Proc. of the European Safety and Reliability Conference (ESREL 2026)
Edited by José C. Matos, Paulo B. Lourenço, Michael Beer, Daniel Oliveira, Edoardo Patelli, Hélder S. Sousa, Rui A. Silva and Monica Santamaria
 Published by Research Publishing, Singapore.
doi: 10.3850/ESREL2026061419_esrel26-p27747-cd

Comparing identification of human failure events with two HRA methods in an ex-control room action

Ilkka Karanta, Essi Immonen

Severe accidents team, VTT Technical Research Centre of Finland Ltd., Finland. E-mail: firsname.lastname@vtt.fi

We compare two human reliability assessment methods, THERP and Phoenix, in human failure event (HFE) identification in an ex-control room setting. First, we consider briefly what HFE identification should encompass. Then we introduce the example scenario used, a part of a post-earthquake scenario where two operators attempt to even out water levels in steam generators utilizing an emergency water source. We describe briefly how HFE identification is conducted in the two methods, and conduct HFE identification in the scenario with each method. We compare the methods by conducting HFE identification with them on the example scenario. A major difference between the two is that THERP is procedure-based whereas Phoenix is model-based. Another difference is that THERP does not guide HFE identification much, which gives analysts freedom to apply their judgment, but may lead to considerable differences in analysis results by different analysts. In contrast, the HFE identification process of Phoenix is structured, model-based and with considerable guidance, and therefore likely promotes reduction of differences in analysis results between different analysts.

Keywords: human reliability analysis, human failure event, ex-control room action, THERP, Phoenix, seismic.

1. Introduction

In human reliability analysis (HRA), a human failure event (HFE) means that a human action does not meet some objective(s) set for it. For example, the action may take too much time, it may result in the system considered (e.g., a nuclear power plant unit) entering a trajectory leading to an accident, or it may result in failure in the system's objectives (e.g., loss of production).

In probabilistic risk assessment (PRA), HFEs play an important role: they represent human contribution to risk and thus connect HRA model to the PRA model. HFE may feature in the PRA model as a basic event in a fault tree or a section in an event tree, always marking an event that a human action failed in a way that has import to the PRA model.

Human failure events quite often come to the HRA expert from the main PRA model. Even if they don't, it is usually quite straightforward to tell what they are: an HFE is the event that the human action under consideration fails. HFE identification aims at something much more nontrivial: identifying what can go wrong with the human action considered. Besides this, HFE identification usually aims at finding out what can cause the particular kind of failure, that is, a cause or causes.

Several methods for identification and characterization (definition) of HFEs exist. HFE identification is also a part of any comprehensive HRA method, because it is an essential part of the HRA process.

In this paper we will compare HFE identification with two methods, THERP and Phoenix. The comparison is based on a scenario at a nuclear power plant. All activities in the scenario occur ex-control room.

2. Human failure events

Alternative definitions of human failure event (HFE) exist (see, e.g., Kirwan 2008 and Paglioni et al. 2022). In (Paglioni et al., 2022), it is defined as "*the failed state of some overarching objective, defined by the analysts in accordance with the scenario and analysis requirements*". Such objectives include, for example, that the action is carried out within some time limit, that no errors affecting the action's success are made, or that the system under consideration is in a given state as a result of the action.

This definition is theoretically satisfying, because it states exactly what we need to look for when identifying HFEs: some system objectives or requirements that are not satisfied due to the way the action under consideration was performed. It also has some practical merit, because such objectives may be available, for example, as operational limits. However, the definition also has a couple of issues. First, such objectives or requirements are not necessarily readily available; even when they are, the contradiction between the requirements and the results of the human action considered need to be verified by, e.g., simulation of plant response. Second, leaving HFE at finding a state that does not satisfy some objectives will leave us not knowing what exactly in the state of the affairs can be characterized as a failure, what caused the failure and what factors influenced it.

