The Petro-HRA Guideline

Revision 1

Vol. 1

IFE/E-2022/001

Research for a better future

Report number: IFE/E-2022/001	ISSN: 0000-0000	Availability: Public	Publication date: 17.01.2022
Revision: 1	ISBN: 978-82-7017-937-4	DOCUS-ID: 55192	Number of pages: 99
Client: (Original) Norges Forskningsråd; (Rev. 1) Equinor			
Title: The Petro-HRA Guideline, Rev.1, Vol.1			

Summary:

Petro-HRA is a method for qualitative and quantitative assessment of human reliability in the petroleum industry. The method allows systematic identification, modelling and assessment of tasks that affect major accident risk. The method is mainly intended for use within a quantitative risk analysis (QRA) framework but may also be used as a stand-alone analysis. Petro-HRA should be used to estimate the likelihood of human failure events (HFEs) in post-initiating event scenarios.

The method was developed in an R&D project for Norges Forskningsråd and was published in 2017. Since then, it has been applied in several petroleum projects in Norway. In 2020, Equinor funded a project with DNV and IFE to update the method. Recommendations for improvements were collected via a review of 10 Petro-HRA technical reports to Equinor and a series of structured interviews with Petro-HRA method users and stakeholders. The guideline has been split into two documents for ease of use. The text in some sections has been modified for clarity, and new or modified examples have been provided to better explain how to apply the guidance.

Author List for Original Guideline Document:
Andreas Bye[1], Karin Laumann[2], Claire Blackett[1], Martin Rasmussen[2], Sondre Øie[3], Koen van de Merwe[3], Knut Øien[4], Ronald Boring[5], Nicola Paltrinieri[4], Irene Wærø[4], Salvatore Massaiu[1], Kristian Gould[6].

Author List for Revision 1:
Claire Blackett[1], Jan Erik Farbrot[1], Sondre Øie[3], Marius Fernander[3].

[1]IFE, [2]NTNU, [3]DNV, [4]SINTEF, [5]INL, [6]EQUINOR

Prepared by:	Claire Blackett (IFE)
Reviewed by:	Andreas Bye (IFE)
Approved by:	Sizarta Sarshar (IFE)
Report distribution:	For external, open

Institute for Energy Technology
P.O. Box 40, NO-2027 Kjeller, Norway / P.O. Box 173, NO-1751 Halden
Telephone: +47 63 80 60 00/ +47 69 21 22 00
www.ife.no / firmapost@ife.no

Contents

Abbreviations

ASME	American Society of Mechanical Engineers
BOP	Blowout Preventer
CCTV	Closed Circuit Television
DSHA	Defined Situations of Hazard and Accident
EPA	Emergency Preparedness Analysis
ERA	Error Reduction Analysis
ERM	Error Reduction Measure
ERO	Engine Room Operator
ERS	Error Reduction Strategy
ESD	Emergency Shutdown
ETA	Event Tree Analysis
FTA	Fault Tree Analysis
HAZID	Hazard Identification
HAZOP	Hazard and Operability Study
HEI	Human Error Identification
HEART	Human Error Assessment and Reduction Technique
HEP	Human Error Probability
HF	Human Factors
HFE	Human Failure Event
HMI	Human Machine Interface
HRA	Human Reliability Analysis
HSE	Health Safety and Environment
HTA	Hierarchical Task Analysis
IE	Initiating Event
IFE	Institute for Energy Technology
LOPA	Layers of Protection Analysis
NHEP	Nominal Human Error Probability
NTNU	Norwegian University of Science and Technology
OAET	Operator Action Event Tree
PRA/PSA	Probabilistic Risk/Safety Assessment
PSF	Performance Shaping Factors
QRA	Quantitative Risk Assessment
SHERPA	Systematic Human Error Reduction and Prediction Approach
SME	Subject Matter Expert
SPAR-H	Standardized Plant Analysis Risk – Human Reliability Analysis
THERP	Technique for Human Error-Rate Prediction
TRA	Total Risk Analysis
TTA	Tabular Task Analysis

List of Figures

List of Tables

Useful Definitions

Action	Operator actions can take the form of individual control actions (e.g., turning a switch to a particular position; turning a pump on or off) or a sequence of actions intended to achieve a particular goal (NUREG-2114, 2012). The motion(s), decision(s), or thinking of one or more persons required to complete a mission defined by the context of an accident scenario (NUREG-1921).
Event tree	A logic diagram that begins with an initiating event or condition and progresses through a series of branches that represent expected system or operator performance that either succeeds or fails and arrives at either a successful or failed end state (ASME, 2009b).
Facility	Petroleum producing platform, drilling platform, refinery, floater, ship operated by dynamic positioning, or any other industrial facility used in the petroleum industry.
Fault tree	A deductive logic diagram that depicts how a particular undesired event can occur as a logical combination of other undesired events (ASME, 2009b).
Goal	A goal is an overall aim which can be achieved by a varying range of tasks, based on set objectives to achieve the goal (Kirwan & Ainsworth, 1992).
Human error	Any human action that exceeds some limit of acceptability, including inaction where required, excluding malevolent behavior (ASME, 2009b).
Human error probability (HEP)	A measure of the likelihood that plant personnel will fail to initiate the correct, required, or specified action or response in a given situation, or by commission performs the wrong action. The HEP is the probability of the human failure event (ASME, 2009b).
Human factors (HF)	The scientific discipline concerned with the understanding of interactions among humans and other elements of a system, and the profession that applies theory, principles, data and methods to design in order to optimize human well-being and overall system performance (Human Factors and Ergonomics Society, 2014).
Human failure event (HFE)	A basic event that represents a failure or unavailability of a component, system, or function that is caused by human inaction, or an inappropriate action (ASME, 2009b).
Human reliability analysis / assessment (HRA)	A structured approach used to identify potential human failure events and to systematically estimate the [numerical] probability (HEP) of those events using data, models, or expert judgment (ASME, 2009b).
Initiating Event (IE)	An event either internal or external to that which perturbs the steady state operation of the plant by challenge plant control and safety systems whose failure could potentially lead to severe Defined Situations of Hazard and Accident (DSHAs). These events include human-caused perturbations and failure of equipment from either internal plant causes (such as hardware faults, floods, or fires) or external plant causes (such as earthquakes or high winds) (Adapted from ASME, 2009b).

Performance shaping factor (PSF)	A factor that influences human error probabilities as considered in a […] human reliability analysis and includes such items as level of training, quality/availability of procedural guidance, time available to perform an action, etc. (ASME, 2009b).
Procedure	A procedure is a written document (including both text and graphics) that represents a series of decisions and action steps to be performed by the operator(s) to accomplish a goal safely and efficiently. The purpose of a procedure is to guide human actions when performing a task to increase the likelihood that the actions will safely achieve the task's goal (O'Hara et al., 2000).
Post-Initiating Event	Referring to the time period in the scenario after the IE, typically containing mitigation actions in order to handle the scenario/accident.
Process Safety Time	The time period between a failure occurring in the process or the basic process control system (with the potential to give rise to a hazardous event) and the occurrence of the hazardous event if the safety instrumented function is not performed (IEC61511 part 2 (2003)).
Quantitative Risk Assessment (QRA)	Quantitative risk assessment (QRA) is a formal and systematic approach to estimating the likelihood and consequences of hazardous events, and expressing the results quantitatively as risk to people, the environment or your business. (DNV GL, 2014).
Subtask	A part of a task that when performed with one or more additional sub-tasks will result in successful task completion (Kirwan & Ainsworth, 1992).
Task	A task is a set pattern of operations which alone, or together with other tasks, may be used to achieve a goal (Kirwan & Ainsworth, 1992).
Task analysis	Task analysis is a method of describing what an operator is required to do, in terms of actions and/ or cognitive processes, to achieve a system goal. It is a method of describing how an operator interacts with a system, and with the personnel in that system. (Kirwan & Ainsworth, 1992).
Task Step	A task step is an arbitrary division of a task or subtask that usually includes the following: some type of information presented to the operator, some degree of operator processing of the information, and some type of required response (Swain & Guttmann, 1983).

I. Introduction to the Petro-HRA Method

Petro-HRA is a human reliability analysis (HRA) method that should be used to estimate the likelihood of human failures in post-initiating event scenarios, also referred to as Type C Human Failure Events (HFEs), in the onshore and offshore petroleum industry. Petro-HRA applies both qualitative and quantitative assessments for systematic identification, modelling and assessment of tasks that affect major accident risk. The method is mainly intended for use within a risk model framework such as Quantitative Risk Assessment (QRA), but may also be used as a stand-alone analysis, e.g., to support a Human Factors Engineering analysis, or as part of other risk analyses such as Layers of Protection Analysis (LOPA). For simplicity, we use the generic term "risk analysis/model" throughout this guideline, but it is acknowledged that the method has a much broader applicability.

The probability of the HFE is called the human error probability (HEP) and can be input directly to the risk model. However, the qualitative results of an HRA are just as important as the error probability. Petro-HRA constitutes a thorough analysis of human actions in risk situations and may also be used for analysing the effects of early design choices, e.g., decisions on design options dependent on various timing requirements for the operators involved. The thoroughness of the Petro-HRA approach supports rigorous human error reduction, meaning that it enables the analyst to pinpoint factors and systems (such as the Human-Machine Interface (HMI), training program or operating procedures) that can be improved in order to reduce the HEP and the overall system risk. Quantification provides a means to prioritize human error reduction initiatives, as well as contributing to a more thorough overall risk assessment.

The Petro-HRA method was developed for evaluation of the likelihood of human failures in post-initiating event scenarios in the petroleum industry, also called Human Failure Events (HFEs) or Type C events. These events typically occur on the right-hand side of the bow tie diagram that is often used in petroleum risk assessment, as shown in Figure 1.

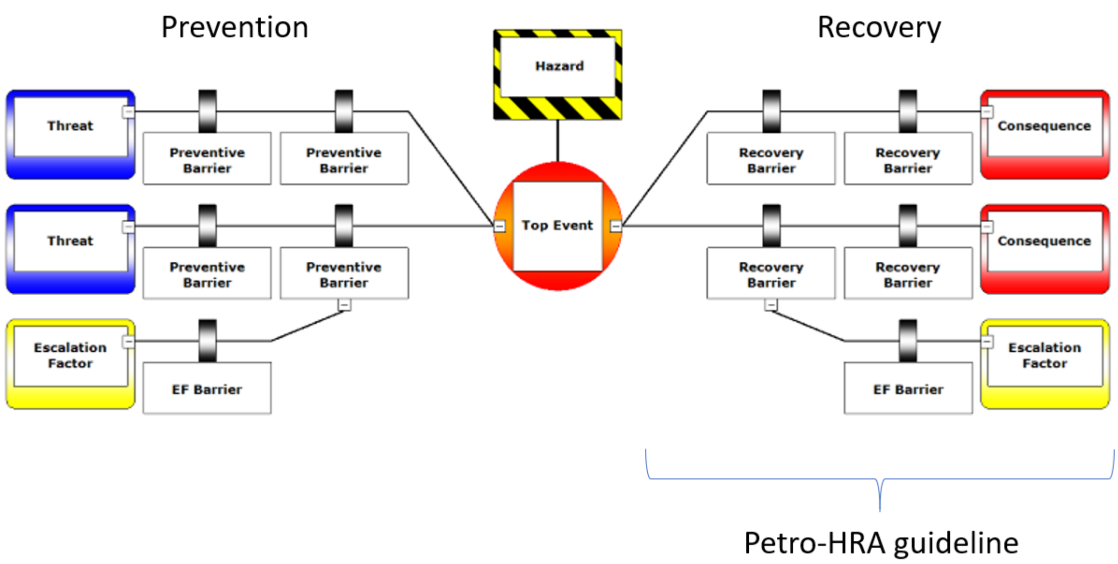


Figure 1: A typical bow-tie diagram used in petroleum risk assessment

A separate guideline has been developed for qualitative analysis of pre-accident events, also called Type A (pre-initiator) and Type B (initiating) events, which typically occur on the left-hand side of the bow-tie diagram. This method is called Analysis of Pre-accident Operator Actions (APOA; Øie & Fernander, 2022).

I.I Background to the Petro-HRA Guideline

This guideline was developed by the Petro-HRA project, a knowledge-building project for the business sector funded by the Research Council of Norway's PETROMAKS program (project number 220824/E30). The Institute for Energy Technology (IFE) was the project owner. SINTEF, the Idaho National Laboratory and the Norwegian University of Science and Technology (NTNU) were consortium partners. Equinor and DNV were industry partners.

The aim of the Petro-HRA project was to test, evaluate and adjust a suitable HRA method to post-initiating events in the petroleum industry. This project chose the Standardized Plant Analysis Risk-Human Reliability Analysis, or SPAR-H method (Gertman, Blackman, Marble, Byers & Smith, 2005), as the primary method to adjust to the petroleum industry. The choice was based on a review by Gould, Ringstad and van de Merwe (2012), which concluded that SPAR-H was the most promising method after having evaluated different methods for analysing human reliability in post-initiating events in the petroleum industry.

A main goal for Petro-HRA was to make the SPAR-H method suitable for the petroleum industry. The method includes context-specific guidance on qualitative data collection and analysis and quantitative analysis, as well as integration in QRA.

In 2020, Equinor funded a project with DNV and IFE to update the method. Recommendations for improvements were collected via a review of 10 Petro-HRA technical reports to Equinor and a series of structured interviews with Petro-HRA method users and stakeholders. Typographical and grammatical errors have been corrected throughout the document. The text in some sections has been modified for clarity, and new or modified examples have been provided to better explain how to apply the guidance.

I.II Purpose of the Petro-HRA Method

The Petro-HRA method should be used to qualitatively and quantitatively assess the likelihood of human failure. Although a thorough qualitative analysis is essential, the quantitative analysis has considerable value. The main purpose of quantitative analysis is to identify which tasks are most sensitive to human error, and which performance-shaping factors have the greatest influence on error probability. Human errors can be compared with hardware/software faults and other events in an overall risk assessment. This allows better prioritization of risk and risk-reducing measures.

I.III Scope of the Petro-HRA Method

Figure 2 shows the main steps in the Petro-HRA method. This figure indicates where the Petro-HRA interfaces with the risk analysis at the beginning to define the scenario and again when the HEP has been quantified, and directly with the facility/client through the provision of recommendations from the human error reduction analysis (Step 7), and the HRA report. The dotted lines indicate the iterative nature of the main steps.

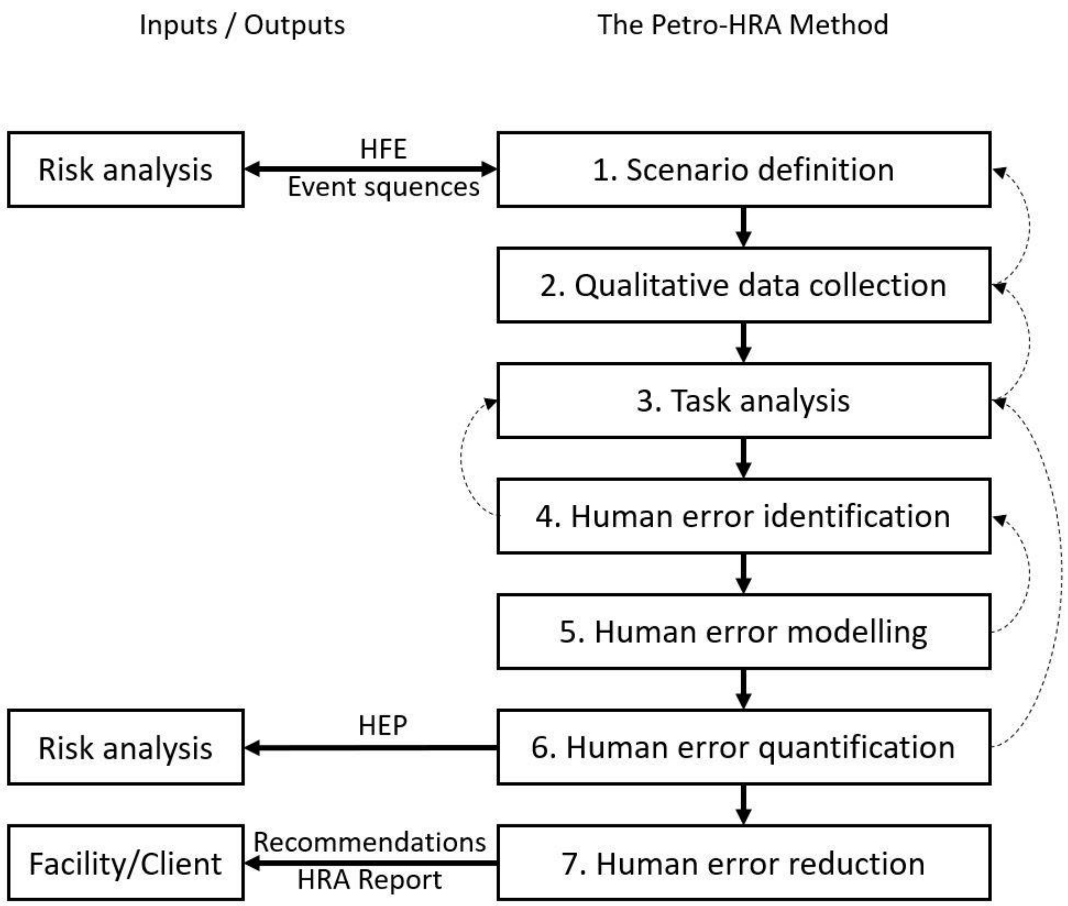


Figure 2: Petro-HRA; a complete HRA method

Human error is evaluated through the analysis of a Human Failure Event (HFE), a basic event that represents the failure of a component, system, or function in which humans are involved. The HFE is often defined in a risk model but can also be defined and/or modified by the HRA itself. One of the main purposes of the HRA is to provide quantitative input to risk analysis in the form of a Human Error Probability (HEP) of the HFEs. As shown in Figure 2, the Petro-HRA method details all steps in the HRA process, both qualitative and quantitative. Many HRA methods only provide guidance for quantification.

Although the steps are numbered and presented in consecutive sections in this guideline, it is essential for the analyst to understand that HRA is not a linear process. In reality, there is often iteration within and between steps throughout the whole process (illustrated by the dotted arrows in Figure 2). The HRA analyst must be flexible in their approach and be prepared to revisit and even repeat some steps in the process as necessary to ensure a robust, complete and comprehensive analysis. For example, the qualitative data collection provides essential inputs to all of the succeeding steps, and the quantification takes as much input from the task analysis and the human error identification as it does from the human error modelling.

This document includes practical guidance on how to execute a Petro-HRA to produce results suitable for use in QRA event tree models (see also van de Merwe et al., 2015a) by:

- Identifying operator actions and HFEs relevant for the (risk) analysis.
- Establishing scenarios which reflect risk event sequences in which HFEs are modelled.

- Ensuring that HFE "successes" and "failures" are defined according to the risk model.
- Executing the various analyses (task analyses, etc.) to substantiate the calculated HEP for the identified HFE(s).

The HRA may influence the overall risk model by modifying it based on outcomes from the task analysis, the human error identification, or the human error modelling (e.g., by providing clearer definition of the scenario, operator tasks or HFE(s)).

The level of detail in the HRA depends on the size and complexity of the major accident scenario(s) under analysis. Practical constraints related to, for example, time or facility access may also vary. As such, it may be necessary for the analyst to use their judgment and experience to combine or alter some of the activities described in the guideline.

I.IV Limitations of the Petro-HRA Method

A human error may be a cause of, or a partial cause of a major accident scenario, i.e., as a pre-initiator. Alternatively, human error can occur during a response to a major accident, i.e., as a post-initiator. The Petro-HRA method has been developed for analysis of post-initiator (Type C) human errors. It is recommended to use the new APOA method (Øie & Fernander, 2022) for analysis of Type A (pre-initiator) and Type B (initiator) events.

The Petro-HRA method has been developed to analyse control room tasks as performed in, for example, process control, drilling or maritime (bridge) operations. The method may also be used to analyse tasks that occur outside of the control room as long as the Performance Shaping Factors (PSFs) defined in this guideline are considered the most influential factors. If not, it should be considered whether an alternative HRA method should be used.

I.V How to Use this Guideline

In this second revision, the Petro-HRA guideline has now been separated into two documents to facilitate ease of use:

- Part 1 The Petro-HRA Method: Step-by-Step Instruction (this document; The Petro-HRA Guideline, 2022, Rev.1, Vol. 1)
- Parts 2 & 3 Case Study Example & Background Information for the Petro-HRA method (The Petro-HRA Guideline, 2022, Rev.1, Vol. 2)

The analyst should become familiar with both documents before applying the method documented in Part 1. Before using the method for the first time, the analyst should read through the case study example in Part 2 to gain a practical understanding of how the method is applied, and how each step builds on the previous one. It is also recommended to have read the background information in Part 3 at least once as it provides valuable context and additional information for each step of the Petro-HRA method.

I.VI Intended Readers and Users of this Guideline

This guideline is intended for HRA and QRA analysts who will either apply the method or use results from prior application of the method. This method is not intended for novice users, unless they are working under the supervision of an experienced analyst. To use the method, the analyst(s) should have the following minimum qualifications:

- Training and experience in applying human factors methods (task analysis, human error identification analysis, human error representation methods, timeline analysis).
- Familiarity with qualitative and quantitative risk analysis methods (fault- or event tree modelling, QRA).
- Knowledge about PSFs and their effect on performance.

It is recommended that the qualitative data collection, review and analysis are performed by a team of at least two analysts to maximize the efficiency and thoroughness of the data collection and analysis and to allow for cross checking. It is difficult for a single analyst to, for example, conduct an interview and take notes at the same time. Additionally, when reviewing collected data in isolation there is an increased risk of misinterpretation. Having a second analyst present reduces this risk.

Part 1
The Petro-HRA Method: Step-by-Step Guidance

1 Step 1: Scenario Definition

Scenario definition is one of the most important steps in the HRA, as it defines the scope and boundaries of the analysis and shapes the subsequent qualitative and quantitative analyses. Scenario definition can be difficult, depending on how well the Human Failure Events (HFEs) have been defined in the risk analysis. Therefore, it is strongly recommended that the analyst should spend some time here to make sure that the scenario has been described in detail before proceeding with Step 2 of the method.

It is essential that the Petro-HRA analyst spends some time up-front reviewing the risk model with a risk analyst. This is important not only to identify HFEs to be included in the analysis, but also to understand the operational context within which these HFEs occur and how these may impact the performance of safety barriers. It is also important to understand the contribution to overall risk of the HFEs as this will determine the amount of effort that should be spent on the Petro-HRA. Low or zero-risk HFEs might not need to be analysed as thoroughly as HFEs that have a higher impact on the overall risk model.

1.1 Participate in Initial Meetings

To develop a suitable scenario description the analyst needs to collect information about the scenario to understand how it is defined in the risk analysis, how the scenario is likely to unfold and the role of the human operator throughout the scenario. To collect this information, the analyst should participate in the following meetings. Note that some of these meetings may be arranged as part of the overall risk analysis project, and some meetings may need to be arranged by the Petro-HRA analyst.

1. **General risk analysis kick-off meeting**. This meeting is typically arranged by the risk analysis team and/or project manager. The HRA analyst should attend this meeting to ensure that HRA is included on the agenda and to inform the other discipline representatives that an HRA will be performed. It is unlikely that this initial meeting will go into any detail about the risk model or HFEs, and so the purpose here is mostly to raise awareness of the HRA and identify key contacts for future meetings. It would be beneficial for the Petro-HRA analyst to already have reviewed relevant documentation, and to be familiar with risk analyses in general. This would help focus the discussion on applicable themes.

2. **General Hazard Identification (HAZID) meeting**. This activity is usually performed at an early stage in the risk analysis to identify hazards related to the facility, system, operation and maintenance. The HRA analyst should attend this meeting to assist with the identification of HFEs and human performance-related hazards. The HAZID is also a useful learning opportunity for the analyst, to help with understanding how the overall facility and systems work, as well as the concerns of the other discipline representatives that will be in attendance. It is important that the HAZID facilitator is briefed and trained on how to include identification of HFEs and human performance-related hazards in advance of the meeting.

3. **HRA kick-off meeting**. The HRA analyst should arrange an HRA-specific kick off meeting to discuss and agree the scope of the HRA, confirm the scenario(s) to be analysed and confirm which HFE(s) are present in that scenario. It is important to include a risk analyst in this meeting to discuss how the HFEs are represented in the risk analysis, and how the HRA will be integrated with the risk model. It may also be useful to include a facility representative (e.g., experienced operator or supervisor) in this meeting to provide supplementary high-level

information about the HFEs or the scenario. This meeting should also confirm expected deliverables, timescales and key activities for the HRA.

4. **Scenario meeting**. This meeting is focused on discussing the scenario(s) that are to be analysed in the HRA. The meeting should include as a minimum the HRA analyst and two or three operators from the facility. It is recommended to include a risk analyst or other facility personnel such as an experienced operator, supervisor or a trainer. The scenario should be discussed in detail in this meeting; if possible, a high-level talk through of the scenario should be performed to help the HRA analyst understand the key operator activities, and to define key parameters for the scenario. The analyst should define what is meant by “success” and “failure” for each of these activities; for example, is partial blowdown considered a success in the scenario under analysis? A full blowdown may take many hours to complete, so it is important to know what is meant by “blowdown failure” in the risk analysis. The analyst should also seek to identify relevant documentation (e.g., operating procedures, system description documents, previous analyses, etc.) that will provide useful background information and inform the scenario description.

Some key questions that the analyst should try to answer in the HRA kick-off meeting and scenario meeting are listed below:

- What are the relevant Defined Situations of Hazard and Accident (DSHA) for this scenario?
- How does the risk model define the relevant major accident scenario(s)?
- What HFEs are currently modelled in the risk analysis and what constitutes success or failure for these HFEs?
- Will it be possible to amend the existing HFEs based on the findings from the HRA?

It should be noted that it might take several meetings with different groups of people to piece together the necessary information to generate a detailed scenario description and to define the scope of the HRA. However, experience shows that it may not always be possible, due to availability of personnel, time restraints, budget limitations, etc. to arrange separate meetings with different groups of people. Therefore, the analyst must also be prepared for the case where they have to, for example, combine the HRA kick-off meeting and scenario meeting, although the analyst should always strive to have separate meetings to allow more focused discussion.

Another point to note is that the timing of the HRA can also affect the ability to perform the analysis to the level of detail required. If the HRA is requested very early in the risk analysis process, the scenario may not be sufficiently defined to perform an HRA. In this case, it may be better to wait until the risk analysis has progressed to the point where the scenario is well defined before starting the analysis; otherwise, it may require significant re-work later on if some key details in the scenario definition change. Alternatively, it may be the case that the HRA is required to assist with definition of the risk model, in which case it is expected that the scenario may change during the process. The timing of the HRA and maturity of the risk analysis is important and needs to be clarified at the beginning of the project, to understand what inputs will be needed for both sides. Regular communication with the risk analyst is key throughout the HRA.

1.1.1 Resources to Support the Analyst in the Initial Meetings

Table 17 in Appendix A contains a list of questions that may be useful for the analyst to review and consider as part of the preparations for the HRA kick-off meeting and scenario meeting. It is unlikely that all of these questions will be answered in the HRA kick-off meeting or scenario meeting. Therefore, the analyst should revisit this list of questions periodically throughout the scenario definition step to check whether there are any knowledge gaps and should follow up with an appropriate contact.

