring the unit so that AEFW will pump the water to the SGs), and keeping the AEFW-SG system operational sufficiently long.

According to operating procedures, this human action falls mainly to three field operators:Turbine Technician (TrT), Field Operator (primary circuit) (FOPrim), and I&C Technician (ICT).

TrT coordinates the deployment of AEFW, configures it by opening and closing valves, and operates it. A simplified activity network of the Turbine Technician's actions is presented in Figure 1. The network, as well as the other activity networks in this section, are based on operating instructions in use at Loviisa NPP. TrT first sends ICT to read and communicate pressure and water level measurements of steam generators, and FOprim to the inner annular space to open valves so that water will flow from AEFW to operational steam generators. After checking that AEFW valves are in correct positions and that the pump and pipeline connecting it to steam generators do not seemingly leak, TrT starts AEFW pump. While operating AEFW manually, TrT tries to keep water levels in the steam generators close to each other.

Field Operator (primary circuit) (FOPrim) configures water flow in the secondary circuit in such a manner that water will flow from AEFW to those steam generators that are operational. The actions of FOprim are presented in Figure 2. His part of the work starts when TrT informs him of the situation and sends him to the inner annular space. His job is the simplest of the three, consisting basically of picking the right keys, calling Radiation Supervisor to help, walking to the inner annular space, and configuring valve positions of each steam generator as needed. Additionally, if he has been asked to do so, FOprim walks to the SG space and combines the SGs through a bypass duct. If FOprim does not have to go to the SG space, Radiation supervisor is not needed. For simplicity, we have here left out that possibility and incorporated only the more conservative (in this case, time-consuming) course of action, where he visits both spaces and possibly has to wait for Radiation Supervisor to arrive.

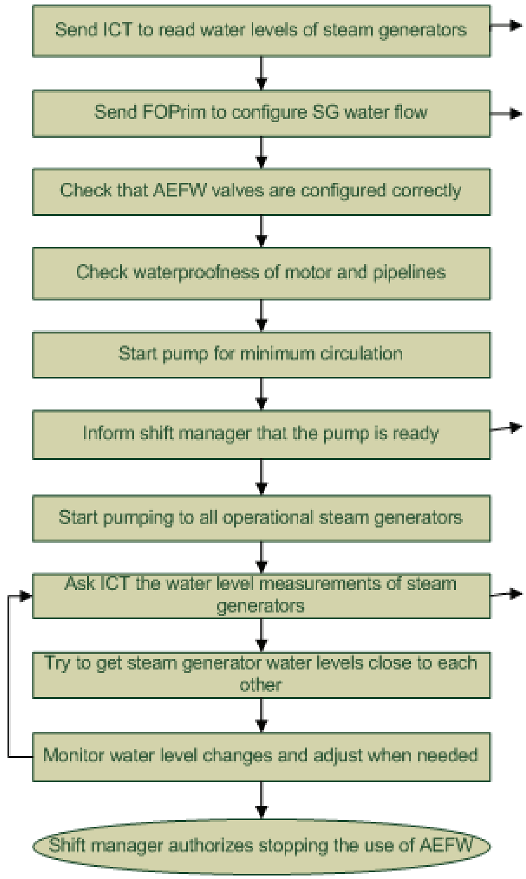

Fig. 1. Activity network of Turbine Technician's actions. Arrows to the right mark activities where TrT interacts with other crew members.

ICT conducts water level and pressure measurements needed by the Turbine Technician manually. Actions of ICT are presented in Figure 3. His job starts when TrT informs him of the situation and sends him to the automation room of the SGs. ICT first picks up tools and keys needed, then walks to the steam generators. While there, ICT starts carrying out measurements and reporting them to TrT, moving from one operational steam generator to another, for as long as needed. On each measurement round, ICT measures water