To alleviate the latter problem, we propose that the definition arrived at is augmented with the following:

A human failure event is a state of affairs where one or more of the objectives or requirements set for the system considered or the human action itself are not satisfied. It is characterized by the mode, causes and influencing factors of the failure.

In short, this means that besides identifying what can go wrong (in terms of objectives or failed actions) we believe that the specification of a human failure event should also consider possible mechanisms and causes of the failure.

3. The action considered

We consider a part of the following seismic scenario described in (Karanta and Hotakainen 2025). An earthquake has occurred at a pressurized water reactor nuclear power plant unit. Scram (insertion of control rods to reactor core to shut down the reactor) is successful, but the main control room and automation racks are lost. The crew's main duty now is to perform the necessary safety function of securing residual heat removal (RHR). This is achieved by deploying the additional emergency feedwater system (AEFW), a safety system that is in a separate building on the site and provides feedwater from its own tank utilizing Diesel generators and pumps. After configuration of the pipeline system, AEFW starts pumping water to undamaged steam generators (SG). The crew's main task now is securing that the water levels in the steam generators are approximately equal. An event sequence diagram of the scenario is depicted in Figure 1.

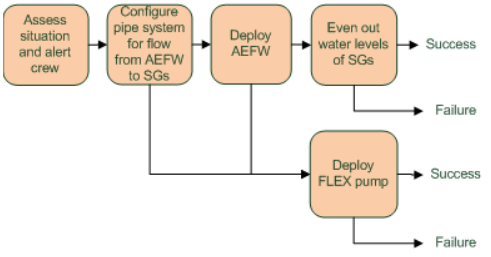

Fig. 1. Event sequence diagram of a seismic scenario at a nuclear power plant. The human action considered in this paper is "Even out water levels of SGs". For illustration purposes, also one possible recovery action, "Deploy FLEX pump", is shown.

The action considered in this paper is this evening out of water levels in the SGs. There are two field operators that are responsible for this: Turbine Technician (TrT) and I&C Technician (ICT). TrT's responsibility is to open wider valves of pipes leading from AEFW to SGs with water levels below the desired range, and close more tightly valves of pipes leading from AEFW to SGs with water levels above the desired range. TrT gets the water level information (and certain other data) from ICT, whom TrT regularly sends to round through the SGs and measure the water level of each with a field calibrator.

This description is somewhat simplified from the real-world scenario that the scenario is based on: for example, in real life, it is possible to connect the steam generators via an assembly, and this could happen in the real-world scenario. However, these are not considered here because they would complicate presentation without significantly affecting the comparison of two HRA methods, the topic of this paper.

The activity network of this action is shown in Figure 2.

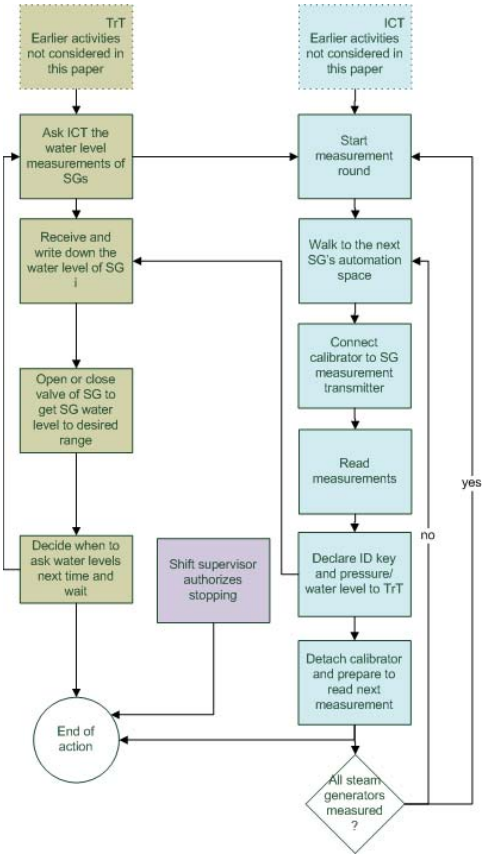

Fig. 2. Activity network of the evening out water levels in SGs action.