1.1.2 Expected Outcomes of the Initial Meetings

The expected outcomes from the initial meetings are:

1. A shared understanding amongst team members and other risk analysts of the contribution of the Petro-HRA to the risk analysis.
2. A qualitative screening of the events trees, scenarios and HFEs relevant to the Petro-HRA, and those which require further examination (e.g., via document review or additional meetings).
3. A plan for the Petro-HRA including main activities, timescale/schedule, roles and responsibilities for integrating the Petro-HRA into the risk analysis.

1.2 Perform a Document Review

Once the analyst has established the key parameters of the scenario and HFEs from the initial meetings, a document review should be performed to gather additional information to define the analysis scenario. As noted previously, it would be beneficial for the analyst to review documentation before the risk analysis kick-off meeting as well. The objective of the document review is to collect and understand information about:

- The role of the operator in the scenario, and the tasks that operators are required to perform.
- The function of facility systems in the scenario, and where human-system interaction is likely to occur.
- The location and layout of relevant facility systems and HMIs.
- The systems, tools and other resources that the operators are likely to use in the scenario.
- The results of previous analyses performed that are relevant to the scenario.

One of the purposes of the documentation review is to establish what information is readily available, and where there are information gaps or uncertainties in the analyst's understanding of the scenario. These will form the basis of the qualitative data collection activities in Step 2 of the HRA. Any questions, knowledge gaps, areas of uncertainty or assumptions should be documented for incorporation into the later data collection activities.

1.2.1 Resources to Support the Analyst in the Document Review

Table 18 in Appendix A contains a list of documents that would typically be reviewed during a Petro-HRA. The list is not exhaustive and there may be other documents available that are useful for the Petro-HRA and for defining the scenario. Similarly, all of the documents in the table might not be available, or they may be called by different names at different sites. However, this list is useful as a starting point.

1.2.2 Expected Outcomes of the Document Review

The expected outcomes from the document review are:

- An increased understanding of the role of the operator in the scenario.
- Sufficient information about the parameters and context of the scenario to develop the scenario description.

- Sufficient information about the HFEs and critical operator tasks to develop an initial task analysis.

1.3 Develop the Scenario Description

By now the analyst should have enough information to develop the scenario description. The main objective for doing this is to create a more detailed description of the event sequences modelled in the risk analysis event trees. It is important that the scenario description is concise and contains specific information, which reflects the logic of the risk model. This description forms the basis for the subsequent qualitative data collection and task analysis. By creating a specific scenario description, it is possible to determine the boundaries of the HRA and document the assumptions made. More importantly, the scenario description acts as a communication platform and helps to create and maintain a common understanding of the scenario between the different people involved in the HRA and risk analysis processes.

The analyst should be aware that there are advantages and disadvantages to developing a very specific scenario description. The advantages are that it reduces the amount of uncertainty and ambiguity about the scenario, making data collection and analysis easier. However, if the scenario description is too specific, then the Petro-HRA may become too narrowly focused and representative of just one branch of the risk model, which could in turn necessitate several Petro-HRAs for each branch featuring a human action. Take, for example, the assessment of a hydrocarbon leak; if the Petro-HRA specifically defines the size of the leak, then the results may only be valid for that leak size, and additional Petro-HRAs may need to be performed for different leak sizes.

The analyst should strive to identify a suitably representative (or “bounding”) scenario that is specific enough to allow for detailed analysis, but that is representative enough to provide useful input to the risk model. A representative scenario may be a worst-case scenario or may be an amalgamation of scenario conditions where the consequences of the different scenario conditions can be grouped into one representative scenario. Taking again the example of the hydrocarbon leak, instead of performing separate Petro-HRAs for a small, medium or large leak, these could be bound into a single representative scenario, especially because the required operator actions in response to the scenario may be similar regardless of the leak size. If, for example, the timing of the operator response does impact on the consequences of the scenario, then the worst-case condition could be analysed. If the outcome of this analysis is considered acceptable in terms of risk contribution, then logically the less-severe conditions will also be acceptable to the risk model.

In addition to analysing the scenario identified in the risk analysis and/or in the initial meetings, the analyst should be aware that deviations of this scenario may exist that should also be considered for analysis. A deviation scenario can be defined as a scenario that deviates from the nominal conditions normally assumed for the risk model sequence of interest, which might cause problems or lead to misunderstandings for the operating crews (adapted from Forester et al., 2007).

There are several ways to describe the scenario, but as a minimum it should include the following:

- **Location of event**. The exact location of the event (e.g., the gas leak), and the location of other relevant events, activities (e.g., the control room) or conditions. Should also include the location of other relevant actors (e.g., emergency response team).

- **External environmental conditions**. The physical layout of the facility, geography, time of day, or weather conditions. These may not always be relevant to the scenario but should be recorded to avoid incorrect assumptions. For example, in the case of a gas leak, wind direction and natural ventilation may influence the severity of the incident and how it is dealt with by operators.

- **Operational mode**. The operational mode of the facility at the time of the event.

- **Safety system/barriers**. The function and performance of the various safety systems/barriers involved in the scenario, i.e., what the systems "do" and how they do it. For example, the Emergency Shutdown (ESD) system isolates the leaking segment by closing the ESD valves. The performance requirements for each safety system/barrier can also be documented here, such as the time it takes for a valve to close after activation. Interaction and dependency between systems should also be investigated and documented here.

- **Personnel roles and responsibilities**. The main actors involved in the scenario and their responsibilities.

- **Initiating event**. The event that initiates the scenario should be clearly defined. Examples include gas leakage, water ingress, drift off, drive off, well kick, etc. It is important to detail the type and severity of the event. For example, merely stating "loss of containment" is too ambiguous; instead, the description should state what is leaking (e.g., gas, oil, etc.), the type of leakage (e.g., jet, flow, spray), the direction of the leak (e.g., towards piping, towards a drain), and the rate/size of the leak (e.g., in kg/s).

- **Intermediate events**. The events that occur after the initiating event, which escalate the scenario. For example, how a gas leak increases or decreases in size, reaches new locations, and is influenced by wind or physical or geographical surroundings. The description should specify what happens, when it occurs and the potential implications for the scenario.

- **End of event sequence**. This is the "cut-off" point in which the scenario ends. For most QRAs, this will typically be before the major accident consequence has occurred, at the point when human intervention no longer makes any difference to the scenario outcome.

- **Duration of scenario**. This is the amount of time from the initiating event to the end event. The duration should be estimated in collaboration with QRA analysts and other Subject Matter Experts (SMEs, such as process engineers) so that the scenario remains credible.

The analyst may have to make assumptions about some of these topics because there is insufficient information available, or because there are too many variables. Assumptions should also be documented with the scenario description for transparency. Once the scenario description has been developed, the analyst should verify this with the QRA team and facility representatives to ensure it is valid and credible.

Table 1 shows a recommended template for capturing information about the scenario description. Questions for further investigation (including assumptions or uncertainties) should be documented in the "Actions" column. The table should be supplemented with a text description of the scenario.

Table 1: Suggested template for the scenario description, with completed example

Topic	Description	Comments	Actions
Event sequence			
Initiating event	An undefined DP failure initiates the drive-off. All thrusters are pointing aft, giving forward thrust. Thrusters are at zero revolution giving zero forward thrust at the starting point. Error in the DP control initiates the thrusters to accelerate up to full forward thrust: 6 thrusters running in calm water.	It is not important to define the actual cause (i.e., failure mode) of the drive-off. This is because the response pattern and required actions will more or less be the same regardless of the failure mode. For more than 6 thrusters, calculations show that the scenario duration reported below is too long and the automatic EDS will activate before the DPO activates the manual EDS.	
Intermediate events	The DP Operator will do the following: • Detect drive-off • Diagnose the situation • Decide the next steps • Activate emergency thruster stop • Activate the Red Alert and EDS	From the DP manual: "*In a Drive-Off event, stop thrusters, Initiate Red Alert and enable EDS immediately*." The DPO2 may notify the driller.	It is assumed that DPO activates the emergency stop of the thrusters. This is done to save time and reduce possible damages to the wellhead. The unit will still be drifting off position, but at a lower speed. • ACTION: check this assumption
End of event sequence	(Successful) Successful manual shutdown of the thrusters followed by manual activation of the EDS results in a timely and safe disconnection of the LMRP from the BOP. (Unsuccessful) For this scenario the Automatic EDS is enabled with a safety margin to prevent damage to the well and rig. As such, unsuccessful manual disconnection only results in the Automatic EDS being activated. However, in case both manual and automatic activation of EDS fails, this will cause damage to the wellhead, subsea equipment (e.g., BOP) and potentially equipment, structures and personnel located in the Moon Pool area.		

Location and external environment			
Location of event	The well is located on the Norwegian Continental Shelf.		
External environmental conditions	The water depth at the selected well is 294 meters. A previous DP study and evaluation performed for this unit assumes calm weather and water for drive-off. It is assumed that no vessels are nearby (i.e., no collision hazard)	In Norway, shallow water is defined as 320 meters or less	
System and task context			
Operational mode	Normal open reservoir drilling. EDS 2 mode is assumed	EDS 2 is the casing shear mode	
Safety system/barriers	In the event of a DP incident, the unit can conduct an EDS in which the LMRP separates from the BOP. If tubular are inside the BOP, they are sheared during the EDS. If the EDS is successful, the well will be shut in and the vessel will drift away without causing permanent damage to the wellhead. Automatic EDS is enabled. When the system is in AUTO mode, the EDS will be activated when the Unit crosses the red position limit or the red position and angle limit is achieved. The DPO can still activate the EDS buttons manually. As described in the DP Manual, the DPO is the primary barrier and the automatic EDS is considered an additional barrier. EDS 2 takes 30 seconds from activation (either manually or automatic) to completion of the sequence. The unit utilizes a maximum of 6 thrusters during calm weather conditions, as assumed in the Drive-off evaluation study. The DP Manual	A panel with three push buttons is located in the MCR to enable / disable an EDS manually. • Lamp test button • Enable button: Will enable the EDS button • EDS button: Will initiate an EDS. In order for this button to work, the Enable button has to be held down (ON) when the EDS button is pushed. The DPO has to hold the button down until the button is lit, which indicates that the EDS has been initiated. Auto-EDS will activate when the Unit crosses the red position limit or the red position and angle limit is reached. DPO can still activate the EDS buttons manually. The Acoustic BOP control systems can be operated from one of the three following surface command stations: • Panel on DPOs consoles in MCR • Panel on DPOs console in BCR • Portable acoustic control unit	

	recommends power distribution mode and thruster configuration. DP Alert can be manually or automatically activated – based on deviation from the watch circle / riser angle. It displays the current Automatic Disconnect status (duration) on the driller view. There is an alarm with sound for red limit.		
Personnel roles and responsibilities	DPO1 is on DP duty and DPO2 is on the bridge handling other tasks that are part of the Marine department's responsibility, such as approving work permits.	From the DP Manual: "*When the DPO is on-duty at the DP Desk he shall not stand down until such time as the off-shift operator relieves him. The DPO on the DP desk shall reside at the DP desk and he shall only undertake such communication duties as he can achieve without leaving his position.*"	It is assumed that the engine room operator is always present in the MCR. • ACTION: check this assumption
Timescale			
Duration of scenario	The drive-off is changed into a drift-off by manually stopping the thrusters at after 43 seconds The Emergency Quick Disconnect (EQD) is initiated two seconds later at 45 seconds. The Emergency Disconnect of the drilling riser will take 30 seconds, and the disconnect is to be completed before the riser angle reaches 8 degrees Hence the total time until completed riser disconnect is estimated to be at 75 seconds.	As defined in the timeline analysis, based on input provided by DPOs' during the workshop, the task analysis and documentation available containing relevant information on time parameters (Drive-off evaluation report, DP manual, WSOC).	
(Optional) Deviation Scenario(s)			
Possible deviation scenario(s)	N/A		

1.3.1 Expected Outcomes of the Scenario Description

The expected outcomes from the development of the scenario description are:

- A detailed description of the scenario to be analysed, that is relevant to the risk analysis and that accurately reflects how the scenario is likely to unfold.
- Documentation of the assumptions and boundaries of the scenario and the HRA.
- A list of questions or areas for further investigation during the qualitative data collection step of the HRA.

1.4 Perform an Initial Task Identification

The analyst should now perform an initial task identification using the information from the scenario description. The analyst can use this to organize the information collected to date about the operator tasks and to check whether there are any knowledge gaps in their understanding of how tasks relevant to the scenario are performed, which can be addressed in the qualitative data collection step. A simple Hierarchical Task Analysis (HTA) format is useful for performing the initial task identification, and this also provides a good visual aid for talking through the scenario and discussing the task steps with operators and other subject matter experts (SMEs) during the data collection step. More details on how to develop a HTA are provided in Step 3 (Task Analysis).

The analyst should start by identifying the overall goal of the operator task(s) in the analysis scenario, and then identifying the task steps that are necessary to achieve that goal. As a starting point, the analyst may wish to use a simple cognitive behavioural model to help identify operator actions, as shown in Figure 3.

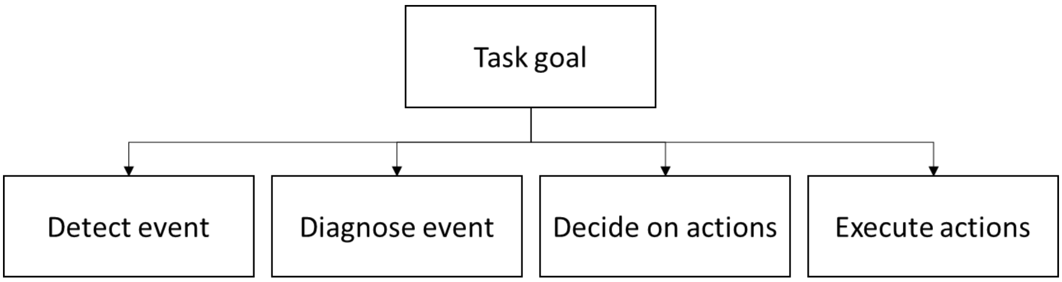


Figure 3: A basic cognitive model for operator tasks

At this stage in the Petro-HRA, the analyst might not have enough information about the tasks to identify subtasks below the first level. If this information is available to the analyst (e.g., from the talk-through of the scenario in the initial meetings, or from the document review), then it should be included in the initial HTA and then checked with operators and other SMEs during the qualitative data collection. Alternatively, the analyst can use the simple model shown in Figure 3 to facilitate a discussion about the tasks and then fill in the missing information as it is received.

The main benefit of using a visual model of the tasks, such as the HTA, is that it allows the analyst to quickly identify where there might be knowledge gaps or uncertainty about how the operator responds in the scenario. It is important that the initial HTA is consistent with the scenario description and that it is as specific and precise as possible. Assumptions and uncertainties should always be checked and verified with SMEs.

Figure 4 shows an example initial HTA, demonstrating how the Detect - Diagnose - Decide - Act/Execute cognitive model can be used as a basis for performing the initial task identification. Since this is the initial HTA, it is unlikely that the analyst has enough information to decompose all of the tasks, but they may be able to decompose some of them (as shown in Figure 4). It may not be possible to decompose the HTA beyond one or two levels, as that level of detail usually comes after the analyst has had discussions and talk-through/walk-through with operators during the qualitative data collection step. The purpose of the initial HTA is to organise the information that the analyst has at this point, in preparation for discussion with operators during Step 2.

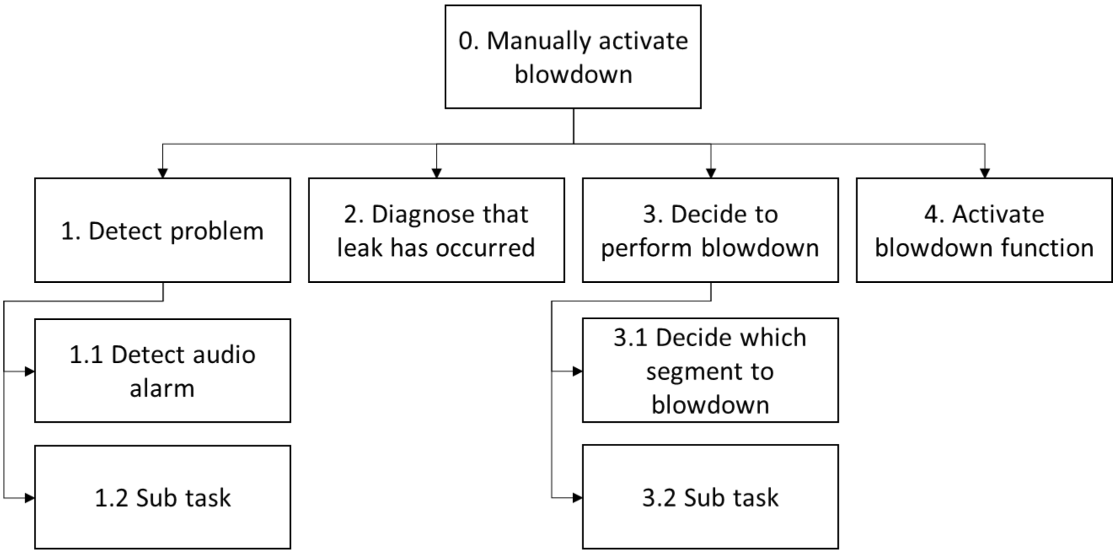


Figure 4: Example of an initial HTA, based on the cognitive model

1.4.1 Expected Outcomes of the Initial Task Identification

The expected outcomes from the initial task identification are:

- A high-level understanding of the operator tasks that are performed during the scenario.
- A visual representation of the tasks that can be used as a basis for discussion during the qualitative data collection step.
- Identification of knowledge gaps about how the operator will respond in the scenario.

2 Step 2: Qualitative Data Collection

The analyst will have already started collecting qualitative data about the scenario from the initial meetings and document review in Step 1 of the method. Step 2 of the HRA involves a more specific and focused data collection to enable a detailed task description, which includes information about factors that may (positively or negatively) affect human performance and the outcome of the scenario. This formal qualitative data collection step is usually performed via a scenario walk- and talk-through, observation of operators working in situ, interviews and discussions with operators and other SMEs and the collection and review of additional documentation. These activities generally take place either during a site visit to the facility, or a workshop with operators, or both.

2.1 Arrange a Site Visit and/or Workshop

A visit to the facility is recommended whenever possible because the analyst will have the advantage of seeing the environment and workspace where the scenario events will take place, as well as seeing how the operators normally work in that environment. The analyst may also identify local constraints or conditions that could have an impact on the HRA but that might not be revealed in off-site discussions or workshops.

Unfortunately, due to the high-hazard nature of petroleum and the often-remote location of petroleum facilities, a site visit might not always be possible. In this case, a workshop may be the most appropriate setting for qualitative data collection, although effort should be made to host the workshop in person. It is not recommended to conduct the workshop by video meeting, as this can negatively impact the quality and quantity of the data collection.

There are benefits with an in-person workshop setting. For example, participants are away from their normal work duties and therefore can dedicate time, energy and focus to the workshop with less chance of external distraction. The workshop setting also enables group discussion, which can reveal similarities or differences between operators or operating crews that might not otherwise be identified through interviews with individuals.

It is recommended that the analyst performs both a site visit and a workshop whenever feasible. It is also recommended that the initial task analysis is updated on an iterative basis throughout the qualitative data collection process, as the analyst collects more information about the scenario and operator tasks/actions.

2.2 Perform a Scenario Talk-/Walk-Through

One of the first activities that the analyst should perform is to talk and/or walk through the scenario with the operator(s). The purpose of the talk-/walk-through is for the analyst to gain a more detailed understanding of:

- The task steps that would be performed by the operator(s), and the sequence of steps.
- The time it will take to perform the task steps.
- The working environment within which the task steps will be performed.
- The systems and interfaces that the operator(s) will use.
- The use of operating manuals, procedures, instructions or other supporting documentation.
- Communication and teamwork throughout the scenario.

Stanton, Salmon, Walker, Baber, & Jenkins, (2005, p. 479) describe a walkthrough analysis: "*A walkthrough involves an operator walking through a scenario, performing (or pretend performing) the action that would occur, explaining the function of each control and display used. The walkthrough is also verbalized, and the analyst(s) can stop the scenario and ask questions at any points about the controls, displays, labels, coding consistency, sightline, decision(s) made, situation awareness, and error occurrence, etc. The walkthrough could be recorded by video or photos and/or notes on the problem(s) with the interface should be taken*."

A talk-through can be performed anywhere, although it is typically held in an "offline" location, such as a meeting room, due to restrictions on access to the scenario location and/or to avoid disturbing or distracting workers in the location. The ideal situation would be to perform the talk-/walk-through at the operator's place of work, to enable the analyst to physically see the workspace, facility items and controls and displays that the operator would use. However, it can also be performed in a workshop setting if the analyst has access to relevant photographs, layout drawings, etc. that the operators can point to as they talk through the scenario.

2.2.1 Resources to Support the Analyst in Performing a Scenario Talk-/Walk-Through

Table 19 in Appendix A.3 contains a list of topics that may be useful for the analyst to review and consider as part of the preparations for a scenario talk-/walk-through. This table should also be consulted prior to performing observations.

2.2.2 Expected Outcomes of the Scenario Talk-/Walk-Through

The expected outcomes of the scenario talk-/walk-through are:

- Detailed information about the operator(s) roles and responsibilities in the scenario, the tasks that they would perform and the time it would take to perform these tasks.
- Detailed information about the relevant equipment, tools, displays and controls that the operator(s) would use during the scenario.
- Detailed information about the local contexts and constraints within which the operators would respond to the scenario and how these might affect human performance.

2.3 Observe Operator Tasks or Training Exercises

Task and training observations can provide valuable qualitative data regarding how operators work, interact with each other and the facility systems around them as well as how they react in abnormal situations. There are two main types of observations the analyst could perform:

- **Observation of normal working conditions in a normal working environment**. This is the most likely type of observation that analysts will perform during a site visit. In this case, the analyst may be allowed to spend some time watching the operators as they perform their usual duties either in the control room or in the field. The analyst can observe how the operators work together, use the tools, equipment, displays and controls that are available to them, make decisions and carry out normal tasks.

- **Observation of training exercises**. It may be possible for the analyst to observe a training exercise. In an ideal situation, the analyst would observe the actual operator response to the exact scenario being analysed, including any difficulties that are encountered and also whether the human intervention succeeds or not. If it is not possible to observe the actual analysis scenario, it can still be useful to observe the operators in other training scenarios because the analyst can still collect information about the general response to an event, how the operating crew works together, how they communicate, how they use procedures or other documentation, how they use controls and interfaces, how they solve problems and how they make decisions.

Of course, observations of normal working conditions or training scenarios are not possible in a workshop setting, and so the analyst must rely on a detailed talk-through of the scenario instead.

2.3.1 Resources to Support the Analyst in Performing Observations

The topics listed in Table 19 of Appendix A.3 are also useful for the analyst to review and consider when preparing to carry out observations.

2.3.2 Expected Outcomes of the Task or Training Observations

The expected outcomes from the task or training observations are:

- A more detailed understanding of how operators work in normal conditions and/or in major accident scenarios and of the time it takes to perform certain actions, for example, to detect and diagnose an alarm, to decide on a course of action, and to execute the action.
- A more detailed understanding of the factors that might affect human performance.

2.4 Conduct Interviews/Workshop Discussions with Operators and SMEs

The analyst should strive to interview a range of different people for a more balanced view, rather than building the analysis on the thoughts and opinions of a single individual. The range of people the analyst may wish to speak with includes:

- Operators
- Shift supervisor or manager
- Training supervisor
- Site QRA analyst/end user
- Operational integrity advisor
- Section leaders (e.g., marine, drilling, etc.)
- Health Safety and Environment (HSE) advisor
- Operations engineer

It is possible to combine the interview or discussion with the scenario talk-/walk-through; this is usually the case for HRA, because it is natural to ask questions and discuss aspects of the scenario and tasks during the talk-/walk-through. This is usually followed up with a more structured interview or discussion afterwards, where the analyst can focus on specific areas of interest or concern.

In addition to collecting information about the scenario and task steps, the analyst should also try to collect qualitative data about both potential human errors that could occur and PSFs that could affect human performance. See Section 6.2 for the full list and definitions of the Petro-HRA PSFs. This information will inform the subsequent human error identification and performance shaping factor evaluation as part of the human error quantification respectively.

2.4.1 Resources to Support the Analyst in Conducting Interviews/Workshop Discussions

Table 20 in Appendix A.4 contains questions, prompts and advice to assist the analyst in collecting information about the tasks, potential human errors and PSFs during interviews and discussions. The analyst should review the table prior to conducting any interviews or workshop discussions to help prepare for the data collection activity and highlight or note any specific questions that they wish to focus on during the interview or discussion. The analyst should refer back to this table as needed to refresh their memory or for prompts about what to ask next. This guide and prompt sheet should be used in conjunction with the scenario description and initial task identification developed in Step 1. The analyst should use relevant photographs, diagrams, documentation and event reports as appropriate to support the conversation. During the interviews/workshop, the analyst should also aim to collect information to support the later human error identification and PSF evaluation.

2.4.2 Expected Outcomes of the Interviews/Workshop Discussions

The expected outcomes of the interviews/workshop discussions are:

- An in-depth understanding of the task, task steps, which operating personnel involved and at what points during the scenario, and the main interfaces used.
- An initial understanding of the potential human errors that could occur during the scenario and the consequences of these errors.
- An initial understanding of the PSFs that may affect human performance during the scenario.

2.5 Conduct an Initial Timeline Analysis

Time is often an important, if not critical, factor in petroleum incidents, with operators having to respond within minutes or even seconds of the initiating event to control and mitigate the effects of the scenario. Therefore, a timeline analysis is often required to understand the relationship between operator actions, the time required to perform the necessary actions and the time available to the operator to perform these actions.

The site visit/workshop provides a good opportunity to develop an initial timeline of the events and operator tasks in the scenario. These facts can be checked and confirmed with operators during the interviews/discussions to ensure that the timeline is credible and reflects their experience or thoughts as to how the scenario might unfold. The analysis maps out the length of major tasks (usually measured in seconds or minutes) and identifies where tasks may be carried out in parallel, or where there may be dependencies between tasks (e.g., one task cannot be started until a previous task has been completed). Figure 5 shows how a timeline diagram can be constructed.

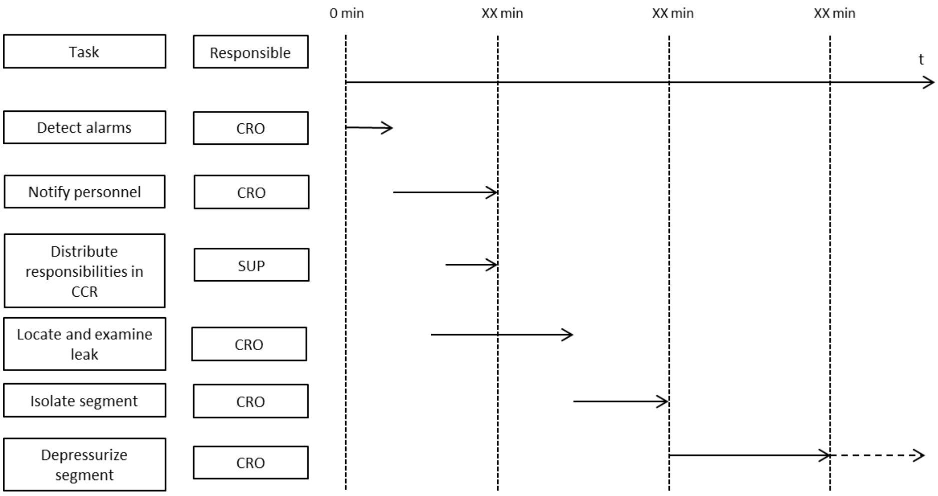


Figure 5: A typical timeline diagram

A simple method for conducting a timeline analysis as part of the HRA workshop is outlined as follows:

1. Task steps on the first level in the task analysis (i.e., level 1.0) are listed vertically together with who is responsible for carrying out each action.

