The Petro-HRA Guideline

Revision 1

Vol. 2

IFE/E-2022/002

Report number: IFE/E-2022/002	ISSN: 0000-0000	Availability: Public	Publication date: 17.01.2022
Revision: 1	ISBN: 978-82-7017-938-1	DOCUS-ID: 55193	Number of pages: 141

Client: (Original) Norges Forskningsråd; (Rev. 1) Equinor

Title:
The Petro-HRA Guideline, Rev.1, Vol.2

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
ATHEANA	A Technique for Human Event Analysis
BOP	Blowout Preventer
BVP	Blood Volume Pulse
BWR	Boiling Water Reactor
C&E	Cause and Effects
CAP	Corrective Action Program
CCR	Central Control Room
CCTV	Closed Circuit Television
CSE	Concept Safety Evaluation
DGPS	Differential Global Positioning System
DSHA	Defined Situations of Hazard and Accident
EDS	Emergency Disconnect Sequence
EPA	Emergency Preparedness Analysis
EPA	Environmental Protection Agency
EQD	Emergency Quick Disconnect
ERA	Error Reduction Analysis
ERM	Error Reduction Measure
ERO	Engine Room Operator
ERS	Error Reduction Strategy
ESD	Emergency Shutdown
ETA	Event Tree Analysis
F&G	Fire and Gas
FTA	Fault Tree Analysis
GSR	Galvanic Skin Response
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
HPR	Hydroacoustic Position Reference
HR	Heart Rate
HRA	Human Reliability Analysis
HTA	Hierarchical Task Analysis
IDHEAS	Integrated Decision-tree Human Error Analysis System
IE	Initiating Event
IEM	Internal Error Modes
IFE	Institute for Energy Technology
IR	Infra-Red

LEL	Lower Explosion Limit
LELm	Lower Explosion Limit -meter
LMRP	Lower Marine Riser Package
LOPA	Layers of Protection Analysis
LPSD	Low Power and Shutdown
N2	Nitrogen
NASA-TLX	National Aeronautics and Space Administration Task Load Index
NTNU	Norwegian University of Science and Technology
OAET	Operator Action Event Tree
OS	Operator Station
OSD	Operational Sequence Diagrams
PA	Public Announcement
PLC	Programmable Logic Controller
PLL	Potential Loss of Lives
PRA/PSA	Probabilistic Risk/Safety Assessment
PSF	Performance Shaping Factors
PST	Process Safety Time
QRA	Quantitative Risk Assessment
RCS	Reactor Coolant System
RHR	Residual Heat Removal
SGTR	Steam Generator Tube Rupture
SHARP	Systematic Human Action Reliability Procedure
SHERPA	Systematic Human Error Reduction and Prediction Approach
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SME	Subject Matter Expert
SPAR-H	Standardized Plant Analysis Risk – Human Reliability Analysis
STEP	Sequential Time Event Plotting
TA	Task Analysis
THERP	Technique for Human Error-Rate Prediction
TRA	Total Risk Analysis
TRACEr	Technique for the Retrospective and Predictive Analysis of Cognitive Errors
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).
Potential Loss of Lives (PLL)	The potential loss of life (PLL) is the expected number of fatalities within a specified population (or within a specified area A) per annum.
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).

1 Introduction

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 in the petroleum industry, also called Human Failure Events (HFEs) or Type C events. The probability of the HFE is called the human error probability (HEP) and this inputs directly to the quantitative risk assessment (QRA). The qualitative results of an HRA are just as important as the quantitative results. 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 consists of the following steps:

1) **Scenario definition**. The scenario definition defines the scope and boundaries of the analysis and shapes the subsequent qualitative and quantitative analyses. This step includes reviewing the QRA model to understand the context of the HRA within the overall risk assessment and system for managing safety barriers.
2) **Qualitative data collection**. Collect specific and focused data from site visits, interviews and discussions with operators and documentation reviews, 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.
3) **Task analysis**. Describe the steps (i.e., human actions) that are carried out as part of an activity. Task analysis provides a systematic means of organizing information collected around the tasks with the aim of translating this into a level of detail suitable for the HRA and QRA.
4) **Human error identification**. Identify potential errors associated with task steps in the scenario, describe the likely consequences of each error, identify recovery opportunities, and describe the performance shaping factors (PSFs) that may have an impact on error probability.
5) **Human error modelling**. Model the tasks in such a way that when individual tasks are quantified according to Step 6, the model logic can be used to calculate the HEP for the HFE that is then input to the QRA.
6) **Human error quantification**. Quantify each chosen task or event based on a nominal value and a set of PSFs. Check the reasonableness of the HEPs.
7) **Human error reduction**. Develop risk-informed improvement initiatives to reduce the human contribution to risk. Such improvements aim at either preventing the occurrence of human errors or mitigating their consequences.

Documentation of the Petro-HRA is not included as a methodological step, but it is mentioned here as it is considered an essential part of the HRA process. Key information should be documented throughout the HRA, such as information about the scope and boundaries of the analysis, any assumptions made about the scenario, system or human operators, screening decisions made during the analysis, etc. This information is important to document to ensure traceability and transparency of the Petro-HRA, and to provide a solid evidence base for the analysis results. Advice on how to document the HRA is provided later in this guideline.

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. 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.

1.1 How to Use this Guideline

The original Petro-HRA guideline (published in 2017) included three main parts:

- Part 1 includes the method description, presented as a step-by-step instruction.
- Part 2 includes a detailed case study example, demonstrating how the method was applied to the analysis of drive-off scenario for an offshore semi-submersible drilling unit.
- Part 3 includes background information on the scientific basis for the PSFs, as well as a wider discussion of the method.

For this updated version, the guideline has now been separated into two documents to facilitate ease of use:

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

Part 2
The Petro-HRA Method:
Case Study Example

2 Case Study 1: Drive-off of a Semi-Submersible Drilling Unit

Note: All error probabilities shown in this case study example are fictive and not related to the actual case. They are included here for illustrative purposes only.

This case study describes the analysis of a drive-off scenario of a semi-submersible drilling unit (Figure 1) in shallow waters (320m or less) on the Norwegian Continental Shelf. To avoid potential damage during a drive-off, the drilling unit should maintain position above the wellhead where the drilling operations are carried out. Positioning is maintained autonomously, without a mooring system, through the action of a set of thrusters controlled by the Dynamic Positioning (DP) system.

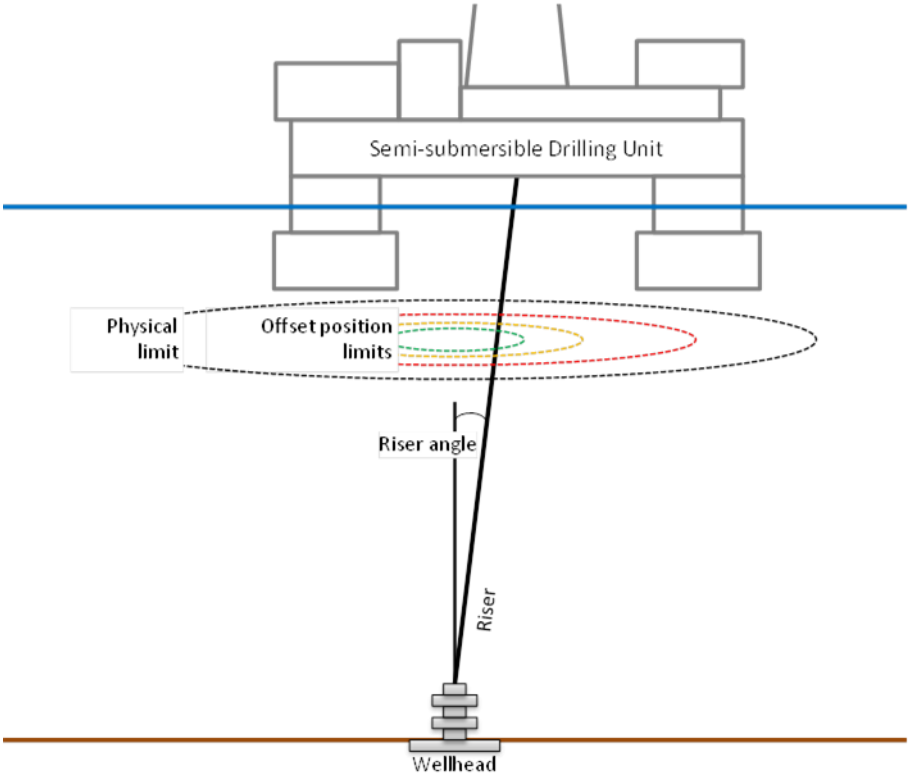

Figure 1: Case Study 1 - Dynamic Positioning drilling operations

Input to the DP system is provided by a diverse position reference system, including a Differential Global Positioning System (DGPS) and a Hydroacoustic Position Reference (HPR) system. A Dynamic Positioning Operator (DPO) is located in the Marine Control Room (MCR) on the drilling unit at all times and is responsible for constant monitoring of DP panels and screens, and for carrying out emergency procedures if needed.

The position of the drilling unit can be lost because of a number of reasons. In this case study, it is assumed that some undetermined failure in the DP system initiates six out of the 8 thrusters to accelerate to full thrust in one direction, resulting in a “drive-off”. This is a low-probability but high-consequence event. In order to establish whether the unit is located within the safe operation area, specific offset position limits are defined (as shown in Figure 1). These limits are defined based on riser angle, position data and environmental variables (such as wind, current, etc.). The riser has a relatively low capacity of inclination, despite the upper and lower flex joints, and the maximum angle it can reach is 12 degrees. Exceeding this maximum limit can result in damage to the wellhead, the Blowout Preventer (BOP) that seals the well, or the Lower Marine Riser Package (LMRP), which connects the

riser and the BOP. For this reason, a conservative maximum angle of 8 degrees is considered in the limit calculation.

If the rig moves to an offset position, specific alarms will sound and indicate that the DPO should stop the thrusters and initiate the manual Emergency Disconnect Sequence (EDS) to disconnect the riser from the BOP. If the manual EDS fails, an automatic EDS will activate at the ultimate position limit (red limit) allowing the riser to safely disconnect from the BOP. Stopping the thrusters is considered a critical task; in shallow waters, if the thrusters have not been stopped before initiating EDS, the riser angle will be too steep to safely disconnect from the BOP. This is true even for automatic activation of the EDS. Operations in shallow waters also imply a shorter time for detection and position recovery for both the system and the human operators. For this reason, automatic EDS is always enabled in shallow waters.

2.1 Step 1: Scenario Definition

The first step in this case study was to define the major accident scenario that would be analysed using the Petro-HRA method. Information about the scenario was collected from a series of telephone meetings, as listed below.

- Kick-off meeting with representatives from the drilling unit operating company to discuss and agree the scope and plan for the Petro-HRA.
- Meeting with QRA analysts to understand how the drive-off scenario is modelled in the QRA event tree and to discuss whether there were any particular aspects that the Petro-HRA should focus on.
- Meeting with operating staff representatives to discuss the operator tasks and actions during the scenario, to discuss potential deviation scenarios and to clarify expectations and deliverables.

This information was supplemented by a review of documentation provided by the unit operating company, including system description documentation, system operating manuals and previous analyses that had been performed for that facility.

The scenario description template was used to collate the information collected at this point. At first, there were some information gaps in the scenario description, but these were later filled in after the qualitative data collection workshop. The full scenario description is shown in Table 1.

Table 1: Case Study 1 - Full scenario description

Topic	Description	Comments
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 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.	• 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
Personnel roles & 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*." • The engine room operator is always present in the MCR.
	Event sequence and duration	
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	• 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. • From the DP manual: "*In a Drive-Off event, stop thrusters, Initiate Red Alert and enable EDS immediately*." • The DPO2 may notify the driller.

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.	
End of event sequence (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.	
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).

Figure 2 (next page) shows an example of how the Human Failure Event (HFE) for this scenario would typically be represented in the QRA event tree (figure taken from Pedersen, 2015).

In this example, the HFE is represented as a single human task in the QRA, which is activation of the Emergency Quick Disconnect (EQD), also known as Emergency Disconnect Sequence (EDS). However, during discussions to define the scenario, the analysis team identified another essential operator action that occurs before activation of the EQD/EDS, which is to stop the thrusters. EDS takes 30 seconds from initiation to completion; if the thrusters are not stopped then the drilling unit will continue to move forwards during this time which could result in an incomplete disconnect from the well and subsequent damage to the wellhead and/or hydrocarbon release.

Note: The error probabilities shown in this example are fictive and are used for illustrative purposes only.

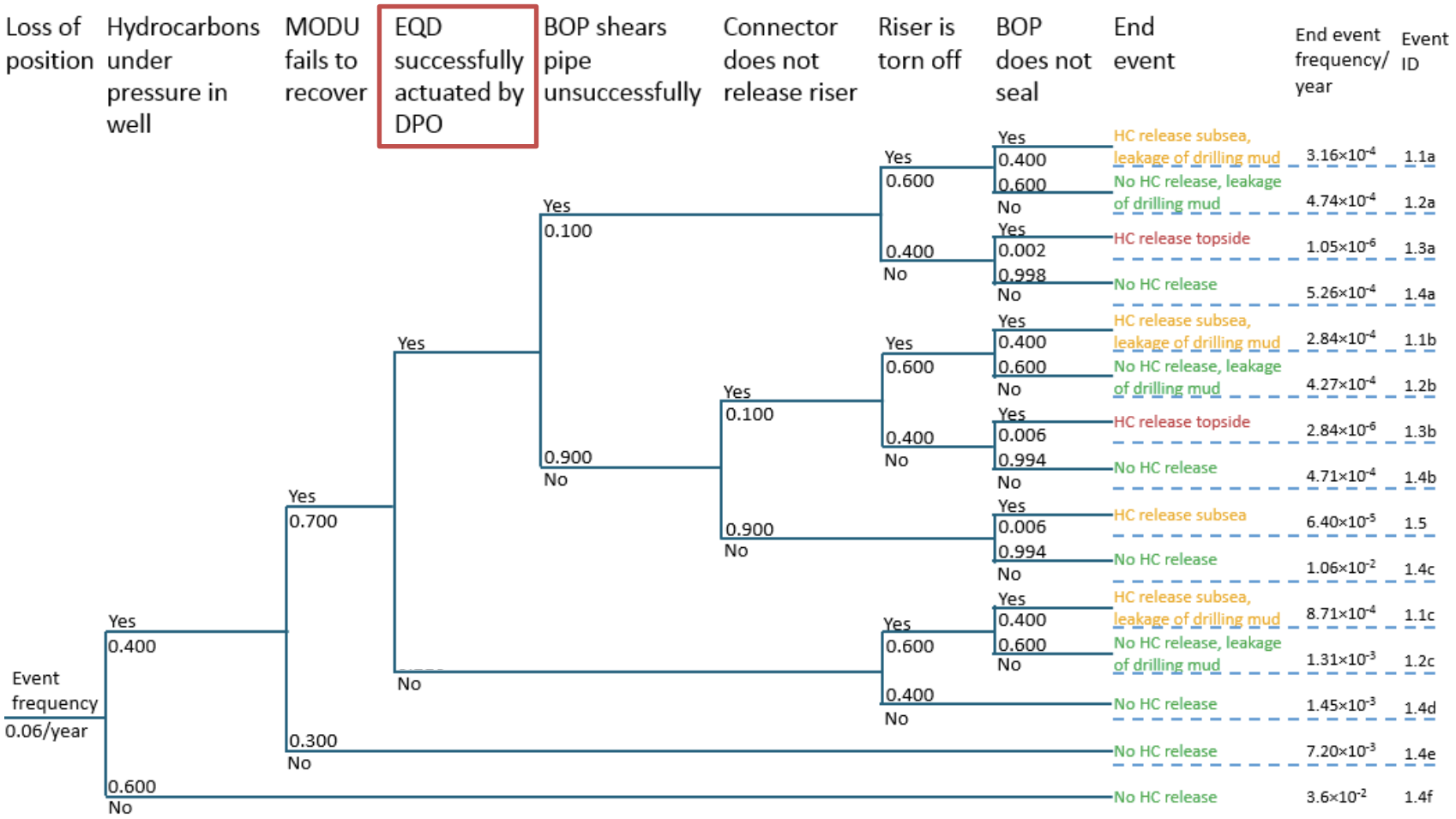

Figure 2: Case Study 1 - QRA event tree

2.2 Step 2: Qualitative Data Collection

The qualitative data collection for this case study was primarily conducted during a two-day workshop with four DP operators and a supervisor from the drilling unit. To prepare for the workshop, the HRA team reviewed and discussed the scenario information and documentation collected to date. The team developed a high-level Hierarchical Task Analysis (HTA), shown in Figure 3 (next page).