The action consists of water level adjustment rounds by the TrT, and the associated SG water level measurement round by ICT.

Each round begins with TrT sending ICT to a measurement round. ICT walks to SG1, conducts the measurement and reports the water level to TrT. Trt writes the water level down and opens the valve of the pipe leading from AEFW to SG1 if the water level is lower than the lower limit of desired range, closes it if the water level is higher than the upper limit of desired range, and otherwise does nothing to the valve. In the mean while ICT walks to the next SG, and the measurement-reporting-adjusting action between TrT and ICT is repeated. This continues until all SGs have been gone through for this round. Then ICT may take a break, and TrT decides when the next round is needed and may also take a break.

These rounds are repeated until the shift manager gives permission to stop the action.

To simplify matters, we do not consider recoveries in this paper although in real life there are of course many recovery possibilities in the scenario. It should also be borne in mind that both operators may have failed in some activities before the "evening out the water levels of SGs" action. For example, ICT may have forgot to take some keys, radiophone or field calibrator with them, or dropped some of these on the way to the steam generators; this will of course affect his performance at least by causing delays to his activities. However, these are out of the scope of this paper.

4. HFE identification with THERP

Technique for Human Error Rate Prediction (THERP) is a HRA method presented by Alan Swain in 1962 and later formalized in NUREG/CR-1278 (Swain and Guttman, 1983). THERP is still a widely used method alongside the newer generation HRA methods. While THERP may be more focused in the quantification approach of human error probabilities, also HFE identification is part of the method.

4.1 *HFE identification approach*

HFE identification with THERP is carried out as a part of task analysis. (Swain and Guttman, 1983). Alternatively, the steps of a procedure can be used as the starting point (Kirwan, 1992). For the task steps, possible errors are identified, considering the different error modes in connection with any relevant performance shaping factors (Swain and Guttman, 1983, Bell and Swain, 1983). The error modes recognised in NUREG/CR-1278 include errors of omission (omitting an entire task, or a step in a task) and commission (selection errors, error of sequence, time error, and qualitative error). Also, extraneous errors are mentioned, but seen difficult to recognise in entirety. Finally, possible recovery paths and the significance of each undetected failure event are considered.

4.2 *Case study with THERP*

4.2.1 *Hierarchical task analysis*

Hierarchical task analysis (HTA) was performed for the action of adjusting the water levels of steam generators to an approximately equal level.

Figure 3 illustrates part of the HTA task hierarchy. For clarity, only part of the analysis is described all the way to the subtask (operation) level.

For the action "Even out the SG water levels", one branch of the task hierarchy of TrT is included in Figure 3. The task is to ask ICT for measurements of the SG water levels and adjust the water levels accordingly. This step is repeated until stopping has been authorized by shift manager. Task 1 is divided into six sub-tasks. In step 1.1 TrT calls ICT and asks to measure all SG levels. Steps 1.2-1.5 describe the steps that ICT and TrT perform to conduct the SG level measurements and to communicate the measured values, as shown in the activity diagram of Figure 2. In step 1.6 TrT adjusts the SG water levels to get them to a desired range. Step 1.1 is performed first, and steps 1.2-1.6 are then repeated until all SG water levels have been measured and adjusted accordingly. Finally, step 1.6 is divided further into two operations, 1.6.1 where TrT turns the valve of the feedwater line leading to SG towards open position, performed when measured SG water level is low, and 1.6.2 where TrT turns the valve of the feedwater line leading to SG towards closed position, performed when measured SG water level is high.