2. A timeline is then drawn horizontally using a scale suitable for the duration of the task and scenario being analysed.

3. Time = 0 is defined by the physical initiation of the event, e.g., when the gas leak, well kick, water ingress or drive-off occurs.

4. The next point in time will be the first cue presented to operators indicating the initiating event. This is typically an alarm, a visual observation of the event, or a physical sensation.

5. The duration of each following task step is then discussed using the details captured in the task analysis:
    a. Assess the time required to complete each individual action (i.e., sub-tasks) under each task step illustrated in the timeline diagram.
    b. Consider impact of task sequences and frequency by reviewing the task analysis plans – e.g., look for repetitive or simultaneous (parallel) actions.
    c. Examine whether the availability of equipment and information influences the duration or time required to perform various actions.
    d. Ask about how long it takes to perform cognitive or interpersonal actions – e.g., individual or collective problem-solving and decision-making.
    e. Include time passed due to expected various disturbances and distractions, such as people entering the control room, phone calls and radio communication, etc.
    f. Ask how the operators are trained to respond to the task (fast or slow).
    g. Check for shortage of time within the entire task – e.g., are there steps within the task which have limited time available, and what is the consequence of failure?

6. Time estimates are recorded in a table containing the following columns (see example Table 2):
    a. Task step: Name of task step with numerical reference to the task analysis.
    b. Duration: The estimated duration of each task step being considered.

c. Comments: Notes about clarifications, uncertainties or additional information.

7. Conclude on when the last action required to successfully accomplish the task is taken. The duration from Time = 0 to Time = task completion equals the estimated time required.

8. For completeness, mark the time when the effect of the task is evident – e.g., when:
   a. The emergency shutdown valves have been closed.
   b. The process segment has been depressurized.
   c. The BOP shuts in the wellbore.
   d. The rig is disconnected from the lower marine riser package.

An excerpt of a timeline analysis table is shown in Table 2. This helps to summarise the information from the timeline analysis diagram, which is used as input to evaluation of the Time PSF in the quantification step. Note that this table shows the timeline information for a single detection task only. The table would usually be expanded to include the relevant information for the subsequent tasks also (i.e., diagnosis, decision, action).

Table 2: Excerpt from a timeline analysis table

Task step	**Duration**	**Comments**
1.0 Detect loss of position	0. Drive-off failure occurs at 0 seconds. 1. After Time=XX seconds, at approximately 50% thruster force, DPO will hear noise generated from abnormal thruster rev. 2. From Time=XX seconds to Time=YY seconds the thrusters will continue to ramp up, and a thruster force yellow warning (visual only) is presented at 60%. The DPO will check the “bars” (i.e., columns) on the HMI indicating thruster force in percentage and tons increasing. 3. At approximately Time=ZZ seconds the DPO will be presented with a red (visual and audible) thruster force alarm at 80%. Simultaneously the rig will be 3 meters off position which initiates a position warning (visual only).	• The cue for DPO to check the (visual) yellow thruster warning is abnormal increase in thruster noise. Another cue is alarms for start-up of standby generators detected by the Engine Room Operator (ERO), who again can notify the DPO. • Parameters stated in 3. are based on the DP drive-off evaluations report using the same scenario assumptions as stated in this report. They were also discussed with the DPOs during the workshop. • The parameters for presentation of the red thruster force alarms (80% thrust) and position warning (3 meters) provided by the DPOs are not the same as what is stated in the WSOC.

2.5.1 Expected Outcomes of the Timeline Analysis

The expected outcomes of the timeline analysis are:

- An estimated of the time required to perform the task.
- Substantiation of the time estimate documented in a timeline diagram and table.

3 Step 3: Task Analysis

A task analysis is a description of the steps that are carried out as part of an activity, and it provides a systematic means of organizing information collected around the tasks. The level of detail in a task analysis can vary considerably, although the general guidance is to tailor the level of the analysis to the requirements at hand. For example, a task analysis to support the design of a new system might have a very detailed analysis of ways to improve the design. In contrast, a task analysis to support HRA will tend to be heavily grounded in identifying sources of human error. The aim of the task analysis is to understand the activities that are being analysed and to translate these details into the level of detail suitable for the HRA and QRA. The task analysis helps to both define the HFE and identify the human errors that may be present in an activity. The task analysis serves as the basis for understanding the impact of the PSFs on the human tasks and thereby the basis for the quantification.

3.1 How to Perform a Task Analysis in Petro-HRA

The information collected by the HRA analyst should be organized into a Hierarchical Task Analysis (HTA) and also a Tabular Task Analysis (TTA) (see Kirwan, 1994). The HTA decomposes tasks hierarchically according to goals at the top level and the task steps at the lower levels that are required to accomplish the goals. HTA provides a graphical overview of the task(s) involved in the analysis scenario, and it can provide a useful job aid to point to during discussions and interviews if, for example, discussing a particular sequence of task steps. The HTA can also help the analyst determine whether there are any significant information gaps, and pinpoint critical tasks or human errors that they may wish to focus on. However, the HTA contains only a limited amount of information about the tasks, and therefore a TTA should also be developed as this allows for richer information capture and better data organization.

3.1.1 When to Perform the Task Analysis

In a Petro-HRA, an initial task identification is typically performed during the scenario definition phase, and an initial HTA is developed as described in 1.4. The analyst will collect additional task information during Steps 1 and 2 of the Petro-HRA, and this information is used to update the initial HTA. The HTA can be considered complete when all information necessary to catalogue the tasks is sufficiently captured and incorporated. Generally, it can take two or three iterations of the task analysis, including feedback from the SMEs before the task analysis is finalized. The TTA is a central placeholder for collected data, and provides the background for the analyses and documentation, and thus is updated throughout the entire Petro-HRA process.

3.1.2 Hierarchical Task Analysis (HTA)

HTA decomposes a given human-performed activity into goals, tasks, and task steps. The goal (i.e., main task) represented at the top level, and the subgoals (i.e., task steps) are represented at the next subordinate level. The task steps, in turn, may be decomposed into more detailed human actions (i.e., sub-steps) represented as nested boxes below each task step. Figure 6 shows an example of an HTA in graphical format (from Øie et al., 2014).

More information on how to conduct HTA can be found in any of the various summary articles by Annett published in the early 2000s (2000, 2003a, 2003b).

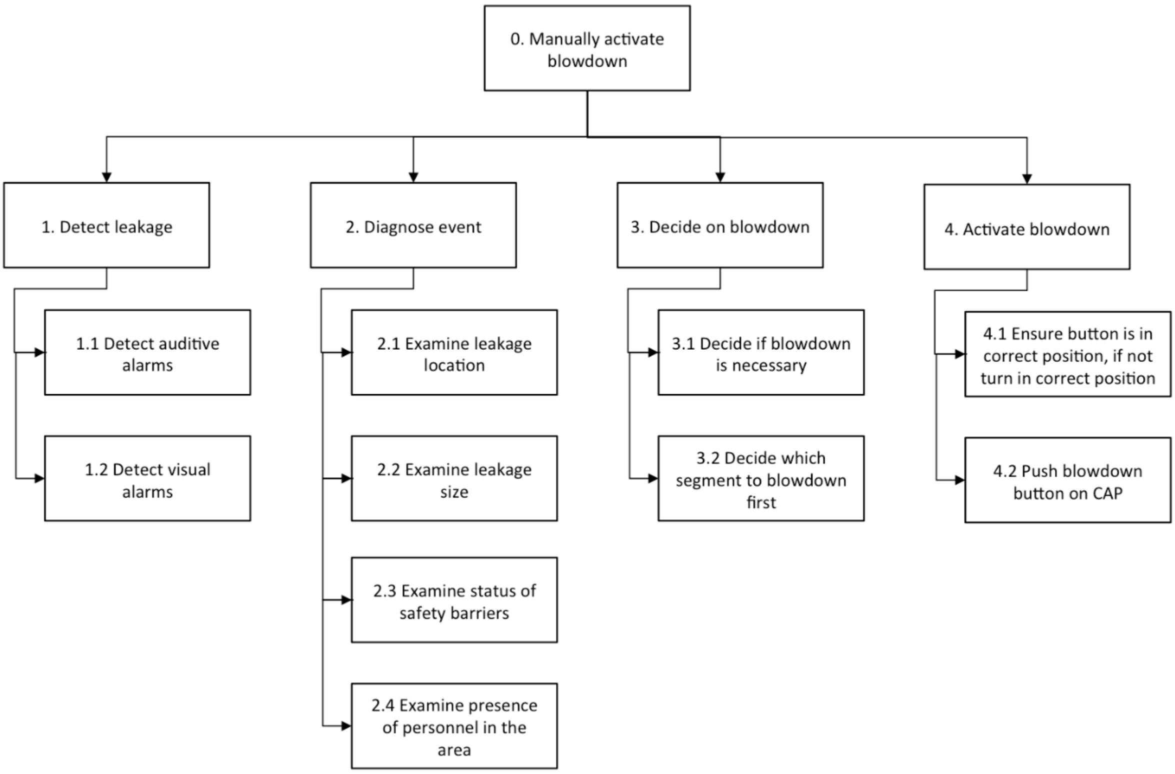


Figure 6: Example of an HTA in graphical format

The following steps describe how to develop an HTA:

1. **Collect data to support and document the task decomposition**. The analyst should work closely with operators and SMEs and make use of available documentation to ensure that the HTA accurately and completely represents the tasks at hand. Key assumptions made by the analyst that would be helpful to understand the analysis or later replicate it should be included in descriptions of the task.

2. **Determine the overall goal**. This may correspond with the HFE as defined in the scenario analysis (Step 1). This goal should be defined broadly but also specific enough to constrain the analysis to the topic at hand. The goal is typically defined in terms of maintaining a safe system state or bringing about a safe system state following an upset. The goal is framed in terms of system function, while tasks often correspond to subsystems or components that must be used by the operator. Refer back to the guidance on initial task identification in 1.4.

3. **Determine task and task steps**. The goal (i.e., main task) should be decomposed into the task steps necessary to complete that goal. In turn, the task steps should be decomposed into more detailed sub-steps (i.e., human actions) necessary to complete the task. This may refer to both physical and cognitive actions as well as individual or interpersonal decisions. The steps capture the actions or decisions that must be taken and the information that must be gathered to support these actions or decisions. As a rule, the analyst should aim to have no less than four, and no more than ten task steps, describing the overall goal. To identify the main task steps, the analyst should consider how the operator is likely to react in terms of (i) detecting the problem (e.g., from an alarm cue), (ii) diagnosing the event, (iii) deciding on a course of action and (iv) implementing that action. These four steps resemble the cognitive model in Figure 3.

4. **Determine the stopping point of the task decomposition**. Align the level of task decomposition to the purpose of the analysis. If the sub-step description is not informative to achieving the goal, it is probably at a finer granularity than is necessary for the analysis. Kirwan and Ainsworth (1992) provide a good discussion of stopping rules in their chapter on HTA as highlighted here:

    a. Iterate the task breakdown with SMEs until the detail is accurate and sufficient. It may be beneficiary to make a different granularity of the task analysis at the various stages of the HRA process.

    b. The initial task identification should be done before the qualitative data collection to provide a simple overview of the tasks of interest for the HRA and to aid data collection activities such as scenario talk-through. The analyst may not want to decompose all of the top-level task steps at this point, and may wish to focus instead on steps that have been identified as critical to the overall analysis. For example, task steps that are particularly complex or that may have a significant impact on the overall successful outcome of the task, or that may adversely affect a safety barrier if performed incorrectly.

    c. For human error identification (HEI), decompose tasks according to the level that HEI is possible.

    d. To meet the PSF assessment needs in the quantification another level of detail may be needed. For quantification, the task context is used to evaluate the PSFs for that particular HFE or task. One must here assure that the task analysis is on a level of detail such that the descriptions of the context for the task capture the main impact of the PSFs on the task. For example, if a difficult scenario is under analysis, the tasks must be described on a level of detail so that it is possible to understand and capture the complexity PSF related to the right context for the task. If it is a time-constrained task, one must be able to evaluate the time it will take for the operator to complete the task, understand the situation and execute the task. For this, a detailed scenario walk-through or talk-through is instrumental to expand the task analysis to its needed level of detail.

5. **Screen tasks for the most significant operations**. Determine that the consequence of a task step can cause the overall task goal to fail – otherwise the task step should not be considered further in the analysis. Just as it is important to document all task steps that are modelled in the HTA, it is important to document task steps that are not analysed any further. These may be retained in the outline or graphical HTA but should be denoted (e.g., greyed out) as items that are not elaborated in the analysis. The analysis should include assumptions as to why particular task steps are not included.

In a Petro-HRA, the HTA needs to be decomposed to the level where the analyst can look concretely at opportunities for error. For HRA-specific purposes (in contrast to human factors work focused on the design of new systems), an analyst would not necessarily need to look at means to remedy these potential failures, although the analyst should identify opportunities for recovery from any potential failures in the data collection.

3.1.3 Tabular Task Analysis (TTA)

The HTA should be extended into a tabular form to allow for the inclusion of more information than can be contained within the diagrammatic HTA. Although the TTA is more complex to develop than the HTA, it is more useful as a working document to allow the analyst to arrange more information in a logical and structured manner.

The analyst must decide what data is needed for inclusion in the TTA, informed by the scenario definition and qualitative data collection steps. As a simple example, if there is a particular concern regarding a control room operator's ability to diagnose the post-initiator event from the HMI in the control room, then the TTA should be focused towards collecting information relevant to the HMI. In this case, tasks carried out in the field (i.e., outside the control room) may not be considered so important to the analysis and do not need to be represented in any great detail in the TTA. Alternatively, if there is some concern regarding the field operator's ability to locate and close a particular valve, then the TTA should focus on collecting information about the work environment, etc. in the field. In this case, detailed analysis of the control room HMI might not be relevant. The analyst should use their judgement (based on the earlier data collection) to determine the appropriate focus for the TTA.

Proposed categories for the initial TTA are listed below. These represent a good starting point for a generic TTA, but these should be adapted to fit the specific task and operational environment for the scenario being analysed.

- **Task (step) number**. The number of the task step as per the HTA. Using the same numbering system will allow for cross-reference between the two task analyses.
- **Task step description**. Brief description of what the operator does to perform this task step.
- **Cue**. A brief description of the cue for the operator to carry out this task step. For example, this may be an alarm, a step in another operating procedure or instruction, or an indication on an instrument panel.
- **Feedback**. A brief description of the feedback that the operator receives to know that the task step has been correctly performed. For example, a red indicator light changes to green.
- **HMI, displays and controls**. A list of the displays and/or controls used to perform the task. If there are known issues with these, the issues should be noted in the TTA (e.g., in the Notes column).
- **Responsible**. Responsible operator or role.
- **Assumptions**. Any assumptions for the task, specific assumptions about the roles involved, etc.
- **Notes**. Additional notes.
- **Procedure/Document reference**. Document number and procedural step number, if these are available.

An example of an initial TTA layout is shown in Table 3. Additional categories for the TTA are provided in 4.1. These categories are related to the HEI and assessment step (Step 4). It can be useful to include these categories in the initial TTA as well, as they can act as prompts to gather relevant information during the formal data collection activities. An example of an expanded TTA with additional columns for HEI and PSF assessment is shown in Table 4.

Table 3: Excerpt from an initial TTA showing typical column headings

Step No.	Description	Procedure / Document Ref.	Cue / Feedback	HMI / Display / Control	Person Responsible	Assumptions / Uncertainties	Notes / Comments
0	**Manually activate blowdown**						
Plan 0	*Do 1 to 4 in order*						
1	Detect leakage						
Plan 1	*DO 1.1. and 1.2 in any order*						
1.1	Detect audible alarms		Audible alarm in control room	Main control display	Control room operator	Will both the audible and visual alarm be activated at the same time?	Check this during the workshop
1.2	Detect visual alarms		Alarm tile illumination (orange) on screen	Main control display	Control room operator		
2	Diagnose event						
Goal 2	*Do 2.1 to 2.4 in any order*						
2.1	Examine leakage location	AR-1234 Alarm Response procedure					
2.2	Examine leakage size						
2.3	Examine status of safety barriers					How does the operator check this?	Ask during the workshop
2.4	Examine presence of personnel in the area			CCTV camera display			
…	…						

Table 4: Expanded TTA showing additional HEI & PSF column headings

Step No.	Description	Procedure / Document Ref.	Cue / Feedback	HMI / Display / Control	Person Responsible	Potential Error	Likely consequences	Recovery opportunities	Further Analysis?	Event Tree Reference	Performance Shaping Factors	Assumptions / Uncertainties	Notes / Comments
0	**Manually activate blowdown**												
Plan 0	*Do 1 to 4 in order*												
1	Detect leakage												
Plan 1	*DO 1.1. and 1.2 in any order*												
1.1	Detect audible alarms		Audible alarm in control room	Main control display	Control room operator	Failure to detect audible alarm	Delayed response to leakage	Visual alarm (Step 1.2)	Y			Assume that if, e.g., is mistakenly silenced without being acknowledged, it will re-activate until it is acknowledged	
1.2	Detect visual alarms		Alarm tile illumination (orange) on screen	Main control display	Control room operator	Failure to detect visual alarm	Delayed response to leakage	Audible alarm (Step 1.1)	Y				
2	Diagnose event												
Goal 2	*Do 2.1 to 2.4 in any order*												
2.1	Examine leakage location	AR-1234 Alarm Response procedure				Fail to check leak location Misdiagnose leak location	Operator may not initiate the correct response (e.g. may not activate blowdown)	No recovery opportunity identified	Y				
2.2	Examine leakage size					Fail to check leak size Miscalculate leak size	Operator may not initiate the correct response (e.g. may not activate blowdown)	No recovery opportunity identified	Y				
2.3	Examine status of safety barriers												
2.4	Examine presence of personnel in the area			CCTV camera display									
...	...												

It is likely that the analyst will only be able to populate part of the TTA prior to the formal data collection activities. However, the TTA can help to guide the data collection activities in terms of highlighting where the focus of the data collection should be. Therefore, it is worth spending some time up front preparing the TTA to maximise the effectiveness of the formal data collection. It may not be possible to populate the remainder of the TTA as data collection activities are carried out; it may not be feasible or practical to bring a computer or large amount of paper when for example, observing tasks in the field. Therefore, the analyst should review the TTA before each data collection activity and make a note of the information they hope to obtain during that activity. Then, return to the TTA as soon as possible afterwards and populate the relevant columns. The TTA can then be updated and serve as a focal point of storing data for all the steps following, for the HEI, the human error modelling (HEM) and the quantification.

3.1.4 Expected Outcomes of the Task Analysis

The expected outcomes from the task analysis are:

- A detailed understanding of the operator tasks performed during the scenario.
- A visual representation of the tasks in an HTA used as a basis for the HEM.
- A detailed representation of the tasks in a TTA that serve as the basis for the succeeding HEI and for the quantification, by an initial evaluation of PSFs for tasks:
    - Can a PSF be considered a performance driver for the entire task? E.g., “Do they train systematically on this task?”
    - Can a PSF be considered a performance driver for any detailed task step? E.g., “Are there any specific parts of the task for which complexity is in particular a performance driver?”

The TTA will be expanded in Step 4, linking each task to potential errors and PSFs. It should be updated throughout the analysis and serve as an overview of the scenario and the analysis.

4 Step 4: Human Error Identification

The objectives of the human error identification (HEI) step are to: identify potential errors related to actions or task steps in the scenario; identify and describe the likely consequences of each error; identify recovery opportunities; and identify and describe performance shaping factors (PSFs) that may have an impact on error probability. HEI should be carried out in conjunction with (or following) the task analysis. A complete task analysis is required for HEI to be possible.

4.1 How to Perform Human Error Identification

The error taxonomy from the Systematic Human Error Reduction and Prediction Approach (SHERPA; Embrey, 1986) is recommended for HEI, although other error taxonomies may also be used. The original taxonomy (Table 21 of Appendix A.5) has been extended for the Petro-HRA method to include decision errors, as described in Table 22 of Appendix A.5. This taxonomy allows a structured evaluation of error modes, consequences, recovery opportunities and PSFs, as described in the following steps:

1. **Review task steps against the error taxonomy**. At each task step and sub-step, consider the error taxonomy (see Table 21 and Table 22 of Appendix A.6) and identify potential errors. For example, Step 2.2 in Figure 6 is “Examine leakage size”. According to the SHERPA taxonomy, a potential error could be a failure to perform the check (i.e., “C1 – check omitted”) or a misdiagnosis of the leakage size (i.e., “R2 – wrong information obtained”). Errors should be reviewed with a Subject Matter Expert (SME) to ensure that only credible error modes are included in the analysis.

2. **Identify and describe likely error consequences**. The consequence of an error has implications for its criticality and must therefore also be identified and described. It is important to be specific about the consequences of the identified errors as this information will contribute to the later screening which will determine which errors should be considered for further analysis and error reduction. To define the error consequences, the analyst should consider both the immediate and long-term (or delayed) effects of the error. For example: Does the consequence have an effect on subsequent task steps, i.e., could it introduce errors of omission or commission in later task steps? Does the consequence have an effect on how the incident escalates, i.e., could it have an effect on the safety barriers or on the hazard? The following categories may be used as prompts to help with identification and description of consequences:

    a. *Direct consequence*. A consequence of an error which can directly cause the human failure event (HFE) to occur.
    b. *Indirect consequence*. A consequence of an error which can indirectly cause the HFE, e.g., in combination with other subsequent errors.
    c. *No consequence*. A consequence of an error with no effect on the HFE. These errors are typically screened out of the analysis at this point as it is not necessary to analyse them any further.

3. **Evaluate recovery opportunities**. If possible, determine the recovery potential of the identified error. Recovery opportunities may present themselves immediately (e.g., if the operator is unable to continue with the next task step because of an error in the previous task step), or at a later point in the scenario (e.g., if there is a peer check or verification of a performed task). Alternatively, there might not be any opportunity to recover from the error. The following categories may be used as prompts to help with identification and description of recoveries:

a. *High recovery potential*. The operator will immediately identify that they have done something wrong through a subsequent task step, check or system intervention.
b. *Medium recovery potential*. The operator will identify and can recover the error later in the task via e.g., a peer check.
c. *Low/No recovery potential*. There is little chance of recovery from this error as there is no subsequent cue for the operator to check, and no system interventions (e.g., interlocks) to prevent further incorrect actions.

4. **Determine criticality**. Identify human errors which can cause the task to fail (based on the direct or indirect consequences identified in Step 2) and for which there is medium or low/no recovery potential. Make note of which should be included for further analysis, e.g., more in-depth PSF evaluations.

5. **Identify PSFs**. For each task and error, identify and describe the PSFs that may influence performance, positively or negatively. It is important throughout the HEI to consider the effects of the different PSFs by asking questions such as "Is time a factor for the error potential on this task?" or "Could the quality of procedures affect the potential error for this task?" Task steps with mostly positive PSFs should normally be screened out from the analysis. The PSFs will be evaluated in greater detail as part of the quantification in Step 6 (Human Error Quantification). See also Step 5 (Human Error Modelling) for a discussion on how the impact of the various tasks should be taken into account in calculating the HEP for the HFE.

Make a note of any assumptions or uncertainties about the errors, consequences, recovery opportunities or PSFs, and flag these for confirmation with an SME such as an operator or QRA analyst. The TTA can be expanded to include the information collected in the above steps. An example of an expanded TTA is shown in Table 4 and the method for expanding the TTA is described in 4.3.

The analyst should revisit the error identification several times throughout the remainder of the analysis as new information (e.g., from confirmation of assumptions) is received, to check that the identified errors are still credible and that the associated information is still correct.

4.2 Cognitive Dependency and Human Error

When human actions are involved, there is another error inducing phenomenon present, called cognitive dependency. If an operator makes an error on one task, she/he is more likely to make an error on a subsequent similar or related task or action. Swain and Guttmann (1983, p. 2-6) define this as: "*Dependence between two tasks refers to the situation in which the probability of failure on one task is influenced by whether a success or failure occurred on the other task. The dependence may exist between two tasks performed by one person, or between the tasks performed by different persons*."

Cognitive dependency is considered in HRA when the first task step fails; the idea being that if an operator fails to perform the first task step, they are more likely to fail to perform the second task step also. The Petro-HRA approach is taken from SPAR-H (Gertman et al., 2005, pp. 29-31 and p. A-7), which is inherited from Technique for Human Error-Rate Prediction (THERP; Swain & Guttmann, 1983, p. 2-6 and pp. 10-1 – 10-38), and is shown in Figure 7.

Petro-HRA models dependency based on four factors:

- Do the HFEs involve the same or a different crew?
- Do the HFEs occur close in time or not?
- Do the HFEs involve the same or a different location?

- Do the HFEs rely on the same information or additional information (to help diagnose the event)?

During the HEI step, the analyst should consider whether cognitive dependency could be present, which may increase the likelihood of errors occurring on subsequent task steps. This should be noted in the TTA. See Section 5.2.3 for further information about how to model dependency.

Part IV. DEPENDENCY

For all tasks, except the first task in the sequence, use the table and formulae below to calculate the Task Failure Probability With Formal Dependence ($P_{w/d}$).

If there is a reason why failure on previous tasks should not be considered, such as it is impossible to take the current action unless the previous action has been properly performed, explain here: ______________________

Dependency Condition Table

Condition Number	Crew (same or different)	Time (close in time or not close in time)	Location (same or different)	Cues (additional or no additional)	Dependency	Number of Human Action Failures Rule ☐ - Not Applicable. Why?______________
1	s	c	s	na	complete	When considering recovery in a series e.g., 2nd, 3rd, or 4th checker If this error is the **3rd error in the sequence**, then the dependency is at least **moderate**. If this error is the **4th error in the sequence**, then the dependency is at least **high.**
2				a	complete	
3			d	na	high	
4				a	high	
5		nc	s	na	high	
6				a	moderate	
7			d	na	moderate	
8				a	low	
9	d	c	s	na	moderate	
10				a	moderate	
11			d	na	moderate	
12				a	moderate	
13		nc	s	na	low	
14				a	low	
15			d	na	low	
16				a	low	
17					zero	

Using $P_{w/od}$ = Probability of Task Failure Without Formal Dependence (calculated in Part III):

For Complete Dependence the probability of failure is 1.
For High Dependence the probability of failure is $(1+ P_{w/od})/2$
For Moderate Dependence the probability of failure is $(1+6 \times P_{w/od})/7$
For Low Dependence the probability of failure is $(1+19 \times P_{w/od})/20$
For Zero Dependence the probability of failure is $P_{w/od}$

Calculate $P_{w/d}$ using the appropriate values:

$P_{w/d}$ = (1 + (_______ * _______))/ _______ = ☐

Figure 7: The SPAR-H Dependency Condition Table and calculation formula

4.3 Expanding the TTA to Include HEI Information

The TTA can be expanded to document the results from the HEI; this approach is recommended to collate relevant task information and for easier review and screening of errors for the subsequent modelling, quantification and human error reduction steps. Proposed additional columns for the TTA are listed below and shown in the TTA in Table 4.