Population of the initial HTA was difficult as there were no operating procedures or instructions describing the required operator response in this scenario. The analysis team was provided with a document called the DP Manual which contained a single sentence descripting the response – "In a Drive-Off event, stop thrusters, Initiate Red Alert and enable EDS immediately" – but otherwise there was no documented information available detailing the operator tasks. Therefore, the initial HTA was decomposed to only two levels below the goal due to a lack of detail at this point in the analysis.

The initial HTA was used along with the detailed scenario description in Step 1 as a basis for discussion with the operators to understand the human actions that are performed in a drive-off scenario.

The main activities carried out during the workshop including reviewing and expanding the initial scenario description table, clarifying assumptions and uncertainties about the scenario, defining the boundaries of the scenario, reviewing and expanding the initial HTA, discussion of potential human errors and consequences of these errors and discussion of Performance Shaping Factors (PSFs) and the effects of these. The updated HTA is shown in Figure 4.

Figure 3: Case Study 1 - Initial HTA

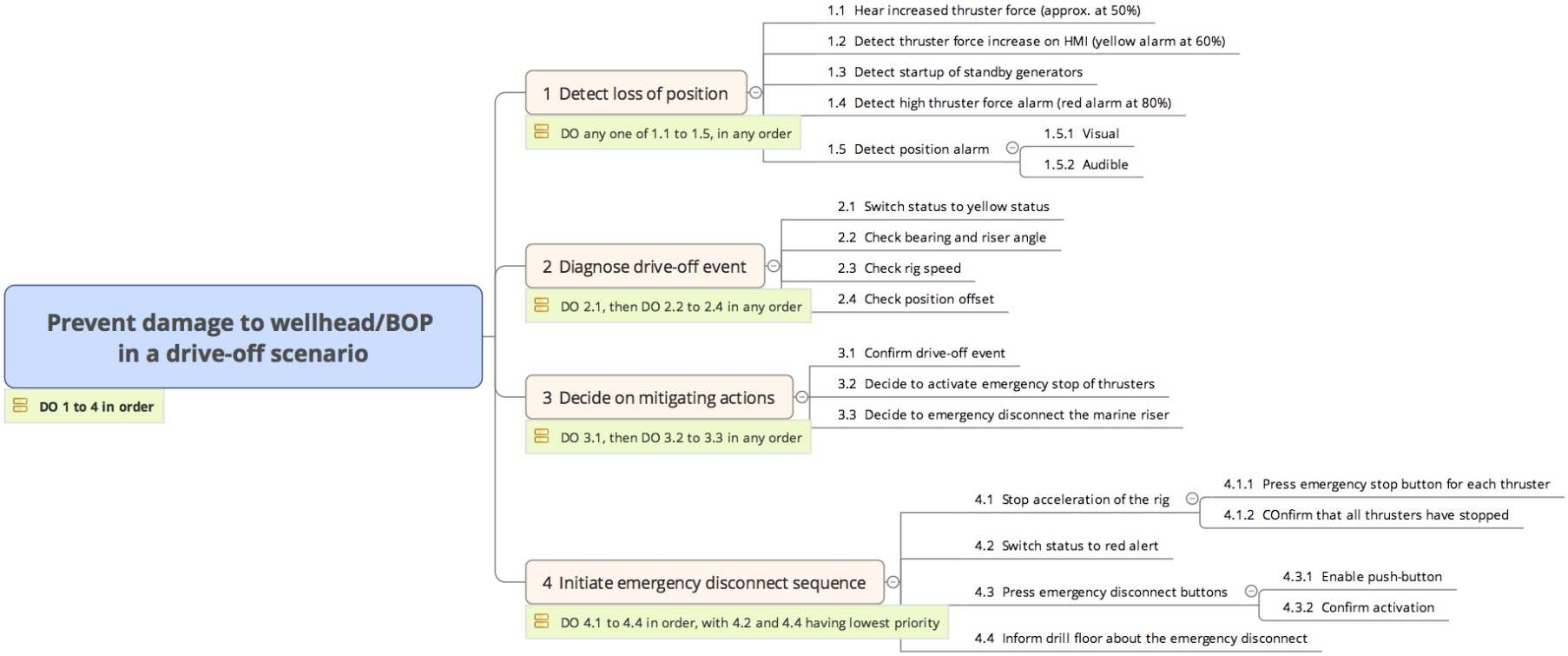

Figure 4: Case Study 1 - Updated HTA

2.3 Step 3: Task Analysis

As noted in the previous section, there was little documented information available describing the operator response to a drive-off scenario, and therefore the initial HTA was kept at a very high level. However, from the information provided by the DPOs and the supervisor in the workshop, it was possible to develop a more detailed HTA. The analysis team agreed that two levels of task decomposition (as shown in Figure 4) were sufficient for this case study because decomposition below this level would not have offered any additional insight into how the task was performed. For example, it was sufficient to describe Task 4.1.1 as “Press emergency stop button for each thruster” without having to list the task step for each button press below this. The action would be the same for each button press, and so it was sufficient to capture this in a single statement at a higher level.

2.3.1 Tabular Task Analysis

After the HTA was updated with information from the workshop, this was translated into a Tabular Task Analysis (TTA), to enable the team to document more details about the individual task steps and to use as a basis for error analysis and PSF evaluation. The TTA is shown in Figure 5, Figure 6, and Figure 7 on the next pages.

As these figures show, the task analysis has been expanded to include details about cues and feedback for each task step, the relevant HMIs and who is responsible for the step. The TTA also contains useful information about assumptions and uncertainties related to the task steps, relevant notes and additional information that the HRA team considered useful and that may be informative later on during error analysis or PSF evaluation

Step No	Description	Cue	Feedback	HMI	Person responsible	Assumptions	Notes
0	**PREVENT DAMAGE TO WELLHEAD / BOP IN CASE (FAST) DRIVE-OFF SCENARIO**					This is an analysis of a fast drive-off scenario, in which 5 out of 8 thrusters go from 0% to 100% thruster force in about 5 seconds. This scenario assumes calm weather conditions and no other vessels nearby.	
PLAN 0	DO 1 to 4 in order						
1	DETECT LOSS OF POSITION						
PLAN 1	DO one or more of 1.1 to 1.5 in any order						
1.1	Hear increased thruster force (at approx. 50%)	Audible sound of thruster increase			DPO 1	A sudden increase in force from 0% to 100% would create some unexpected noise that the DPO will be able to hear on the bridge.	
1.2	Detect thruster force increase on HMI	Increase in thrust force indicator bars; visual yellow warning at 50%		DPOS	DPO 1		DPO will always have the thruster main view open on the screen, showing thruster force.
1.3	Detect startup of standby generators						
PLAN 1.3	DO 1.3.1 and 1.3.2 in order						
1.3.1	Detect standby generator alarm	Visual and audible alarm		Power Management System (PMS) SVC	ERO	*The ERO is normally located in the Marine Control Room (MCR) during his watch. *The ERO could get some other alarms at the same time that could hide the standby generator alarm. *If the DPO has not already heard the thrusters increase or seen the increase in load on the HMI, then he is unlikely to notice these at this point – reliance on detection of alarms from here.	The ERO will first see a reduction in power, as power is diverted to the thrusters. The DPO will also see this on the DPOS.
1.3.2	Contact DPO to check system status	Standby generator alarm indicating thruster force increase	DPO will check and report on status		ERO	Because the ERO is located in the MCR, he can just talk to the DPO – does not have to contact him by telephone.	
1.4	Detect high thruster force alarm	Visual and audible red alarm at 80%		DPOS	DPO 1		
1.5	Detect position alarm	Visual alarm at 3m offset		DPOS	DPO 1	This analysis assumes that the position inputs are correct.	Operator sets the position offset limits, usually 3m warning (with a visual yellow warning) and 5m alarm (with an audible and visual red alarm).
2	DIAGNOSE DRIVE-OFF EVENT						The DPO contiuously monitors these screens as a normal part of his job. It could take up to 5 seconds from the thrusters starting up before he will see any change in rig position on the screens, therefore the DPO would have to check the screens a few times to be sure that a drive-off is occurring.
PLAN 2	DO 2.1 to 2.3 in any order, then DO 2.4						

Figure 5: Case Study 1 – TTA (1/3)

2.1	Check bearing and riser angle	Indications from Step 1.1 that rig status has changed		DPOS	DPO 1	The DPO will have been monitoring these screens anyway, as part of his normal duties while on watch, and so will quickly notice if there is an unexpected deviation in bearing or riser angle (or the other parameters listed below).	
2.2	Check rig speed	Indications from Step 1.1 that rig status has changed		DPOS	DPO 1		
2.3	Check position offset	Indications from Step 1.1 that rig status has changed		DPOS	DPO 1		
2.4	Confirm drive-off event	Parameter readings			DPO 1	Because this is such a fast scenario, the DPO will not have time to discuss or confirm what is happening with anyone else. He will make this diagnosis himself based on Steps 1.2 and 2.	This is a cognitive action that the DPO will perform himself.
3	DECIDE ON MITIGATING ACTIONS						
PLAN	DO 3.1 and 3.2 in any order						
3.1	Decide to initiate emergency stop of thrusters	DPO training and system knowledge			DPO 1	If the automatic EDS is initiated, the thrusters will also be automatically stopped.	The position offset of the rig is the most important parameter when diagnosing a drive-off event and deciding that the thrusters must be stopped. The riser angle is less vital, but supports the diagnosis based on position offset.
3.2	Decide to initiate emergency disconnect from the marine riser	DPO training and system knowledge			DPO 1		

Figure 6: Case Study 1 - TTA(2/3)

4	INITITATE EMERGENCY DISCONNECT SEQUENCE						The DPO will usually wait and monitor the rig for a few seconds to see how it is moving (i.e. Monitoring riser angle, rig speed, position offset, etc.). The drive-off evaluation report gives the DPO 30 seconds to diagnose the situation and decide what to do.
PLAN 4	DO 4.1 to 4.5 in order; 4.2 and 4.4 are highest priority						
4.1	Switch status to yellow alert	Diagnosis of drive-off event	Yellow light on DP Alert panel and yellow alarm line on DPOS	DP Alert Panel on DP Console	DPO1 or DPO2		This gives a pre-warning to the drill floor to prepare for disconnection. If the has time, the DPO would do this before the thrusters reach 100% force, but this is not a priority. The DP alert switch is located directly above the EDS initiation buttons, and so it is easy to access quickly.
4.2	Stop acceleration of the rig						
PLAN 4.2	DO 4.2.1 and 4.2.2 in order						
4.2.1	Press emergency stop button for each active thruster	Need to stop acceleration of the rig	Each emergency stop button will light up red when it is pressed, and DPOS will also indicate that thruster has been stopped	Thruster control panel	DPO1 or DPO2		
4.2.2	Confirm that thrusters have stopped	DPO has pressed the stop buttons for all active thrusters	RPMs on thruster panel and on DPOS, red light on each thruster control indicating emergency button pressed.	Load indicators on thruster heading panel	DPO1 or DPO2		
4.3	Switch status to red alert	DPO is about to initiate EDS	Red light on DP Alert panel and red alarm line on DPOS	DP Alert Panel on DP Console	DPO1 or DPO2		
4.4	Press emergency disconnect (EDS) buttons		EDS button lights up when pressed	EQD on DP Console	DPO1 or DPO2		The DPO must press the ENABLE and EDS buttons simultaneously to initiate the EDS.
4.5	Inform drill floor of disconnect	EDS has been manually initiated	Red flashing light & audible alarm on drill floor when EDS initiated.		DPO1 or DPO2		

Figure 7: Case Study 1 - TTA (3/3)

2.3.2 Timeline Analysis

It was evident from the beginning of the analysis that time is a critical factor in this fast-occurring scenario. After event initiation there is limited time to safely disconnect the rig from the well before damage to the well and subsea equipment can no longer be prevented. In this scenario, successful disconnection relies on the DPO detecting that something has gone wrong, diagnosing this as a drive-off event, and then acting to push the emergency thruster stop for each active thruster and initiate the EDS, all within seconds of the event occurring.

A timeline analysis was performed during the workshop with DPOs to estimate how much time would be required to perform the actions necessary to successfully disconnect from the well. The analysis identified how long each task step would take, measured in seconds, and whether it was possible for some task steps to be carried out in parallel. The estimates were based on the DPOs experience and knowledge of the system.

The timing and sequence of the main operator tasks identified in the task analysis are shown in Figure 8, with tasks plotted along the vertical axis and time in seconds plotted along the horizontal axis. The plotted numbers correspond to the descriptions provided in Table 2.

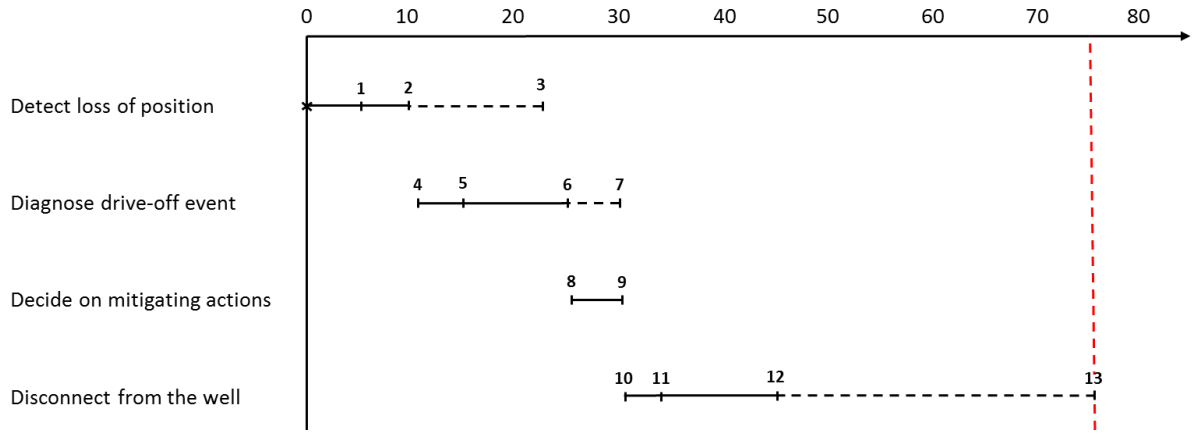

Figure 8: Case Study 1 - Timeline analysis diagram

Table 2: Case Study 1 - Timeline analysis table

Task	Step times	Comments
Detect loss of position	0. Drive-off failure occurs at 0 seconds. 1. After Time=5 seconds, at approximately 50% thruster force, DPO will hear noise generated from abnormal thruster rev. 2. From Time=5 seconds to Time=10 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=23 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 DP Drive-off Evaluation study 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. • NOTE: According to the results from the Drive-off Evaluation study, 50% thruster force will be achieved at approximately 0.60 to 0.70 meters offset and after 12-13 seconds. This is 7-8 seconds later than what was reported by the DPOs. Nevertheless, the input from the DPOs is used as basis in this timeline analysis.
Diagnose drive-off event	4. 5 seconds after noticing increased thruster rev and sound, at Time=10 seconds, the DPO starts diagnosing the event by checking riser angle, rig speed, and position offset. 5. Realizing that the rig is in a degraded situation, the DPO switches to yellow status at Time=15 seconds. At this time it would also be natural to call on the second DPO for support. 6. 15 to 20 seconds is required to confirm drive-off by iteratively examine trends of various parameters, making the diagnosis last until approximately Time=10 to 25 (or 30) seconds. 7. The last 5 seconds of performing the diagnosis, from Time=25 to 30 seconds, the DPO(s) start deciding on how to act.	• In the workshop it was argued that 20 seconds for diagnosis is a conservative estimate.
Decide on mitigating actions	8. The decision to stop thrusters and disconnect happens during the final stages of diagnosing the event, from Time=25 to 30 seconds. This involves the cognitive and interpersonal (i.e. communication) actions required for the DPO to conclude on how to deal with the drive-off. 9. Decision to stop thrusters and activate EDS was assessed to be made at approximately Time=30 seconds.	• It can be argued that 5 seconds for decision making is optimistic, especially if it involves some communication between DPO1 and DPO2.