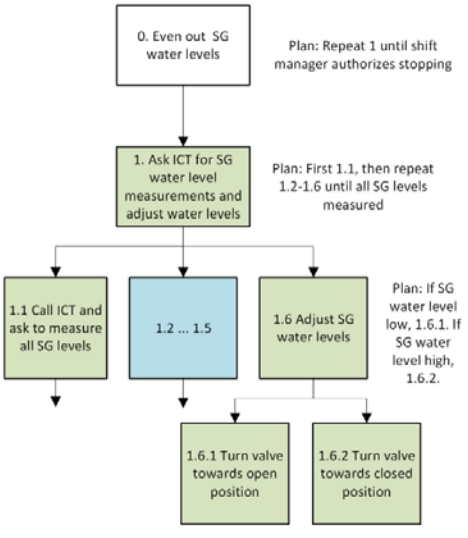

Fig. 3. Task breakdown from HTA.

4.2.2 *HFE identification*

Human failure events are identified for the operations resulting from the HTA. To describe the process, TrT step 1.6.1 "Turn SG valve towards open position" is discussed in more detail. The identification of error possibilities is performed using the emergency operation procedures as a support, and no specific walkthrough or talk through with crew members were performed.

The following error possibilities were identified:

- TrT opens a wrong SG valve
- TrT turns the valve to a wrong direction
- TrT turns the valve too little or too much
- TrT doesn't turn the valve at all

All of the above may result in a failure of one of the steam generators, assuming that the SG has a low water level to start with when the feedwater flow is further decreased, or not increased if the correct valve isn't opened. In reality, the timespan of the situation is likely long enough, that there is time to notice the error and make the necessary recovery actions.

For the PSFs that contribute to the error possibilities of the step of opening the valve, the post-initiator PSFs listed in NUREG-1792 (NRC, 2005) have been considered. The PSFs that are likely to contribute to the likelihood of all of the identified error possibilities are the clarity of procedures and time since the latest training. The seismic situation is not common to Nordic NPPs and may not have been trained frequently. The valves are typically operated from the control room rather than manually, so the unfamiliar situation may increase error possibilities. As ICT is giving measurements for all the SGs, there's a possibility that TrT should adjust more than one SG feedwater valve during one measurement round, which could result in confusing one valve for another, especially when in combination with a stressful task environment. Post-earthquake conditions at the plant may include problems with lighting and power loss, noise due to alarms, unavailability of equipment and possible fallen debris in route. The conditions are likely to increase stress and affect concentration to the task on hand.

It is assumed that the failures made when adjusting the valve are noticed when the next round of SG water levels are reported by ICT. Otherwise, recoveries are not considered in this paper.

5. HFE identification with Phoenix

Phoenix is a model-based HRA method (Ekanem et al. 2016, Ekanem et al. 2024) . It was originally developed for control room operations at nuclear power plants, but has later been extended to many application fields and directions, including ex-control room actions (Al-Douri et al. 2023, Cheng et al. 2025).

4.1 *HFE identification approach*

Qualitative analysis part of Phoenix assumes that an event sequence diagram (ESD), such as the one in Figure 1, or an event tree (ET) exists; it describes the scenario, including human actions.

From the ESD or ET, a crew response tree is generated; this tree is a "crew-centric visual representation of the crew-plant scenarios" (Ekanem 2013), and it contains the human actions, possibly including recovery actions, and crew-plant interaction; the "nodes or branch points of the CRT can include operator decisions and actions, relevant plant/system functional states, as well as crew interactions" (Ekanem 2013). A flowchart for constructing the CRT is given in Figure 5-1 of (Ekanem 2013). Human failure events in Phoenix are failures of human actions in the CRT.