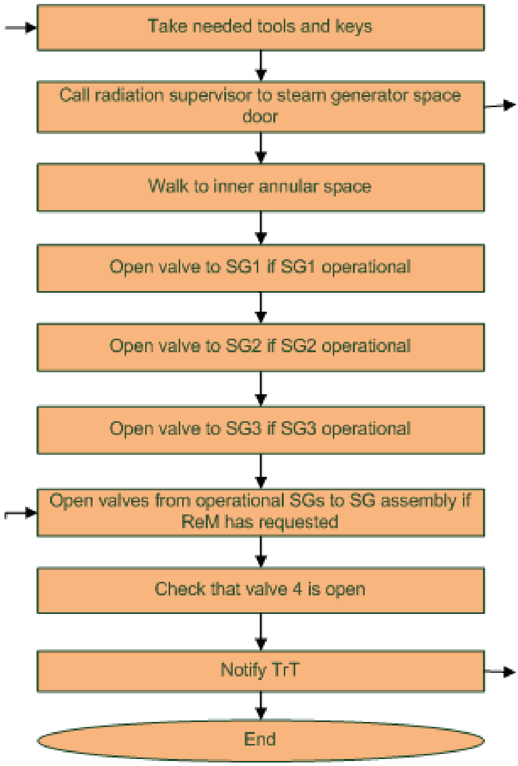

Fig. 2. Activity network of primary circuit Field Operator's actions.

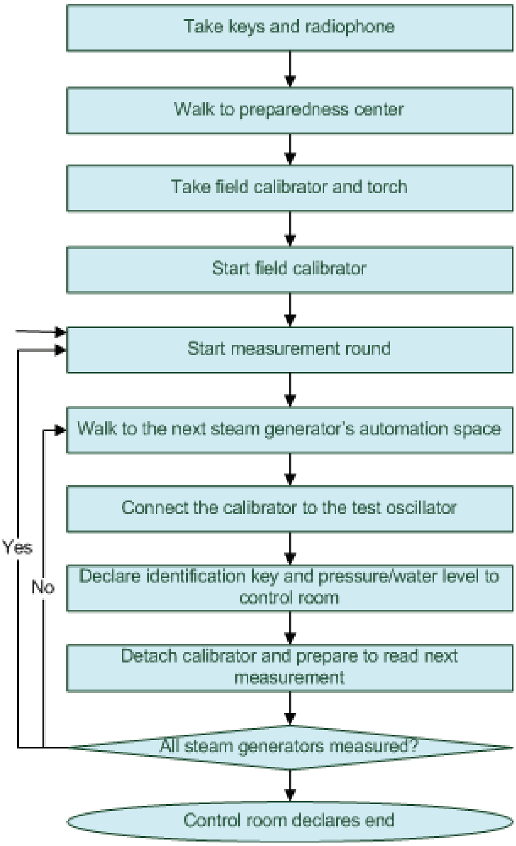

Fig. 3. Activity network of I&C Technician's actions. Note the loop that results from ICT conducting measurements on the steam generators for as many times as needed.

levels in all SGs.

In addition, two other crew members participate in the scenario in more minor roles. The Shift Supervisor's role is to decide when the use of AEFW can be stopped. Radiation Supervisor comes to the door of steam generator space when asked, measures radiation level, and lets FOPrim in if feasible. Reactor operator and others are present but do not actively participate in the scenario.

A schematic view of the whole activity network, including the connections between TrT's, FOprim's and ICT's activities, is shown in Figure 4. In addition to the activities conducted by the three, the network shows Radiation Supervisor's activities (yellow). It also shows three activities (white) for which the exact set of participants is not defined: diagnosis that the main control room must be left, transfer from the main control room to the reserve control room, and diagnosis on what must be carried out in the present situation. Diagnosis that the MCR must be left covers the time from the earthquake to the time that the decision to leave the MCR is made.

The activity network visualizes one aspect of the scenario: manual control of the SGs has to be continued for an indefinite time. From time to time, TrT needs to figure out if water levels in the SGs are OK. Then TrT calls ICT to measure them and relay the information. Once ICT has done that, TrT decides if water levels in some SGs need to be adjusted and does that. That creates the loop in TrT's activity network and the two loops in ICT's activity network.