Initiate emergency disconnect sequence	10. At Time=30 seconds the DPO activates red status to alert the drill floor that the rig is about to disconnect from the well. 11. Three seconds later, at Time=33 seconds, the DPO starts stopping the 6 thrusters in service, which is estimated to take approximately 10 seconds (completed at Time=43 seconds). 12. Two seconds after having stopped all 6 thrusters the DPO activates the EDS by pushing the EQD push-button at Time=45 seconds (enable button plus EQD activation button). 13. The EDS2 takes 30 seconds to complete which makes the LMRP disconnect from the BOP at Time 75 seconds.	• During the workshop it was argued that for some DPOs on duty it would be natural for DPO1 to call on DPO2 for assistance from this point. DPO1 would be calling the shots, telling DPO2 to stop the thrusters while he or she activates red status (if time) and pushes the EDS button. However, this is not written anywhere and there is no training and work practice on how to share these tasks. Consequently, the Petro-HRA team argues that the sharing of tasks between the DPOs cannot be claimed. Instead the Petro-HRA analysts have updated the timeline analysis to account for only one DPO carrying out the task (with the exception of some communication between the DPO1 and DPO2 during the diagnosis and decision making stage). • 10 seconds for stopping 6 thrusters in service equals about 1.7 seconds per emergency push-button. For this task alone, i.e. stopping the thrusters, this can be argued as being an optimistic estimate.

2.4 Step 4: Human Error Identification

During the workshop, the analysis team asked the DPOs about potential human errors that could occur during this scenario, and the likely consequences of these errors. There was not enough time during the workshop to do a detailed error analysis with the DPOs; however, the analysis team collected sufficient information about the scenarios to perform a detailed error analysis afterwards.

Using the TTA as a basis for the analysis, for each task step and sub-step, the analysis team considered what errors could occur, what the consequences of those errors might be, and whether there were opportunities for the operator to recover from these errors. The TTA was expanded to include additional columns to document the output of the analysis for the relevant task step or sub-step.

Next the analysis team performed a short screening exercise to decide whether each error would be analysed further for the remainder of the Petro-HRA. Errors that were considered to have (relatively) insignificant consequences for this scenario and/or that had high potential for recovery were not analysed further. This screening exercise enabled the analyst team to focus on the errors that the believed were more likely to cause problems during a drive-off scenario.

Figure 9, Figure 10, Figure 11 and Figure 12 show the TTA with additional columns for human error identification. Note that all of this information is contained within a single spreadsheet; some of the columns from the TTA have been hidden in the figures on the next pages for improved readability in this guideline.

Step No	Description	Potential Error	Likely Consequences	Recovery Opportunity	Further analysis?	Basic Event Ref.	PSF
0	**PREVENT DAMAGE TO WELLHEAD / BOP IN AHE (FAST) DRIVE-OFF SCENARIO**						
PLAN 0	DO 1.1 to 1.4 in order						
1	DETECT LOSS OF POSITION						
PLAN 1	DO one or more of 1.1 to 1.5 in any order						
1.1	Hear increased thruster force (at approx. 50%)	DPO does not hear sound of thrusters increasing	Delayed detection of the event	Additional indications in Steps 1.2 to 1.5	N		
1.2	Detect thruster force increase on HMI	DPO does not detect increase in thruster force on HMI	Delayed detection of the event	Additional indications in Steps 1.3 to 1.5	N		
1.3	Detect startup of standby generators						
PLAN 1.3	DO 1.3.1 and 1.3.2 in order						
1.3.1	Detect standby generator alarm	ERO does not detect standby generator alarm	Delayed detection of the event	Additional indications (for DPO) in Steps 1.4 or 1.5	N		
		ERO misdiagnoses standby generator alarm	Delayed detection of the event	Additional indications (for DPO) in Steps 1.4 or 1.5	N		
1.3.2	Contact DPO to check system status	ERO does not contact the DPO to check system status	Delayed detection of the event	Additional indications (for DPO) in Steps 1.4 or 1.5	N		
1.4	Detect high thruster force alarm	DPO does not detect high thruster force alarm	Delayed detection of the event	Alarm at Step 1.5	Y	*1 *4	*HMI (-) *Teamwork (+)
1.5	Detect position alarm	DPO does not detect position alarm	Unlikely to detect loss of position before automatic EDS is initiated	None (but automatic EDS will initiate)	Y	*2 *5	*HMI (-)

Figure 9: Case Study 1 - Human error identification table (1/4)

2	DIAGNOSE DRIVE-OFF EVENT				Y	*2 *5	*Experience/Training (-) *Teamwork (+)
PLAN 2	DO 2.1 to 2.3 in any order, then DO 2.4						
2.1	Check bearing and riser angle	DPO does not check bearing and riser angle	Uncertainty or delay in diagnosis of event	Additional checks in Steps 2.2 and 2.3	N		
		DPO misreads/ misdiagnoses bearing and riser angle indications	Unlikely to diagnose loss of position before automatic EDS is initiated	Additional checks in Steps 2.2 and 2.3	(Y)		
		Check takes too long	Insufficient time to manually activate EDS	None (but automatic EDS will initiate)	(Y)		
2.2	Check rig speed	DPO does not check rig speed	Uncertainty or delay in diagnosis of event	Additional checks in Steps 2.1 and 2.3	N		
		DPO misreads/ misdiagnoses rig speed	Unlikely to diagnose loss of position before automatic EDS is initiated	Additional checks in Steps 2.1 and 2.3	(Y)		
		Check takes too long	Insufficient time to manually activate EDS	None (but automatic EDS will initiate)	(Y)		
2.3	Check position offset	DPO does not check rig speed	Uncertainty or delay in diagnosis of event	Additional checks in Steps 2.1 and 2.2	N		
		DPO misreads/ misdiagnoses rig speed	Unlikely to diagnose loss of position before automatic EDS is initiated	Additional checks in Steps 2.1 and 2.2	(Y)		
		Check takes too long	Insufficient time to manually activate EDS	None (but automatic EDS will initiate)	(Y)		
2.4	Confirm drive-off event	DPO does not diagnose that this is a drive-off event	DPO will not stop thrusters and disconnect	None (but automatic EDS will initiate)	Y	*2 *5	*Experience/Training (-)

Figure 10: Case Study 1 - Human error identification table (2/4)

3	DECIDE ON MITIGATING ACTIONS						
PLAN 3	DO 3.1 and 3.2 in any order						
3.1	Decide to initiate emergency stop of thrusters	DPO does not realise that thrusters should be stopped first before initiating EDS	Minor damage to wellhead / BOP if rig continues to move after EDS is initiated	None	Y	*2	*Procedures (-)
		Decision to stop thrusters takes too long	Insufficient time to manually activate EDS	None (but automatic EDS will initiate)	Y	*1	*Threat Stress (-) *Adequacy of organization (-)
3.2	Decide to initiate emergency disconnect from the marine riser	DPO decides not to initiate EDS	EDS not manually initiated (but automatic EDS will initiate)	None (but automatic EDS will initiate)	Y	*5	*Threat Stress (-) *Adequacy of organization (-)
		Decision to initiate EDS takes too long	Insufficient time to manually activate EDS	None (but automatic EDS will initiate)	Y	*4	*Threat Stress (-) *Adequacy of organization (-)
4	INITITATE EMERGENCY DISCONNECT SEQUENCE						
PLAN 4	DO 4.1 to 4.5 in order; 4.2 and 4.4 are highest priority						
4.1	Switch status to yellow alert	DPO does not switch status to yellow alert	Drill floor not warned to prepare for disconnect	N/A (consequences not significant for this analysis)	N		
		DPO does not switch status to yellow alert in time	Drill floor not warned to prepare for disconnect	N/A (consequences not significant for this analysis)	N		
4.2	Stop acceleration of the rig						
PLAN 4.2	DO 4.2.1 and 4.2.2 in order						
4.2.1	Press emergency stop button for each active thruster	DPO does not press the emergency stop buttons for all active thrusters	Rig continues to move off position, potential minor damage to wellhead / BOP	Confirmation at Step 4.2.2	N		
		DPO takes too long to press the buttons for all active thrusters	Rig continues to move off position, potential minor damage to wellhead / BOP by the time the EDS is initiated	None	Y	*1	*HMI (-)
		DPO stops the wrong thrusters (i.e. The wrong 6 out of 8)	Rig continues to move off position, potential minor damage to wellhead / BOP by the time the EDS is	Confirmation at Step 4.2.2	Y	*3	*HMI (-) *Threat Stress (-) *Available time (-)

Figure 11: Case Study 1 - Human error identification table (3/4)

4.2.2	Confirm that thrusters have stopped	DPO does not confirm that all active thrusters have stopped	Rig continues to move off position, potential minor damage to wellhead / BOP by the time the EDS is initiated	None	Y	*3	*Procedures (-) *Experience / Training (-)
4.3	Switch status to red alert	DPO does not switch status to red alert	Drill floor not warned that EDS has been initiated	N/A (consequences not significant for this analysis)	N		
		DPO does not switch status to red alert in time	Drill floor not warned that EDS has been initiated	N/A (consequences not significant for this analysis)	N		
4.4	Press emergency disconnect (EDS) buttons	DPO does not press EDS buttons	EDS not manually initiated (but automatic EDS will initiate)	None (but automatic EDS will initiate)	Y	*5	*Threat stress (-) *Adequacy of organization (-) *Available time (-)
		DPO takes too long to press EDS buttons	Automatic EDS initiated	None (but automatic EDS will initiate)	Y	*4	*Available time (-)
4.5	Inform drill floor of disconnect	DPO does not inform drill floor that EDS has been initiated	Drill floor not warned that EDS has been initiated	N/A (consequences not significant for this analysis)	N		

Figure 12: Case Study 1 - Human error identification table (4/4)

2.5 Step 5: Human Error Modelling

The original branch of the QRA event tree for this drive-off scenario was not very detailed and contained only two actions: “close BOP” (Blow Out Preventer) and “disconnect riser”. Both of these actions are actually contained within a single operator action, which is to activate the Emergency Disconnect Sequence (EDS). The EDS automatically performs the actions of closing the BOP and disconnecting the riser.

As noted earlier, the QRA event tree did not include an operator action to stop the thrusters, although this was later identified as a critical action in the Petro-HRA. Therefore, a separate Operator Action Event Tree (OAET) was developed to adequately capture the human actions in this scenario, as shown in Figure 13.

As the figure shows, the top events in the OAET closely align with the main task steps in the task analysis – namely the detection, diagnosis, decision and action steps. Each of these top events is considered a Human Failure Event (HFE) and is subsequently quantified separately. Each HFE may be the result of one or several of the potential errors identified in the previous human error identification step.

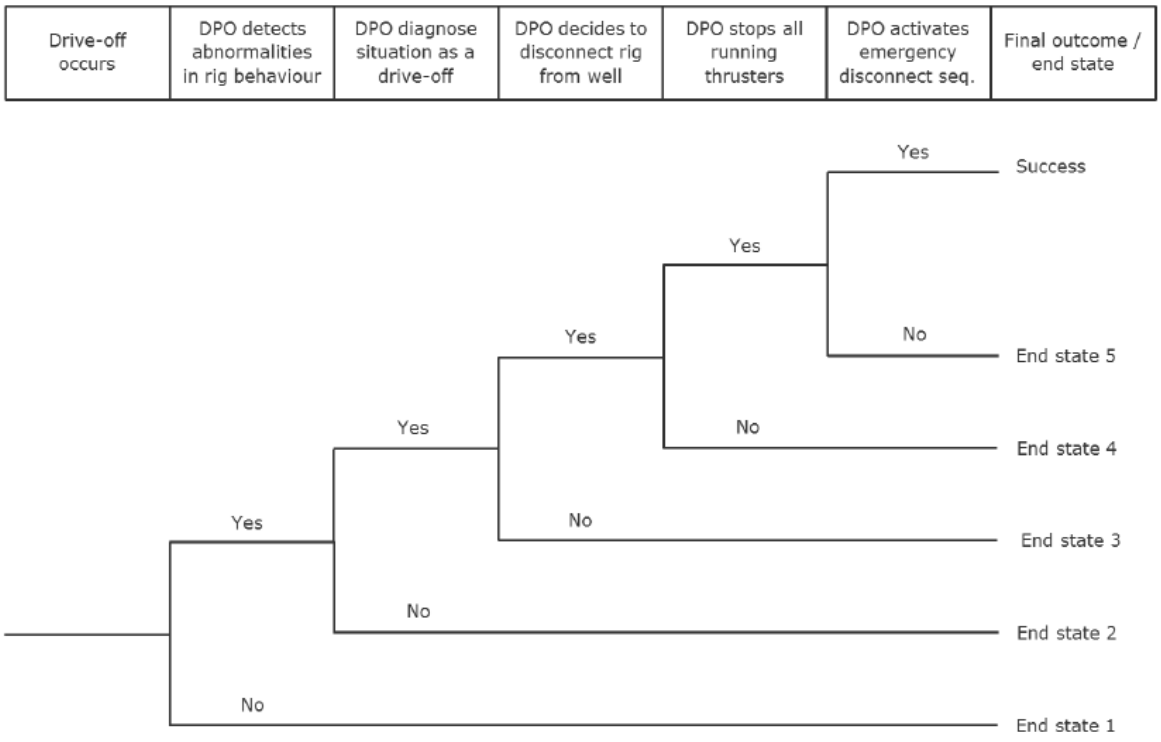

Figure 13: Case Study 1 - Operator action event tree

The links between the identified errors and the HFEs are described in a OAET table, Table 3. This table was used to cross-check that all important errors identified in the HEI are accounted for, and that none were double counted. The table also provided a useful overview of the link between the task analysis and the human error modelling and provided transparency for the end users of the analysis results.

Table 3: Case Study 1 - OAET table showing link to human error identification

Event ID	Event Description	HFE Details	HEP	Potential Errors (from HEI)	Final Outcome / End State
0	Drive-off occurs	Initiating event: A drive-off occurs due to DP failure.	N/A	N/A	N/A
1	DPO detects DP abnormalities (TTA Ref. Task Step 1.0)	HFE1: Failure to detect DP abnormalities. The drive-off is not detected, or is detected too late by the DPO, making him/her unaware of the drive-off being initiated.	-	• DPO does not hear sound of thrusters increasing (or too late). • DPO does not detect increase in thruster force on HMI. • DPO does not detect high thruster force alarm. • DPO does not detect position alarm.	The automatic EDS is activated according to the offset position limit defined in the WSOC. Due to the speed of the rig, the riser angle may be too steep for the disconnection to be successful. Damage or breakage of equipment, with potential environmental impact (e.g. spill of mud).
2	DPO diagnoses situation as drive-off (TTA Ref. Task Step 2.0)	HFE2: Failure to diagnose drive-off. The DPO does not realize that the abnormalities indicate a drive-off (as described in the scenario description): For example, he/she fails to recognize the type of event, or its severity.	-	• DPO does not diagnose that this is a drive-off event. • DPO misinterprets indications & misdiagnoses the event. • DPO does not check correct indications on HMI. • Diagnosis check takes too long.	See outcome for Event 1 above.
3	DPO decides to disconnect rig from well (TTA Ref. Task Step 3.)	HFE3: Failure to decide on correct mitigating actions. The DPO decides not to stop thrusters and/or disconnect , or fails to make a decision in time, or decides to attempt a different recovery (e.g. regain position), or doesn't reach a decision (e.g. "freezes" due to stress).	-	• DPO does not realise that thrusters should be stopped first, before activating EDS. • Decision to stop thrusters takes too long. • DPO decides not to activate EDS. • Decision to activate EDS takes too long.	See outcome for Event 1 above.

4	DPO stops all running thrusters (TTA Ref. Task Step 4.2)	HFE4: Failure to step all running thrusters. The DPO fails to stop any thrusters, or does this too late or fails to stop all running thrusters.	-	• DPO takes too long to press stop buttons for all active thrusters. • DPO stops the wrong thrusters (i.e. wrong 6 out of 8, leaving 2 thrusters still running). • DPO does not confirm that all active thrusters have stopped.	See outcome for Event 1 above. For partial or delayed stop of the thrusters, damage can be less than if the thrusters are not stopped at all.
5	DPO activates emergency disconnect sequence (TTA Ref. Task Step 4.4)	HFE5: Failure to activate the emergency disconnect sequence (EDS). The DPO fails to activate the EDS at all, or fails to do this in time before the automatic EDS is activated.	-	• DPO does not press EDS buttons. • DPO takes too long to press EDS buttons.	Assuming that the automatic EDS is enabled and that the DPO stops the thrusters in a timely manner, there are no impacts associated with this event.