HFE identification - that is, the identification of human failure mechanisms and causes – is completed in the next step, construction of the human performance model. This model is based on the crew-centered version of the Information, Decision and Action (IDA) cognitive model (Smidts et al. 1997). It consists of constructing fault trees for failures of human actions in the CRT. These fault trees are called human response model (HRM) fault trees, and they are of a specific form: they represent the failures as disjunctions of so-called crew failure modes (CFM). CFMs represent the mechanisms by which failures occur in each IDA phase, and there are 9 of them in for Information, 7 for Diagnosis, and 3 for Action phase of IDA in the original method. In addition to these, we utilized the two extra CFMs proposed by (al-Douri et al. 2023): D8 "premature termination of procedure" for the Diagnosis phase and A4 "no action taken on object or component" for the Action phase. The CFMs are defined and explicated in section 7.2 of (Ekanem 2013). A set of fault trees aiding in the selection of relevant CFMs for each CRT branch point for each scenario are given in (Ekanem 2013, section 6), based on (Hendrickson et al. 2010) and (Oxstrand et al. 2012).

4.2 *Case study with Phoenix*

The starting point of the analysis is the ESD presented in Figure 1. We consider only the last node, "Even out water levels of SGs".

First, we construct a CRT for this node. As the procedures applicable in the selected part of the scenario are presented in Fig. 2 (though in a concentrated form), following the CRT construction procedure of Phoenix we arrive at the following failure events for humans (H) and system (S) (we mainly follow the notation of Cheng et al. 2025):

- H1: TrT asks ICT to measure the water levels of SGs
- H2: ICT starts measurement round
- H3: ICT walks to the next operating SG
- H4: ICT connects calibrator to the SG's measurement transmitter
- H5: ICT reads calibrator measurements
- H6: ICT calls TrT and declares ID key of SG and pressure/water level to TrT
- H7: TrT receives and writes down the water level of the SG
- H8: TrT opens or closes valve of the SG to get SG water level to desired range
- H9: TrT decides when to ask water levels next time
- H10: ICT detaches calibrator and prepares to read next measurement
- T1: availability of communication connection between TrT and ICT
- T2: availability of a safe route to the SG
- T3: calibrator availability
- T4: measurement transmitter availability
- T5: calibrator works correctly
- T6: writing instruments are available
- T7: control valve in the AEFW-SG pipe is available

The failure events here are simply that the activity in question fails, for example HFE5 would be "ICT fails in reading calibrator measurements".

The resulting CRT is simple and linear, because there are no alternative courses of action in the part of the scenario we are considering (in real life there are), and no recoveries are modelled. It is presented in Fig. 4.

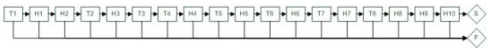

Fig. 4. Crew response tree of the evening out the water levels of SGs action.

The last step in the HFE identification process is construction a HRM fault tree for each human activity in the CRT (H1-H10).

We present here the HRM fault tree of H1, "TrT asks ICT to measure the water levels of SGs", in Fig. 5. This task is a communication task, and it can fail in two ways. One is that communication does not take place at all. In terms of CFMs, this can occur in two ways: TrT decides to stop gathering data on water levels and pressures in SGs (I4) or will not check those measurements often enough. It is likely that these failures occur after sufficiently many repetitions of the measurement cycle – as explained in section 3, the cycle or measuring, reporting measurements and writing them down is repeated an indefinite amount of times – when tiredness and getting bored of repeating the cycle may set in, and measurement results do not seem to change much. The other failure possibility is related to miscommunication: TrT or ICT may say something unclear or messy, or mishear what the other says.

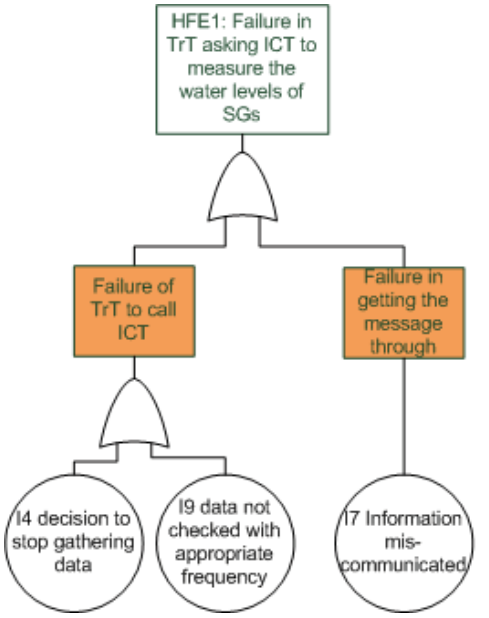

Fig. 5. Human response model fault tree of the "TrT asking ICT to measure the water levels of SGs fails" HFE.