Even if the crew efforts to secure RHR fail,

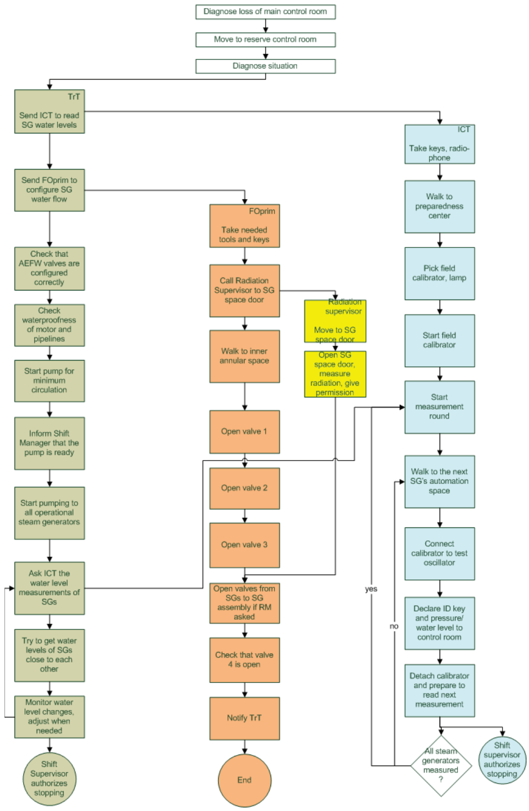

Fig. 4. A schema of the crew activity network of the scenario. Turbine Technician's activities are in green, Field Operator's in orange, I&C Technician's in blue, Radiation Supervisor's in yellow and MCR crew's actions in white.

there are considerable resources to prevent and mitigate core damage and its consequences, such as the preparedness organization with its preplanned actions and support to crew. However, success of the crew would mean a turn of the incident to a direction where the most severe consequence is loss of production.

3. Modeling aspects of the scenario from human performance point of view

The scenario combines the general features of seismic scenarios in HRA with special features that come with the loss of automation and main control room.

Some general features of seismic scenarios include

- seismic hazards are nonspecific: virtually any system, structure or component (SSC) may fail as a result of a sufficiently strong earthquake.
- seismic events may induce other phenomena such as landslides, soil liquefaction, tsunamis, floods, and fires. Of these, internal floods and fires are relevant at the Loviisa site. There are often aftershocks, that is, subsequent earthquakes. There may be aftershocks one month after the first earthquake, and even later.

At a nuclear power plant, an earthquake may cause serious consequences:

- loss of offsite power, usually because poles of power lines topple
- blackout, as was the case at Fukushima Daiichi due to the tsunami
- failures of various systems
- cracks in pipes, vessels and other structures
- hindrances to movement, for example fallen ceiling panels, failed lock systems, damaged roads

These features may have profound implications on human performance:

- the situation may be complex: operators may have to figure out proper actions in a situation where several of the systems referred to in operating procedures are not operational, and these systems may also be otherwise unrelated. Some measurements may be unavailable or misleading. Several alarms may have been triggered that need to be prioritized. Many tasks, for example inspections, need to be coordinated with field operators.
- the situation may be uncertain: initially it is not sure which systems have failed and which are operational. Some measurements may be unavailable due to instrumentation failures. Aftershocks and seismic-induced hazards may also generate uncertainty.

- the situation may be stressful: time available for actions may be short, operators who often live close to the plant may worry about their close ones and homes, a seismic situation may increase workload considerably. There might be noise in the control room due to multiple alarms and people communicating. An earthquake starts unexpectedly, and including aftershocks and realization of induced hazards, emergency situation may endure for days. Also the high stakes involved - possibility of radionuclide release, possibility of causing great damage if making errors - may cause stress. In the scenario considered in this paper, entering the containment is stressful due to the possibility of leak in primary circuit.
- the situation may be such that the crew's experience and the training it has received do not serve actions well. In northern Europe, earthquakes are rare, and it is likely that in a given crew nobody has firsthand experience on earthquakes and dealing with them. NPP operators have likely participated in training where coping with seismic events have been considered, but it is less certain that they have participated in such a training regularly. It is unlikely that they would have participated in training where the scenario treated in this paper would have been considered.
- procedures for handling seismic incidents may be inadequate.

In the case considered in this paper, extra complexity is brought by having to conduct manually actions that are normally taken care of by automation. Stress is brought by knowledge that securing residual heat removal has to be conducted manually and within a relatively short time span. Also some workers may have been injured due to falling of the MCR ceiling, which affects crew performance.