2.6 Step 6: Human Error Quantification

Each human failure event in the OAET (Figure 13) was quantified, using a separate PSF summary worksheet. An example of a completed PSF summary worksheet for HFE2: “Failure to diagnose drive-off” is shown in Table 4 (next page). Again, it should be noted that the numbers used in this example are fictive and are only shown here to illustrate the method.

The analysts discussed each PSF in turn and rated the multiplier for each HFE, referring back to the TTA and human error identification as necessary to review the information collected about the relevant task steps, operator actions and potential errors. The chosen multiplier for each PSF was highlighted in yellow, and the justification for choosing this multiplier was documented in the right-hand column. The chosen multipliers and PSF justifications were then reviewed again to ensure there was no double counting between this HFE and the other HFEs in this scenario.

Table 4: Case Study 1 - PSF summary worksheet

Petro-HRA PSF summary worksheet				
Facility/installation	**Offshore Semi-Submersible Drilling Unit**		**Date**	**17 April 2015**
HFE ID & description	**HFE 2 Failure to diagnose drive-off**			
HFE scenario	**Drive-off of a semi-submersible drilling unit**			
Analysts	**Analyst 1 & 2**			
HEP Calculation	**0.01 x 5 x 5 x 0.5 = 0.125**			
PSFs	**PSF levels**	**Multiplier**	**Substantiation: Specific reasons for selection of PSF level**	
Available time	Extremely high negative	HEP=1	While time is a critical factor throughout the scenario, the effect will not be significant until the final stopping of the thrusters and activation of the ESD.	
	Very high negative	50		
	Moderate negative	10		
	Nominal	1		
	Moderate positive	0.1		
	Not applicable	1		
Threat stress	High negative	25	Once the DPO realises that a drive-off is occurring, he/she is likely to experience some degree of threat stress. However, it is not considered to have a significant effect on this operator action.	
	Low negative	5		
	Very low negative	2		
	Nominal	1		
	Not applicable	1		
Task complexity	Very high negative	50	The task is relatively simple and only includes some iterative checks of a small number of indicators.	
	Moderate negative	10		
	Very low negative	2		
	Nominal	1		
	Moderate positive	0.1		
	Not applicable	1		
Experience/training	Extremely high negative	HEP=1	General training of DP systems and navigation is good. DPOs also have desktop discussions and some personal experience of similar events. However, training does not specifically cover drive-off scenarios and how to correctly diagnose whether or not it is necessary to disconnect.	
	Very high negative	50		
	Moderate negative	15		
	Low negative	5		
	Nominal	1		
	Moderate positive	0.1		
	Not applicable	1		
Procedures	Very high negative	50	The operating manuals contain some information about which parameters define a drive-off. However, this information is not always clear and is scattered across several documents. There is no unambiguous single procedure for operator response to this scenario.	
	High negative	20		
	Low negative	5		
	Nominal	1		
	Low positive	0.5		
	Not applicable	1		
Human-machine interface	Extremely high negative	HEP=1	The HMI that displays the indications used to diagnose a drive-off (i.e. riser angle, position offset, rig speed) is easy to understand and readily available in front of the DPO.	
	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	Attitudes to Safety, Work and Management Support are not considered a performance driver for this step.	
	Moderate negative	10		
	Nominal	1		
	Low positive	0.5		
	Not applicable	1		
Teamwork	Very high negative	50	This task step is carried out by the DPO on watch only. The DPO on watch has responsibility for managing the drive-off scenario.	
	Moderate negative	10		
	Very low negative	2		
	Nominal	1		
	Low positive	0.5		
	Not applicable	1		
Physical working environment	Extremely high negative	HEP=1	The physical working environment on the bridge is acceptable and according to NORSOK standards.	
	Moderate negative	10		
	Nominal	1		
	Not applicable	1		

Once all of the PSFs have been rated and documented, the HEP for that HFE can be calculated. The calculation process for HFE 2 ("Failure to diagnose drive-off") is shown in Figure 14. As this figure shows, the Petro-HRA nominal HEP (0.01) is multiplied by the chosen multiplier for each PSF in the summary worksheet. Note that multipliers judged to be equal to 1 (i.e., nominal) are not shown in this figure as they have no effect on the HEP calculation.

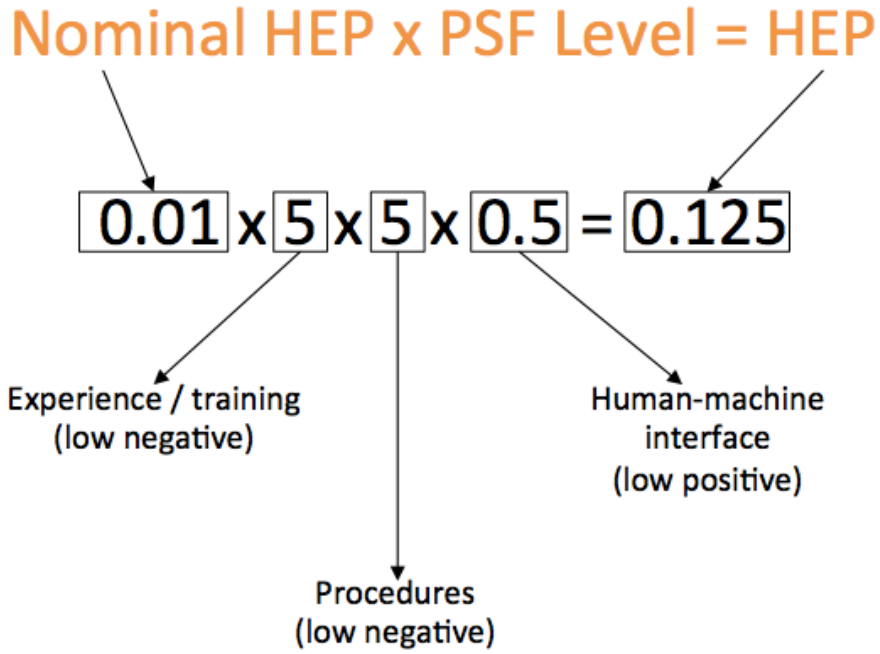

Figure 14: HEP calculation for a single HFE

Therefore, the HEP for HFE 2 is calculated to be 0.125. The HEP calculation is also recorded on the PSF summary sheet in the header section. This process is repeated for each of the other four HFEs in the OAET. The HEPs can then be added to the OAET, as shown in Figure 15.

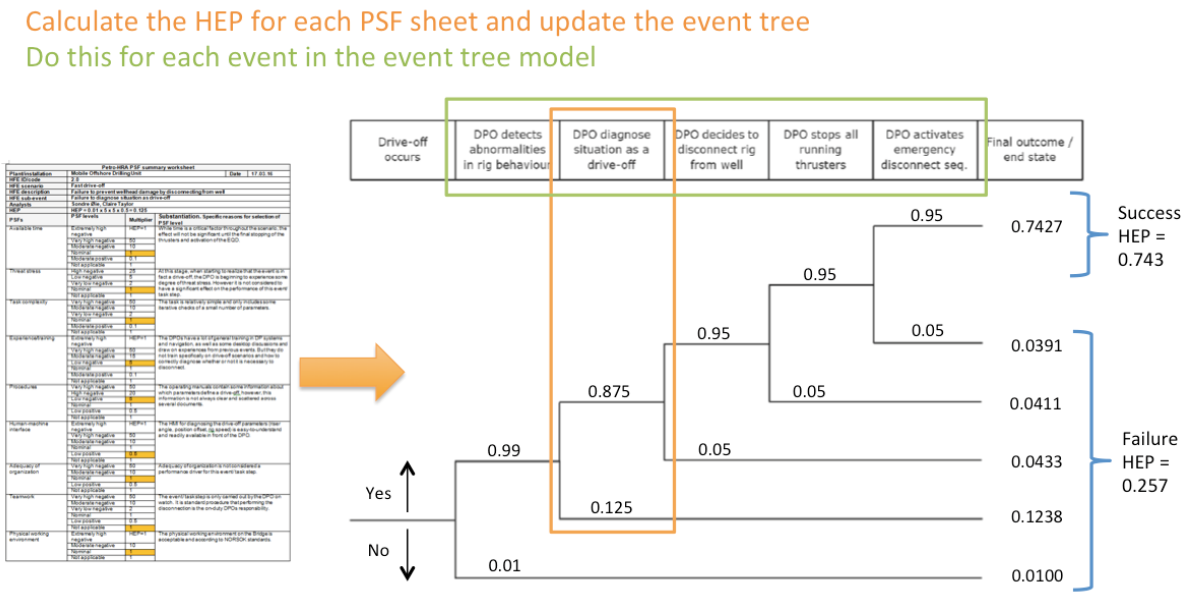

Figure 15: Case Study 1 - Integration of HEPs to the OAET

As Figure 15 shows, the probability for both success and failure of each HFE is added to the OAET. Again, please note that the numbers shown here are fictive and are used for illustrative purposes only.

The failure probability (i.e., HEP) for each HFE in the event tree is calculated using the PSF summary worksheet method as described previously. To calculate the success probability for each HFE, the HEP is simply subtracted from 1. For example, for HFE 2, the calculated HEP is 0.125. Therefore, the probability of success of that HFE is 1 – 0.125 = 0.875.

The end state probabilities for each branch of the OAET are calculated by multiplying the probabilities along each branch, as shown below:

- Success: 0.99 x 0.875 x 0.95 x 0.95 x 0.95 = 0.7423
- End State 5: 0.99 x 0.875 x 0.95 x 0.95 x 0.05 = 0.0391
- End State 4: 0.99 x 0.875 x 0.95 x 0.05 = 0.0411
- End State 3: 0.99 x 0.875 x 0.05 = 0.0433
- End State 2 0.99 x 0.125 = 0.1238
- End State 1: 0.01

There is only one success outcome for this OAET, whereas there are five failure outcomes. To calculate the overall HEP for this OAET, the end state probabilities for each failure end state are added together, as shown below:

- 0.0391 + 0.0411 + 0.0433 + 0.1238 + 0.01 = 0.257

The final success HEP and final failure HEP should together always add up to 1. In Figure 15, the numbers add up to 0.9993, because the end state HEPs have been rounded up or down for simplicity; this is ok because the total error probability is very close to 1.

- 0.7423 (success probability) + 0.257 (overall failure probability) = 0.9993

2.7 Step 7: Human Error Reduction

The HEP was integrated into the QRA event tree as shown in Figure 16 (next page). Four PSFs were determined to have the most significant impact on human performance in this scenario, and so were selected for error reduction: time, training, HMI and procedures. The following error reduction strategies (ERS) and error reduction measures (ERMs) were developed based on the findings from the Petro-HRA.

- **PSF: Time**. The entire scenario takes place in under two minutes, but it is not possible to "create" more time for this scenario because it would require a total redesign of the drilling unit.
    - **ERS 1**. An ERS was identified to provide feedback to designers of future installation builds, to take into account the effect the design of the system has on time and operator performance in such scenarios.
- **PSF: HMI**. Although the HMI of the operator display screen for diagnosing the event was considered good, the design and layout of the operator workstation for stopping the thrusters was not optimal. As a result, the action to stop the individual thrusters used up valuable time in this fast-paced scenario.

- **ERM 1**. An ERM was identified to add a single emergency stop button to shut down all running thrusters at the same time. This would save the operator valuable seconds when responding to this and similar scenarios.

- **ERS 2**. An ERS was identified to provide feedback to designers of future installation builds to add a single emergency stop button to the thruster panel.

- **PSF: Training**. The DPOs do not receive specific training on the correct response to a drive-off event and must rely on experience and process knowledge to know what to do.

  - **ERM 2**. An ERM was identified to provide regular simulator training to DPOs to drill them in the expected operator response to drive-off and similar events (e.g., one to two times per year).

  - **ERM 3**. An ERM was identified to provide regular on-site training (e.g., via desktop exercises) to drill them in the expected operator response at their own facility for drive-off and similar events (e.g., three to four times per year).

- **PSF: Procedures**. There are no procedures available to the DPOs to clearly specify what the operators should do in a drive-off or similar event.

  - **ERM 4**. An ERM was identified to provide an appropriate operator procedure to clarify the required response actions, which should be reinforced by training.

The results of the human error reduction analysis were documented in a report to the client along with the results from the Petro-HRA.

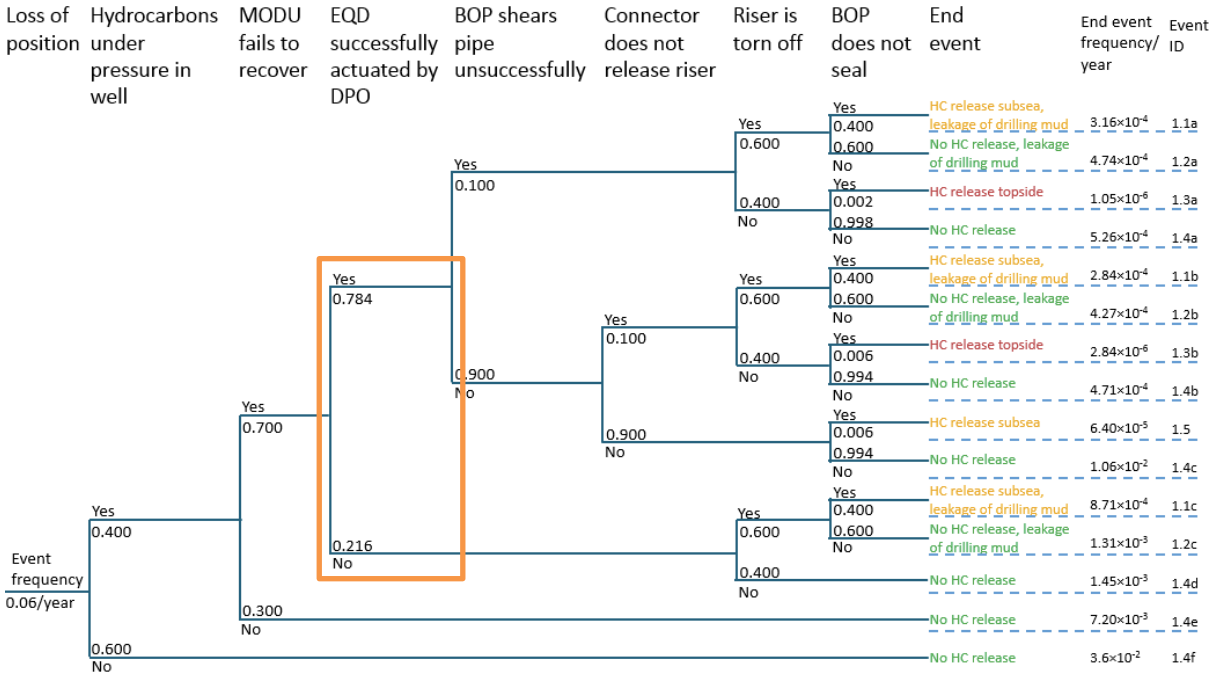

Figure 16: Case Study 1 - Integration of HEP to the QRA event tree

3 Case Study 2: Gas Leak Scenario

The purpose of this case study is to provide the reader with an example of how the Petro-HRA method can be applied as an integral part of a Quantitative Risk Analysis (QRA). The study case is a gas processing facility in Norway for which the QRA was to be updated. As several of the safety functions for the plant required operator actions to be activated, the client requested a Human Reliability Analysis (HRA) using the Petro-HRA method to calculate the error probabilities for the barriers working on demand.

The structure of this case study follows the seven steps as described in the Petro-HRA method. Each of the steps are explained through tables and figures. Where the analysts experienced challenges, e.g., for defining “time available”, important decisions are further explained and substantiated.

3.1 Step 1: Scenario Definition

The purpose of this chapter is to explain the relationship between the Quantitative Risk Analysis (QRA) model and Human Failure Events (HFEs) that are addressed in this case study. The subsequent sub-chapters will provide an example on how to describe a scenario by utilizing the scenario table included in the Petro-HRA guideline.