- **Potential error**. Describe the potential error(s) that could occur for the task step or sub step, noting that there may be more than one type of error that could occur. For clarity, it is recommended that the actual error is described, rather than the error taxonomy mode, i.e., “operator misdiagnoses leakage size” rather than “wrong information obtained”.

- **Likely consequences**. Describe the likely consequences of the potential error, considering both immediate and long-term/delayed consequences.

- **Recovery opportunity**. If there is an opportunity to recover from the potential error, this should be noted here. For example, if there is a checking step later in the process, note the step number.

- **Further analysis (Y/N)**. Some basic screening of the errors can be performed at this point to determine which errors should be taken forward for analysis, modelling and quantification. To screen the errors, the analyst should ask: "Is the error (and its consequence) relevant and does it fall within the scope of the analysis?" If so, this error should be investigated in more detail. If not (e.g., if the error could result in a minor delay but time is not an issue for this scenario), then there is no need to assess it further. If the error is screened out at this time, it is important to note the justification for this (in the Comments column), for transparency and so that it can be reviewed later if necessary. Errors which have a potential impact on the task outcome, and for which there is no, or weak recovery, should be considered as part of further analysis

- **Event tree reference.** This column is used to cross reference to the Operator Action Event Tree (OAET) model in Step 5.

- **Performance Shaping Factors (PSF)**. The factors that are likely to affect operator performance, either positively or negatively. See Step 6 for a list and description of the Petro-HRA PSFs.

Any assumptions or uncertainties made about the potential errors, consequences or recoveries should be added to the Assumptions column of the TTA, to be checked at a later point. Additionally, any other information (such as noting that a particular error has been screened out of the analysis) should be documented in the Comments column for transparency and traceability.

4.3.1 Expected Outcomes of the Human Error Identification

The expected outcomes from the HEI are:

- A set of potential errors for inclusion in the human error model (Step 5), representing the most credible errors that could result in failure of the scenario. These are the same errors that the PSF analysis and human error reduction analysis will be based on.
- A detailed understanding of the potential errors, likely consequences and recovery opportunities for the tasks that are performed during the scenario.
- A detailed representation of the errors and tasks in a TTA that links the tasks, errors, consequences and recoveries.
- A detailed representation of the tasks and errors in a TTA that serves as the basis for the succeeding quantification, by a further evaluation of PSFs, e.g.:
    - Can a PSF be considered a performance driver for this error for the task? E.g., "Is time a factor for the potential error identified?"

5 Step 5: Human Error Modelling

Human activities of interest to HRA do not generally occur in isolation but rather in interaction with technical/hardware systems. This section focuses on modelling the tasks in such a way that the links between the errors, task steps, PSFs and the HFE that interfaces to the QRA are clarified. This enables an overview of the task and a means for quantifying failure and success of the Human Failure Event (HFE). A discussion on general modelling issues of human actions may also help risk analysts who are responsible for the QRA modelling. Human error modelling (HEM) enables the risk analyst to identify which of the human actions and/or HFEs contribute the most to the overall risk, and how these different failures interact.

There are two approaches that are relatively standard in risk analysis modelling: Event Tree Analysis (ETA) and Fault Tree Analysis (FTA). There are many sources available on how to perform ETA and FTA (e.g., Kirwan, 1994) and a detailed description is beyond the scope of this guideline. Petro-HRA recommends using event trees for HEM. Event trees are suitable for representing sequential actions that are triggered by an initiating event. Fault trees may also be used for pre-initiating analyses; the analyst is recommended to look up FTA method descriptions for additional guidance.

A clear definition of what constitutes operator failure ensures that only relevant failure events are included in the model. As discussed earlier, what constitutes success and failure in the scenario under analysis is crucial as, first, it determines which failure events are represented in the HRA model. A clear failure or success criteria determines how far into the event sequence the HRA team should perform the analysis. Second, it determines the timeframe to consider in the HRA. The time it takes for an operator to complete the tasks required to activate the safety system/barrier is a function of the scope of the analysis. As such, understanding success and failure criteria for the scenario under analysis is important as it directly influences the events represented in the failure model and thereby the HEP. It is therefore suggested to keep an open dialogue between the HRA team and the QRA team throughout the analysis to ensure the criteria for the failure models stay aligned. It is equally important to understand and define the success and failure for each event modelled. For example, what is meant by a phrase like “delayed detection”? The timing aspect needs to be incorporated in each event definition. This will also influence the evaluation of the time for succeeding events.

5.1 How to Perform Human Error Modelling

The objective of the HEM is to model the task steps or failure events in such a way that, when these are quantified according to Step 6, the model logic can be used to calculate the HEP for the HFE that enters the QRA. Additionally, the HEM should aim to clarify the links between the task step or failure event that is chosen for quantification in Step 6, the errors identified in Step 4 (HEI), and the PSFs that contribute to those errors. These relations are then used qualitatively when each individual task is evaluated and quantified as described in Step 6. Choosing which task step/failure event to quantify in Step 6 is done here in the modelling phase.

HEM is normally performed after human error identification (HEI) and before quantification. The HRA analyst should be in continuous discussion with the QRA team to ensure that the models being developed by the HRA and QRA teams are compatible. The HEM comprises five steps, as described in the following subsections.

5.1.1 Build an Event Tree for the Operator Actions

If a HFE model has not been provided by the risk analysis, then an operator action event tree (OAET) can be developed based on the task analysis. The OAET applies event tree logic and includes the sequence of task steps (i.e., actions) required to successfully accomplish the task goal. Figure 8 shows a simple OAET developed for the blowdown scenario that was earlier referred to in Figure 6. The event tree in Figure 8 shows the actions from the first level of the task analysis in Figure 6.

An important part of the modelling is to choose which task steps or failure events will be quantified in Step 6. In Petro-HRA, each failure event modelled in the event tree should be quantified. In the example in Figure 8, this means that each of the actions “Detect leakage”, “Diagnose event”, etc. will be quantified in the next step. The event tree can be made more detailed, including sub-task steps, but it should be noted that this can make the model overly complex and also create difficulties for the analyst during the quantification step, such as increasing the risk of “double counting” PSFs. See 6.3 for more information about this issue.

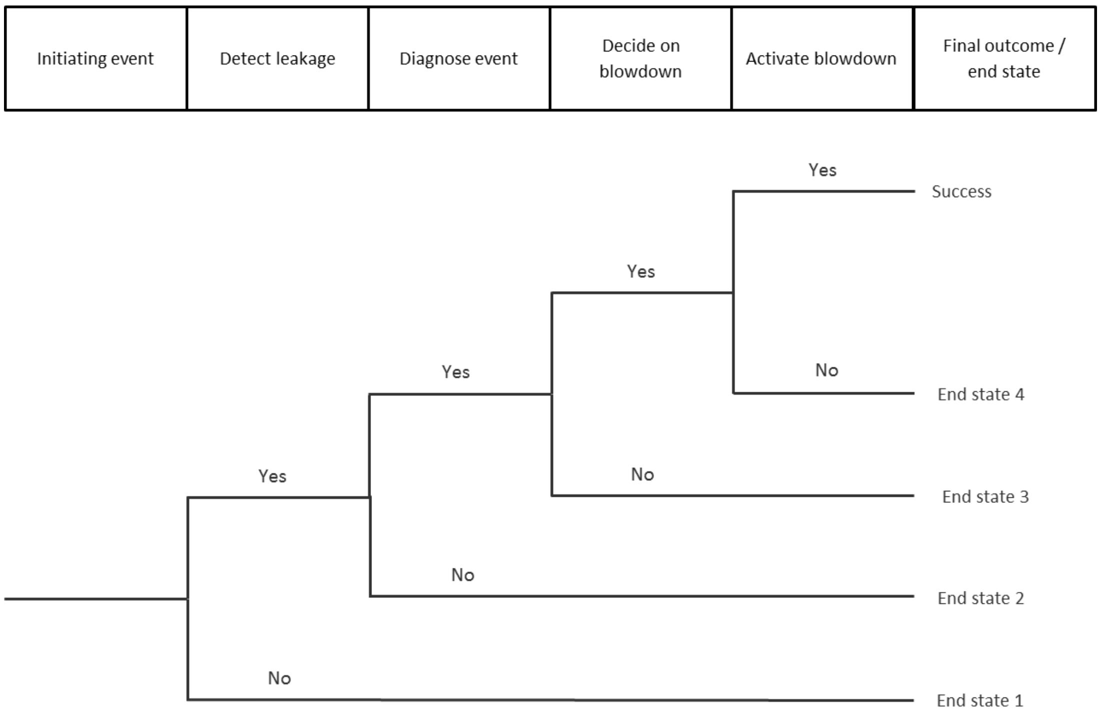


Figure 8: Example of an operator action event tree (OAET)

If the model contains many technical/hardware failures mixed with human actions, this modelling might be done in the QRA itself. One should seek to work with the QRA analysts in order to synchronize the OAET with the QRA model. If the HFE at the QRA level contains a large number of actions, it is recommended to develop a separate OAET for each HFE, to determine the HEP for the individual HFEs. These can be combined in a higher-level event tree at the QRA level.

5.1.2 Evaluate Errors that Contribute to Failure of the Chosen Task

Potential errors and likely consequences were identified in the previous step, Human Error Identification (HEI). However, before continuing to the quantification step, the analyst must identify which errors are most likely to impact the task in the event tree. Some identified errors may have no effect, or a negligible effect on the overall HFE, and so these can be screened out so that the quantification can focus on those errors that are more critical.

The extended TTA that was developed in Step 4 can be used for this screening process, as demonstrated in the excerpt shown in Figure 9 (see the column labelled “Further Analysis?”).

Step No.	Description	Potential Error	Likely consequences	Recovery opportunities	Further Analysis?	Event Tree Reference	Performance Shaping Factors	Assumptions / Uncertainties	Notes / Comments
0	**Manually activate blowdown**								
Plan 0	*Do 1 to 4 in order*								
1	Detect leakage								
Plan 1	*DO 1.1. and 1.2 in any order*								
1.1	Detect audible alarms	Failure to detect audible alarm	Delayed response to leakage	Visual alarm (Step 1.2)	Y			Assume that if, e.g., is mistakenly silenced without being acknowledged, it will re-activate until it is acknowledged	
1.2	Detect visual alarms	Failure to detect visual alarm	Delayed response to leakage	Audible alarm (Step 1.1)	Y				
2	Diagnose event								
Goal 2	*Do 2.1 to 2.4 in any order*								
2.1	Examine leakage location	Fail to check leak location Misdiagnose leak location	Operator may not initiate the correct response (e.g. may not activate blowdown)	No recovery opportunity identified	Y				
2.2	Examine leakage size	Fail to check leak size Miscalculate leak size	Operator may not initiate the correct response (e.g. may not activate blowdown)	No recovery opportunity identified	Y				

Figure 9: Excerpt from TTA showing error screening

Human error screening is done to identify those errors which dominate the HFE, as these are the errors which will be taken further for quantification. The following steps describe how to identify the dominating errors:

- Review each task step/sub-step in the TTA resulting from the HEI, looking specifically at the consequences and recovery opportunities for each human error identified. Use the column called "Further analysis" and flag those errors you think are relevant.
- For each error consider the following questions:
  - "Does the consequence of error have an effect on the event chosen for quantification?"
  - "Can the error be easily recovered?"
- Errors that have no effect on the chosen event and/or have very good recovery potential can be screened out (place an "N" in the further analysis column) and will not be included in the further analysis. An error that can lead to the event and/or has little chance of recovery must be flagged for inclusion in the analysis (place a "Y" placed in the further analysis column).

5.1.3 Develop an OAET Table to Explain the Event Tree and Link the Analyses

Next, the analyst should create an operator action event tree (OAET) table to show the link between the events, the failure description of the event, the selected potential errors, the HEP and the end state. The OAET table is necessary not only to explain the event tree, but also as a means of demonstrating the link between the task analysis, human error identification and human error quantification. It is an important summary tool for communicating the results of the analysis to the QRA team and end users at site.

Table 5 shows an excerpt from an OAET table. The "Event Description" relates to the top events described in the event tree (Figure 8). The potential errors correspond with those identified during Step 4 (HEI) that were documented in the extended TTA (Table 4). Note that the human error probability (HEP) column is empty at this time, as the errors will not be quantified until Step 6, after which time the OAET table should be updated.

Table 5: Excerpt from an OAET table

Event ID	Event Description	HFE Details	HEP	Potential Errors (from HEI)	PSFs	Final outcome / End state
0	Hydrocarbon leak	Initiating event	N/A	N/A	N/A	N/A
1	Detect leakage (TTA Ref. Task Step 1.0)	Event 1: Failure to detect alarms		• Operator fails to detect audible alarm (task 1.1) • Operator fails to detect visual alarm (task 1.2)	HMI Experience / Training	Response to the leak is omitted or delayed which creates a risk of the leak size increasing rapidly to the point where blowdown is no longer possible.
2	Diagnose leakage (TTA Ref. Task Step 2.0)	Event 2: Failure to diagnose leakage		• Operator fails to diagnose/misdiagnoses the leak location (task 2.1) • Operator fails to diagnose/misdiagnoses the leak size (task 2.2)	HMI Experience / Training Procedures	Operator initiates blowdown in the wrong location, or does not initiate blowdown in the correct sequence due to misunderstanding of the leak size.
…	…					

5.1.4 Identify PSFs That Contribute to Failure or Success

For each error selected for impact in Table 5, identify the PSFs that impact the error and thereby the task. Note that at this point in time the analyst will begin to judge the impact of PSFs on the event and task step, and there might be a considerable overlap with the quantification judgements done in Step 6 (Section 6). The procedure in Step 6 is for evaluating the impact of PSFs on one task step. It is important to evaluate to which extent the PSF for one error or subtask influences the task step that is going to be quantified. For example, if two PSFs are noted for "potential error 1.2.1" for task 1.2, the important qualitative evaluation to be done by the analyst is to evaluate to which extent these PSFs impact task 1, "detect leakage", given that task step 1.2 is only a part of task step 1. For example, if the PSF HMI is evaluated to be poor since the visual alarm is hidden or difficult to read, this must be evaluated together with the audio alarms for task 1.1 since both impact the "detect leakage" task step.

An alternative way of modelling this example would be to include the sub-steps 1.1 and 1.2 in the event tree and quantify each of them using the PSFs impacting each of them directly. A set of advice might be given for this:

- If the task steps or actions are very interlinked, it might be difficult to model them separately. E.g., if in a detection task there are three different detection means (sub-tasks) and these sub-tasks normally happen in parallel and the operator should act if 2 out of 3 indicators (3 different sub-tasks) are on, it may be difficult to model this. In this case, a qualitative judgement for the upper task is better.
- If the PSFs for sub-steps are the same or strongly linked, it may also be an advantage to do a qualitative judgement of these PSFs for a higher-level task.

All the information gained on PSFs in this step is immediately afterwards used in the PSF evaluation in the quantification in Step 6, for the task chosen. The PSF evaluation is in practice to select PSF levels for each event in the event tree. A PSF worksheet is filled out including clear substantiation about why the PSF can be considered a performance driver for the task step and event. See Section 6 for more on this topic.

The PSF substantiation developed for quantifying the OAET should be done in combination with extracting the most critical human errors for each event in the OAET. The negative outcome (i.e., failure pathway) for each event is represented by one or several human errors identified in the HEI. The most critical human error(s) should be identified, along with how these can result in the HFE (task failure and end event in the OAET), and how the PSF can cause the error to occur. In this way one identifies the "main driver" for the error and failure of the overall event or scenario. This is important for subsequent human error reduction.

Care should be made to avoid double counting PSFs, not selecting the same PSF for several or all of the actions in the OAET. For example, it may seem logical to select Threat Stress or Experience/training for the entire task. However, the assessment should target those parts of the task in which Experience/training is most important and which actions are most prone to negative influence by Threat Stress. In other words, one should evaluate each PSF thoroughly for each event/task chosen to be quantified. E.g., available time must be evaluated carefully, not just stating that it is "busy" for all the sequential task steps. One should rather evaluate the time used in a normal sequence of task steps and consider at which point the crew is really getting problems with the time. In many cases one may apply shortage of time for the last event in the sequence, meaning the last action required to successfully accomplish the task goal.

5.1.5 Quantify the HFE That Enters the QRA

When HEPs have been calculated for all events in the OAET by the method described in Step 6, the failure probabilities for each end state can be calculated according to the event tree logic. E.g., in Figure 10, if the HEP for "Detect leakage" is 0.01, this is the value for the failure branch (labelled "No" in Figure 10), which corresponds to the value for End state 1. The value for success (labelled "Yes" in Figure 10) of the same branch is 1-0.01=0.99. If the HEP for "Diagnose event" is 0.01, the value for End state 2 is 0.99*0.01=0.0099, which approximates to 0.01. In this way the values of all the end states are calculated.

In the same example, the HFE that enters the QRA is "manually activate blowdown". The HEP for this is found by adding all the HEPs for the end states leading to failure. In the model in Figure 10, this HEP is found by adding all the End states 1 to 4, since all these are failures to activate blowdown.

5.2 Considerations for Event Tree Modelling

5.2.1 Modelling Events that Combine Human and Technical/Hardware Failures

The human failure event (HFE), and its position in the event tree structure, is typically defined by the QRA, in combination with other technical/hardware or human failures. However, this may be modified or extended during HRA modelling to enable better definition of the HRA scenario. Modifications or extensions to the event tree structure should be done in discussion and collaboration with the QRA team.
Figure 10 shows a simplified example of an event tree, demonstrating how human actions can be combined with hardware failure logic in the QRA.

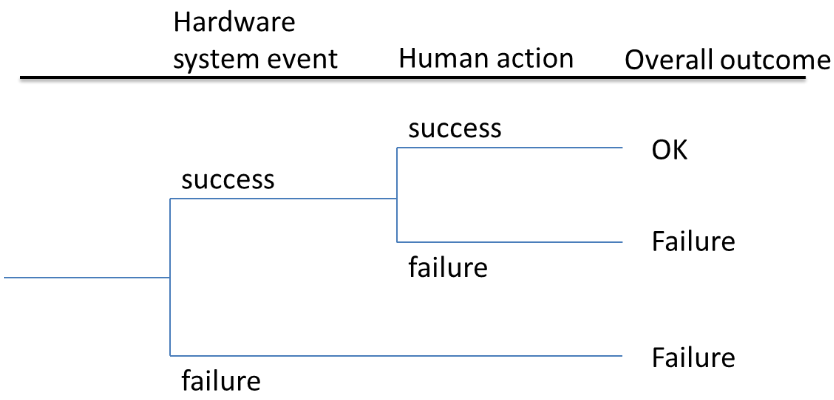


Figure 10: Simplified event tree example

Both the human action and the hardware system event must be successful to produce a successful outcome. In other words, a failure in either the hardware system or the human action will cause the overall event to fail. A typical example of this is a blowdown system that has to be activated manually.

5.2.2 Modelling Recovery in Operator Action Event Trees

In Figure 10, if the hardware system event fails, then the overall scenario will fail, i.e., there is no opportunity for recovery. Equally, if the human action fails, there is no recovery option. This means that overall success in this scenario is dependent on success of the human action in addition to the success of the hardware system.

Most, if not all, facilities today are constructed with several safety barriers in place, which may include physical engineering controls, technical controls, administrative practices, operational practices, etc. The principle is that if one barrier fails, the next barrier can still control the situation. For example, if the automatic blowdown system fails to initiate, blowdown can be manually initiated by the operator instead. In other words, the human action acts as a recovery barrier to failure of the hardware system. Figure 11 illustrates how to graphically demonstrate recovery in an event tree.

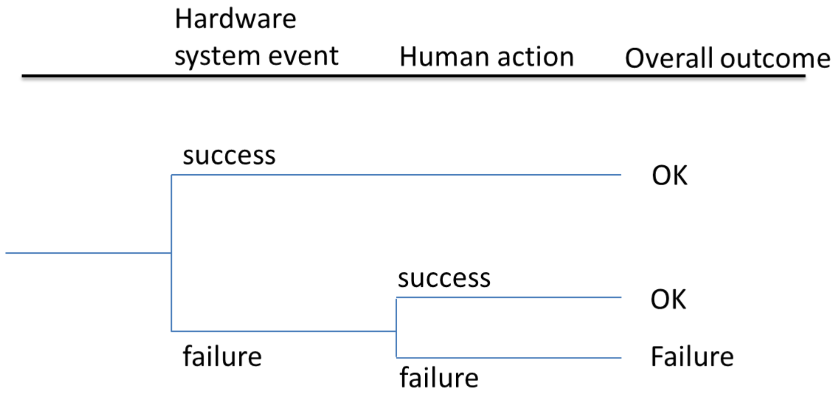


Figure 11: Human action as a recovery barrier for hardware system failure

Recovery represents a failure path that has been restored to a success path. In an event tree, branching points have two outcomes, an upper success path and a lower failure path. Recovery marks the point where there is a return to the success path. Recovery should not be assumed, and it rarely occurs spontaneously. However, many systems and processes feature second checks to help recover from a failure path. For example, when a hardware safety system fails to activate, an alarm may sound to draw the operator's attention to a fault. Alternatively, a procedure may ask the operator to verify the proper functioning of the system, or a second operator may verify the actions of the first operator, as shown in Figure 12.

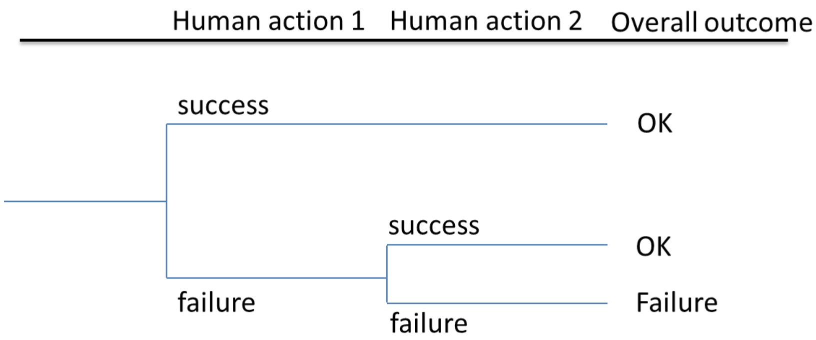


Figure 12: A human action recovers a human failure

All of these are mechanisms toward recovery. The analyst should carefully look for such recovery mechanisms and credit them in the HRA and QRA where appropriate. Refer to 4.1 for guidance on how to identify recovery opportunities in the HEI step. One way of deciding which errors to model from the HEI is to apply a criterion like "potentially significant consequence" x "degree of recovery".

Sometimes such events should be modelled explicitly in the OAET, especially if a detailed OAET is used for human error modelling. However, sometimes recovery options must be qualitatively judged within an event or HFE, if the whole event is evaluated at once. In this case the recovery option must be evaluated when evaluating the PSFs for the task, i.e., by considering how robust the task itself is.

If the recovery events are modelled in the QRA, this gives the HRA a rather simple way to analyse these events. The recovery concept is then modelled in the QRA event tree itself, and one may analyse each event individually without thinking of the mathematics of the relation. This will be taken care of by the event tree logics in the QRA. This will be the case when the events are clearly separated in time and are built into the design of the system, e.g., as consecutive safeguards. One example is when a pump breaks, an alarm is issued, and the operator has a responsibility to act upon this signal.

Another type of recovery is when a person recovers her/his own action, such as a slip, almost immediately. The opportunity for this must be identified when evaluating each task and should be included in the evaluation of the PSFs for that HFE. For example, the operator may receive feedback from the HMI such as “Do you really want to close valve C?” or may immediately notice a process alarm that is set off due to an action and still have the possibility to undo or redo this action.

Yet another type of recovery can be a peer check or an independent verification by a team member. In this case it may be natural to model this in an event or fault tree, since it is a barrier feature built into the system or organisation of the tasks and will probably be separated in time. This type of recovery is normally not modelled in the QRA, so it is up to the HRA analyst to model this type of robustness in the system.

The SHERPA error taxonomy (see 4.1) considers various cues and subsequent tasks as recovery opportunities. These should be evaluated when considering recovery. There is also a thorough discussion on this topic of modelling recoveries at the event level in PRA/QRA versus modelling these phenomena by evaluating PSFs, in the SPAR-H documentation (Gertman et al., 2005, p. 42).

5.2.3 Modelling Dependency

In QRA and HRA there are two kinds of dependencies that can occur. In the barrier and event modelling performed by the QRA, discussed in 5.2.2, a systems analyst could say that in order to secure a successful outcome, the system depends on two consecutive successes of events or barriers, as illustrated in Figure 13:

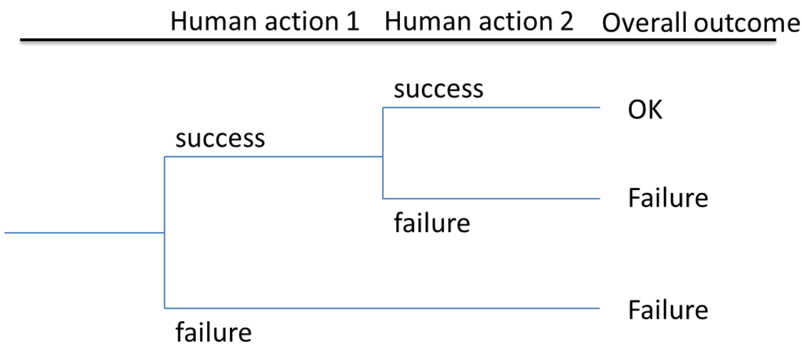


Figure 13: Two consecutive human actions; both are required to succeed

Modelling of these kinds of dependencies should be considered together with recovery options as described previously. In Figure 13 there is no recovery option after a failure of the first human action, since the second human action is irrelevant in this case. The event tree model assumes a successful outcome of the first task, i.e., the operator will only ever perform “Human action 2” if “Human action 1” has been successfully completed. Therefore, there is no need to consider dependency between the two task steps. It is only if the first task step results in failure that the analyst must consider dependency between any subsequent actions (e.g., recovery actions).

In case of Figure 12, however, a recovery action is modelled in which the second human action can, if successful, recover the failure of the first human action so the outcome is success. In this case, one should consider the cognitive dependency between these two tasks: is it so that if the first action is failed, the probability of failing the second action also increases due to the cognitive dependency? Refer back to 4.2 for guidance on how to evaluate cognitive dependency.

When considering dependencies, one must also be aware of the nature of the HFEs or tasks modelled. Are the tasks modelled in the event tree actually consecutive/subsequent tasks, or does the model represent the same task in two different ways, perhaps with more time and/or additional cues. In this case, cognitive dependency as discussed here and in 4.2 may not actually be present. For more on this topic, see the discussion in Forester et al., (2014, pp. 90-91).

5.3 Expected Outcomes of the Human Error Modelling

The expected outcomes of the HEM are:

- A representation of the basic events in an event tree that serves as the basis for the subsequent quantification;
    - The choice of which task step/event to quantify in Step 6 is made here: each event modelled in the OAET must be quantified.
    - As a general rule, the first level tasks in the task analysis should be modelled. These are normally the main task steps, in level "1" of the HTA.
    - When the elected actions or task steps are subsequently quantified in Step 6, this model will provide the logic for quantifying the combination of the tasks into the overall HEP for the HFE, which is then entered into the QRA.
- A detailed understanding of how the errors, task failures and PSFs impact the tasks/events and the HFEs in the scenario, as well as the consequences of the errors.
    - This includes an understanding of how recovery opportunities for errors can modify the impact on events, or whether a potential error can be screened out.
- A table explaining the event tree, as shown in Table 5, that together with the extended TTA explains the links between the errors, tasks, end states and PSFs.