4. The HRA approach

In HRA models, errors are usually handled reasonably thoroughly, considering all factors that could affect them. However, tardiness - that is, that the human action as a whole takes more time than is available - is usually tackled quite simplistically, relying on timeline analysis (see (Kirwan, 1994, Section 5.2.4.9)). This analysis is simple - just assessing things like diagnostic time and execution time for the whole action. On the downside, it does not take into account uncertainties in individual activities that the action consists of, or the time structure of the action (for example, how does cooperation and other interaction within the crew affect execution time).

For better consideration of the time component of risk, a two-pronged approach is proposed for modeling the scenario. It is based on the notion that failure potential consists of two events: the crew makes an error that causes the residual heat removal to fail, or it makes no such errors but uses too much time (considering how much is available). These events are mutually exclusive, since in one event a human error occurs and in the other it does not. Therefore the probability of crew failure (often called human error probability) is

$$HEP_{RHR} = P_{late} + P_{error}, \qquad (1)$$

where P_{late} is the probability that residual heat removal starts working too late, and P_{error} is the probability that one or more errors are made that lead to failure of starting RHR.

The notion that any error will lead to failure is based on the assumption that there is too little time for recovery from the error. This assumption is reasonable and plausible in the scenario considered in this paper, because the time available is short. However, concerning minor recoveries such as opening a valve, it is definitely conservative.

Next we will look at how P_{late} and P_{error} can be calculated.

4.1. *Assessment of timings*

The problem that an action (or some of its parts) take too much time is known as schedule risk problem. A time-honored way (Siegel and Wolf

(1969), Ehmaghraby (1977)) to solve such problems is to construct an activity network from the activities, and then simulate the network with Monte Carlo simulation to obtain a numerical distribution(s) of some time quantities of interest. From this distribution, the probability of the action taking longer than the given time available, that is, P_{late}, can be computed. Our activity network (Figure 4) forms of course a basis for that.

The remaining job is to specify a probability distribution for the execution time of each activity in the network.

There are many probability distributions that can be used for modeling execution time of an activity. However, the lognormal distribution is commonly used for modeling time to perform an activity, for example repair times (Rausand et al., 2021, p. 185).

There are some ways in which earthquakes may affect execution time of activities. Our approach here relies on publicly available operating experience. In that, we rely on the following sources. Presley et al. (2013) have reviewed 59 seismic operating experience reports. Siu et al. (2013) and Siu et al. (2019) present lessons learned from the Fukushima Daiichi nuclear accident.

Operating experience indicates that delay in operator actions is likely after earthquakes: ”most operating experiences showed multiple instances of delayed operator actions” Presley et al. (2013). These delays were usually attributed to complexity, novelty, confusion, stress, communication between people and other factors related to the general operating environment. It is unclear whether these delays show as a delay between receiving a cue and the actual action, or as lengthening of execution. If we assume that both occur, the following may serve as a suitable functional relation between expected activity duration when a seismic event hasn't occurred T_{exe}, and expected activity duration after a seismic event $T_{seismic}$:

$$T_{seismic} = \alpha PGA + (1 + \beta PGA)T_{exe}, \quad (2)$$

where $\alpha > 0$ is the delay coefficient and $\beta > 0$ is the execution lengthening coefficient, and PGA (peak ground acceleration) serves as a measure of the earthquake's intensity at the plant. α and β may be estimated from simulator training data and earthquake incidence reports (provided they contain time information on actions).

Whereas we may assume that for most activities, only the delay parameter α matters (that is, $\beta = 0$), this is not the case for activities that involve movement. Namely, Siu et al. (2016) note that in the Fukushima Daiichi accident, access to venues of several ex-control room activities were restricted or blocked due to debris, structural damage, failed access systems, and in later stages also radiation; it is also clear that activities requiring travel such as FLEX activities may be delayed by damage to roads. These access problems naturally cause delays. In Fukushima, also delays in obtaining information, uncoordinated evacuation of staff and contractors (who had for example information on the location of needed equipment) and changing conditions during the accident caused delays. If the scenario considered is such that these factors may cause delays, they should be included in the timing model; in the scenario considered in this paper, β is probably a significant factor only in actions involving movement.