3.1.1 QRA Model and Interface with HRA

The QRA model is an event-tree which calculates risk based on factors such as leak location, leak size (small, medium, large), wind speed and wind direction. The model also takes credit for implemented barriers/safety functions. In the QRA model used for the project, the safety functions include auto-detection, isolation of segment, blowdown, and release of fire water. For this facility, several of the listed barriers can only be manually activated, either locally from the field or from the Central Control Room (CCR). This means that the reliability of the barriers is dependent on human actions. Hence, the “technical reliability” (hardware and software) cannot be used alone to calculate the likelihood of these barriers performing on demand. Therefore, a Petro-HRA study was performed to estimate the reliability of these barriers. The following barriers and associated HFEs were defined after examining the model.

Table 5: Case Study 2 - Barriers and Human Failure Events

Safety Function	Human Failure Event	Methods of Activation
Ignition source isolation of group 2 equipment	HFE 1: Failing to isolate ignition sources group 2 within acceptable time	Manual isolation of ignition sources from HMI or activation of ESD 1 or 2
Isolation of process segments	HFE 2: Failing to isolate process segments within acceptable time	Manual closing of safety valves from HMI or activation of ESD 1 or 2
Depressurization	HFE 3: Failing to activate blow down	Manual opening of blow down valves or activation of ESD 2

3.1.2 Limitations

As mentioned above, the QRA model contains different leak sizes, but this report only includes operator response to leaks larger than 1 kg/s, which corresponds to medium and large leaks in the QRA model. Hence, the reliability estimates provided in this report are only valid for these leak sizes. Another limitation is related to the ignition time which is also modelled in the QRA. For the purpose of this HRA example, it is assumed that no immediate ignition occurs as this is a separate branch in the QRA event tree. From a HRA perspective, it could be argued that it is less relevant to examine

these scenarios further as it will be impossible to activate the relevant preventive safety functions in time. However, human reliability may still be important in terms of mitigating consequences, i.e., timely depressurization that can reduce the potential for escalation.

3.1.3 Scenario Description

The template for the table below comes from the Petro-HRA guideline and provides a good structure to describe sequence of events, context, relevant environmental information, barriers in place, roles and responsibilities, timescale and potential deviating scenarios.

Table 6: Case Study 2 - Scenario description table

Topic	Description	Assumptions / uncertainties and comments
Event sequence		
Initiating event	Hydrocarbon leak in the process facility (> 1 kg/s).	Alarms from 5 gas detectors in the process area raised in the CCR.
Intermediate events	• Automatic deactivation of ignition sources (group 1) and activation of Public Announcement (PA) by the Fire & Gas (F&G) system. • CCR operators detect the alarms, diagnoses the severity/criticality of the situation, and decides to activate ESD 1 (isolate segments and disconnect ignition sources). • CCR operators continue to search for leak location after isolation is performed but are not able to identify the leak. It is therefore decided to depressurize the plant by activating ESD 2.	Isolation of group 1 ignition sources and general alarm is automatically activated upon single gas (10% LEL or 0,1 LELm). Given the number of detectors triggered, it is assumed that the operators interpret this as a big leak and decide to activate ESD 1 to isolate the leak (ref. procedure). It is further assumed that the operators are not able to identify the leak location after isolation has been performed. This implies that they will decide to activate ESD 2 to depressurize the facility (ref. procedure).
End of event sequence	Successful activation of ESD 1 within 2 minutes followed by ESD 2 to depressurize facility.	CCR operators spends some time to identify leak location after ESD 1 but decides to activate ESD 2 as the leak location cannot be identified (following a local procedure).
Location and external environment		
Location of event	Process facility	The area consists of several sub-areas and systems including process area; cooling and compression; gas turbine generator; cold box (for cooling and removal of N2).
External environmental conditions	Daytime, clear skies and fresh breeze from south-east.	Due to heavy congestion in area, wind direction does not have any significant influence on gas dispersion in this area.
System and task context		
Operational mode	Normal production.	
Safety system/barriers	• Gas detection: IR point and line detectors • Fire detectors: Flame detectors • Ignition source isolation: Group 1 isolated automatically upon single gas. Isolation of group 2 (e.g. rotating equipment is dependent on operator response). • Isolation and blow-down valves are installed at strategic locations to limit size of segments and allow for depressurization.	Upon 10% LEL or 0,1 LELm single alarm is raised in CCR and general alarm is activated in the area. Upon single detection, group 1 ignition sources will be isolated/disconnected. The flare calculation report shows that it will take approximately 30 minutes to depressurize the plant from normal operating

	• Firefighting systems: Deluge and fire monitors are the primary means for firefighting. • CCTV cameras installed at strategic locations	pressure to 4 barg after full sequential depressurization (ESD 2) has been activated.
Personnel roles and responsibilities	Manning in CCR Control room operators (panel operators): • 1 panel operator (cold box) • 1 panel operator (drying/Co2) • 1 panel operator (Fire&Gas) • 1 panel operator (loading/offloading and subsea) Other CCR staff: • 2 panel operators on the job training • 1 panel operator for support • 1 shift supervisor • 1 assistant shift supervisor Field operators • On a normal day 2-5 field operators is expected to be in the area	In case of a fire or gas leak, the leak will first be detected and diagnosed by the operator situated on the F&G panel. The panel operator responsible for the "leaking system" will be the "owner" of the leak. Together with the shift supervisor, the F&G operator and the system responsible will together, as a team, decide on the appropriate response in order to handle the situation.
Timescale		
Duration of scenario	• 100 seconds to activate ESD 1 (isolation and disconnect ignition sources) • 120 seconds to activate ESD 2 (depressurization) after ESD 1 has been activated • 30 minutes to depressurize facility down to 4 barg	Please note that the scenario starts when the alarm is presented in the CCR (not the exact time for leak). See timeline analysis in 3.3.5 for further details.
(Optional) Deviation Scenario(s)		
Possible deviation scenario(s)	The complete HRA analysis which this case study is based on covers additional scenarios than described in this report (including smaller leaks and immediately ignited leaks). This example only covers leak sizes > 1 kg/s which are not ignited. Expected operator responses to smaller leaks and fire scenarios will typically trigger other actions, meaning that the human error probabilities calculated for the scenarios covered by this HRA should not be used for such initiating events.	

3.2 Step 2: Qualitative Data Collection

Qualitative data collection is a continuous and iterative activity that follows the project from start to end. In this project, the following data provided the most valuable input in order to perform the analysis.

- Documentation
  - Existing QRA report
  - Guideline/procedure for handling hydrocarbon leaks
  - Safety/barrier strategy
  - ESD and Depressurizing System Engineering report
- Site visit (in control room and plant)
- HRA analyst participation in the QRA Hazard Identification (HAZID) session
- HRA workshop to identify credible human errors in responding to a gas leak.

3.3 Step 3: Task Analysis

This section provides a description of the main tasks that are performed by the control room operators from the time the gas leak is detected until blowdown has been activated. The section begins with explaining a procedure/guideline that was established in the aftermath of an actual gas leak at the facility. The purpose of this procedure is to simplify decision-making if similar incidents were to reoccur. This is important to include as the task analysis is primarily based on this procedure. In the subsequent sections, a brief description of the main task steps is provided. The section ends with extracts from the Hierarchical Task Analysis (HTA) and the Tabular Task Analysis (TTA) which were prepared for this project.

3.3.1 Guideline for Handling Gas Leaks

After a previous gas leak where the time spent to execute mitigating actions allowed the scenario to escalate, the operating company decided to develop a procedure with the purpose to simplify decision support. The guideline/procedure was established as a simple flow-chart with some basic principles which are explained below.

The first principle is to evaluate the size of the gas leak through calculation of LEL-factor. This is done by summarizing % LEL on all "triggered" gas detectors in the affected area. For a point-gas detector, 80% LEL corresponds to a LEL-factor of 80. For line gas detectors, the reading of the detector (in LELm) is multiplied by 100, meaning that 0,7 LELm corresponds to a LEL-factor of 70. ¨

Examples

Example 1: 1 line gas detector shows a value of 0,8 LELm and two point gas detectors show 80% LEL each.
Calculation: LEL-factor = (100 x 0,8) + (2 x 80) = 240

Example 2: Two point gas detectors show readings on respectively 80% LEL and 70% LEL
Calculation: LEL-factor= 80 + 70 = 150

According to the guideline/procedure, the operator shall activate ESD 1 (which includes isolation of segments and ignition sources) if the LEL-factor exceeds 220 within 3 minutes after the leak was detected. Applying these principles to the examples provided above, this implies that ESD 1 function shall be activated in the first case, but not in the second case.

The guideline also includes a time-curve which is only briefly described as it is not directly relevant to the scenario in question. The rationale behind having this curve is that a there may be situations where the LEL-factor does not initially exceed the acceptance criteria of 220, but the leak may still cause a significant risk to the facility (due to long duration). The time curve is meant to provide guidance in such scenarios, and the acceptance criteria for activating ESD 1 decreases as a function of time. For instance, 10 minutes after the leak is detected, the acceptance criterion is 100 (not 220). After 20 minutes, the criterion is 50. This time curve is especially applicable for situations with small/diffuse leaks that are not directly relevant to the scenario covered in this report.

For depressurization, the procedure states that "blow-down" shall be activated as soon as possible after the leak has been contained. If the leak location is known, the operators may try to perform this manually by opening blow-down valves from the HMI. If the leak location is unknown, the procedure recommends that ESD 2 is activated. ESD 2 will start a full sequential blow-down sequence. The time

to depressurize the process facility down to 4 barg after activation of ESD 2 is estimated to take approximately 30 minutes.

3.3.2 Description of Main Task Steps

The following is a short summary of the main task steps performed by the operators from the time the gas leak is detected in the CCR to activation of the relevant ESD-functions.

1. Detect and confirm gas alarm:
   Gas alarms are raised in the CCR both in terms of audible and visible alarms. The alarms are available at a dedicated F&G/ESD matrix (Critical Action Panel, CAP) and all operator stations. Alarms from the CAP are easily available for all personnel in the CCR. There is a F&G panel with a dedicated operator responsible for handling F&G-alarms. The operator in this sequence of the scenario is responsible for confirming the leak. The criterion for a confirmed leak is that one or multiple gas detectors shows more than 20% LEL/ 0.2 LELm or by receiving a visual confirmation from a field operator. To get a visual confirmation, the F&G panel operator will according to the procedure request that a "check and report" (physical observation) is performed in the field. This is however only done if the area is considered safe to approach and observe.

2. Notify according to the emergency response plan:
   After the alarm has been identified, a dedicated operator is responsible for notifying relevant personnel/stakeholders. The task is typically to announce a pre-defined message over the Public Address (PA) system. After the message has been delivered, other parties that can assist in handling the scenario are notified (including fire department, guard, and 2nd line emergency response). This task is important to evacuate personnel and contact resources such as the fire department which may contribute to handling the situation. However, as this task step is not directly linked to activating the safety functions, it is excluded from the critical timeline of the analysis.

3. Diagnose gas leak:
   The purpose of performing this task step is to obtain more information about the severity of the situation. Important information will be to check how many gas detectors have been triggered, check LEL-reading on individual detectors and try to identify which medium is leaking by observing process parameters on the various process and utility systems. In addition to the F&G system and process/utility systems, operators can use CCTV to check the area. There is no direct interface between the F&G system and CCTV cameras, so the operators have to spend some time to display the correct camera on the screen in the control room. Diagnosing the situation may also include evaluating local and environmental conditions such as wind, congestion in areas, etc. For the scenario in question, it should be noted that the sub-tasks/actions performed in this part of the sequence are repeated/continued in later stages after ESD 1 has been initiated.

4. Decide on isolation and blow-down:
   The outcome of this task step is to decide on the preferred response according to the scenario in question. As the leak appears to be significant due to number of triggered gas detectors, it is expected that the operators decide to activate ESD 1. Activating ESD 1 will isolate segments and disconnect ignition sources (group 2). For smaller leaks where it is doubted that the LEL-factor is higher than 220, it is expected that the operators will calculate the LEL-factor for decision support. If the shift supervisor is available, they may also be consulted and involved in the decision process.

5. Isolate segments and ignition sources:
   This task step is a direct result of decision made under task step 4. In the current example, the preferred response is to activate ESD 1 from a push-button on the CAP. This will ensure that all isolation valves close and ignition sources (group 2 equipment) are disconnected. For less severe events, an alternative option may be to use the HMI on the operator stations to manually close isolation valves and disconnect ignition sources. However, this is not defined as a favorable response in this scenario and will also conflict with the guideline/procedure.

6. Depressurise plant/segments:
   After the plant has been isolated and ignition sources disconnected, the next step is to depressurize limited segments or the entire facility. In this scenario it is assumed that the operators spend some time after ESD 1 has been activated to identify the leaking segment. This task will typically include monitoring changes in process parameters (same tasks as performed for task step 3). If the leaking segment can be identified, a partial blow-down of the leaking segment can be considered as this will decrease depressurization time. In this case study, it is assumed that the leak cannot be identified. According to the guideline, activating ESD 2 is then the desired response. After ESD 2 has been activated, the operators will typically confirm that all actions are executed according to a cause and effect (C&E) diagram.

3.3.3 Hierarchical Task Analysis

Based on the collected data (see 3.2), a HTA was established early in the project and continuously updated as new information became available. The complete HTA is shown in Figure 17.

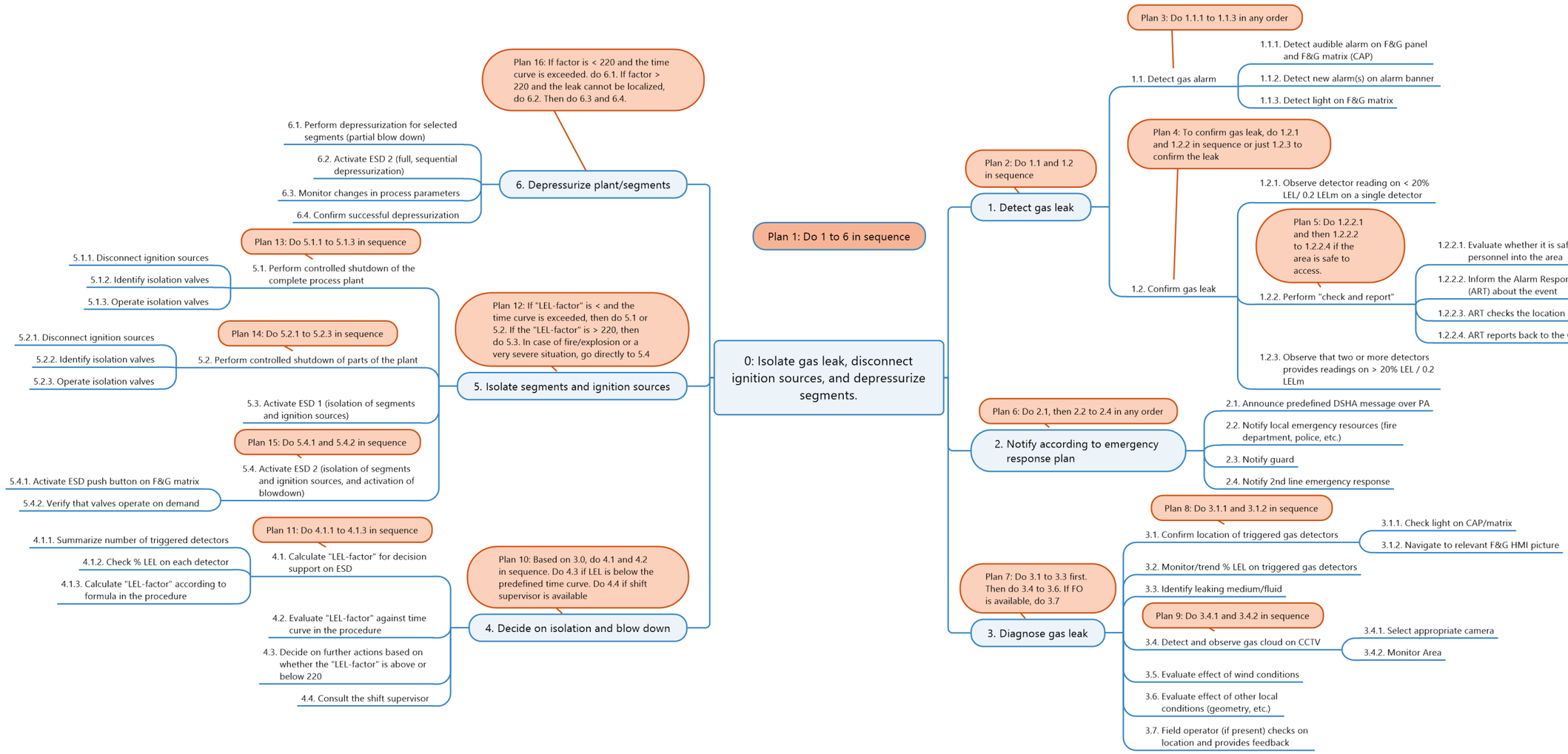

Figure 17: Case Study 2 – Hierarchical Task Analysis

3.3.4 Tabular Task Analysis

A HTA such as the example presented in Figure 17 provides a good overview of the tasks performed by the control room operators from detecting a gas leak to initiating the proper response actions. While the HTA is a good tool to structure and visualize information, it is not a suitable format to record detailed task information. To record additional information about the tasks, a TTA was established according to the recommendations in the Petro-HRA guideline. The TTA is presented in Table 7. The TTA allows the analyst(s) to record more detailed information about the tasks including:

- Description of the task: Detailed description of the tasks
- Cue/feedback: Cues that provide the operators information that shall trigger the task and feedback from the system after the task has been executed.
- HMI, displays and controls: Information about the HMI and equipment used to perform the task
- Person responsible: Person(s) responsible for (or involved in) executing the task
- Assumptions/uncertainties

In addition, the TTA table can be used to record any additional information that may be relevant for the HRA.