An example of how to develop an OAET table is provided as part of the case study in Part 2 of this guideline (The Petro-HRA Guideline, 2022, Rev.1, Vol. 2).

6 Step 6: Human Error Quantification

This section describes how a human error probability (HEP) of one failure event or task step is quantified based on a nominal value and a set of performance shaping factors (PSFs).

6.1 How to Perform Human Error Quantification

The tabular task analysis (TTA) and knowledge from the human error identification (HEI) and the human error modelling (HEM) steps should now contain the necessary information for quantification. The results from these earlier steps should be used as inputs to the quantification, especially the analyst's knowledge of the scenario and the context for the task to be quantified.

The main elements for quantification of one task or failure event are the nominal human error probability (NHEP) and the nine Petro-HRA PSFs. From these, the HEP is calculated. Cognitive dependency (see Section 4.2) should also be considered here to determine if it has an impact on the HEP.

When having calculated a HEP for an event, it is good practice to do a sanity check, or reasonableness check. This check could be seen as a separate step, but in Petro-HRA it is considered a sub-step of the quantification. In addition, one should include a normal quality assurance of the documentation; see Part 3 of the Petro-HRA guideline (The Petro-HRA Guideline, 2022, Rev.1, Vol. 2) for more information on how to do this.

6.1.1 Decide the Appropriate Task Level for Quantification

Before applying the nominal HEP and evaluating the PSFs, the analyst must decide at which task level the quantification should be performed. This is a common challenge for HRA, as there are advantages and disadvantages to quantification at different levels of task decomposition. Experience suggests that if quantification is performed at the highest task level (i.e., for the overall scenario) then very few negative PSFs can be selected before the overall HEP for the event becomes unrealistically high. However, if quantification is performed at a lower task level (e.g., a HEP is calculated for each task step in the behavioural model (detection, diagnosis, decision, action)), then the final HEP may be overly optimistic and/or the risk of double counting is increased because certain PSFs (such as time pressure, threat stress and experience/training) can be difficult to assess for individual task steps.

As noted in Taylor, Øie & Gould (2020), another challenge related to identifying an appropriate decomposition level for quantification occurs when a PSF influences only some part of a task, but not others. For example, there may exist no procedure to support the operator in diagnosing a problem, but once the operator has decided on an action, there may be a very good procedure available to support implementation of that action. In this case, "good procedures" cannot be credited for the whole task (detection, diagnosis, decision & action), but only the action part of the task.

The Petro-HRA method recommends task decomposition to at least one or two levels below the task goal, as well as the use of operator action event trees (OAET) to model events and calculate HEPs. This approach enables the analyst to account for the influence of different PSFs at different times during the scenario and recommends documentation of where and how the PSFs influence different task steps. The analyst is cautioned to be aware of the risk of double-counting, although experience from the application of the Petro-HRA method indicates that the PSFs naturally lend themselves to different parts of the task (depending on the cognitive action—detection, diagnosis, decision or action—being performed), which helps to avoid this problem (Taylor, Øie & Gould, 2020).

6.1.2 Apply the Nominal Human Error Probability

The nominal human error probability (NHEP) is a value of human error probability that is supposed to contain all small influences that can contribute to task step errors that are not covered by the PSFs. The NHEP in Petro-HRA is 0.01 for all tasks, which means that a task step fails 1 out of 100 times. This NHEP is the same as for the diagnosis NHEP in SPAR-H (Gertman et al., 2005; Whaley, Kelly, Boring, & Galyean, 2011) and this value was chosen because most task steps in an accident scenario involve a large cognitive component (Forester et al., 2014).

The SPAR-H method distinguishes between two task types – diagnosis tasks, and action tasks – and provides a separate NHEP for each. The separation between diagnosis (cognition) and action task steps in SPAR-H is not included in the Petro-HRA method because we consider that all task steps include a combination of diagnosis and action. In SPAR-H, action tasks include automatic information processing where a lower degree of cognitive activity is needed. Task steps become automatic if they are highly trained for. If this is the case, in the Petro-HRA method the moderate level positive effect on performance in the Training/Experience PSF should be used. If this level is used the HEP becomes 0.001 which is the same as for an action nominal task step in SPAR-H.

Many of the HFEs represented in a petroleum QRA are likely to be of a cognitive, decision-making nature; refer to the basic cognitive model shown in Figure 3. Note that the “execute” (or action) task step on this level in the scenario still contains cognitive components and therefore can be evaluated using the same nominal value.

It is important to note that if a PSF is considered “nominal”, that does not mean that the PSF is not present or does not have an effect on human performance for that task step. Rather, it means that the PSF is present, but it does not have a particularly positive or negative effect on human performance, i.e., it has a nominal effect.

6.1.3 Evaluate the Performance Shaping Factors

“*A PSF is an aspect of the human’s individual characteristics, environment, organization, or task that specifically decrements or improves human performance, thus respectively increasing or decreasing the likelihood of human error*” (Boring & Blackman, 2007, p. 177).

Nine performance shaping factors (PSFs) that have been shown in general psychological literature and in other HRA methods to have a substantial effect on human performance when performing control room task steps (or steps similar to control room steps) are included in Petro-HRA. These are:

1. Time
2. Threat Stress
3. Task Complexity
4. Experience/Training
5. Procedures
6. Human-Machine Interface (HMI)
7. Attitudes to Safety, Work and Management Support
8. Teamwork
9. Physical Working Environment.

The PSF definitions and multipliers have been modified from those used in the SPAR-H method. Detailed arguments for the modifications are presented in the background information in Part 3 of this guideline (The Petro-HRA Guideline, 2022, Rev.1, Vol. 2).

6.1.4 Rate the PSF Levels and Multipliers

Each PSF has several levels with corresponding multipliers. The multipliers for each PSF are explained in 6.2. A human error probability (HEP) is calculated from the nominal values, the chosen levels, and corresponding multipliers. The HEP gives information about how likely the operator is to fail on the action or task step that is analysed.

The multipliers used in the Petro-HRA method are shown in Table 6. It should be noted that not all PSFs include all of the multipliers shown in this table. More information is provided in 6.2.

Table 6: Description of levels and multipliers in Petro-HRA

Levels	Multipliers	Meaning of multipliers
Extremely high negative effect on performance	HEP=1	Failure is certain. All operators will fail on the task step. It is sufficient that one PSF has this value for the HEP of the task step to be 1. (Note that HEP=1 is therefore not a multiplier but is the actual HEP for the failure event if this PSF level is selected).
Very high negative effect on performance	50	50 out of 100 will fail. There will be many failures if all crews/operators were to experience this task step.
High negative effect on performance	20-25	20-25 out of 100 will fail on this task step. A quarter of the operators will fail on the task step.
Moderate negative effect on performance	10-15	10-15 out of 100 will fail on the task step. There will be occasional failures on the task step.
Low negative effect on performance	5	5 out of 100 will fail on the task step. There will be few occasional failures on the task step.
Very low negative effect on performance	2	2 out of 100 will fail on the task step. There will be very few occasional failures on the task step.
Nominal effect on performance	1	1 out of 100 will fail. The level of difficulty is quite low and one would see very few failures if all the crews/operators were to experience this task step.
Low positive effect on performance	0.5	5 out of 1000 will fail. Failure on the task step is very unlikely.
Moderate positive effect on performance	0.1	1 out of 1000 will fail. It is almost inconceivable that any crew/operator would fail in performing the task step.

In the description of the PSFs and its multipliers (6.2), the method contains as clear definitions as possible, giving advice to the analyst on how to choose the correct PSF multiplier for the task step under analysis. The purpose of this is to reduce the variability between analysts. However, the analysis should not be carried out as a purely "mechanistic" exercise. It is the responsibility of the analyst to evaluate whether the PSF has an effect on the performance of the operator(s) for the given task step. This must be documented and substantiated for each PSF. The purpose of this is to improve the transparency and reproducibility of the results.

When evaluating the appropriate multiplier level for a PSF, the analyst must evaluate all the levels and choose the one that fits best. One must especially consider the level above and the level below, and the border conditions between these multiplier levels, including considering the uncertainties in the evaluations. The choice must then be substantiated and documented.

6.1.5 Calculate the Human Error Probability for the Task

The human error probability (HEP) is calculated by multiplying the NHEP with the multiplier for each PSF, i.e.,

> *HEP = 0.01(Nominal HEP) x multiplier(Time) x multiplier(Threat Stress) x multiplier(Task Complexity) x multiplier(Experience/Training) x multiplier(Procedures) x multiplier(HMI) x multiplier(Attitudes to Safety, Work and Management Support) x multiplier(Teamwork) x multiplier(Physical working environment)*

If all PSF ratings are nominal, then the task human error probability will be calculated as 0.01. If one (or more) PSF multipliers is rated as 1, then the HEP for the whole task step shall be set to 1 regardless of any other multipliers for the other PSFs. In this case, the PSF for which the multiplier is rated as 1 is considered a dominant performance driver and the task step is certain to fail because of this PSF.

For each task step quantified, the analyst must adjust the value if a very low HEP or a HEP higher than 1 is found. If a failure probability (HEP) higher than 1 is found, the failure probability shall be set to 1. The lowest HEP that should be given on a single event or task step is 0.00001 or 10^{-5} since any HEP lower than this will have minimal impact on the overall OAET. This is the same advice as given in Whaley et al. (2011).

Refer to Section 4.2 to evaluate whether cognitive dependency should be applied to the calculated HEP.

It is important to understand the effect on the final HEP when deciding between the different multipliers for an individual PSF. For example, when considering the negative effects of task complexity, the difference between “moderate negative” (10) and “very high negative” (50) can have a significant impact on the overall HEP. Without considering any other PSFs, the effect of “moderate negative” task complexity on the nominal HEP is 0.01 x 10 = 0.1; in other words, the operator will fail 1 out of every 10 times that task is performed. The effect of “very high negative” task complexity on the nominal HEP is 0.01 x 50 = 0.5; in other words, the operator will fail 1 out of every 2 times that the task is performed.

This can have a profound impact on the overall HRA and QRA results, and so a reasonableness check (see 6.6) is strongly recommended to ensure that the final HEP results are credible and can be backed up with qualitative justification. If the analyst is unsure about which multiplier to select, then it is better to re-examine the qualitative evidence and (if possible) discuss with an SME to ensure that an appropriate multiplier is selected. If no SME is available, the analyst may try to do the reasonableness check her/himself. The obvious danger of the analyst performing a reasonableness check on their own work is that they might not identify any errors in the analysis or HEP calculation, nor can they confirm that claims and assumptions are correct.

6.2 The Petro-HRA PSF Definitions, Levels and Multipliers

This sub-section presents the PSF definitions, levels and multipliers for the Petro-HRA method, as well as guidance on how to evaluate and obtain data for each of the PSFs.

6.2.1 Time

Definition: The Time PSF considered the influence on human error probability as a result of the difference (i.e., the margin) between available and required time, as shown in Figure 14. **Available time** is defined as the time from the presentation of a cue for response to the time of adverse consequences if no action is taken (i.e., the "point of no return"). **Required time** is defined as the time it takes for operators to successfully perform and complete a task (i.e., to detect, diagnose, decide and act).

The analyst must evaluate if the operator has enough time to successfully carry out the task. If there is not enough time available to complete the task, failure is certain. If there is enough time to complete the task, the analyst should decide if time is limited to such an extent that it is expected to have a negative effect on performance. For example, if there is limited time available the operator(s) may complete the task in time but have failed to perform all the actions correctly due to time pressure[1]. If there is considerable extra time available, this PSF is expected to improve operators' performance.

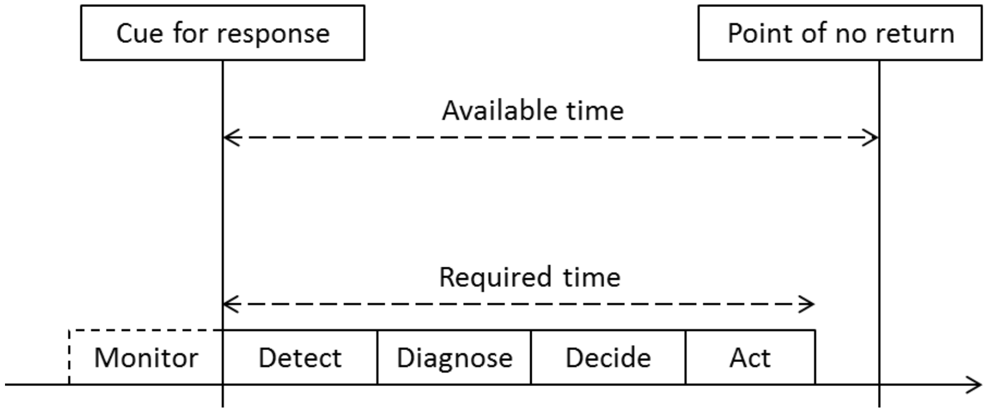


Figure 14: Relationship between available time and required time

Levels and multipliers: The levels and multipliers for the Time PSF are shown in Table 7.

Table 7: Levels and multipliers for the Time PSF

Time		
Multipliers	*Levels*	*Level descriptions*
HEP=1	Extremely high negative effect on performance.	Operator(s) does not have enough time to successfully complete the task.
50	Very high negative effect on performance.	The available time is the minimum time required to perform the task or close to the minimum time to perform the task. In this situation the operator(s) has very high time pressure or they have to speed up very much to do the task in time.

[1] In a Petro-HRA analysis one may treat objective time pressure and subjective time pressure as the same construct, and thereby collect data in "subjective" interviews, etc. However, one should be aware that it is objective time pressure, and whether the operator actually has to speed up to perform the actions in time that is important for the analysis. This might differ from subjective perceptions of time pressure. If the operator experiences subjective time pressure when, objectively, there is no time pressure, this should be considered as a negative influence of Training/Experience, since the operators then do not have a realistic experience of the available time for the task or scenario. In the opposite case, if the operator doesn't feel any time pressure, but time actually is limited, this is also an influence of Training/Experience. However, in this case the Time PSF must also be considered, since there really is objectively limited time. If Training/Experience is adequate the operators should have a realistic picture of the available time and then the subjective experience of available time and the objective available time should be highly correlated.

10	Moderate negative effect on performance.	The operator(s) has limited time to perform the task. However, there is more time available than the minimum time required. In this situation the operator(s) has high time pressure, or they have to speed up much to do the task in time.
1	Nominal effect on performance.	There is enough time to do the task. The operator(s) only has a low degree of time pressure, or they do not need to speed up much to do the task. When comparing the available time to the required time the analyst concludes that time would neither have a negative nor a positive effect on performance.
0.1	Moderate positive effect on performance.	There is extra time to perform the task. In this situation the operator(s) has considerable extra time to perform the task and there is no time pressure or need to speed up to do the task in time.
1	Not applicable.	This PSF is not relevant for this task or scenario.

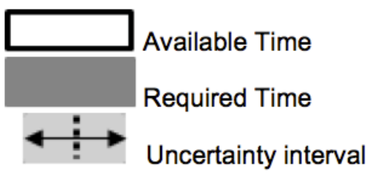
<u>Method for how to analyse Time</u>: In determining the appropriate PSF level the analyst should consider:

- How much time does the operator(s) have to complete the task before it is too late for the operator to affect the outcome of the scenario (i.e., the "point of no return")? This is the available time.
- How much time will the operator(s) need to complete the task actions? This is the required time.

The analyst must then select the multiplier level based on the difference between the available time and the required time to complete the task, i.e., the time margin. The margin between time available and time required can have a potentially large impact on the final results of the HRA and ultimately the QRA. Before being able to select the appropriate Time PSF level it is therefore important that the analyst obtain as accurate measures as possible of the time required and time available for the task in question.

The margin between available time and required time that defines the different levels for Time is illustrated in the following series of diagrams, with explanations of each. It can be difficult to estimate the exact time required for a task or task step. In some cases, e.g., if there is an objective measurement of time required, it could be possible to estimate the time exactly and then an uncertainty interval is not necessary. However, in most cases it is not possible to estimate time required exactly and so to be conservative, some extra time in an uncertainty interval should be added to the estimated required time. Thus, the upper boundary in the interval for required time should include a conservative estimation of time required.

The diagrams for each multiplier level use the following key:



- The black frame represents the available time. Note that in the following figures there are no uncertainties represented for the available time. This might be the case and should be taken into account when necessary.
- The white area within the border of available time (if any) represents the positive time margin between the upper uncertainty boundary and time available.
- The dark grey area represents the minimum time required and lower uncertainty boundary of the time required estimate.

- The light grey area (and double arrow) represents the uncertainty interval of the time required estimate, with time required as the Mean (illustrated with dotted line). Note that this interval may be found by qualitative judgement; it is not necessarily a mathematical representation of uncertainty.

HEP = 1: Extremely high negative effect on performance

- The time available is shorter than time required, even when accounting for uncertainties in the time estimates. The lower uncertainty boundary of time required cannot be argued to be less than the time available.
- Time pressure is extremely high, and it is almost impossible for the operators to complete the task.
- In this case, the overall HEP is set to 1, since the task will always fail if the operator does not have enough time to complete the required steps/actions.

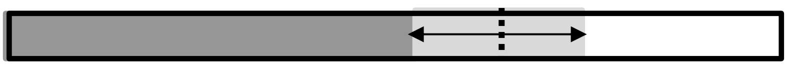
Multiplier = 50: Very high negative effect on performance

- The time available is equal to the time required or very close to the time required. The upper uncertainty boundary of time required can be argued to be equal, but not exceed, the time available.
- The time pressure is high; operators experience that time is one of the most critical factors in handling the event. They must perform actions quickly and at a very high speed throughout the event to fulfil the task in time.

Multiplier = 10: Moderate negative effect on performance

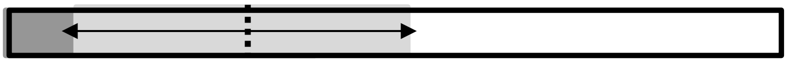
- The time available is greater than the time required, and there is a small but positive time margin beyond the upper uncertainty boundary of the time required.
- However, the time available is so limited compared to the required time that the operator is expected to experience high time pressure. They must perform actions at a high speed throughout the event.

Multiplier = 1: Nominal effect on performance



- The time available is greater than the time required, and there is a positive time margin beyond the upper uncertainty boundary of the time required.
- There is so much time available compared to the required time that the operators are expected to experience only a low degree of time pressure. They can perform most (if not all) actions at a calm and steady pace, with task-oriented pauses in-between. The operators may experience that time is a factor, however, not to the extent that it has a negative influence on task performance.

Multiplier = 0.1: Moderate positive effect on performance



- The time margin between time available and time required is extensive. The upper and lower uncertainty boundaries of time required can be argued to create a positive time margin which is greater than or equal to the time required (i.e., more than 50% of the time margin).
- There is so much extra time that it has a positive influence on performance because the operators experience no time pressure to perform the task. They can perform all actions at their own preferred speed.

Note that the analyst should not interpret the illustrations too literally and must use data-driven judgement on a case-by-case basis to decide on the appropriate level. As with other PSFs it is important that the level selection is accompanied by sufficient substantiation. If the available time is less than 2 minutes the analyst needs accurate time estimates and/or a good substantiation for not selecting extremely or very high negative effect on performance. Unless the task is very simple, and the HMI and training is very good, there is not much room to perform actions reliably in such a short time span.

<u>Guidance on determining the available time and required time</u>: The available time may be challenging to determine as it depends on the facility, the severity of the scenario and the environmental circumstances in which the scenario occurs. Available time should be discussed, clarified and defined in collaboration between the HRA team, QRA team and the client to ensure a common understanding and definition.

Beyond the numeric value of the available time, a common understanding should be established about what it entails. As such, it is helpful to describe in common prose, for example, "*at T = 5 minutes, the semi-submersible drilling unit will have gained such momentum from spurious thruster activation that regardless of the corrective actions of the operator, a collision with the neighbouring facility is unavoidable*". By describing the available time in such a way, the value is clear ("5 minutes") as well as its meaning ("unavoidable collision with neighbouring facility").

It should be noted that the value and definition of the available time is closely linked with the success/ failure definition for the scenario under analysis as discussed previously. That is, a clear and common understanding of what constitutes success and failure for the scenario is required in order to define the available time for the operator to achieve the outcome.

Finding the required time is as much of a challenge, and this should be done by a thorough timeline analysis. An initial timeline analysis should be done as part of the interviews or workshop with operators, as described in 2.5.

<u>Guidance on obtaining data on Time</u>: Information on the minimum required time to do the task should be obtained from interviews/ workshops with operators and from measuring the time the operators use by simulating the performance of the task(s) on the relevant interface. The operators might sometimes be overly optimistic when estimating the time required to perform a task. The analyst should evaluate the realism of the time estimates given by the operators, e.g., by performing a walk-through or talk-through in addition to interviewing operators (refer back to 2.2). The analyst should be especially aware that context (for example communication and distractions) might affect the time required to do the task.

The analyst can collect information about minimum time required by observing simulator training, if the same or similar scenarios are trained. Training scenarios might not be entirely representative of a real-life situation, e.g., the operators might be more prepared and therefore use less time. However, it is still good to do these observations if possible as the analyst can learn a lot about how the crew works together, how they use procedures and HMIs, how they communicate, and how they make decisions.

Accident and incident reports can also provide information about how much time the operators have used to perform a task in similar types of incidents/accidents in the past, although it should be noted that accident reports may not always contain a detailed timeline of the sequence of events.

An important note about integrating the Time PSF into the human error model: The Time PSF is typically used for quantifying the final actions, for which the consequences are directly impacted by the time margin, such as activating a safety system by pushing a control panel button. While most task steps may be prone to human errors causing delays in the execution of the task, the consequence will not necessarily have an effect on the overall outcome of the task until the final actions. Therefore, although available and required time should be considered for each task step and event in the human error model (HEM), to avoid double counting, the error influence should only be credited to final actions with a direct impact on the task outcome.

For example, in a scenario where Time is evaluated as having a moderate negative effect on performance (multiplier = 10), using the basic cognitive model (detect, diagnose, decide, act) the Time PSF would be rated as “nominal” for the detection, diagnosis and decision task steps, and rated as 10 for the final action task step, since this is where the effect of inadequate time will actually be revealed.

6.2.2 Threat Stress

Definition: Threat stress is defined as: “*The anticipation or fear of physical or psychological harm*” (Salas, Driskell, & Hughes, 1996, p. 23). A threat-provoking situation is one in which dangerous and novel environmental events might cause potential pain or discomfort (Salas et al., 1996, p. 23). Examples of situations that might cause threat stress are situations where the operator’s life, or other people’s lives could be in danger. Another example of threat stress might be a threat to self-esteem or professional status if performing a wrong decision or action.

Levels and multipliers: The levels and multipliers for the Threat Stress PSF are shown in Table 8.

Table 8: Levels and multipliers for the Threat Stress PSF

Threat Stress		
Multipliers	*Levels*	*Level descriptions*
25	High negative effect on performance.	The operator(s) experiences very high threat stress. In this situation the operator’s own or other person’s life is in immediate danger.
5	Low negative effect on performance.	The operator(s) experiences moderate threat stress. The operator experiences that there is a threat to their own or others’ personal safety or a very high threat to self-esteem or professional status.
2	Very low negative effect on performance	The operator(s) experiences some threat stress. The operators experience some threat to their self-esteem or professional status.
1	Nominal effect on performance.	Operator(s) does not experience threat stress. Threat stress has not a negative effect on performance.
1	Not applicable.	This PSF is not relevant for this task step or scenario.

Method for how to analyse Threat Stress: In determining the appropriate PSF level the analyst should consider:

- Does threat stress affect the performance of this task step?
- What is the level of threat stress for this task step?

When analysing threat stress an important question is: Is Threat Stress a performance driver? Threat Stress might not be a negative performance driver if, for example, the operators have received adequate Experience/Training on the task(s) and adequate stress exposure training (see for example Johnston & Cannon-Bowers, 1996).

Guidance on obtaining data on Threat Stress: Data on Threat Stress should be found by investigating the consequences of the scenario to find out if the scenario is likely to be experienced as threatening to the operator's life, or other people's lives, or if there are high consequences for the operator's self-esteem if they make an error. Information about Threat Stress should also be obtained during interviews and workshops. Training programs will give information about Experience/Training on the task and stress exposure training.

6.2.3 Task Complexity

Definition: Task Complexity refers to how difficult the task step is to perform in the given context. More complex actions have a higher chance of human error. Task Complexity can be broken down into various complexity factors that alone or together increase the overall complexity of a task step.

Factors that affect Task Complexity include:

- **Goal complexity**: the multitude of goals and/or alternative paths to one or more goals. The complexity of a task will increase with more goals/paths, especially if they are incompatible with each other (e.g., parallel or competing goals and no clear indication of the best path/goal).
- **Size complexity:** the size of the task and the number of information cues. This also includes task scope, which includes the subtasks and whether faults related to this task can affect other tasks. The complexity of a task will increase as the amount and intensity of information an operator must process increases.
- **Step complexity:** the number of mental or physical acts, steps, or actions that are qualitatively different from other steps in the task. Complexity of a task will increase as the number of steps increases, even more so if the steps are continuous or sequential.
- **Connection complexity**: the relationship and dependence of elements of a task (e.g., information cues, subtasks, and other tasks). Task Complexity will increase if the elements are highly connected, and it is not clearly defined how they affect each other.
- **Dynamic complexity**: the unpredictability of the environment where the task is performed. This includes the change, instability, or inconsistency of task elements. Task Complexity will increase as the ambiguity or unpredictability in the environment of the task increases.
- **Structure complexity**: the order and logical structure of the task. This is determined by the number and availability of rules and whether these rules are conflicting. Task Complexity will increase when the rules are many and conflicting or if the structure of the task is illogical.

Levels and multipliers: The levels and multipliers for the Task Complexity PSF are shown in Table 9.

Table 9: Levels and multipliers for the Task Complexity PSF

Task Complexity		
Multipliers	*Levels*	*Level descriptions*
50	Very high negative effect on performance.	The task contains highly complex steps. One or several of the complexity categories are present and influence performance very negatively. For example, several parallel goals are present, the size of the task is huge with many information cues and many steps, it is unclear which task elements to perform, if an order is relevant, if tasks have any effect on the situation, and the task environment changes.
10	Moderate negative effect on performance.	The task is moderately complex. One or several of the complexity categories are present and influence performance negatively.
2	Very low negative effect on performance.	The task is to some degree complex. One or several of the complexity categories are to some degree present and are expected to have a low negative effect on performance.
1	Nominal effect on performance.	The task is not very complex and task complexity does not affect operator performance. Task complexity has neither a negative nor a positive effect on performance.
0.1	Low positive effect on performance.	The task is greatly simplified, and the problem is so obvious that it would be difficult for an operator to misdiagnose it. E.g., detecting a single alarm, or sensory information such as clear visual and auditory cues.
1	Not applicable.	This PSF is not relevant for this task or scenario.

Method for how to analyse Task Complexity: In determining the appropriate PSF level the analyst should:

- Identify which of the Task Complexity factors are present in the task and analyse how they affect performance.
- Assess the severity of the Task Complexity factors that are present. Note that some of the Task Complexity factors have more of an influence on human error than others.
- Set the Task Complexity PSF multiplier level based on the presence and severity of the various Task Complexity factors present in the task. Note that one Task Complexity factor alone can be judged to have a very high or moderate negative effect on performance.