There are several sources of uncertainty in the timing model. For example, there is not much data available that could be used to estimate parameters of equation 2, and thus the equation's predictions will be imprecise. Recoveries have not been considered in the model; while they increase the likelihood of carrying out the action successfully, they take time.

4.2. *Assessment of human errors*

On the human error (or crew error) side, the earthquake itself does not seem to affect operator performance significantly: operator actions remain highly reliable after the event (Presley et al. (2013)). However, an earthquake may change circumstances markedly, as noted in Section 3. In HRA, circumstances are usually taken into account in performance shaping factors (PSF), and this will be also our approach here. Modern HRA methods, such as SPAR-H (Gertman et al. (2005)), provide frameworks in which to assess the value of each PSF. For most PSFs, it is sensible to use value obtained from such frameworks. Here we consider a few PSFs where special features of seismic scenarios, or special features of the particular scenario considered, merit deeper consideration.

It should be noted that sufficiency of time need not be addressed on the human error side in our model, because that has been addressed already in the form of P_{late} (see eq. 1).

We take on the factors listed in Section 3 and see how they could be treated as PSF's, considering the special features of the situation.

- Complexity. It is clear that in seismic scenarios, failures of systems and seismic-induced hazards have major effect on this when they occur. This has been captured by Hakata et al. (2010) who specify the value of this PSF as a quadratic function of the number of initiating events (in addition to the seismic event, internal initiating events could include failures of some central systems, and also seismic-induced hazards such as fire could be such). Having such a basis of calculating PSF of course also means that the value of the PSF may change in the course of accident progression: the value of the PSF changes whenever a new initiating event occurs. In the scenario considered in this paper, also moving to the reserve control room and then working in an environment where the unit's crew usually don't work adds to the complexity.
- Uncertainty. Although uncertainty may be a significant issue all through the scenario (due to postshocks and seismic-induced hazards), it is likely to be at peak immediately after the first earthquake.
- Stress. Kirchner et al. (2011) note rightly that initially the crew's stress level is probably quite high due to the necessity of responding to the earthquake's effects in a short period of time. It is likely that the effect is more pronounced in regions of low seismicity like Finland, because the situation is new to everyone, though it has been addressed in training. Kirchner et al. (2011) note further that stress may also increase due to disorientation concerning appropriate response, trauma or injury caused by the event, or work environment affected by loss of lighting, dust in the air, or clutter. It is likely that after the initial hectic phase, stress levels go down. However, aftershocks and realization of seismic-induced hazards are likely to drive stress level up again. In later phases, also other kinds of stress sources may emerge: Hakata et al. (2010) in their multi-unit model raise the stress level of operators in a unit if there has been a radionuclide release from another unit at the site; this was later confirmed in the Fukushima Daiichi accident, where ”operators were clearly worried about their personal safety” Siu et al. (2013) due to releases. In this paper's scenario, having to leave the MCR is likely a source of stress to the crew; it is also worth considering whether staying in the unit whose MCR and automation is lost, which may bring to mind that there could be some undetected damage in the unit, is a source of stress to TrT, FOprim and ICT.

A final issue to be dealt with here is how to handle the repeating cycle of TrT asking ICT the surface level measurements of SGs, ICT measuring and reporting them, and TrT adjusting the water levels accordingly. The number of cycles needed is unknown. Ultimately, repeating the cycle will be made unnecessary by repair of the automation system. Alternatively, residual heat removal may be arranged in some other way, which is probably a quicker option.

Let us conservatively assume that human error on any round will lead to failure of crew action. Then, there are two ways in which repeating the cycle ends: either to human error or to successful recovery of automatic RHR in some way. Let us denote the probability of human error while conducting the measurement-adjusting cycle in round i by $p_{HE,cyc}(i)$, probability that automatic RHR is recovered successfully by $p_{rec}(i)$, and probability that conducting the measurement-adjustment cycle fails (that is, ends due to human error) by $P_{HE,cyc}(i)$. Then,

$$P_{HE,cyc}(i) = \prod_{j=0}^{i-1}(1 - p_{HE,cyc}(j))(1 - p_{rec}(j)) \\ p_{HE,cyc}(i), \tag{3}$$

where we assume that the probability of human failure in cycle activities is 0 before the cycle begins, and probability of successful recovery before the cycle begins is 0 (because the cycle would not be started if successful recovery had taken place). These two conditions can be expressed as $p_{HE,cyc}(0) = 0$ and $p_{rec}(0) = 0$.