Table 7: Case Study 2 - TTA and Human Error Identification for selected task steps

Step No.	Description	Procedure / Document Ref.	Cue / Feedback	HMI / Display / Control	Person Responsible	Potential Error	Likely consequence	Recovery Opportunity	Further Analysis?	Event Tree Reference	Performance Shaping Factors	Assumptions / Uncertainties	Notes / Comments
	Task Analysis					**Human Error Identification**							
0	**Goal: Isolate gas leak, disconnect ignition sources, and depressurize segments.**												
Plan 1	*Do 1 to 6 in sequence*												
1	Detect gas leak												
Plan 2	*Do 1.1 and 1.2 in sequence*												
1.1	Detect gas alarm												
Plan 3	*Do 1.1.1 to 1.1.3 in any order*												
1.1.1	Detect audible alarms on F&G panel and F&G matrix (CAP)	NA – only for decision support	Cue: Task knowledge Feedback: NA	F&G panel F&G matrix/CAP	Control room operator (F&G panel)	Not any credible errors identified.	NA	Recovery later is the task or by feedback from other personnel.	N	Event 1	**Teamwork**: Several people present in the control room may notice the alarm. **HMI:** Redundancy in the HMI in terms of alarm banners on all operator stations		Not perceived a credible error that an F&G alarm will go unnoticed as there are several people situated in the control room. In addition, there are multiple systems available.
1.1.2	Detect new alarms on alarm banner	NA – only for decision support	Cue: Task knowledge Feedback: NA	Alarm banners available at all panels (OSs)	Control room operator (all panel operators)	Not any credible errors identified	NA	See item 1.1.1	N	Event 1	See item 1.1.1		
1.1.3	Detect light on F&G matrix (CAP)	NA – only for decision support	Cue: Task knowledge Feedback: NA	F&G matrix (CAP)	All personnel in the control room may notice light on the CAP.	Not any credible errors identified	NA	See item 1.1.1	N	Event 1	**Teamwork**: See item 1.1.1		
…	…	…	…	…	…	…	…	…	…	…	…	…	…
3	Diagnose gas leak												
Plan 6	*Do 3.1 to 3.3 first. Then do 3.4 to 3.7*												
3.1	Confirm location of triggered gas detectors.	NA – only for decision support	Cue: Gas alarm Feedback: NA	CAP/matrix F&G panel F&G HMI	Control room operator (F&G panel)	1. Delayed response due to the need for excessive navigation. 2. Operators do not detect critical alarms due to a high number of consequence alarms 3. Operators may forget LEL-factors that exceeded 10/20% LEL, that subsequently decreased.	1 & 2: Delay in task execution may allow the incident to escalate 3. The operators may misdiagnose the situation which may increase the potential for escalation (selecting improper response)	No immediate recovery identified except that the task can be performed later.	Y	Event 2	**HMI:** The navigation may be cumbersome and can be simplified (see recommendation) **HMI**: The alarm load is currently higher than the requirements. Improvements should be considered (see recommendation). **Time:** Extended time needed for navigation may have negative impact on available time.		
3.2	Monitor/trend % LEL on triggered gas detectors.	NA – only for decision support	Cue: Gas alarm Feedback: NA	F&G HMI (trend display)	Control room operator (F&G panel)	The operators are unable to diagnose the information due to information overload.	The incident may escalate before the leak has been located.	No immediate recovery, but alarms on multiple detectors will raise attention.	Y	Event 2	**Training/experience**: The operators are familiar with trending %LEL on gas detectors.		
3.3	Identify leaking medium/fluid	NA – only for decision support	Cue: Gas alarm Feedback: NA	Panel controlling the system where the leak has occurred.	Panel operator.	Operator not able to identify the leaking segment due to high congestion of equipment/systems in the area.	1. May cause delayed response time and allow the scenario to escalate. 2. Incorrect segment may be isolated if the operators try to perform manual isolation.	1. No immediate recovery identified except that the task can be performed later. 2. Operator may activate ESD 1 at a later stage if manual isolation fails.	Y	Event 2	**Training/experience**: The operators are familiar with trending %LEL on gas detectors.		
…	…	…	…	…	…	…	…	…	…	…	…	…	…

3.3.5 Timeline Analysis

A timeline analysis is an important activity to determine how long time is required by the operators to execute the task steps and complete the task. It is essential to perform this activity for determining the effect time (as a PSF) has on the nominal Human Error Probability (HEP) value. The time PSF is determined based on the relative gap between time required and time available.

Time available

"Time available" was decided by subject matter experts based on an examination of different consequence plots (see e.g., Figure 18). It was assumed that the operators should be able to activate ESD 1 within 2 minutes in a gas leak scenario. This time criterion is applicable for gas leaks > 1 kg/s. For smaller leaks (< 1 kg/s), the same time requirement was decided to be 3 minutes due to less severe consequences. The reader should note that in this case study there is no deterministic relationship between the leak duration and the consequence. The consequence may materialize both before and after the time defined as time available has been reached, but ignition is less likely if early action is taken.

Figure 18 was produced by the QRA and indicates how the expected ignition frequency is a function of time. The graph shows an almost linear relationship between time and ignition frequency that increase approximately 12% per minute if the ignition sources are exposed. Similar curves were also provided for other consequences, but these curves were less steep, meaning that rapid activation of other safety functions are less time critical.

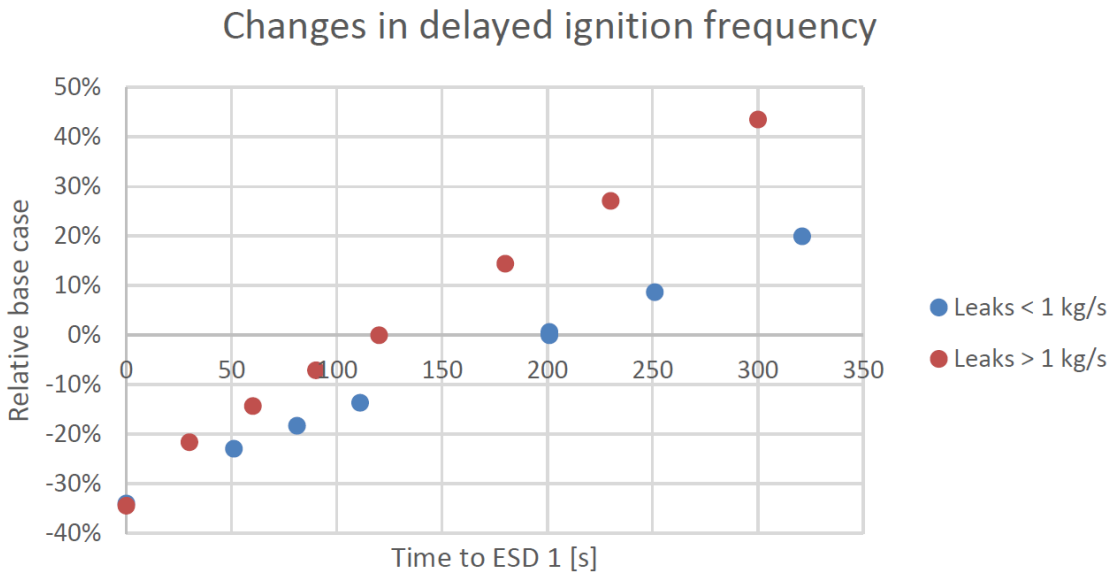

Figure 18: Case Study 2 - Changes in expexted ignition frequency as a function of time

For other areas of applications, the "time of no return" is easier to define than for typical gas leak scenarios. If the pressure source is known, it is quite easy to define a time criterion for when a pipe/vessel will get damaged or burst. For this analysis, input from subject matter experts were used to define "time available" as it was not possible to define any absolute time criterion.

Time required

The timeline analysis provided for this case study is presented in Figure 19. The result of the timeline analysis shows that the operator will need approximately 100 seconds to activate ESD 1. An estimated

additional 120 seconds is thereafter required to activate blow-down (ESD 2). It should be noted that the timeline analysis does not capture technical aspects such as signal response/delay time, travelling time for valves, etc.

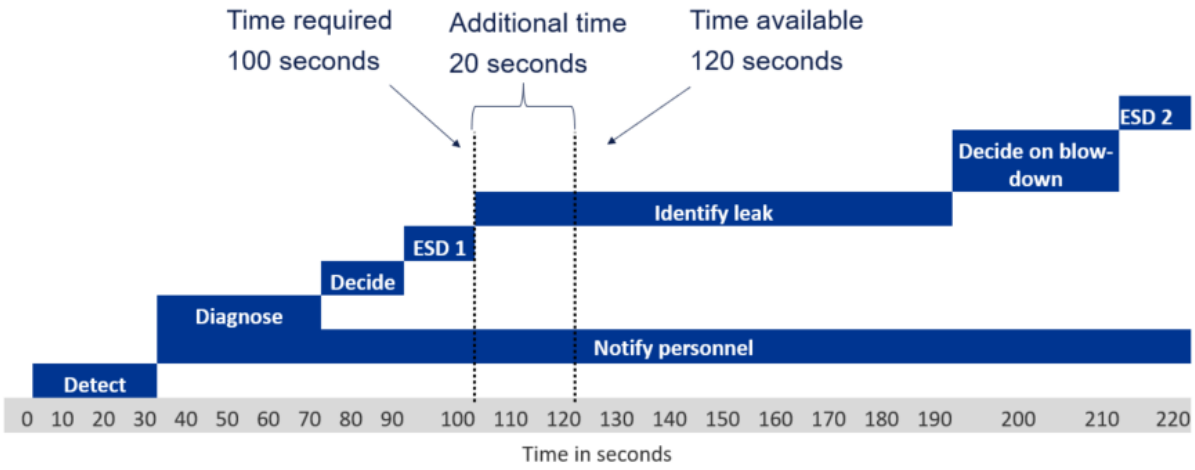

Figure 19: Case Study 2 - Timeline analysis

3.4 Step 4: Human Error Identification

HEI was for this project mainly performed as a workshop activity, where the verified TTA was expanded to include columns to record information regarding potential errors, likely consequences, recovery opportunities and information about factors that may influence operator performance (PSFs). Table 8 shows an extract of the HEI. An example of a combined TTA/HEI table is included in Table 7.

Table 8: Case Study 2 - Extract from the HEI

Step No.	Description	Potential error	Likely consequence	Recovery opportunity	Further analysis?	Event-tree ref.	PSFs
…	…	…	…	…	…		…
1.1.1	Detect audible alarm on F&G panel and F&G matrix (CAP).	No credible errors.	NA	NA	N	Event #1	**Teamwork**: Several persons present in CCR will decrease the likelihood of an alarm going unnoticed. **HMI:** F&G alarm will have the highest priority. Alarms will be available at all panels (but may require some navigation). No alarm list on LSD (see recommendation).
1.1.2	Detect new alarm(s) on alarm banner.						
1.1.3	Detect light on F&G matrix.						
…	…	…	…	…	…	…	…
3.1	Confirm location of triggered gas detectors.	Delayed response due to the need for excessive navigation.	Delay in task execution may allow the incident to escalate	No immediate recovery identified except that the task can be performed later.	Y	Event #3	**HMI**: The navigation may be cumbersome and can be simplified (see recommendation) **HMI**: The alarm load is currently higher than the requirements. Improvements should be considered (see recommendation). **Time**: Extended time needed for navigation may have negative impact on available time.
		Operators do not detect critical alarms due to a high number of consequence alarms					
		Operators may forget LEL-factors that exceeded 10/20% LEL, that subsequently decreased.	The operators may misdiagnose the situation which may increase the potential for escalation (selecting improper response)				
3.2	Monitor/trend % LEL on triggered gas detectors.	The operators are unable to diagnose the information due to information overload.	The incident may escalate before the leak has been located.	No immediate recovery, but alarms on multiple detectors will raise attention.	Y	Event #3	**Training/experience**: The operators are familiar with trending %LEL on gas detectors.

3.5 Step 5: Human Error Modelling

The purpose of an Operator Action Event Tree (OAET) is to provide a good high-level description of the post-initiating event scenario and the associated tasks performed by the operators. The OAET showed in Figure 20 was developed to visually describe the scenario and establish a logic structure that was further used to calculate the HEPs for activation of the safety functions which are modelled in the QRA (i.e., the HFEs). For this QRA/HRA, the barriers 1) isolation of segments; 2) isolation of ignition sources, and: 3) blow-down are modelled. At this point in the HRA, the HEPs for the HFEs were not yet calculated. The same OAET including HEPs is included in 0.

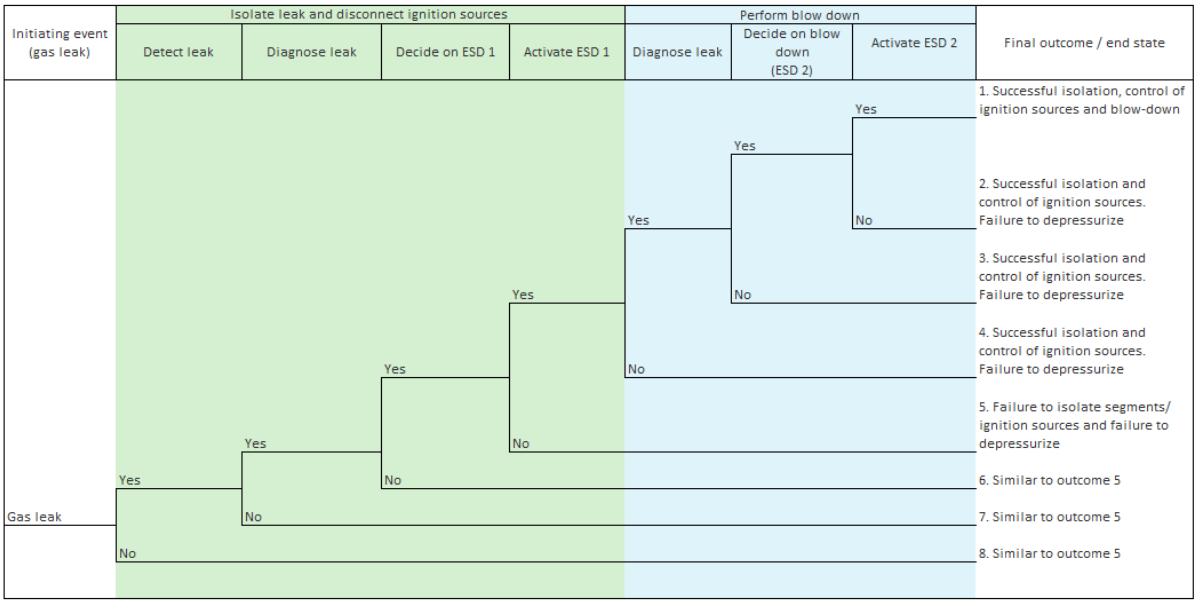

Figure 20: Case Study 2 - Operator Action Event Tree

3.6 Step 6: Human Error Quantification

The first step to calculate the HEP for the (entire) task is to calculate the HEP for each of the individual events/branches as included in the OAET. In this specific case, seven events/branches are included in the model. To calculate the HEP for a specific event, the analyst shall first evaluate and describe whether, or to what degree, different PSFs may positively or negatively contribute to task performance for this specific event. This is performed to determine the PSF levels (PSF multiplicator). In Petro-HRA, the nominal HEP is 0.01, and the nominal value is then multiplied with all the PSF-multipliers which are not assigned a nominal value (or are not applicable).