To effectively analyse Task Complexity, the analyst needs to obtain a deep understanding of the task and the scenario in question. It is important to note that, when analyzing complexity, the analyst must consider the total scenario and not only each separate task. It may be the case that the complexity of the task is only evident when considering the whole task, and not the individual task steps. Therefore, when deciding on the multiplier, the analyst must consider how the individual task step is influenced by the complexity of the overall task or scenario.

Guidance on obtaining data on Task Complexity: To analyse Task Complexity all information available on the scenario and task is useful. The analyst should develop a clear description of the scenario that is being analysed. The task analysis is also useful to understand how the task is performed by the operators. Information about Task Complexity should be obtained in interviews, workshops, and talk through/walk through of the task(s) with the operators.

6.2.4 Experience/Training

Definition: Experience is defined as how many times in the past the operator(s) has experienced the task steps or scenario in question. Training is defined as a systematic activity performed to be able to promote the acquisition of knowledge and skills to be prepared for, and to do, the task step or scenario in question (definition based on Salas, Tannenbaum, Kraiger, & Smith-Jentsch, 2012). The outcome of experience and training is the knowledge and skills that are necessary to be prepared for, and to perform, the task steps in the scenario being analysed.

Research (Arthur, Bennett, Stanush, & McNelly, 1998) has shown that 92 percent of training outcomes are lost after one year if the knowledge and skills are not used. The types of training might vary, from simulator training, on-the-job training, classroom training, and mental training (mentally rehearsing the task steps). The analyst should evaluate if the operator has the necessary knowledge and skills to do the task steps in this scenario from either experience or training. The analyst should not only check that the operators have the necessary education and certificate; they should specifically look at the level of experience and training for the task step(s) in the scenario that is analysed.

Levels and multipliers: The levels and multipliers for the Experience/Training PSF are shown in Table 10.

Table 10: Levels and multipliers for the Experience/Training PSF

Experience/Training		
Multipliers	*Levels*	*Level descriptions*
HEP=1	Extremely high negative effect on performance.	There is a strongly learned knowledge or skill (either from experience or training) that is a mismatch with the correct response to this task step in this scenario. An example could be that the operator(s) during experience or training has developed a strong mindset about the development of a scenario and actions that do not fit with the scenario in question and therefore cannot be expected to perform the task correctly.
50	Very high negative effect on performance.	The operator(s) does not have any experience or training and does not at all have the necessary knowledge and skills to be prepared for and to do the task step(s) in this scenario.
15	Moderate negative effect on performance.	The operator(s) has low experience or training and does not have the necessary complete knowledge and experience to be prepared for and to do the task step(s) in this scenario.
5	Low negative effect on performance	The operator(s) has experience or training but this is lacking, and they do not have the complete knowledge and experience to be fully prepared for and to do the task step(s) in this scenario.
1	Nominal effect on performance.	The operator(s) has experience and/or training on the task step(s) in this scenario and has the necessary knowledge and experience to be prepared for and to do the task step(s) in this scenario. Experience/Training does not reduce performance nor to a large degree improve performance.
0.1	Moderate positive effect on performance.	The operator(s) has extensive experience and/or training on this task step and the operator(s) has extensive knowledge and experience to be prepared for and to do the task step(s) in this scenario.
1	Not applicable.	This PSF is not relevant for this task step or scenario.

Method for how to analyse PSF: In determining the appropriate PSF level the analyst should consider:

- Does Experience/Training have an influence on the performance of this task step? Are there some characteristics of this task step that makes Experience/Training on this step/scenario superfluous? If so, the multiplier level "not applicable" should be used. To define which task steps should be trained for, the table on page 12 of DOE Handbook 1078[2] can be used. However, it is a general expectation that there should be training for highly safety-critical tasks and scenarios.
- If Experience/Training has an influence on performance on this task step, the analyst must decide which level of relevant Experience/Training the operator(s) has for the task step in this scenario.

The following may be indications that Experience/Training levels have a very high negative effect on performance:

- If the operators cannot explain the task steps or scenario.
- If different operators have different descriptions of how the scenario develops or the tasks steps involved.
- If the operators do not believe that the scenario could happen.

When the analyst investigates if the operators have the necessary knowledge and skills from experience and training, the analyst should also consider:

- How similar is the experience/training environment to the actual scenario and task step?
- Is the training method adequate?
- Are the trainers qualified?
- Is the outcome of the Experience/Training evaluated? This gives information about how sure one can be that the operators have obtained the necessary knowledge and skills from training.
- How recent/updated is the Experience/Training?
- Is the Experience/Training for the task step(s) and scenario planned, and is a systematic training program developed? Or, is Experience/Training something that is more randomly occurring which makes it difficult to decide if all operators have the necessary knowledge and skills?

Guidance on obtaining data on PSF: To evaluate the adequacy of Experience/Training the analyst should observe training such as simulator training if possible, investigate training programs, interview trainers, and interview operators about their Experience/Training for the scenario or task step(s) as well as their knowledge/skills about the task step(s) and the scenario.

6.2.5 Procedures

Definition: "*A procedure is a written document (including both text and graphic) that represents a series of decisions and action steps to be performed by the operator(s) to accomplish a goal safely and efficiently*" (O'Hara, Higgins, Stubler, & Kramer, 2000, p. 4-1). "*The purpose of a procedure is to guide human actions when performing a task to increase the likelihood that the actions will safely achieve the task's goal*" (O'Hara et al., 2000, p. 4-1).

Procedures are primarily used when performing a task, but they can also be used as a means to be prepared for a task, for example in scenarios with limited time to read the procedures. The operators

[2] This table can be found at: http://energy.gov/sites/prod/files/2013/06/f2/hdbk1078.pdf

may know the procedures so well that the procedures are not a performance driver. The analyst should evaluate whether the procedures are a performance driver or not.

It is increasingly common, especially on newer installations, for operators to use electronic procedures and documentation, rather than (or in addition to) paper copies. The following definitions of levels and multipliers should be relevant for evaluation of electronic procedures as well as paper procedures. If evaluating electronic procedures, the analyst should also take care to evaluate the interface that the procedures are presented on (see 6.2.6, and also refer to the advice on double counting in 6.3).

Levels and multipliers: The levels and multipliers for the Procedures PSF are shown in Table 11.

Table 11: Levels and multipliers for the Procedures PSF

Procedures		
Multipliers	*Levels*	*Level descriptions*
50	Very high negative effect on performance.	No procedures available or the procedures are not used during the scenario or training. This level should also be used if the procedures are strongly misleading in such a way that they are not helpful for the operator(s).
20	High negative effect on performance.	The procedure lacks steps and important information that is needed to do the task or the procedures are briefly used during scenario or training. An example could be that they are briefly looked at in the beginning of the scenario. This level should also be used if the procedures themselves are highly complex or it is very difficult for the operators to navigate between different procedures
5	Low negative effect on performance.	The procedures are complete but there are some problems (formatting, language, structure) with the procedures, or the procedures are not followed in an optimal way. This level should also be used if the procedures are complex (e.g., revealed through interviews) or if there are some problems to navigate between different procedures
1	Nominal effect on performance.	The quality of the procedures is adequate, and they are followed. The quality of procedures does not affect performance either positively or negatively.
0.5	Low positive effect on performance.	Procedures are exceptionally well developed, they are followed, and they enhance performance.
1	Not applicable.	This PSF is not relevant for this task or scenario.

Method for how to analyse Procedures: In determining the appropriate PSF level the analyst should consider:

- Is there a formal written procedure available?
  - If not, should there be? In some cases, there is no procedure available, but this might be seen as normal in the industry and fully accepted for the task. In this case, label "not applicable".
- Will the operator follow the procedures for this task or scenario?
- How is the quality of the procedures?
  - Do the procedures correctly and logically describe every task and task steps?
  - Is the format of the procedure good (text, tables, matrices, etc.)?
  - Is the language easy to understand for the operator?
  - Does the operator know where to find the procedure?
  - Does the operator have to switch between several procedures to do the correct task?
  - Does the procedure only include relevant information (and exclude irrelevant information)?
  - Does the operator know the procedure(s) and the procedure step that should be performed in the scenario?

The analyst should evaluate the procedure for each task step, but also for the entire scenario and the context that the task and scenario occur in. In analysing Procedures this guideline can be used: O'Hara, J.M., et al. (2000). Computer-based procedure systems: technical basis and human factors review guidance. No. J-6012. Upton, NY: Brookhaven National Laboratory.

Guidance on obtaining data on Procedures: To evaluate the quality of the procedures, the analyst should check the procedure(s) used and make an evaluation of the points described previously. Procedures should be compared to the task analysis, which describes how each task step is performed in the scenario, to check that the procedures include the same or similar information.

Information about use of Procedures should be obtained from interviews and workshops with the operators. The analyst should ask the operators about how they would use a specific procedure during the scenario being analysed and the perceived quality of the Procedures. However, the analyst should also perform his/her own evaluation of the quality of Procedures. The analyst could also obtain information about how procedures work and are used by observing simulator training.

6.2.6 Human-Machine Interface

Definition: The Human-Machine Interface (HMI) PSF refers to the quality of equipment, controls, hardware, software, monitor layout, and the physical workstation layout where the operator/crew receives information and carries out tasks. Examples of HMI problems include:

- Difficulties in obtaining relevant information or carrying out tasks through the safety and automation system.
- Layout organization or colours that are not stereotypical.
- Communication difficulties due to communication technology (walkie-talkies, phones, messaging systems).

In systems that use inter-page navigation it should be evaluated if it is likely that this will cause masking of relevant information or difficulties in carrying out a task due to several page shifts.

Levels and multipliers: The levels and multipliers for the HMI PSF are shown in Table 12.

Table 12: Levels and multipliers for the HMI PSF

Human-Machine Interface		
Multipliers	*Levels*	*Level descriptions*
HEP=1	Extremely high negative effect on performance.	A situation where it is not reasonable to assume that the operator/crew will be successful in carrying out the task. An example of this would be a situation where the HMI does not provide the operator/crew with the required information or possibility to perform the task. Alternatively, the information provided is misleading to the extent that the operator will not correctly carry out the task.
50	Very high negative effect on performance.	The HMI causes major problems in either obtaining relevant information or carrying out the task. For example, the HMI is not designed for the task leading to a difficult work-around, some of the relevant information required for a reliable decision is not made available or, the inter-page navigation creates severe difficulties in obtaining the relevant information or carrying out the task.
10	Moderate negative effect on performance.	The HMI causes some problems in either obtaining relevant information or carrying out the task. For example, the HMI does not conform to the stereotypes the operators are used to (e.g., icons, colors, and intuitive placements) or, several page changes in the inter-page navigation increases the difficulty in obtaining the required information or carrying out the task.

1	Nominal effect on performance.	While the HMI is not specifically designed for making the human performance as reliable as possible for this task/tasks of this type, it corresponds to the stereotypes held by the operators. All of the safety critical information is easy available and no HMI related issues are interfering with carrying out the task. HMI does not reduce performance nor to a large degree improve performance.
0.5	Low positive effect on performance.	The HMI is specifically designed to make human performance as reliable as possible in this task/tasks of this type.
1	Not applicable.	This PSF is not relevant for this task or scenario.

Method for how to analyse HMI: The grading of this PSF should be made based on how the HMI works for this specific task/scenario. Inputs/comments on the quality of the HMI in general or aspects of the HMI that are not relevant for this task should not influence the grading of this PSF.

In determining the appropriate PSF level the analyst should evaluate:

- Does the task rely on the HMI? If not, the “Not Applicable” level should be selected.
- If the HMI related issues are influencing task performance the analyst should decide on the levels and multipliers. Issues that result in less efficiency but do not influence reliability should not be taken into consideration when evaluating this PSF.

Guidance on obtaining data on HMI: Walkthrough analysis could be used to evaluate HMI and to show the analyst how a task or scenario is performed on the HMI. The analyst should evaluate the user-friendliness of controls, displays, labels, coding consistency, alarms and sightline during the walkthrough.

6.2.7 Attitudes to Safety, Work and Management Support

Definition: Attitudes to Safety, Work and Management Support consists of two related factors that have been found to predict safety outcomes in studies of safety culture.

Attitudes are defined as the individual's positive or negative evaluation of performing the behaviour (Ajzen, 1985). Attitudes to safety and work conduct contribute to a safety conscious work environment. An example of how Attitudes to Safety and Work Conduct could negatively affect task performance is that other concerns such as production are prioritized higher than safety when it is appropriate to prioritize safety. Another example is that the operator does not perform tasks as described in work descriptions, rules, and regulations, for example not monitoring when they should. Another example of how Attitudes to Safety and Work Conduct could negatively affect safety is that the operators are not mindful of safety. The management of the organization is responsible for developing these attitudes.

Management support means the operators experience elicit support from managers in performing the task(s) in question. An example is that the operators experience support from the management to shut down production when appropriate even if this might have large practical/economic consequences. Also, the operator does not fear any negative consequences of performing an action that they believe is a safety conscious action even if this action is later found to be wrong.

Levels and multipliers: The levels and multipliers for the Attitudes to Safety, Work and Management Support PSF are shown in Table 13 (next page).

Table 13: Levels and multipliers for the Attitudes to Safety, Work and Management Support PSF

Attitudes to Safety, Work and Management Support		
Multipliers	*Levels*	*Level descriptions*
50	Very high negative effect on performance.	In this situation safety is not at all prioritized over other concerns when it is appropriate or there are extremely negative attitudes to work conduct (for example the operators are not monitoring or awake when they should be). There is very low mindfulness about safety. The operators do not experience management support, for example in strong management pressure for production even if safety is clearly in question.
10	Moderate negative effect on performance.	In this situation it is not specified by management that safety should be prioritized when that is appropriate. The operators are uncertain if safety should be prioritized or not, or the operators are uncertain about rules and regulations that are important for performing the task.
1	Nominal effect on performance.	The operators have adequate attitudes to safety and work conduct and there is management support to prioritize safety when that is appropriate. The operator(s) shows mindfulness about safety. Attitudes to safety, work and management support have neither a negative nor a large positive effect on performance.
0.5	Moderate positive effect on performance	The operator(s) has very good attitudes to safety and work conduct and there is explicit management support to prioritize safety when that is appropriate. The operator(s) shows a very high degree of mindfulness about safety.
1	Not applicable.	This PSF is not relevant for this task or scenario.

Method for how to analyse Attitudes to Safety, Work and Management Support: This PSF is more subjective than most of the other PSFs and the analyst should be very careful to present the evidence for the selection of levels and multipliers for this PSF. The data and evidence for the level and multiplier should be clearly described. The levels should not be based on a general feeling. The analyst has to state explicitly why a level is chosen.

Guidance on obtaining data on Attitudes to Safety, Work and Management Support: Information about attitudes to safety, work and management support should be obtained from interviews and workshops.

6.2.8 Teamwork

Definition: "*Team is defined as two or more individuals with specified roles interacting adaptively, interdependently, and dynamically toward a common and valued goal*" (Salas, Sims, & Burke, 2005, p. 562). Teamwork is defined as a set of interrelated thoughts and feelings of team members that are needed for them to function as a team and that combine to facilitate coordinated, adaptive performance and task objectives resulting in value-added outcomes (Salas et al. 2005, p. 562). Salas et al. (2005) described teamwork as consisting of five core components (team leadership, mutual performance modelling, backup behaviour, adaptiveness, and team orientation) and three coordinating mechanisms (shared mental models, achievement of mutual trust, and closed-loop communication). In the Petro-HRA method, the team is defined as everyone who is involved in the task(s) or scenario (including management).

Levels and multipliers: The levels and multipliers for the Teamwork PSF are shown in Table 14 (next page).

Table 14: Levels and multipliers for the Teamwork PSF

Teamwork		
Multipliers	*Levels*	*Level descriptions*
50	Very high negative effect on performance.	The teamwork is very poor on one or several teamwork factors that have been identified as important for the performance of the task or scenario in question.
10	Moderately negative effect on performance.	The teamwork is poor on one or several teamwork factors that have been identified as important for the performance of the task or scenario in question.
2	Very low negative effect on performance.	The teamwork is to some degree poor on one or several teamwork factors that have been identified as important for the performance of the task or scenario in question.
1	Nominal effect on performance.	The teamwork is adequate on one or several teamwork factors that have been identified as important for the performance of the task or scenario in question. Teamwork has neither a negative nor a large positive effect on performance.
0.5	Low positive effect on performance.	The team is very good on one or more teamwork factors that have been identified as important for the task(s) or scenario in question and teamwork increase performance.
1	Not applicable.	This PSF is not relevant for this task or scenario.

Method for how to analyse Teamwork: In determining the appropriate PSF level the analyst should consider:

- Is teamwork needed for this task?
- If teamwork is not needed the level "Not Applicable" should be chosen.

The analyst should use Table 23 of Appendix A.6 (from Salas et al., 2005, pp. 560-561) to evaluate whether each of the teamwork factors influences performance of the task. If the teamwork factors in the analysed scenario are evaluated to influence performance the analyst should find out whether they increase or reduce performance for the task(s) in question if (i.e., to determine if Teamwork is a performance driver). The analyst must perform a total evaluation of the factors when deciding on the multiplier levels. It might be, for example, that some factors are not important. These should be evaluated as not affecting performance. Sometimes one factor might be evaluated as very important and then that factor might be the only basis for selection of a positive or negative level. Strong antagonistic relationships are often a sign that there is an issue with several of the teamwork factors.

Guidance on obtaining data on Teamwork: The best data on Teamwork will be obtained by observing the crews in a simulator or during work. If this is not possible, information about Teamwork could also be obtained during interviews and workshops. The analyst should then ask the operators specifically about the Teamwork performance markers in Table 23 of Appendix A.6.

6.2.9 Physical Working Environment

Definition: Physical working environment refers to the equipment used by, accessibility of, and working conditions of the person performing the task. Although ergonomic effects inside a control room such as ventilation, lighting, noise etc. can have an impact on human performance, the effect is rarely large enough to have a significant impact on an HRA. This PSF should primarily be used for tasks outside of the control room. Examples of ergonomic issues include extreme weather conditions, work that should be performed in an inaccessible or hard to reach place, and manually operated functions in the field that are physically demanding (e.g., operating a valve that is difficult to turn). Aspects of the Human-Machine Interface (HMI) are not included in this PSF. These are covered by the HMI PSF (see 6.2.6).

Levels and multipliers: The levels and multipliers for the Physical Working Environment PSF are shown in Table 15.

Table 15: Levels and multipliers for the Physical Working Environment PSF

Physical Working Environment		
Multipliers	*Levels*	*Level descriptions*
HEP=1	Extremely high negative effect on performance.	The task cannot be completed due to the tools required or the area in question being inaccessible or unavailable.
10	Moderate negative effect on performance.	There are clear ergonomic challenges in completing the task. This could be due to the area where work is conducted being hard to reach, the manual field activation is difficult or physically demanding, or there are extreme weather conditions that decrease performance.
1	Nominal effect on performance.	Physical working environment does not have an effect on performance.
1	Not applicable.	This PSF is not relevant for this task or scenario.

Method for how to analyse Physical Working Environment: In determining the appropriate PSF level the analyst should consider:

- Does the physical working environment affect task performance? If not, the “Not Applicable” level should be chosen.
- If the physical working environment affects task performance the analyst has to decide at what level it affects performance.

Guidance on obtaining data on Physical Working Environment: The walkthrough of tasks and scenario, as defined for the Human-Machine Interface PSF, should also be used to obtain information about the Physical Working Environment.

6.3 Advice on Double Counting

When selecting the PSF levels and corresponding multipliers, the analyst should keep in mind that it is the effect on the likelihood of error or performance as a result of the PSF that should be evaluated, not only the presence of the PSF. A PSF might be present without having an effect on performance. The analyst should also evaluate whether they have enough information to evaluate the PSF; if not, more information should be collected.

Table 24 in Appendix A.7 provides information about how to select between different PSFs and how to avoid double counting the effect of the same phenomenon through including it in several PSFs for the task. When the same influence/issue involves more than one PSF, the analyst should be very careful to not double count the same influence, as this can result in an overly conservative error probability.

For example, task time and task complexity can be related, since more complex tasks generally take longer to complete than simpler tasks. The analyst must consider which of these two PSFs has the greater impact on the task, and which is a side-effect of the other PSF. "*For example, if the primary hurdle for [an operator] in a particular situation is the fact that they have five minutes in which to act, then the available time is the primary performance driver. If, on the other hand, in a different situation if the primary challenge is that the [operator] has to deal with multiple system malfunctions, multiple procedures, inexplicable plant response, and multiple indication errors, then the primary performance driver is the complexity of the situation*" (Whaley et al., 2011). In the second instance, the complexity of the situation will likely increase the time required, but time required is a side-effect of the primary performance driver (task complexity) and so the analyst should only include a negative assessment of the Task Complexity PSF. A negative assessment of both task complexity and time for this task step would be considered double counting.

It is important to note that analysts should only include a negative assessment of multiple PSFs if there is evidence that each PSF has a separate effect on the operator for that task step. For example, if the operator has only 1 minute to complete the action AND the action is complex, then both Time and Task Complexity will have separate, negative impacts on performance and both PSFs should be included in the assessment. The analyst should precisely describe their arguments for the chosen PSF levels.

6.4 Summary Quantification Worksheet

A summary quantification worksheet (Table 16, next page) should be completed for each event in the OAET. If using the basic cognitive model as the basis for the OAET, that means the analyst must complete four worksheets: one each for detection, diagnosis, decision and action.

The purpose of the workshop is to document the PSF multiplier levels that were evaluated for each OAET event, and to clearly document the substantiation or evidence for these PSFs were evaluated in this way. This documentation is vital to help identify performance drivers, and to evaluate where recommendations for improvements could be made to reduce the risk from human error in Step 7.

The HEP for each event is calculated by multiplying the nominal HEP (0.01) with each of the multipliers selected, i.e.,

> *HEP = 0.01(Nominal HEP) x multiplier(Time) x multiplier(Threat Stress) x multiplier(Task Complexity) x multiplier(Experience/Training) x multiplier(Procedures) x multiplier(HMI) x multiplier(Attitudes to Safety, Work and Management Support) x multiplier(Teamwork) x multiplier(Physical working environment)*

The final HEP should also be documented on the summary quantification worksheet, in the row labelled "HEP Calculation".

Table 16: The Petro-HRA summary quantification worksheet

Petro-HRA PSF summary worksheet			
Facility/installation		**Date**	
HFE ID & description			
HFE scenario			
Analysts			
HEP Calculation			
PSFs	**PSF levels**	**Multiplier**	**Substantiation: Specific reasons for selection of PSF level**
Available time	Extremely high negative	HEP=1	
	Very high negative	50	
	Moderate negative	10	
	Nominal	1	
	Moderate positive	0.1	
	Not applicable	1	
Threat stress	High negative	25	
	Low negative	5	
	Very low negative	2	
	Nominal	1	
	Not applicable	1	
Task complexity	Very high negative	50	
	Moderate negative	10	
	Very low negative	2	
	Nominal	1	
	Moderate positive	0.1	
	Not applicable	1	
Experience/training	Extremely high negative	HEP=1	
	Very high negative	50	
	Moderate negative	15	
	Low negative	5	
	Nominal	1	
	Moderate positive	0.1	
	Not applicable	1	
Procedures	Very high negative	50	
	High negative	20	
	Low negative	5	
	Nominal	1	
	Low positive	0.5	
	Not applicable	1	
Human-machine interface	Extremely high negative	HEP=1	
	Very high negative	50	
	Moderate negative	10	
	Nominal	1	
	Low positive	0.5	
	Not applicable	1	
Attitudes to Safety, Work and Management Support	Very high negative	50	
	Moderate negative	10	
	Nominal	1	
	Low positive	0.5	
	Not applicable	1	
Teamwork	Very high negative	50	
	Moderate negative	10	
	Very low negative	2	
	Nominal	1	
	Low positive	0.5	
	Not applicable	1	
Physical working environment	Extremely high negative	HEP=1	
	Moderate negative	10	
	Nominal	1	
	Not applicable	1	

6.5 Integration of HEPs with the OAET

When HEPs have been calculated for all events in the OAET, the failure probabilities for each end state can be calculated according to the event tree logic. The process for doing this can be illustrated using the example of the blowdown OAET from 5.1, shown in Figure 15. Note that the HEPs shown in this figure are fictive and used for the purposes of illustration only.

Figure 15: Calculating the end state HEPs

Using this example, if the HEP for “Detect leakage” is 0.01, this is the value for the failure branch (labelled “No” in Figure 15), which corresponds to the value for End state 1. The value for success (labelled “Yes” in Figure 15) of the same branch is 1-0.01=0.99. If the HEP for “Diagnose event” is 0.01, the value for End state 2 is 0.99*0.01=0.0099, which approximates to 0.01. In this way the values of all the end states are calculated.

In the same example, the HFE that enters the QRA is “failure to manually activate blowdown”. The HEP for this is found by adding all the HEPs for the end states leading to failure, i.e., end states 1 to 4 of Figure 15. Thus, the overall HEP for “failure to manually activate blowdown” is calculated as 0.11546 (Failure HEP = end state 1 + end state 2 + end state 3 + end state 4). The overall HEP for success in manually activating blowdown is calculated in the same way, only adding the end states that lead to success. In Figure 15, only one end state leads to success.

A useful tip to check whether you have correctly calculated the HEPs for each end state is to add them all up (failure end states + success end states); together they should equal 1.

The OAET table (developed in Table 5) should also be updated with the end state HEPs.

6.6 Perform a Reasonableness Check

The analyst should perform a reasonableness check of the HEPs obtained from the analysis. If individual HEPs deviate significantly from other HEPs in the analysis, or is very dominant, or in other ways does not seem reasonable, one should re-visit the calculation and the qualitative analysis constituting the basis for the number. A subject matter expert (SME) should be involved in the reasonableness check – ideally a QRA analyst and/or process expert/facility operator. They should be consulted to consider whether the HEP is realistic for the scenario, to ensure that all claims and assumptions are valid, credible and correct, and that the analysis accurately represents the task. The SME should have been involved in the HRA to some degree (e.g., during scenario definition, qualitative data collection and/or task analysis) to make sure they understand the context of the scenario and the analysis.

HEP reasonableness can be checked as follows:

- First get an overview of the various HEPs for the different HFEs and also for all the individual tasks that have been analysed and quantified.

- Check if any of these seem very high or very low.
    - Is it likely that the obtained HEP(s) is realistic based on the estimated PSF levels?

- Check if any of these "stand out" and seem not realistic for the task in question.
    - If there are two analysts, this might be found by separately calculating the HEPs, and then checking whether there are HEPs for the same HFE/task with more than one order of magnitude difference.
    - An SME should be involved in this step, go through the tasks and HEPs with the SME.
    - Does the HEP(s) seem realistic when comparing tasks within this scenario or with other analyses? Do tasks where one expects the highest HEP have the highest HEP? If not, this needs explanation and discussion.
    - Is there agreement between the operator(s) views on the likelihood of errors on a task(s) and the HEP(s)? If there is disagreement this needs discussion and explanation as to why the analysis is more correct than the operators' expectations.

- For any unreasonable HEP identified during the three steps above:
    - Re-visit the calculation and find the dominant driver for the number.
    - Re-visit the qualitative analysis and verify the substantiation for the PSFs that drove the HEP to a noticeable small or big number. This should be done together with the SME.
    - Document the reasonableness check.