Finally, we get the probability that the crew action fails due to human error in the measure-adjust cycle as

$$P_{HE,cyc} = \sum_{i=1}^{\infty} P_{HE,cyc}(i) \tag{4}$$

Repetition also brings the modeling challenge that repeating the same set of activities may lead to boredom and also tiredness before change of shift, these may result in the loss of focus by TrT or ICT, and this loss of focus may lead to human errors such as slip. This would show up in the equations above in the form that $p_{HE,cyc}(i)$ is not constant but varies by i. Naturally, if automation system recovery time has a probability distribution, it is to be used in calculating $p_{rec}(i)$'s.

Also concerning human error, there are several sources of uncertainty. A salient one is that we do not accurately know the effects of PSFs on human error. This is true in ordinary circumstances, and even more true in circumstances after an earthquake for which data is scarce. Also the fact that actions outside the control room, such as the one considered in this paper, have received less attention in HRA than actions carried out in the main control room is a source of uncertainty in analysis.

Acknowledgement

The authors thank Jukka Koskenranta, Taisto Laato, Ilkka Paavola and Sami Sirén (all Fortum) for insightful and useful comments, and the staff of Loviisa NPP for providing important information concerning the scenario and operating procedures used in it. The study has been partly funded by National Nuclear Waste Management Fund through SAFER2028 research programme.

References

Ehmaghraby, S. E. (1977). *activity networks - project planning and control by network models*. John Wiley & Sons.

Gertman, D., H. Blackman, J. Marble, J. Byers, and C. Smith (2005). The spar-h human reliability analysis method. Report NUREG/CR-6883, U.S. Nuclear Regulatory Commission.

Hakata, T., K. Hasegawa, A. Endo, and S. Aoi (2010). Dynamic human reliability method in seismic psa for multi-unit-site. In *10th International Conference on Probabilistic Safety Assessment and Management 2010, PSAM 2010*, Volume 2, pp. 1433–1442.

Kirchner, R., E. Burns, V. Andersen, O. Zuchuat, and Y. Bayraktarli (2011). Human reliability modeling in the kernkfaftwerk mühleberg seismic hra. In *ANS PSA 2011 International Topical Meeting on Probabilistic Safety Assessment and Analysis (PSA 2011)*, Volume 3, pp. 2108–2118.

Kirwan, B. (1994). *A Guide To Practical Human Reliability assessment*. Taylor & Francis.

Park, J., Y. Kim, J. H. Kim, W. Jung, and S. C. Jang (2015). Estimating the response times of human operators working in the main control room of nuclear power plants based on the context of a seismic event – a case study. *Annals of Nuclear Energy 85*(1), 36–46.

Presley, M. R., J. A. Julius, J. F. Grobbelaar, and K. D. Kohlhepp (2013). A review of seismic operating experience with implications for human reliability. In *ANS PSA 2013 International Topical Meeting on Probabilistic Safety Assessment and Analysis*, pp. 1597–1608.

Rausand, M., A. Barros, and A. Hoyland (2021). *System reliability theory - models, statistical methods, and applications* (third ed.). Wiley.

Siegel, A. I. and J. J. Wolf (1969). *Man-machine simulation models: psychosocial and performance interaction*. Wiley-Interscience.

Siu, N., K. Compton, S. Cooper, K. Coyne, F. Ferrante, D. Helton, D. Marksberry, and J. Xing (2016). Psa technology reminders and challenges revealed by the great east japan earthquake: 2016 update.

Siu, N., D. Marksberry, S. Cooper, K. Coyne, and M. Stutzke (2013). Psa technology challenges revealed by the great east japan earthquake.

Siu, N., J. Xing, N. Melly, F. Sock, and J. Pires (2019). Qualitative pra insights from seismic events.