Table 9 provides a summary of the PSF-multiplicators selected for all the seven events included in the event tree model. Colour coding is used in the table to highlights PSFs which were considered to have positive or negative influence on the particular events. Substantiation for the selecting the PSF multiplicators are found in the PSF summary sheets enclosed in Table 10 to Table 16.

Table 9: Case Study 2 - Summary of PSF multiplicators per event

Event/PSF		Available time	Threat stress	Task complexity	Experience/training	Procedure	HMI	Attitudes to Safety, Work and Management Support	Teamwork	Physical working environment
Event 1	Failure to detect leak	1	1	0,1	1	1	1	1	1	1
Event 2	Failure to diagnose leak	1	1	2	1	1	1	1	1	1
Event 3	Failure to decide on ESD 1	1	1	1	1	1	1	1	2	1
Event 4	Failure to activate ESD 1	50	1	0,1	1	1	1	1	1	1
Event 5	Failure to diagnose leak (need for blow down)	1	1	1	1	1	1	1	1	1
Event 6	Failure to decide in blow down	1	2	1	1	0,5	1	1	1	1
Event 7	Failure to activate ESD 2	1	1	0,1	1	1	1	1	1	1

When the HEPs are calculated for all events, the HEP for the HFEs and the “complete” task is then calculated by multiplying all the failure rates using the event tree logic. Calculated HEPs for events, HFEs and the complete task is presented in the next section.

Table 10: Case Study 2 - Worksheet 1 Failure to detect leak

Petro-HRA PSF summary sheet			
Facility/installation	**Process Facility X**	**Date**	**XX-XX-XXXX**
HFE ID & description	**Event 1: Failure to detect leak. Applicable for the following HFEs in the QRA event tree:** **- HFE 1: Failure to isolate segments** **- HFE 2: Failure to disconnect ignition sources** **- HFE 3: Failure to depressurize facility**		
HFE scenario	**Gas leak in process facility (> 1kg/s)**		
Task step	**1.0 Detect leak**		
Analyst	**XX and XX**		
HEP Calculation	**0.001**		

PSFs	PSF levels	Multiplier	Substantiation: Specific reasons for selection of PSF level
Available time	Extremely high negative	HEP=1	The effect of available time is only considered for execution of the complete task and is therefore only considered for task step 5 (isolate leak) and 6 (depressurize facility).
	Very high negative	50	
	Moderate negative	10	
	Nominal	1	
	Moderate positive	0.1	
	Not applicable	1	
Threat stress	High negative	25	Threat stress is not expected to have any major influence on task performance in this sequence of the scenario. Fire/explosion could potentially have such effect but is not considered in this case study.
	Low negative	5	
	Very low negative	2	
	Nominal	1	
	Not applicable	1	
Task Complexity	Very high negative	50	The task is not considered to be complex. The task is easy and involves detecting audible and visual alarm in the control room.
	Moderate negative	10	
	Very low negative	2	
	Nominal	1	
	Moderate positive	0.1	
	Not applicable	1	
Experience/Training	Extremely high negative	HEP=1	Operators have experience from handling F&G alarms from previous incidents and testing of the F&G system. DSHA drills are regularly performed.
	Very high negative	50	
	Moderate negative	15	
	Low negative	5	
	Nominal	1	
	Moderate positive	0.1	
	Not applicable	1	
Procedures	Very high negative	50	Procedures are not considered relevant for this task step.
	High negative	20	
	Low negative	5	
	Nominal	1	
	Low positive	0.5	
	Not applicable	1	

Human-Machine Interface	Extremely high negative	HEP=1	There are two separate systems that provide alarms at the same time (CAP/matrix and F&G operator station). Alarms are easily available for all crew working in the control room. It is a risk that a high alarm load may lead to some alarms goes unnoticed. Especially consequence alarms related to ignition source isolation (group 1) may cause a high alarm load. This may lead to delay in task execution. Delay in task execution is covered/accounted for under task step 5 and 6.
	Very high negative	50	
	Moderate negative	10	
	Nominal	1.0	
	Low positive	0.5	
	Not applicable	1	
Attitudes to Safety, Work and Management Support	Very high negative	50	Not considered relevant for this task step.
	Moderate negative	10	
	Nominal	1	
	Low positive	0.5	
	Not applicable	1	
Teamwork	Very high negative	50	Several persons are available in the control room and may increase the likelihood for detecting alarms. This is however not considered as "teamwork", so it has been decided to assign a nominal value for this PSF.
	Moderate negative	10	
	Very low negative	2	
	Nominal	1	
	Low positive	0.5	
	Not applicable	1	
Physical Working Environment	Extremely high negative	HEP=1	No observations were made during site visit that could indicate that the physical working environment in the control room should have negative impact on task performance for this task step.
	Moderate negative	10	
	Nominal	1	
	Not applicable	1	

Table 11: Case Study 2 - Worksheet 2 Failure to diagnose gas leak

Petro-HRA PSF summary sheet			
Facility/installation	**Process Facility X**	**Date**	**XX-XX-XXXX**
HFE ID & description	**Event 2: Failure to diagnose leak. Applicable for the following HFEs in the QRA event tree:** **- HFE 1: Failure to isolate segments** **- HFE 2: Failure to disconnect ignition sources** **- HFE 3: Failure to depressurize facility**		
HFE scenario	**Gas leak in process facility**		
Task step	**3.0 Diagnose leak**		
Analyst	**XX and XX**		
HEP Calculation	**0.02**		
PSFs	**PSF levels**	**Multiplier**	**Substantiation: Specific reasons for selection of PSF level**
Time	Extremely high negative	HEP=1	The effect of available time is only considered for execution of the complete task and is therefore only considered for task step 5 (isolate leak) and 6 (depressurize facility).
	Very high negative	50	
	Moderate negative	10	
	Nominal	1	
	Moderate positive	0.1	
	Not applicable	1	
Threat stress	High negative	25	Threat stress is not expected to have any major influence on task performance in this sequence of the scenario. Fire/explosion could potentially have such effect but is not considered in this specific case study.
	Low negative	5	
	Very low negative	2	
	Nominal	1	
	Not applicable	1	
Task Complexity	Very high negative	50	Task complexity is considered to have "very low negative" effect on task performance for this task step. There are many sources of information available to the operator(s), and they are required to collect and analyze information from different systems to get a correct impression of the situation. Several actions are performed in iteration and in parallel (also involving several people).
	Moderate negative	10	
	Very low negative	2	
	Nominal	1	
	Moderate positive	0.1	
	Not applicable	1	
Experience/Training	Extremely high negative	HEP=1	Correct diagnosis of a gas leak is dependent on familiarity with/in the process facility and a good understanding of the process. All panel operators are qualified to operate on their dedicated panel as they need to pass a formal test in order to operate the panel alone. Training on gas leak scenarios is included in emergency preparedness training and simulator training. Tabletops on these scenarios are also regularly performed. Several of the operators in the control room have experience from handling similar scenarios is real situations.
	Very high negative	50	
	Moderate negative	15	
	Low negative	5	
	Nominal	1	
	Moderate positive	0.1	
	Not applicable	1	
Procedures	Very high negative	50	Procedures are not considered to have any major influence on the ability to diagnose a gas leak. The established procedure is more beneficial when deciding on action.
	High negative	20	
	Low negative	5	
	Nominal	1	
	Low positive	0.5	
	Not applicable	1	

Human-Machine Interface	Extremely high negative	HEP=1	The HMI in the control room is needed in order to diagnose a gas leak. The overall quality of the relevant parts of the HMI used for this purpose is considered good/adequate. It may however, take some time to diagnose such an event as several navigation tasks are required. For instance, there is no direct interface between the F&G system and CCTV which may increase the need for navigation. Excessive time for navigation may delay task execution, but this is covered in task step 5 and 6.
	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	Not considered relevant for this task step.
	Moderate negative	10	
	Nominal	1	
	Low positive	0.5	
	Not applicable	1	
Teamwork	Very high negative	50	Multiple personnel are available in the CCR and may support each other in diagnosing the situation. Differing practices regarding coordination, organizing, and distribution of tasks were observed, and these practices were not formalized nor sufficiently practiced.
	Moderate negative	10	
	Very low negative	2	
	Nominal	1	
	Low positive	0.5	
	Not applicable	1	
Physical Working Environment	Extremely high negative	HEP=1	No observations were made during site visit that could indicate that the physical working environment in the control room should have positive/negative impact on task performance for this task step.
	Moderate negative	10	
	Nominal	1	
	Not applicable	1	

Table 12: Case Study 2 - Worksheet 3 Failure to decide on isolation of segments & ignition sources

Petro-HRA PSF summary sheet			
Facility/installation	**Process Facility X**	**Date**	**XX-XX-XXXX**
HFE ID & description	**Event 3: Failure to decide on isolation and ignition source disconnection. Applicable for the following HFEs in the QRA event tree:** **- HFE 1: Failure to isolate segments** **- HFE 2: Failure to disconnect ignition sources** **- HFE 3: Failure to depressurize facility**		
HFE scenario	**Gas leak in process facility**		
Task step	**4.0: Decide on isolation and disconnection of ignition sources**		
Analyst	**XX and XX**		
HEP Calculation	**0.02**		

PSFs	**PSF levels**	**Multiplier**	**Substantiation: Specific reasons for selection of PSF level**
Time	Extremely high negative	HEP=1	The effect of available time is only considered for execution of the complete task and is therefore only considered for task step 5 (isolate leak) and 6 (depressurize facility).
	Very high negative	50	
	Moderate negative	10	
	Nominal	1	
	Moderate positive	0.1	
	Not applicable	1	
Threat stress	High negative	25	It is not expected that this PSF will have any significant negative impact on deciding whether to perform isolation and disconnection of ignition sources.
	Low negative	5	
	Very low negative	2	
	Nominal	1	
	Not applicable	1	
Task Complexity	Very high negative	50	If the procedure/guideline for handling of HC-leaks are followed, the decision whether to isolate and disconnect ignition sources are not considered to be complex. It is obvious for the operators that the LEL-factor is > 220 without performing any manual calculation. According to the procedure/guideline, ESD 1 shall be activated if the factor is above the acceptance criteria. NB: For smaller leaks, this task may be considered more complex as calculations may be required.
	Moderate negative	10	
	Very low negative	2	
	Nominal	1	
	Moderate positive	0.1	
	Not applicable	1	
Experience/Training	Extremely high negative	HEP=1	Experience/training in use of the procedure/guideline is not considered as applicable for this scenario, as it is obvious that the leak is big (meaning that the LEL-factor > 220 without any need for performing manual calculations). For smaller/diffuse leaks, operator experience and training are expected to have more impact.
	Very high negative	50	
	Moderate negative	15	
	Low negative	5	
	Nominal	1	
	Moderate positive	0.1	
	Not applicable	1	
Procedures	Very high negative	50	A procedure has been developed for operator support, but it is not expected that the procedure will be used as it is obvious that the leak is much bigger than the criteria for activating ESD 1.
	High negative	20	
	Low negative	5	
	Nominal	1	
	Low positive	0.5	
	Not applicable	1	

Human-Machine Interface	Extremely high negative	HEP=1	HMI is not used for this task step. HMI is mainly used for diagnosing the situation and activating the safety functions.
	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	The safety culture has improved after the recent gas leak. The analysts are under the impression that the crew in the control room has a high focus on safety rather than to try to maintain production in such scenario. Feedback from the operators and shift supervisor is that they would activate ESD rather than try to isolate smaller parts of the process and manually disconnect ignition sources. A nominal PSF level is selected.
	Moderate negative	10	
	Nominal	1	
	Low positive	0.5	
	Not applicable	1	
Teamwork	Very high negative	50	Different practices have been established across shifts and it is not clear how tasks are distributed between different personnel, how they collaborate, and how decisions are made. It is considered that this PSF may have a “very low negative" effect on the HEP.
	Moderate negative	10	
	Very low negative	2	
	Nominal	1	
	Low positive	0.5	
	Not applicable	1	
Physical Working Environment	Extremely high negative	HEP=1	No observations were made during site visit that could indicate that the physical working environment in the control room should have negative impact on task performance for this task step.
	Moderate negative	10	
	Nominal	1	
	Not applicable	1	

Table 13: Case Study 2 - Worksheet 4 Failure to isolate segments & ignition sources (ESD 1)

Petro-HRA PSF summary sheet			
Facility/installation	**Process Facility X**	**Date**	**XX-XX-XXXX**
HFE ID & description	**Event 4: Failure to activate ESD 1. Applicable for the following HFEs in the QRA event tree:** **- HFE 1: Failure to isolate segments** **- HFE 2: Failure to disconnect ignition sources** **- HFE 3: Failure to depressurize facility**		
HFE scenario	**Gas leak on process barge**		
Task step	**5.3**		
Analyst	**XX and XX**		
HEP Calculation	**0.05**		
PSFs	**PSF levels**	**Multiplier**	**Substantiation: Specific reasons for selection of PSF level**
Time	Extremely high negative	HEP=1	The timeline analysis shows that the time available (according to the assumptions in the QRA) is 120 seconds. Time required to perform the task is estimated to be approximately 100 seconds meaning that the operators only have 20 additional seconds time. This leads to a significant time pressure and is likely to have negative effect on task performance. See 3.3.5 for further substantiation.
	Very high negative	50	
	Moderate negative	10	
	Nominal	1	
	Moderate positive	0.1	
	Not applicable	1	
Threat stress	High negative	25	Threat stress is not considered to have any major impact on task performance for this task step. Other scenarios like major fires or explosions may one the other hand cause such effect.
	Low negative	5	
	Very low negative	2	
	Nominal	1	
	Not applicable	1	
Task Complexity	Very high negative	50	The task has very low complexity as the operator only needs to press one button on the matrix/CAP. Error on this task step is highly unlikely.
	Moderate negative	10	
	Very low negative	2	
	Nominal	1	
	Moderate positive	0.1	
	Not applicable	1	
Experience/Training	Extremely high negative	HEP=1	The operators are very familiar with the location and function of the ESD 1 push button.
	Very high negative	50	
	Moderate negative	15	
	Low negative	5	
	Nominal	1	
	Moderate positive	0.1	
	Not applicable	1	
Procedures	Very high negative	50	Procedures are not considered to have any effect on the operator's ability to press the ESD push button.
	High negative	20	
	Low negative	5	
	Nominal	1	
	Low positive	0.5	
	Not applicable	1	

Human-Machine Interface	Extremely high negative	HEP=1	The ESD 1 push button is well labeled and is easy to identify.
	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	This PSF is not considered relevant for activation of ESD 1.
	Moderate negative	10	
	Nominal	1	
	Low positive	0.5	
	Not applicable	1	
Teamwork	Very high negative	50	No teamwork is required for activating ESD. Thus, this PSF is not considered applicable for this task step.
	Moderate negative	10	
	Very low negative	2	
	Nominal	1	
	Low positive	0.5	
	Not applicable	1	
Physical Working Environment	Extremely high negative	HEP=1	No observations were made during site visit that could indicate that the physical working environment in the control room should have negative impact on task performance for this task step.
	Moderate negative	10	
	Nominal	1	
	Not applicable	1	

Table 14: Case Study 2 – Worksheet 5 Failure to detect leak location

Petro-HRA PSF summary sheet			
Facility/installation	**Process Facility X**	**Date**	**XX-XX-XXXX**
HFE ID & description	**Event 5: Failure to identify leak/ failure to diagnose need for blow down. Applicable for the following HFEs in the QRA event tree:** **- HFE 1: Failure to isolate segments** **- HFE 2: Failure to disconnect ignition sources** **- HFE 3: Failure to depressurize facility**		
HFE scenario	**Gas leak in the process facility (>1 kg/s)**		
Task step	**3.0 and 6.3**		
Analyst	**Marius Fernander & Sondre Øie**		
HEP Calculation	**0.01**		
PSFs	**PSF levels**	**Multiplier**	**Substantiation: Specific reasons for selection of PSF level**
Time	Extremely high negative	HEP=1	The effect of available time is only considered for execution of the complete task and is therefore only considered for task step 5 (isolate leak) and 6 (depressurize facility).
	Very high negative	50	
	Moderate negative	10	
	Nominal	1	
	Moderate positive	0.1	
	Not applicable	1	
Threat stress	High negative	25	Threat stress is not expected to have any impact on execution of this task step.
	Low negative	5	
	Very low negative	2	
	Nominal	1	
	Not applicable	1	
Task Complexity	Very high negative	50	The operators have already started to locate the leak (ref diagnosis performed prior to decision to activate ESD 1). This task step also involves looking for changes in process parameters after the plant/system has been isolated. These tasks are comparable to what the operators are used to during normal operations. Complexity is thus considered to have a nominal effect on the HEP.
	Moderate negative	10	
	Very low negative	2	
	Nominal	1	
	Moderate positive	0.1	
	Not applicable	1	
Experience/Training	Extremely high negative	HEP=1	See substantiation for event 3.0.
	Very high negative	50	
	Moderate negative	15	
	Low negative	5	
	Nominal	1	
	Moderate positive	0.1	
	Not applicable	1	
Procedures	Very high negative	50	No procedures are available nor needed to perform this task step. Successful task execution is dependent on operator's training and experience.
	High negative	20	
	Low negative	5	
	Nominal	1	
	Low positive	0.5	
	Not applicable	1	