6.7 Expected Outcomes of the Human Error Quantification

The expected outcomes from the quantification of each event are:

- The Human Error Probability as a number from 0 to 1 of the task/event under analysis.
- A detailed understanding of the PSFs that are relevant for the event under analysis. In addition to being instrumental in finding the HEP this information can also be used in the human error reduction.
- A detailed summary PSF worksheet (one per HFE), documenting substantiation for each HFE from the operator action event tree.

7 Step 7: Human Error Reduction

One of the main drivers of HRA is the opportunity it provides for improving system safety and reliability by implementing risk-informed solutions. Such improvements aim at minimizing risk either through the reduction of human error probability or mitigation of the consequences of a human error occurring. The human error reduction process is made up of two closely linked and iterative activities, namely impact assessment and error reduction analysis (ERA).

The objective of human error reduction is twofold. The purpose of an impact assessment is to demonstrate the relative contribution of human error to the overall risk picture of the QRA (or other risk model). Conclusions from the impact assessment help the analyst to determine the scope and depth level of the ERA. The ERA then aims to develop error reduction measures (ERMs) targeting specific human errors, and/or error reduction strategies (ERSs) targeting human performance on a more general level, for example across several tasks and accident scenarios. Human error reduction aims to develop ERM and ERS in a systematic manner by utilizing knowledge and insight gained from analysis techniques commonly performed as part of an HRA.

Impact assessment is performed after the human error quantification step has been completed and starts with integrating the HEPs into the QRA model. The purpose is to determine whether there is a need to further assess the HEP contribution to the overall risk level of the QRA and/or perform an ERA. If it is determined that the human contribution to risk should be reduced, then an ERA is performed. The impact assessment is then repeated after the ERA has been performed, to determine the reduction in risk based on the outputs of the ERA.

7.1 How to Perform Human Error Reduction

7.1.1 Impact Assessment

The first step of the impact assessment is to integrate the HEP values for each of the quantified HFEs into the QRA. How this is done depends on the structure of the QRA, to what extent it can be adjusted to adopt HFEs, the choice of human error model, and more. The Petro-HRA analyst must consult with the QRA analyst to integrate the HEPs to the QRA model.

Once the HEPs have been assigned to the various HFEs in the QRA model, probabilities can be calculated (respectively) for the model's end states, and an assessment can be made to determine whether the HEP is acceptable or not.

The impact of the HEPs may be deemed acceptable if:

- The risk acceptance criteria are not exceeded.
- All HFE HEP values are low (i.e., <0.01); note that this is valid only for post-initiator (Type C) actions.
- There is little or no uncertainty behind the HEPs.
- HFEs are not associated with highly severe end states.

However, if one or more of the conditions in this list are not met, then a more detailed qualitative or quantitative impact assessment should be performed as part of a sensitivity analysis, which can be conducted by the QRA analyst.

7.1.2 Error Reduction Analysis

This section describes the process for performing ERA, including how to utilize the outcomes of previous analyses in the Petro-HRA process to develop ERMs and ERSs.

Select events for risk reduction: The first step in the ERA process is to identify and prioritize the events in the HFE (i.e., human error) model which contributes the most to the overall HEP estimate. A simple method to do this is listed below:

- Check which events have the most negative influence from PSFs and/or the highest HEP.
- Check the severity of the end states for these events.
- Combine these two parameters and generate ERMs or ERSs as appropriate to either reduce the negative PSF influence or improve the positive influence of the other PSFs to compensate for the negative influencing PSFs.

As an example, Figure 16 shows an event tree with two events (A and B) and three event sequence pathways. Each pathway has an end state for which the probability has been calculated by multiplying HEPs for the preceding events. Note that the total HEP for the HFE is the sum of adding together the HEPs for end states resulting from task failures. For the HFE modelled in Figure 16 the total HEP is 0.0199, or HEP = 0.01 + 0.0099. Task success is the remaining 0.9801.

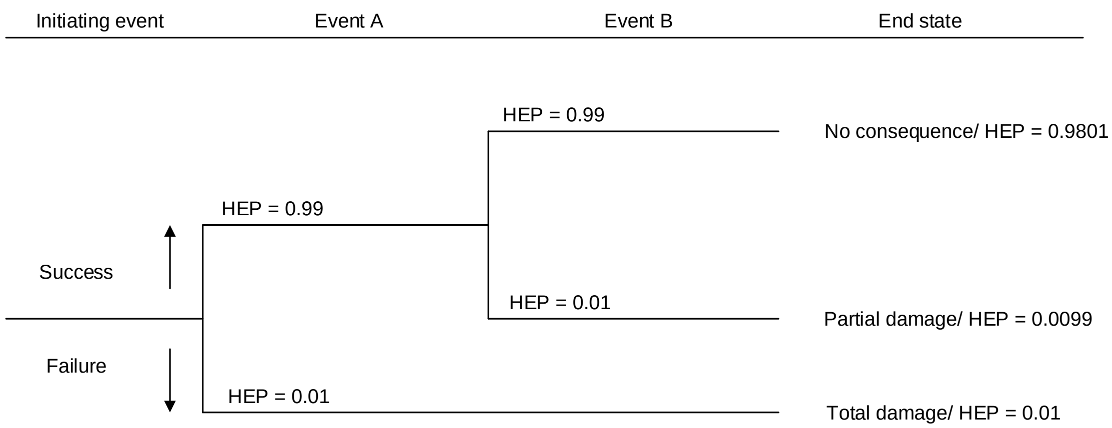


Figure 16: Event tree with example HEPs

In Figure 16, both Event A and Event B have identical HEP values. The HEPs for their associated end state are also approximately the same. Event A, however, is associated with a more severe outcome (i.e., end state HEP of 0.01), and should therefore be prioritized over Event B when developing ERMs. Alternatively, if the HEP for Event B was significantly higher than the HEP for Event A, Event B may be considered more critical despite having a less severe outcome. If the severities of the end states are similar the selection of events for further ERA is solely based on the contribution of each events HEP value.

There are no set rules for how large the differences in HEP and end states must be for one event to be prioritized over the other. This evaluation is up to the analyst's judgement on a case-by-case basis. However, a general recommendation is that for one event to be prioritized over another there has to be at least one order of magnitude difference between the HEPs.

Re-examine the PSFs: In Petro-HRA, the HEPs in the human error model are a direct result of which PSFs and PSF multiplier levels have been selected for each event. After having identified events for risk reduction it is therefore important that the analyst re-visits the substantiation behind the PSF selection. In particular, the analyst should examine which PSFs can be considered performance drivers for various parts of the task. This is necessary to demonstrate risk reduction, i.e., by establishing traceability between the PSF evaluations, calculated HEPs and suggested ERMs and/or ERSs.

Furthermore, risk reduction measures can target other PSFs than the one that has a negative impact on the HEP. For example, it could be that the HEP for an event is negatively influenced by the Threat Stress PSF, while all the other PSFs are rated as Nominal. An ERM could be to improve Experience/Training or Teamwork in ways which can be argued to reduce Threat Stress to the extent that a more positive PSF multiplier level can be chosen. As such, correlations between PSFs must be examined carefully to ensure that risk reduction efforts target the correct PSFs.

Develop ERMs targeting specific human errors: After having selected which events to prioritize for ERA, and re-visiting how the PSFs drive the HEPs, the next step is to identify which specific human errors to target for human error reduction. Each event in the human error model can typically fail as a result from one or several different human errors.

One of the main outputs from the HEI in Step 4 is a list of human errors to be considered further for more detailed analysis. This selection is based on the consequence of the human error combined with the potential for recovery (for more information, refer back to section 4 and 5). The analyst must examine the HEI and consider which human errors are the most critical and should be included in the ERA. As a standalone activity HEI is an efficient method for identifying ERMs for specific task steps.

HEI can be used for human error reduction for the following ERM techniques:

- Error mechanism prevention
- Error pathway blocking
- Error recovery enhancement
- Error consequence reduction

Examples of ERMs include:

- Modification of a specific procedure step to remove ambiguity or add specific information.
- Introduction of a specific HMI feature, e.g., emergency stop button for all components in a specific system to reduce the need to shut down individual components separately.
- Provision of training on a specific task in the emergency response plan to reinforce the preferred response actions.

Develop ERSs targeting overall task performance:

While ERMs aims to achieve risk reduction by targeting specific human errors for specific task steps, ERSs aim to reduce risk by improving task performance across several task steps, or even between different accident scenarios. There are two different approaches for developing ERSs:

- Overall task re-design
- Overall PSF improvement

Examples of ERSs include:

- Establishing procedures for important operation actions that are currently not proceduralised, to reduce variability in how operators perform those actions.

- Improving the quality of HMIs to support operator performance in day-to-day work, as well as in emergency scenarios.
- Evaluating emergency response scenarios to identify ways that time pressure could be reduced, e.g., through the introduction of automated processes, improved delegation of actions between operators, reduction of non-critical actions.

Re-calculate HEPs based on updated PSF justifications: After having developed ERMs and ERSs the analyst must update the PSF substantiations – i.e., the arguments behind selecting each PSF and its multiplier level. The updated substantiations are used to select new multiplier levels so that HEPs for each targeted event can be re-calculated.
Questions facing the analyst could include:

- To what degree does the ERM or ERS impact the PSF?
- How to account and control for correlations between PSFs?

Finally, the human error model is re-run to produce a HEP for the HFE which reflects the predicted risk reduction. The results can then be handed over to the person(s) responsible for integrating the HEP in the QRA and updating the model. If the new risk level is considered to be sufficiently low (e.g., below the risk acceptance criteria), the HRA can be documented and closed. If not, the impact assessment and ERA must be iterated.

How this is done in practice depends on who is doing the analysis, requirements for documentation as well as the timing and sequence of the HRA activities. For example, if an external party is doing the HRA it may be preferred to not re-calculate the HEPs and human error model until after verifying that the ERMs and ERSs have been implemented as recommended and/or have the intended effect.

7.1.3 Predictive Adjustment of HEPs based on Implementation of ERMs or ERSs

It may be the case that the analyst is asked to provide a prediction or estimation of the effect on the HEP for the overall scenario if some or all of the ERMs or ERSs are implemented. This can help to prioritise the recommendations, to determine which would have the most effect on the HEP. To do this, the analyst should look back at how the error reduction measures or strategies were developed, determine the specific task steps or actions that were targeted and the driving PSFs for these, and adjust the PSF multiplier levels as though the ERM/ERS has been implemented. Then a new HEP can be calculated to demonstrate the effect of implementation of the ERM/ERS.

For example, if the HRA identifies that a critical task step is poorly described in a written operating procedure, an ERM may be developed to improve the procedure description for that task step. The HRA analyst may have originally rated the Procedures PSF as "High negative effect on performance" with a multiplier of 20, since it is related to a critical task step. To evaluate the effect of implementation of that ERM, the analyst should revisit the HEP for that task step and adjust the Procedures PSF multiplier accordingly, e.g., reduce it from 20 to 1 as it will now have a "Nominal effect on performance". The analyst should do the same for all PSF multipliers related to the ERM/ERS that are predicted to be implemented, and then recalculate the overall HEP accordingly.

The ability to provide predictive assessments of the effects of implementation of ERM/ERS reinforces the need for the development of specific and detailed recommendations so that the particular effects it will have on the HEP can be more easily determined and substantiated.

For example, the recommendation should state something like "Amend Step 4.1 of Operating Procedure XYZ-123 to state "The valve should be throttled to reduce flow by 50%", instead of a more vague recommendation to "Improve the operating procedure". This activity also requires that the PSFs were well substantiated in the first place, so that the analyst must only review the summary quantification worksheet to see where the ERM/ERS will have an effect. If the original PSF evaluations are not well substantiated, then the analyst may have to go back to the original task analysis to see how/why/where the ERM/ERS were targeted, which becomes a very time-consuming task.

7.2 Expected Outcomes of the Human Error Reduction

The impact assessment and ERA shall result in a set of ERMs and ERSs prioritized based on their predicted effect on the risk level. The impact assessment and ERA should document the following:

- The approach and method used for impact assessment and ERA
- The criteria and arguments for selecting which events to target
- A prioritized set of ERMs and ERSs according to their risk reducing effect
- The link between task steps, human errors, ERMs/ERSs, PSFs and HEP values

It is important to include the relevant persons (e.g., QRA and/or SME) when reviewing the results and documented outcome of the impact assessment and ERA. In particular, the selection of events, PSF justifications, and HEP calculations should be checked by someone with a dedicated Quality Assurance role.

7.3 Good Practices for Human Error Reduction

In addition to the suggested approach, the following good practices are recommended:

- ERSs and ERMs should be specific and actionable (i.e., instead of recommending "more training", the recommendation should point to the specific task or action that requires training, should be linked to the task and error analysis, and should explain what the desired outcome of the training should be).

- ERSs and ERMs perceived as important by the analyst should be documented throughout the HRA process and communicated to the relevant stakeholders (e.g., in a final report) regardless of the conclusions made from the impact assessment. For example, the guidelines for Section 9 in the Norwegian Petroleum Safety Authorities (PSA) state that additional risk reduction shall always be considered, even if the results of risk analyses or risk assessments indicate a level of risk that is within the acceptance criteria. A risk reduction workshop at the end of the TRA is considered a good practice to present the results of the HRA and to develop ERSs and ERMs together with the relevant stakeholders.

- A high HEP value should encourage the analyst and other stakeholders (e.g., the client) to perform an ERA, regardless of whether a high contribution has been quantitatively demonstrated (e.g., by use of risk acceptance criteria). It is considered good practice to conduct an ERA any time the HEP of a HFE equals or is higher than 0.1 (Kirwan, 1994).

- Regardless of the influence of a recovery action on the HEP, implementing recovery actions should be implemented as good practice. Recovery actions may be easy to implement (e.g., supervisory oversight, procedural checks) and therefore not as costly as some more sophisticated human error reduction measures (Kirwan, 1994).

- The Petro-HRA method recommends using relatively high-level human error models, as exemplified in Figure 16. When using such models, targeting (basic) events for ERA can be done by visual inspection of the fault or event trees combined with simple calculations. Any use of slightly more complex modelling should be supported by suitable software and/or personnel with competence in event or fault tree modelling.

8 Documentation of the Petro-HRA

In a Petro-HRA, a final report must be written detailing the results of the Petro-HRA and is issued as an appendix to the QRA. The quantitative results of the Petro-HRA (i.e., the calculated HEPs) will normally be input directly to the QRA fault tree or event tree models. However, the qualitative results are equally important and so must be documented in a way that makes them sufficiently transparent for others who wish to read, understand and use those results. The QRA analysts, and other interested parties, must be able to determine, clearly and unambiguously, the process and methodology that was followed throughout the Petro-HRA, and how the final results were arrived at.

The HRA report should include:

- A description of scope, context, boundaries and limitations of the analysis.
- A clear and unambiguous description of the analysis scenario(s), and its context in the QRA.
- A list and description of the HFEs analysed in this scenario.
- A description of any assumptions made.
- A description of any uncertainties in the analysis.
- The rationale for assumptions made regarding timing of and dependencies between actions.
- Full references to other documents or material used to inform the analysis, facility operating instructions, system descriptions, etc.
- The task analysis diagrams and/or tables.
- Event trees (or equivalent human error models, e.g., fault trees).
- Any supplemental qualitative analyses (e.g., used to substantiate assessment of the PSFs).
- Details of the PSF assessments. For this purpose, use the PSF summary worksheet as given in Section 6.5; one worksheet per task quantified.
- Details of the quantitative calculations and final results.
- Details of the recommendations for human error reduction.

8.1 Good Practices for Documenting the Petro-HRA

To document the analysis the analyst should:

- Describe all data that was collected and how the data was collected.

    - For example, if data were collected from interviews and workshops describe how the workshop was performed. How many persons were interviewed and how many persons participated in the workshop? Document their roles (e.g., operator, shift manager, QRA analyst, training manager, etc.). Were the operators who participated in the interviews/workshop representative of the other operators/crews? Were any follow-up calls made?

    - The scenario description should highlight the important operator actions and when these are required. Also clearly state what cues the operator will receive to take the action, and when during the scenario these will occur. In addition, the scenario description should note the relative complexity of the task (whether it is considered easy or difficult to perform) and whether there are operating procedures or other supporting documentation available to the operator.

    - If including transcripts or excerpts from notes taken during interviews, observations, facility walk-downs or scenario walk-/talk-throughs, the analyst should be careful to maintain the anonymity of the facility personnel who participated in the activities. Transcripts of interviews should only be included in the final HRA documentation if prior permission has been received from the interviewee.

- Describe how the data was analysed.
  - The analysis should describe how the data were structured and analysed. For example, did the analyst sort all information from the qualitative data about each PSF (similar to a thematic analysis)? What kind of data analysis was performed?
- Describe the evidence for the selected PSFs, PSF levels, and multipliers.
  - The analyst should thoroughly describe the evidence from the data for the selection of PSFs, PSF levels, and multipliers. From this documentation it should be possible for reviewers and others to agree/disagree with the choices that the analyst has made from the data. The analysis should be transparent to others.
- Present reasonableness checks of the HEPs and other quality assurance measures.
  - The analyst must document the reasonableness check, how it was performed and results. Especially, if the analysis was updated based on this, the changes must be documented.
  - Internal quality assurance by senior analyst(s) or review and approval by the client / operating company must be included.
  - Lack of information should be documented, and it should normally lead to the use of the "insufficient information" level, i.e., a multiplier of 1 (nominal).

"*In short, the final report should include all information necessary for the system analyst to check his assumptions about the performance situation against yours. It should also include sufficient information so that another human reliability analyst could perform an HRA for the same scenario and arrive at a similar result*" (Bell and Swain, 1983).

In addition, any necessary departures from the Petro-HRA method described in this handbook should be clearly stated in the HRA report.

9 References

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior (pp. 11-39). Berlin: Springer.

Annett, J. (2000). Theoretical and practical influences on task analysis methods. In J.M. Schraagen, S.F. Chipman, and V.L. Shalin (eds.), Cognitive Task Analysis. Mahwah: Lawrence Erlbaum Associates.

Annett, J. (2003a). Hierarchical task analysis. In D. Diaper and N.A. Stanton (eds.), Handbook of Task Analysis in Human-Computer Interaction. Mahwah: Lawrence Erlbaum Associates.

Annett, J. (2003b). Hierarchical task analysis. In E. Hollnagel (ed.), Handbook of Cognitive Task Design. Boca Raton: CRC Press.

Arthur Jr, W., Bennett Jr, W., Stanush, P. L., & McNelly, T. L. (1998). Factors that influence skill decay and retention: A quantitative review and analysis. Human Performance, 11(1), 57-101.

ASME (2009a). Standard for level 1 / large early release frequency probabilistic risk assessment for nuclear power facility applications. New York: The American Society of Mechanical Engineers.

ASME. (2009b). Addenda to ASME/ANS RA-S–2008, Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Facility Applications, ASME/ANS RA-Sa-2009. New York: American Society of Mechanical Engineers.

Boring, R. L., & Blackman, H. S. (2007). The origins of the SPAR-H method's performance shaping factor multipliers. In Human Factors and Power Facilitys and HPRCT 13th Annual Meeting (pp. 177-184). IEEE.

DNV GL (2014). Quantitative Risk Assessment. https://www.dnvgl.com/services/quantitative-risk-assessment-1397

Embrey, D.E. (1986). SHERPA: A systematic human error reduction and prediction approach. International Meeting on Advances in Nuclear Power Systems.

Forester, J., Kolaczkowski, A., Cooper, S., Bley, D., and Lois, E. (2007). ATHEANA User's Guide. Final Report. NUREG-1880. U.S. Nuclear Regulatory Commission, Washington, USA.

Forester, J., Dang, V.N., Bye, A., Lois, E., Massaiu, S., Broberg, H., Braarud, P.Ø., Boring, R., Männistö, I., Liao, H., Julius, J., Parry, G., Nelson, P. (2014). The International HRA Empirical Study – Final Report – Lessons Learned from Comparing HRA Methods Predictions to HAMMLAB Simulator Data. NUREG-2127, U.S. Nuclear Regulatory Commission, Washington D.C.

Gertman, D., Blackman, H., Marble, J., Byers, J., & Smith, C. (2005). The SPAR-H Human Reliability Analysis Method. NUREG/CR-6883. Washington, DC, U.S. Nuclear Regulatory Commission.

Gould, K. S., Ringstad, A. J., & van de Merwe, K. (2012). Human reliability analysis in major accident risk analyses in the Norwegian petroleum industry. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting (Vol. 56, No. 1, pp. 2016-2020). Sage Publications.

IEC61511 (2003). Functional safety – Safety instrumented systems for the process industry sector – Part 2: Guidelines for the application of IEC 61511-1.

Human Factors and Ergonomics Society (2014). http://www.hfes.org/Web/EducationalResources/HFEdefinitionsmain.html

Johnston, J. H., & Cannon-Bowers, J. A. (1996). Training for stress exposure. Stress and Human Performance. In J. E. Driskell, and E. Salas, (Eds.): Stress and Human Performance (pp. 223-256). New Jersey, USA: Lawrence Erlbaum Associates.

Kirwan, B. (1994). A Guide to Practical Human Reliability Assessment. London: Taylor & Francis.

Kirwan, B. & Ainsworth, L.K. (1992). A guide to task analysis. CRC Press: Boca Raton.

O'Hara, J.M., Higgins, J.C., Stubler, W.F., and Kramer J. (2000). Computer-based procedure systems: Technical basis and human factors review guidance. No. J-6012. Upton, NY: Brookhaven National Laboratory.

Øie, S. and Fernander, M. (2022). Analysis of Pre-Accident Operator Actions (APOA). Norway: DNV. ISBN: 978-82-515-0325-9.

Salas, E., Driskell, J.E. & Hughes, S. (1996). Introduction: The study of stress and human performance. In J. E. Driskell, and E. Salas, (Eds.): Stress and Human Performance (pp. 1-45). New Jersey, USA: Lawrence Erlbaum Associates.

Salas, E., Sims, D. E., & Burke, C. S. (2005). Is there a "Big Five" in teamwork? Small Group Research, 36(5), 555-599.

Salas, E., Tannenbaum, S. I., Kraiger, K., & Smith-Jentsch, K. A. (2012). The science of training and development in organizations: What matters in practice. Psychological Science in the Public Interest, 13(2), 74-10.

Stanton, N. A., Salmon, P. M., Walker, G. H., Baber, C., & Jenkins, D. (2005). Human factors methods: a practical guide for engineering and design. Hampshire, England. Ashgate Publishing Limited.

Swain, A.D., & Guttman, H.E. (1983). Handbook of human reliability analysis with emphasis on nuclear power plant applications. NUREG/CR-1278 (Washington D.C.).

Taylor, C., Øie, S. & Gould, K. (2020). Lessons learned from applying a new HRA method for the petroleum industry. Reliability Engineering and System Safety, vol. 194.

van de Merwe, K., Øie, S., Hogenboom S. & Falck, A. (2015a). Guidance on integrating Human Reliability Assessment in Quantitative Risk Assessment. Proceedings of the ESREL 2015 conference, Zurich, Switzerland.

Whaley, A. M., Kelly, D. L., Boring, R. L., & Galyean, W. J. (2011). SPAR-H step-by-step guidance. INL/EXT-10-18533. Idaho Falls, ID: Idaho National Laboratory.

Whaley, A.M., Xing, J., Boring, R.L., Hendrickson, S.M.L., Joe, J.C., Le Blanc, K.L. (2012). Building a Psychological Foundation for Human Reliability Analysis. NUREG-2114. U.S. Nuclear Regulatory Commission, Washington, USA.

US Nuclear Regulatory Commission / Electrical Power Research Institute. (2012). EPRI/NRC-RES Fire Human Reliability Analysis Guidelines, NUREG-1921. Washington, DC: US Nuclear Regulatory

Commission.

Øie, S., van de Merwe, K., Hogenboom, S., Laumann, K., and Gould, K. (2014). Human Reliability Assessment of Blowdown in a Gas Leakage Scenario on Offshore Production Platforms: Methodological and Practical Experiences. In Proceedings of the 12th International Probabilistic Safety Assessment and Management Conference (PSAM 12), Hawaii, USA.

9.1 References utilized during this work, but not directly cited

Bell, B. J. and Swain, A. D. (1983). “A Procedure for Conducting a Human Reliability Analysis for Nuclear Power Facilitys.” NUREG/CR-2254. U.S. Nuclear Regulatory Commission.

Boring, R.L. (2014). Top-down and bottom-up definitions of human failure events in human reliability analysis. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 58, 563-567.

Brooke, J. (1996). SUS: A "quick and dirty" usability scale. In P. W. Jordan, B. Thomas, B. A. Weerdmeester, & A. L. McClelland (Eds.), Usability Evaluation in Industry. London: Taylor and Francis.

Dekker, S. W. A. (2006). The Field Guide to Understanding Human Error. Aldershot, UK: Ashgate Publishing Co.

Embrey, D. (2000). Task Analysis Techniques. Dalton, Lancashire: Human Reliability.

Energy Institute (2004). Safe Staffing Arrangements – User Guide for CRR348/2001 Methodology: Practical application of Entec/HSE process operations staffing assessment methodology and its extension to automated facility and/or equipment. Energy Institute, London.

Energy Institute (2011). Guidance on human factors safety critical task analysis. http://www.energypublishing.org/__data/assets/file/0014/64022/Guidance-on-HF-safety-critical-task-analysis.pdf.

Energy Institute (2012). Guidance on quantified human reliability analysis (QHRA). http://www.energypublishing.org/__data/assets/file/0019/51841/QHRA-Guidance.pdf

Folkard, S., & Tucker, P. (2003). Shift work, safety and productivity. Occupational Medicine, 53(2), 95-101.

Hart, S. G., & Staveland, L. E. (1988). Development of NASA-TLX (Task Load Index): Results of empirical and theoretical research. Advances in Psychology, 52, 139-183.

Hollnagel E. (1998). Cognitive reliability and error analysis method. Oxford: Elsevier Science Ltd.

HSE (2001). Assessing the safety of staffing arrangements for process operations in the chemical and allied industries. Contract Research Report CRR348/2001, HSE Books.

HSE (2021). Health and Safety Executive. Operating Procedures. https://www.hse.gov.uk/comah/sragtech/techmeasoperatio.htm

Kraiger, K., Ford, J. K., & Salas, E. 1993. Application of cognitive, skill-based, and affective theories of learning outcomes to new methods of training evaluation. Journal of applied psychology, 78(2), 311-328.

NORSOK Z-013 (2010). Risk and emergency preparedness assessment, revision 3. https://www.standard.no/en/sectors/energi-og-klima/petroleum/norsok-standard-categories/z-risk-analyses/z-0132/

Nielsen, J. and Mack, R.L. (Eds.) (1994). Usability Inspection Methods, John Wiley & Sons Inc.

OGP (2010). Human Factors in QRA. Report No. 434 – 5. International Association of Oil & Gas Producers.

Omerod, T.C. and Shepherd, A. (2004) Using Task Analysis for Information Requirements Specification: The Sub-Goal Template (SGT) Method. In: D. Diaper and N.A. Stanton (Eds.), The Handbook of Task Analysis for Human-Computer Interaction (pp. 347-365). Mahwah: Lawrence Erlbaum Associates.

Rajan, Wilson and Wood (2005). Control Facilities Design. In J. R. Wilson and N. Corlett (Eds.), Evaluation of Human Work. 3rd Edition. Taylor & Francis Group.