6. Comparison of THERP and Phoenix

Both HRA methods provide sufficient apparatus tp the analysis of ex-control room actions at least in the small example scenario considered in this paper. THERP provides the apparatus as a part of the method itself, Phoenix provides them when slightly extended.

The results of the two methods are similar. In THERP, the task analysis results in more detailed steps, while Phoenix may stay at a coarser level. However, Phoenix results are associated with models (whereas the results of THERP are not), and thus it is likely that Phoenix results are easier to reuse in other HRA analyses.

One big difference between THERP and Phoenix is that Phoenix is more model based. The starting point of Phoenix is the scenario which is expressed as an event tree or event sequence diagram. From that an analyst using Phoenix proceeds to produce a crew response tree, several CRT fault trees, and utilises Bayesian networks to express relationships between PSFs and crew failure modes. On the other hand in THERP, some simple mathematical models (event trees and fault trees) are used, but are not similarly in focus in HFE identification as in Phoenix, and in THERP the HRA event trees are simpler than the crew response trees in Phoenix.

The HFE identification in THERP is simple to adopt, but quite free in format, and thus the quality of the analysis relies quite a bit on the skills and experience of the analyst. In comparison, Phoenix is more structured: there is a clear line of conducting analysis from identifying HFEs and their mechanisms and causes (and beyond). Furthermore, guidance exists for the analysis steps. Thus, one may expect that Phoenix results are less dependent on analyst capabilities and expertise.

The free format of THERP HFE identification gives versatility to the identification process, and original THERP guidelines can be modified by including e.g. different PSFs to the assessment. Phoenix was originally created for HRA of actions in the main control rooms of nuclear power plants. Thus, core Phoenix is not particularly versatile. However, it is relatively straightforward to extend Phoenix to different fields and application domains. On the qualitative side, the only thing that may need rethinking is crew failure modes that may vary from domain to

domain and field to field; for example, (al-Douri et al. 2023) propose two new CFMs for ex-control room actions.

If task analysis if performed in detail, THERP HFE identification may give very thorough results, but also be laborious. In Phoenix, task analysis is not required and all the steps of the analysis process are also included in the final HRA model. In this paper, HFEs were identified from an activity network that could also have been created for other purposes. Phoenix is more flexible on the amount of resources used and can be likely performed with lesser resource consumption than THERP.

Finally, we note that THERP is task-based. This means a statistics-style approach to human error: baseline human error probabilities are derived from data, and human failure mechanisms receive scant attention. Phoenix has cognitive elements in the analysis, and CFMs are failure mechanisms or causes.

10. Conclusions

We have compared two HRA methods, the classic THERP and modern Phoenix, in an ex-control room scenario of a nuclear power plant.

The comparison of THERP and Phoenix in HFE identification is not purely a comparison of two HRA methods, but also to some degree sheds some light on how HFE identification has developed during the three decades from the release of THERP documentation in 1983 to the publishing of Phoenix in 2013. THERP is based on a statistical-type approach where the causes and mechanisms of human failure are given little attention (although the effect of environment in human error is acknowledged in the use of performance shaping factors). On the other hand, Phoenix rests on a cognitive model of human failure that has grounding in cognitive psychology.

Finally, a difference relates to how the analyses are structured. THERP relies on procedure-like steps to systematize the analysis. Phoenix systematizes the analysis by introducing a set of models, approaching the analysis as a sequence of model construction activities.

Acknowledgement

The study has been partly funded by Finnish National Nuclear Waste Management Fund through SAFER2028 research programme. The scenario considered in this paper, together with support materials, has been supplied by Fortum E&P corporation.

References

Al-Douri, A., C. S. Levine, and K. M. Groth (2023). "Identifying Human Failure Events (Hfes) for External Hazard Probabilistic Risk Assessment." *Reliability Engineering and System Safety 235*. https://doi.org/https://doi.org/10.1016/j.ress.2023.109236.

Bell, B.J., Swain, A. D. (1983). A Procedure for Conducting a Human Reliability Analysis for Nuclear Power Plants, NUREG/CR-2254, SNL, Albuquerque, NM

Cheng, T., M. Ramos, and A. Mosleh (2025). Application of Phoenix Human Reliability Analysis Methodology to Model External Operation with Flex Strategies Consideration. Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference, Research Publishing.

Ekanem, N. J. (2013). *A Model-Based Human Reliability Analysis Methodology (Phoenix Method)*. Doctoral dissertation, University of Maryland.

Ekanem, N., A. Mosleh, and S.-H. Shen (2016). Phoenix - a Model-Based Human Reliability Analysis Methodology: Qualitative Analysis Procedure. *Reliability Engineering and System Safety 145*, 301-15. https://doi.org/http://dx.doi.org/10.1016/j.ress.2015.07.009.

Ekanem, N., A. Mosleh, S.-H. Shen, and M. Ramos (2024). Phoenix - a Model-Based Human Reliability Analysis Methodology: Data Sources and Quantitative Analysis Procedure. *Reliability Engineering and System Safety 248*, 26p. https://doi.org/10.1016/j.ress.2024.110123.

Hendrickson, S., A. Whaley, R. Boring, J. Chang, S.-H. Shen, A. Mosleh, J. Oxstrand, J. Forester, and D. Kelly (2010). A Mid-Layer Model for Human Reliability Analysis: Understanding the Cognitive Causes of Human Failure Events. In *Probabilistic Safety Assessment & Management Conference (PSAM 10)*.

Karanta, I., and R. Hotakainen (2025). "Human Performance and Reliability in a Complex Seismic Accident Scenario at a Nuclear Power Plant." In *35th European Safety and Reliability Conference and 33rd Society for Risk Analysis Europe Conference*, Research Publishing.

Kirwan, B. (1992). Human error identification in human reliability assessment. Part 1: Overview of approaches. *Applied Ergonomics 23* (5), 299-318. https://doi.org/10.1016/0003-6870(92)90292-4

Kirwan, B. (2008). Human Reliability Assessment. In E. L. Melnick and B. S. Everitt (eds.). *Encyclopedia of Quantitative Risk Analysis and Assessment*, 22 p.: Wiley.

Nuclear Regulatory Commission (2005). Good Practices for Implementing Human Reliability Analysis (HRA), NUREG-1792, NRC.

Oxstrand, J., D. Kelly, S.-H. Shen, A. Mosleh, and K. Groth (2012). A Model-Based Approach to Hra: Qualitative Analysis Methodology. In 11th Probabilistic Safety Assessment & Management (PSAM 11) and European Safety & Reliability (ESREL) Conference.

Paglioni, V. P., T. Mortenson, and K. M. Groth (2022). "The Human Failure Event: What Is It and What Should It Be?" 16th Probabilistic Safety Assessment and Management Conference (PSAM 16), IAPSAM.

Smidts, C., S.-H. Shen, and A. Mosleh (1997). "The Ida Cognitive Model for the Analysis of Nuclear Power Plant Operator Response under Accident Conditions. Part I: Problem Solving and Decision Making Model." *Reliability Engineering and System Safety 55*, 51-71.

Swain, A. D., and H. E. Guttmann (1983). Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications - Final Report. U.S. Nuclear Regulatory Commission.