Reason, J. (1990). Human Error. Cambridge: Cambridge University Press.

Reason, J. (2013). A life in error – From little slips to big disasters. Surrey: Ashgate Publishing.

Shorrock, S.T., and Kirwan, B. (1999). The development of TRACEr: A technique for the retrospective analysis of cognitive errors in ATC. In D. Harris (ed.), Engineering Psychology and Cognitive Ergonomics, 3. Aldershot, UK: Ashgate Publishing Co.

Shorrock S.T., and Kirwan, B. (2002). Development and application of a human error identification tool for air traffic control. Applied Ergonomics, 33, 319-336.

Stanton, N.A., Salmon, P.M., Rafferty, L.A., Walker, G.H., Baber, C. & Jenkins, D.P. (2013). Human Factors methods. A practical guide for engineering and design. Surrey, UK; Ashgate Publishing Limited.

Swain, A. D. (1990). Human Reliability Analysis: Need, Status, Trends, and Limitations. Reliability and Systems Safety, 29, 301-313. Doi: 10.1016/0951-8320(90)90013-D.

van de Merwe, G.K., Hogenboom, S., Rasmussen, M, Laumann, K. & Gould. K. (2015b). Human Reliability Analysis for the Petroleum Industry: Lessons Learned from Applying SPAR-H. SPE Economics & Management, 6(4).

Whaley, A.M., Kelly, D.L., and Boring, R.L. (2012). Guidance on dependence assessment in SPAR-H. Joint Probabilistic Safety Assessment and Management and European Safety and Reliability Conference, 27-Mo4-4.

Whaley, A.M., Kelly, D.L., Boring, R.L., and Galyean, W.J. (2012a). SPAR-H step-by-step guidance. Joint Probabilistic Safety Assessment and Management and European Safety and Reliability Conference, 27-Mo4-3.

Whaley, A.M., Xing, J., Boring, R.L., Hendrickson, S.M.L., Joe, J.C., Le Blanc, K.L., and Lois, E. (2012b). Building a Psychological Foundation for Human Reliability Analysis, NUREG-2114 (Draft). Washington, DC: U.S. Nuclear Regulatory Commission.

Williams, J. C. (1988, June). A data-based method for assessing and reducing human error to improve operational performance. In Human Factors and Power Facilities, 1988., Conference Record for 1988 IEEE Fourth Conference on (pp. 436-450). IEEE.

Williams, J.C. (1992). A User Manual for the HEART human reliability assessment method. Stockport: DNV Technica Ltd.

Appendix A. Resources to Support the Analyst

A.1 Questions to Ask in Initial Scoping Meetings

Table 17: List of questions for initial meetings

	Question	Purpose
	Questions relevant to the QRA	
1	Which major accident scenario is relevant for this HRA and how important is this scenario to the overall risk picture for the QRA?	Provides information about how the scenario is represented in the QRA and the risk significance of the scenario.
2	How is the scenario likely to unfold, as defined by the QRA?	Provides information about the known sequence of events and timescale.
3	What are the expected facility behaviours, conditions and modes throughout the scenario?	Provides information about the parameters that will help to define the scenario and any limitations or boundaries.
4	When are critical operator actions needed, as defined by the QRA?	Provides information about at what point in the scenario the operator is required to intervene.
	Questions relevant to operations	
5	What is the role of the human operator in this scenario, and where is the operator likely to be located?	Provides information about what the operator is required to do during the scenario and whether these are control room- or field-based actions.
6	What are the critical tasks or operator actions in this scenario, and what factors will play a role in the success of these tasks or actions?	Provides information about which tasks or actions are likely to have the most significant impact on safety barrier functions or successful task outcome if not performed correctly.
7	What cues, alarms, system feedback or other indications is the operator likely to receive?	Provides information about how the operator is expected to know that something has gone wrong and know what to do next.
8	How much time is available for the operator to implement the required actions?	Provides information about whether these actions are achievable within the given timescale.
9	What equipment, tools, information and permissions are required for the operator to perform the required actions?	Provides information on the likely human-system interactions (HSIs) throughout the scenario.
10	When is the operator required to make decisions and what kinds of decisions will they have to make?	Provides information about the resources available to support decision-making and the consequences of making an incorrect decision.
11	Are the operators likely to have experienced a similar scenario before?	Provides information about operating experience or event reports that could inform the analysis.
12	Are the operators trained in how to respond to this scenario?	Provides information about emergency response procedures or other guidance to support the operator, and familiarity of the operators with the required response.
13	Is it possible for the operator to recover from a previous action that may have failed?	Provides information about whether actions checked or verified as they are performed, and whether there is time and resource to re-plan the response.
14	Are there any known problems at this site that could influence successful outcome of this scenario?	Provides information about factors relating to instrumentation, alarms, training, manning levels, etc. that could negatively or positively influence the outcome

A.2 Typical Documents Included in a Review

Table 18: List of documents for review

Document title	Description
HAZID Report	For existing facilities (i.e., not new build projects), HAZID reports are likely to be available. The HAZID report can provide information about: • Which hazards are present in each area of the facility and the potential consequences of these hazards. • The safety systems (barriers) in place to reduce the risk associated with the identified hazards. • Information about safety systems that require manual activation, and the relevant scenarios. • Specific issues that were addressed in the HAZID meeting, such as areas of special concern. The HAZID report is a good starting point for the HRA document review because it can provide the analyst with a good overview of the scenarios of interest (e.g., from the list of DSHAs).
Safety/Barrier Strategies	The facility's safety or barrier strategy is another valuable source of information for the HRA. The strategy document can provide information such as: • Descriptions of the facility. • Major accident hazards. • The safety systems/barriers in place, their role/function in preventing occurrence of hazards, or their role/function in mitigating the consequences of hazard occurrence. • Which safety systems/barriers depend on manual activation. • The requirements for system/barrier performance, including philosophies and principles for how to act in various situations. The strategy document can help to define the scenario as well as identify operator actions and HFEs.
QRA Report	The QRA report can provide information about HFEs and operator actions that are included in the existing QRA models, although experience shows that HRA is currently under-represented in QRA reports and the information on HFEs and operator actions might not contain much detail as yet.
HRA / Human Factors Reports	Previous HRA or Human Factors (HF) reports may be available for review to identify what scenarios were assessed previously, and what conclusions were drawn from these scenarios. The reports should be reviewed against current practices to determine if there have since been any changes which could influence PSFs, such as: • Upgrades to the HMIs. • Changes in manning or organization. • Changes to training and competence development, etc. The task analyses and HEI should also be verified and checked for changes. The analyst should make a judgement (with the assistance of a QRA analyst and/or Human Factors specialist) regarding the quality and validity of previous HRA and HF reports, and therefore the acceptability of using these as a basis for the current HRA.
Function and Task Analyses	Function and task analyses are likely to be available for newer facilities. These may contain valuable information such as: • How the operators interact with safety systems/barriers. • Comments about the degree and type of automation. • Explanations about how functions are allocated between humans and machines. • Explanations about how functions are allocated between different locations. • Descriptions of PSFs such as the HMIs and other types of equipment. NORSOK S-002 and ISO 11064 require task analyses to be performed for allocated functions, tasks and job organization to evaluate and minimize the potential for human error during all operational modes including emergency operations. If these are available, they may include the relevant scenario and HFE, or similar. If so, these can inform the task identification and analysis step of the HRA. Furthermore, they will likely include the requirements that were set for various PSFs such as HMI and communication systems during the HF engineering process.

Emergency Preparedness Analyses (EPA) and plans	The EPA tends to focus more on tasks such as how and when to alert personnel during a scenario, mustering and search and rescue strategies. Less attention is given to tasks performed by control room operators, which is often the scope of the HRA. Nevertheless, the EPA provides good descriptions of accident scenarios and is therefore an important information source for establishing the context for the HRA. Control room operator actions, and other roles in the emergency preparedness organization, are elaborated in the emergency preparedness/response plan; in particular in the action plans for each DSHA.
Hazard and Operability (HAZOP) Study	HAZOPs are commonly used to identify and analyse hazards in production processes or critical operations. The study report can provide information about how deviations from normal operations could occur, and the consequences of these, as well as details about how operator errors or actions could trigger process upsets or trips. The HAZOP report may also contain information about when operator actions are required for acknowledging alarms, manually initiating responses, etc. Note that HAZOP is commonly used for hazard identification, so the results may be contained within the HAZID report.
Technical Audits / Verification of Performance Standards	These reports can give valuable insights into the condition of safety systems/barriers and whether they perform according to pre-defined standards. The reports can also include comments about interactions between operator actions and technical production or safety systems. This information can be used as input to the task analysis, but also may inform the identification of PSFs.
Incident or Accident Investigation Reports	Reports about near-misses, unsafe conditions, incidents or accidents can increase the HRA analyst's understanding regarding the ways in which scenarios unfold as well as event sequences. In particular, details about initiating events and response failures can add realism and credibility to the scenario description as well as HEI.
Operating Manuals / Procedures / Instructions	Operating manuals typically include thorough descriptions of production and safety systems/barriers, including their functions and the philosophies behind their use and technical configurations. In addition, they tend to contain detailed information about how to (and how not to) operate the systems in various operational modes such as testing, maintenance, start-up, shutdown, etc. Operating procedures and instructions tend to contain step-by-step task descriptions which are invaluable for most HRA activities, including scenario descriptions, task analysis and HEI.
Maintenance Logs or other sources of Operational Experience	Similar to the Verification of Performance Standards reports, maintenance logs and similar reports can provide information about the condition and function of equipment. The analyst should look for information about: • Cause and frequency of false alarms. • Overrides of safety systems/barriers. • Test results, etc. Because these reports can be quite detailed and technical in nature, it is advisable for the analyst to ask if any such issues exist first, and only reading the maintenance logs to get more detail if necessary.

A.3 List of Topics for a Scenario Talk-/Walk-Through

Table 19: Suggested topics for Scenario Talk-/WalkThrough

	Topic	Question
1	Clear understanding of the scenario and requirements for operator response	Are the operators able to quickly describe how they would respond in the scenario, or do they need time to think about it? Do all of the operators give the same response, or are there several possible paths for response in the scenario?
2	Ease of use of controls and displays during the scenario	Are the operators able to quickly access the controls and interfaces that they need, or do they have to click on several different screens or go to different locations?
3	Availability and use of supporting documentation, such as emergency response procedures	Are there written procedures for the operators to use in this scenario, and do they provide clear instructions on what the operator should do and when they should do it?
4	Problem-solving, decision-making and action strategies and protocols	Do the operators have clear strategies and protocols for how to solve problems, make decisions and take actions? Are the limits of authority clear to the operators?
5	Level and quality of training on the analysis scenario	Have the operators received training on this major accident scenario (or on similar scenarios)? When was the training received, and how often have the operators received refresher training? What is the perceived quality of that training?
6	Quality of the work environment, displays and controls	Is the work environment comfortable and sufficient for the required tasks? Are the displays and controls in full working order, or are there indications of defects or deficiencies (e.g., indicators not working, maintenance tags, informal labelling, etc.)?
7	Level and quality of teamwork and communication between operators	Do the operators appear to work well together as a team, and is there good communication between team members? Do the operators use any communication protocols, such as 3-way communication?
8	Actual or perceived difficulties associated with responding to the scenario	Do the operators consider the required response to be straightforward or problematic? Why?

A.4 List of Topics for Interviews & Workshops

Table 20: Interview and workshop prompt sheet

<table>
<tr><td colspan="2">General Task Information
• How would the operator detect the event? What alarms or other indications would they expect to get?
• How would the operator begin to investigate or diagnose the event?
• How would the operator decide what to do next, and when to do it? Talk through the main steps that the operator would take.
• Which steps does the operator consider to be the most important or critical? Why?
• What would be the operator’s main concern during this event?</td></tr>
<tr><td colspan="2">Discussing Human Error
• What could go wrong during this scenario, or what could prevent the operator from successfully performing the necessary actions to control the scenario?
• What could happen if a less experienced or less knowledgeable operator was in this situation?
• Try to identify the “what if” situations, e.g., what if an error is made during execution of a particular task step?</td></tr>
<tr><td>Time
• How much time would the operator have to perform the actions required to respond to this scenario? Discuss the time taken for individual actions and the total time required to perform all actions. Is there time pressure?
• Are there any actions that can/would be performed in parallel?
• What factors could influence the amount of time needed to respond, or the amount of time that it would take to respond?</td><td>Threat Stress
• How often would the operator experience an event similar to this?
• What would the atmosphere be like in the control room/in the field during this kind of event?
• Is it likely that this event could threaten the operator’s own personal safety, or the safety of others at the facility?
• Is it likely that an incorrect response to this event could threaten the operator’s reputation, professional status or self-esteem?</td></tr>
<tr><td>Task Complexity
• How many steps are involved in the task, and are these steps carried out in a clear, logical sequential manner?
• Are there any actions that must be repeated or are dependent on each other?
• Are there any reasons to delay any task steps (e.g., to complete a diagnosis or restore a failed system)?
• Is it likely that there could be interruptions to the task sequence?
• How predictable are the required tasks?</td><td>Experience and Training
• What is the balance of experience in a typical control room/field crew?
• How often is this type of scenario covered in training? Does the training focus on task steps and how realistic is the training?
• Is the training simulator or desktop based? Does it include a detailed talk-through and simulation of the event?
• Do control room operators typically have field experience and knowledge of local facility conditions?</td></tr>
<tr><td>Procedures and Supporting Documentation
• Is there a formal written procedure for this event and would the operator typically use this?
• How accurate and relevant are the procedures?
• Are procedures readily available and easy to access? Are they user-friendly?
• Are the procedures regularly updated?
• How familiar are operators with the procedures for this event?
• Are important steps highlighted in the procedures?</td><td>Human-Machine Interface
• Which HMIs are considered most important for this event, and are they easily accessible and usable?
• How familiar are the operators with using the HMIs?
• Is the labelling, use of symbols, colours and other cues consistent?
• Are there any diagnosis / decision support features?
• Are there any features of the HMI that could mislead the operators?</td></tr>
</table>

Attitudes to Safety, Work and Management Support	Teamwork
• Have the operators ever experienced events where they were not sure how to respond with respect to safety? • Is there a formal, written philosophy for how to act in situations of doubt (e.g., if in doubt, shutdown)? • Is there an agreed philosophy between operators for how to act in situations of doubt, and is this different from the formal philosophy? • Is there clear support from management, both prior to and after the event, to prioritize safety in such events?	• Does this event require teamwork in order to successfully control and manage the situation? • Are tasks distributed between several people? Who in the team is responsible for what? • What kind of communication is needed to perform the required tasks successfully? When is this communication needed (at which task steps)? • Does the event require clear leadership or line of command? • How is information shared between the different people involved in the event? • Is there a clear, shared understanding of roles and responsibilities amongst the people involved in the event?
Physical Working Environment • What tools or equipment are needed for the operators to perform the required tasks, and are these easily available and user-friendly? • Can the operator easily access the location where the necessary tasks are performed? • Are there any aspects of the task that are physically demanding? • What are the environmental conditions within which the task is likely to be performed? • For tasks outside the control room, could certain weather conditions make the task more difficult? • For tasks inside the control room (or other room), is the heating and lighting sufficient for the operator to perform the task?	

A.5 The SHERPA Error Taxonomy

The SHERPA (Embrey, 1986) taxonomy presented in Table 21 provides a good approximation for considering errors in the task analysis. This simple taxonomy aligns well with the level of detail in the Petro-HRA method. The analyst can select another error taxonomy if this one better aligns with the types of tasks being modelled through the task analysis. Note that the taxonomy is a tool to prompt the analyst to think about what potential errors could exist. It should not be used as an error classification tool since categorisation of errors, per se, is neither necessary nor useful in Petro-HRA.

The SHERPA taxonomy considers mainly action, checking, and communication errors. It does not explicitly consider decision errors, although they are implied in some taxonomic items like *A10–Wrong operation on wrong object*. For the analyst to consider opportunity for cognitive error adequately, it is recommended that additional decision items be added to the SHERPA taxonomy. Table 22, presents suggested decision errors to augment SHERPA's taxonomy. Note that these decision errors may overlap with items in the SHERPA taxonomy. This overlap is inconsequential to the analysis.

Table 21: The SHERPA error taxonomy

Action Errors	**Checking Errors**
A1-Operation too long/short	C1-Check omitted
A2-Operation mistimed	C2-Check incomplete
A3-Operation in wrong direction	C3-Right check on wrong object
A4-Operation too little/much	C4-Wrong check on right object
A5-Misalign	C5-Check mistimed
A6-Right operation on wrong object	C6-Wrong check on wrong object
A7-Wrong operation on right object	**Retrieval Errors**
A8-Operation omitted	R1-Information not obtained
A9-Operation incomplete	R2-Wrong information obtained
A10-Wrong operation on wrong object	R3-Information retrieval incomplete
Information Communication Errors	**Selection Errors**
I1-Information not communicated	S1-Selection omitted
I2-Wrong information communicated	S2-Wrong selection made
I3-Information communication incomplete	

Table 22: Additional decision error taxonomy

Decision Errors
D1-Correct decision based on wrong/ missing information
D2-Incorrect decision based on right information
D3-Incorrect decision based on wrong/ missing information
D4-Failure to make a decision (impasse)

A.6 Guidance on Assessment of Teamwork Factors

Table 23: Definition of Teamwork factors and behavioural markers for the Teamwork factors

Factors	Definition	Behavioral markers
Team leadership	Ability to direct and coordinate the activity of other team members, assess team performance, assign tasks, develop team knowledge, skills, and ability, motivate team members, plan and organize, and establish a positive atmosphere.	Facilitate team problem solving. Provide performance expectations and acceptable interaction patterns. Synchronize and combine individual team members' contributions. Seek and evaluate information that affects team function. Clarify team member roles. Engage in preparatory meetings and feedback sessions with the team.
Mutual performance monitoring	The ability to develop common understanding of the team environment and apply appropriate task strategies to accurately monitor team-mate performance.	Identifying mistakes and lapses in other team members' actions. Providing feedback regarding team member action to facilitate self-correction.
Backup behavior	Ability to anticipate other team members' needs through accurate knowledge about their responsibilities. This included the ability to shift workload among members to achieve balance during high periods of workload and pressure.	Recognition by potential backup providers that there is a workload distribution problem in their team. Shifting of work responsibility to underutilized team members. Completion of the whole tasks or parts of tasks by other team members.
Adaptability	Ability to adjust strategies based on information gathered from the environment through the use of backup behavior and reallocation of intra-team resources. Altering a course of action or team repertoire in response to changing conditions (internal or external).	Identify causes of a change that has occurred, assign meaning to that change, and develop a new plan to deal with the changes. Identify opportunity for improving and innovation for habitual or routine practices. Remain vigilant to changes in the internal and external environment of the team.
Team orientation	Propensity to take other's behavior into account during group interaction and the belief in the importance of the goals over individual members' goals.	Taking into account alternative solutions provided by team-mates and appraising their input to determine what is correct. Increased task involvement, information sharing, strategizing, and participatory goal setting.
Shared mental models	An organizing knowledge structure of the relationships among the task the team is engaged in and how the team members will interact.	Anticipating and prediction of each other's needs. Identify changes in the team, task, or team-mates and implicitly adjust strategies as needed.
Mutual trust	The shared belief that team members will perform their roles and protect the interests of their team-mates.	Information sharing. Willingness to admit mistakes and accept feedback.
Closed loop communication	The exchange of information between a sender and a receiver irrespective of the medium.	Following up with team members to ensure message was received. Acknowledging that a message was received. Clarifying with the sender of the message that the message received is the same as the intended message.

A.7 How to Select PSFs to Avoid Double Counting

Table 24: Advice for selection of PSFs to avoid double counting

PSF1	PSF2	Advice
Time	Task Complexity	Usually a more complex task takes longer than a less complex task. In the selection of PSF levels the analyst should evaluate if a negative or positive level on Time accounts for the effect of Task Complexity (then only select positive/negative levels on Time) or if the analyst finds evidence that Task Complexity is a performance driver in addition to the complex task taking longer/shorter time.
Time	Experience/Training	If the operator(s) think that there is much more or much less available time than they objectively need (subjective time pressure). This should be accounted for by the Experience/Training PSF since the operator(s) does not have a realistic picture of the scenario development.
Time	Teamwork	Poor teamwork usually causes more time to be spent and good teamwork may require less time. The analyst has to decide if the effect of poor/good teamwork is accounted for by more/less time used (only select Time levels) or if teamwork is also a performance driver beyond the effect on Time (select negative/positive levels on both Time and Teamwork).
Threat Stress	Attitudes to Safety, Work and Management Support	If a negative level of Attitudes to Safety, Work and Management Support is chosen, for example if the operator does not have management support to do the task, this might cause Threat Stress (threat to self-esteem). In this situation only the negative level of Attitudes to Safety, Work and Management Support should be selected since that is the main performance driver.
Threat Stress	Experience/Training	Experience/Training on a task reduces Threat Stress. Specific training for stress exposure also reduces Threat Stress. When evaluating Threat Stress the analyst should look at this PSF in combination with the Experience/Training PSF in such a way that if Experience/Training is high and/or if adequate specific training on stress exposure is given, Threat Stress should not be seen as a performance driver.
Task Complexity	Procedures	If the complexity of the procedures is found to be a performance driver, this should be counted with the Procedures PSF and not Task Complexity. It the task is also high or low on complexity, it should be evaluated if Task Complexity is also a performance driver in addition to Procedures.
Task Complexity	Human-Machine Interface	If Human-Machine Interface causes a task to be complex or low on complexity this should be accounted for by the Human-Machine Interface PSF and not the Task Complexity PSF. It the task is also high or low on complexity, it should be evaluated if Task Complexity is also a performance driver in addition to Human-Machine Interface.
Task Complexity	Experience/Training	If Experience/Training cause a task to be complex or low on complexity this should be accounted for by the Experience/Training PSF and not the Task Complexity PSF.
Task Complexity	Teamwork	A task that is complex or less complex might require more or less demanding teamwork. In this situation the analyst has to decide if it is Task Complexity, or Teamwork, or both, that is the main performance driver.

Experience/Training	Procedures	Experience/Training on the procedures in itself should be accounted for in the Procedures PSF. A poor procedure might not be a performance driver if there is training to compensate for the poor procedure.
Experience/Training	Human-Machine Interface	Training on the HMI should be accounted for in the Human-Machine Interface PSF. A poor HMI might not be a performance driver if the operators have much Experience/Training in using the interface.
Experience/Training	Teamwork	Experience/Training on Teamwork should be accounted for in the Teamwork PSF. If Experience/Training on Teamwork is adequate this would probably improve team performance.
Attitudes to Safety, Work and Management Support	Teamwork	If management take an active role during the scenario/task and they are active team members, this influence should be evaluated under the Teamwork PSF and not Attitudes to Safety, Work and Management Support.

Acknowledgements

The Petro-HRA method was developed in an R&D project called “Analysis of human actions as barriers in major accidents in the petroleum industry, applicability of human reliability analysis methods”, Project no. 220824/E30. The sponsors were the Research Council of Norway and Equinor Petroleum AS, and DNV provided resources as an industrial partner. The method was developed in a joint effort by the Institute for Energy Technology (IFE, project owner), the Norwegian University of Science and Technology (NTNU), DNV, SINTEF Technology and Society, the Idaho National Laboratory and Equinor.

The board of the R&D project met three times per year over the course of this project, and the authors of this guideline want to thank Eli Cecilie Bech, Equinor; Andreas Falck, DNV; and Lars Bodsberg, SINTEF; for their support and good supervisory advice.

Draft versions of the method were applied on two test cases. The first test case was at the Equinor Kårstø processing facility, studying a manually activated blowdown scenario at the facility. The second test case was on the dynamic positioning system of a drilling rig owned by Transocean. The authors of this report want to give a warm thanks to Equinor Kårstø and Transocean for enabling the tests of the method, and to all the people involved in these tests for their help, understanding, and focus to improve safety.

During the autumn of 2016, the method was applied to a First Use case at Hammerfest LNG in Equinor, by Marius Fernander and Sondre Øie, DNV. This case led to several improvements of the method, and the authors want to thank Hammerfest LNG and Marius Fernander for lots of constructive feedback.

The Petro-HRA method used the Standardized Plant Analysis Risk-Human Reliability Analysis (SPAR-H) method as the basis for the quantification model. An early version of Petro-HRA was discussed with one of the main authors of SPAR-H in the summer 2014, at the PSAM-12 conference. The authors want to express a warm thanks to Harold Blackman for good comments and feedback.

The authors want to thank Ron Farris, INL, who has helped tremendously with the Task Analysis library template.

The authors want to thank the following persons from DNV for specific guidance on how to calculate time available, as well as concrete feedback and quality assurance on QRA: Erling Håland; Kjetil Holter Næss; Katharina Gouzy-Hugelmeier; Andreas Falck.

We also appreciate the review and comments from several people in Equinor.

Revision 1 of the method was funded by Equinor. The authors of Revision 1 wish to thank the following people from Equinor for their guidance, feedback and review comments on the second revision: Eli Cecilie Bech, Jan Tore Ludvigsen and Arne Jarl Ringstad.

Major Updates to Revision 1

Since the publication of the method in 2017, it has been applied in several petroleum projects in Norway. In 2020, Equinor initiated a project with DNV and IFE to conduct a series of structured interviews with users and stakeholders. The method has been updated in accordance with the feedback received.

The guideline has now been split into two documents:

- Part 1 The Petro-HRA Method: Step-by-Step Instruction
- Parts 2 & 3 Case Study Example & Background Information for the Petro-HRA method

Some typographical and grammatical errors have been corrected throughout the document. The text in some sections has been modified for clarity, and new or modified examples have been provided to better explain how to apply the guidance. In addition, the following major updates were made:

Section number & title	Explanation of change
1.1 Participate in Initial Meetings	Inclusion of a note regarding the timing of the HRA in relation to the maturity of the QRA, and the need to clarify the expectations from the HRA if performed very early in the QRA process.
2.5 Conduct an Initial Timeline Analysis	Detailed information on how to perform a timeline analysis now included in the Part 1 Step-by-Step guidance.
4.2 Cognitive Dependency & Human Error	Guidance on cognitive dependency and human error has been moved to Step 4: human error identification (originally in Step 5), as this is when the analyst should start investigating whether cognitive dependency could be present.
6.1.1 Decide the Appropriate Task Level for Quantification	Sub-section added to provide guidance on determining the appropriate task level for quantification.
6.1.2 Apply the Nominal Human Error Probability	Clarification of the meaning of “nominal HEP”.
6.1.5 Calculate the Human Error Probability for the Task	Inclusion of an explanation to demonstrate the effect on the Human Error Probability (HEP) of selecting different multipliers; the aim is to illustrate the importance of carefully selecting the most appropriate multiplier to avoid ending up with an overly optimistic/conservative HEP.
6.3 Advice on Double Counting	Inclusion of an example from the SPAR-H Step-by-Step guideline to clarify the guidance on double counting.
7.1.3 Predictive Adjustment of HEPs based on Implementation of ERMs or ERSs	New sub-section added to provide guidance on how to predictively adjust HEPs, to illustrate the effect of implementation of ERMs or ERSs.
7.3 Good Practices for Human Error Reduction	Additional bullet points added to the list of “good practices for human error reduction” to reinforce the need for specific, actionable recommendations.
Appendix A	Specific resources, tables and guidewords for the analyst to use during the HRA have been moved to Appendix A for easier access when applying the method.