Human-Machine Interface	Extremely high negative	HEP=1	The HMI is considered to have high quality and support the operator(s) in monitoring the pressures in the different segments. Trends can be brought up for this purpose but may require some navigation.
	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	PSF is not considered relevant for this task step.
	Moderate negative	10	
	Nominal	1	
	Low positive	0.5	
	Not applicable	1	
Teamwork	Very high negative	50	See substantiation for task step 3.0 (HFE ID 2).
	Moderate negative	10	
	Very low negative	2	
	Nominal	1	
	Low positive	0.5	
	Not applicable	1	
Physical Working Environment	Extremely high negative	HEP=1	No observations were made during site visit that could indicate that the physical working environment in the control room should have negative impact on task performance for this task step.
	Moderate negative	10	
	Nominal	1	
	Not applicable	1	

Table 15: Case Study 2 - Worksheet 6 Failure to decide on blow down

Petro-HRA PSF summary sheet			
Facility/installation	**Process Facility X**	**Date**	**XX-XX-XXXX**
HFE ID & description	**Event 6: Failure to decide on blow down. Applicable for the following HFEs in the QRA event tree:** **- HFE 1: Failure to isolate segments** **- HFE 2: Failure to disconnect ignition sources** **- HFE 3: Failure to depressurize facility**		
HFE scenario	**Gas leak in the process facility (>1kg/s)**		
Task step	**4.0**		
Analyst	**Marius Fernander & Sondre Øie**		
HEP Calculation	**0.01**		
PSFs	**PSF levels**	**Multiplier**	**Substantiation: Specific reasons for selection of PSF level**
Time	Extremely high negative	HEP=1	The effect of available time is only considered for execution of the complete task and is therefore only considered for task step 6.
	Very high negative	50	
	Moderate negative	10	
	Nominal	1	
	Moderate positive	0.1	
	Not applicable	1	
Threat stress	High negative	25	Some threat stress could be expected. It has been perceived by some operators that a full depressurization could damage parts of the facility and lead to big economic losses. Deciding to activate ESD 2 (blow down) could therefore lead to some threat stress. This belief has partly been changed after the incident, but it is assumed that this PSF will have some negative effect on the HEP.
	Low negative	5	
	Very low negative	2	
	Nominal	1	
	Not applicable	1	
Task Complexity	Very high negative	50	If the procedure for handling HC leaks is followed, this task step is not considered to be complex. The procedure clearly states that ESD 2 (sequential automatic depressurization) shall be activated if the leak location cannot be detected. Positive credit for the procedure is accounted for under the PSF for “procedures”.
	Moderate negative	10	
	Very low negative	2	
	Nominal	1	
	Moderate positive	0.1	
	Not applicable	1	
Experience/Training	Extremely high negative	HEP=1	See substantiation for task step 4 (HFE ID 3).
	Very high negative	50	
	Moderate negative	15	
	Low negative	5	
	Nominal	1	
	Moderate positive	0.1	
	Not applicable	1	
Procedures	Very high negative	50	The guideline/procedure provides good decision support for the operators. Both in terms of a flow chart and written instruction on how the situation shall be handled. It is explicitly stated that: Blow down shall be activated as soon as possible from the CAP if the leak location cannot be identified. It is believed that this PSF has positive effect on the nominal HEP.
	High negative	20	
	Low negative	5	
	Nominal	1	
	Low positive	0.5	
	Not applicable	1	

Human-Machine Interface	Extremely high negative	HEP=1	HMI is not considered to have any effect on task execution for this task step. HMI is mainly used for diagnosing the situation and activating the safety function (ESD 2).
	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	The safety culture has improved after the recent gas leak. The analysts are under the impression that the crew in the control room has a high focus on safety rather than to try to maintain production in such scenario. Feedback from the operators and shift supervisor is that they would activate ESD 2 rather than try to depressurize smaller segments of the process if the leak location is not 100% known.
	Moderate negative	10	
	Nominal	1	
	Low positive	0.5	
	Not applicable	1	
Teamwork	Very high negative	50	See substantiation for task step 4 (HFE ID 3).
	Moderate negative	10	
	Very low negative	2	
	Nominal	1	
	Low positive	0.5	
	Not applicable	1	
Physical Working Environment	Extremely high negative	HEP=1	No observations were made during site visit that could indicate that the physical working environment in the control room should have negative impact on task performance for this task step.
	Moderate negative	10	
	Nominal	1	
	Not applicable	1	

Table 16: Case Study 2 - Worksheet 7 Failure to activate blow down (ESD 2)

Petro-HRA PSF summary sheet			
Facility/installation	**Process Facility X**	**Date**	**XX-XX-XXXX**
HFE ID & description	**7: Failure to activate ESD 2. Applicable for the following HFEs in the QRA event tree:** **- Failure to isolate segments** **- Failure to disconnect ignition sources** **- Failure to depressurize facility**		
HFE scenario	**Gas leak on process barge**		
Task step	**6.2**		
Analyst	**Marius Fernander & Sondre Øie**		
HEP Calculation	**0.001**		

PSFs	PSF levels	Multiplier	Substantiation: Specific reasons for selection of PSF level
Time	Extremely high negative	HEP=1	The QRA shows that the risk for the facility is only to a limited degree sensitive for delayed activation of blow-down. This is partly because the process segments are big, and the flare calculation report shows that it will take approx. 30 min to depressurize the process down to 4 barg after ESD 2 has been activated. It is therefore argued that the time PSF should be assigned a nominal multiplier. NB: This substantiation is not applicable for ignited HC-leaks which may escalate to other areas/equipment. See 3.3.5 for further substantiation.
	Very high negative	50	
	Moderate negative	10	
	Nominal	1	
	Moderate positive	0.1	
	Not applicable	1	
Threat stress	High negative	25	Threat stress is not considered to have any major impact on task performance for this task step. Other scenarios like major fires or explosions may one the other hand cause such effect.
	Low negative	5	
	Very low negative	2	
	Nominal	1	
	Not applicable	1	
Task Complexity	Very high negative	50	The task has very low complexity as the operator only needs to press one button on the matrix/CAP. Error on this task step is highly unlikely.
	Moderate negative	10	
	Very low negative	2	
	Nominal	1	
	Moderate positive	0.1	
	Not applicable	1	
Experience/Training	Extremely high negative	HEP=1	The operators are well familiar with the location and the function of the ESD 2 push button.
	Very high negative	50	
	Moderate negative	15	
	Low negative	5	
	Nominal	1	
	Moderate positive	0.1	
	Not applicable	1	
Procedures	Very high negative	50	Procedures are not considered to have any effect on the operator's ability to press the ESD push button.
	High negative	20	
	Low negative	5	
	Nominal	1	
	Low positive	0.5	

	Not applicable	1	
Human-Machine Interface	Extremely high negative	HEP=1	The push button is well labeled and is easy to identify.
	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	This PSF is not considered relevant for activation of ESD 2.
	Moderate negative	10	
	Nominal	1	
	Low positive	0.5	
	Not applicable	1	
Teamwork	Very high negative	50	No teamwork is required for activating ESD. Thus, this PSF is not considered applicable for this task step.
	Moderate negative	10	
	Very low negative	2	
	Nominal	1	
	Low positive	0.5	
	Not applicable	1	
Physical Working Environment	Extremely high negative	HEP=1	No observations were made during site visit that could indicate that the physical working environment in the control room should have negative impact on task performance for this task step.
	Moderate negative	10	
	Nominal	1	
	Not applicable	1	

3.6.1 Results

The OAET presented in Figure 21 shows the same event tree presented in 3.5, with the inclusion of the HEPs for the events/branches in the OAET and probability for all eight potential outcomes. The outcome displayed at the top corresponds to successfully activating ESD 1 within 2 minutes followed by activation of ESD 2 to depressurize the plant. What this visualization does not communicate is the HEPs for all the HFEs which must be included in the QRA. An alternative/supplementary representation of this is shown in Table 17.

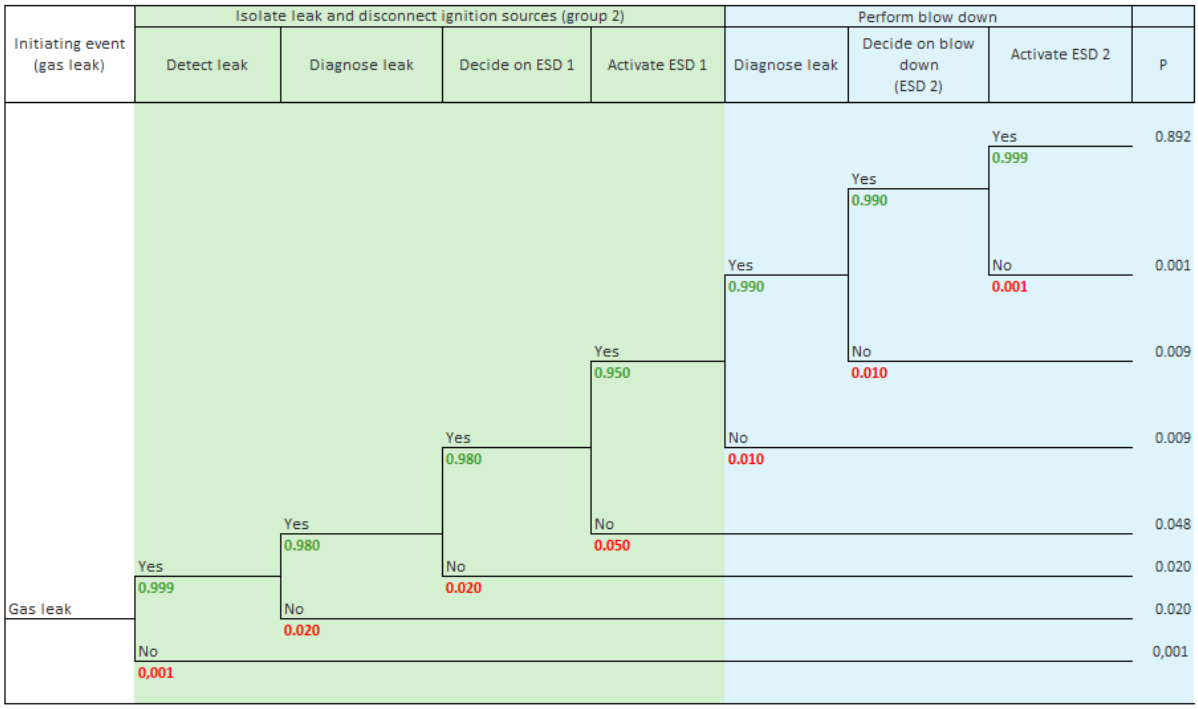

Figure 21: Case Study 2 - Operator Action Event Tree with probabilities

Another way to present the results is by using a tabular format to present the results. In this case study, the QRA required input from the Petro-HRA to determine the reliability of three different safety functions. Table 17 is therefore included to show the results for all individual events in addition to the human reliability estimates for the three safety functions modelled in the QRA.

Table 17: Case Study 2 - Failure probabilities for task steps, HFEs and the complete task

ID	HFE description	HEP
Event 1	Failure to detect leak	0.001
Event 2	Failure to diagnose leak	0.020
Event 3	Failure to decide on ESD 1	0.020
Event 4	Failure to activate ESD 1	0.050
Event 5	Failure to diagnose leak (need for blow down)	0.010
Event 6	Failure to decide in blow down	0.010
Event 7	Failure to activate ESD 2	0.001

HFE 1	HEP ignition source isolation (ESD 1)	0.089
HFE 2	HEP isolation of segments (ESD 1)	0.089
HFE 3	HEP depressurization (ESD 2)	0.021
Task	HEP for complete task	0.108

The HFEs in Table 17 are calculated by multiplying the nominal Petro-HRA HEP (0.01) with the PSF multiplicators shown in Table 8 1 for each event. The next step is to multiply all events by following the OAET logic. An example of how HFE 1 was calculated is shown below.

HFE 1 – Failure to activate ESD 1

- Nominal HEP = 0.01
- Event 1: Failure to detect leak = 0.01 x 0.1 (positive effect of task complexity) = 0.001
- Event 2: Failure to diagnose leak = 0.01 x 2 (negative effect of task complexity) = 0.02
- Event 3: Failure to decide on ESD 1 = 0.01 x 2 (negative effect of teamwork) = 0.02
- Event 4: Failure to activate ESD 1 = 0.01 x 50 (negative effect of time) x 0.1 (positive influence of complexity) = 0.05
- HFE1= 1 – ((1-0.001) x (1-0.02) x (1-0.02) x (1-0.05)) = 0.089

3.6.2 HRA Implications for the QRA Results

The results from the QRA indicates that personnel risk (expressed as PLL) shows little sensitivity in terms of time spent to isolate segments (HFE 2) and activate blowdown (HFE 3). This can be explained by the substantial volumes of some of the process segments, meaning that most leaks will have long duration despite having initiated blow-down of the isolated segment. It must also be highlighted that the time required for the process to depressurize down to 4 barg after ESD 2 has been activated is approx. 30 minutes according to the flare calculation report, so the response time for activating blow-down will most likely play a minor role for the complete time required for depressurizing the plant.

However, timely activation of ESD 2 may still play an important part on risk for escalation. This is because the expected ignition frequency shows higher sensitivity in terms of response time, meaning that timely isolation of ignition sources is time critical. In the QRA it was therefore decided to run sensitivities using the calculated HEP for ignition source isolation to investigate the effect the HEP has on overall personnel risk (expressed as PLL).

In the QRA it was assumed that the operator shall isolate ignition sources within 2 minutes for leaks > 1 kg/s. Figure 18 shows how the ignition probability is expected to increase as a function of time for which the ignition sources in the area are exposed. The graph illustrates an almost linear relationship between the ignition frequency and response time. In general, the graph shows a relative increase in the ignition frequency of approximately 12% per minute of delayed response. This means that delaying the response from two to three minutes will increase the ignition frequency by 12%.

A HEP of 10% for isolation ignition sources within 2 minutes leads to an increase in personnel risk (PLL) in the magnitude of approximately 1%. This assumes that the operators are able to execute the task within 3 minutes. A prolonged delay in response time will further increase the ignition probability and thereby the PLL.

3.7 Step 7: Human Error Reduction

Human error reduction is one of the main objectives of performing an HRA. In this case study, the most significant risk is related to delayed operator response. Any PSFs identified that could lead to delayed response were further investigated to propose adequate risk reducing measures. Table 18 provides examples of observations and risk reducing measures that were proposed for this specific project.

Table 18: Case Study 2 - Observations and recommendations

#	Observation	Recommendation
1	Operators were not fully aware of the criticality of immediate isolation of ignition sources.	1. Ensure that the operators are made aware of the importance of early isolation of ignition sources and implement this into the training and drills. 2. Update the procedure/guideline for handling HC leaks to reflect the importance of early ignition source isolation. 3. Ensure that personnel on all shifts (also newly hired) have a common understanding and are familiar with the purpose and the content of the guideline/procedure. 4. Include a performance criterion for response time in the training scenarios.
2	Some weaknesses were identified in terms of the usability of the HMI. The recommendations mentioned here should be implemented in order to reduce the response time for diagnosing the situation.	5. Improve the alarm system to ensure that critical alarms are not hidden by lower priority consequence alarms. 6. Some observations were made concerning substantial need for navigation to access critical information. A more detailed HMI-study assessment is therefore recommended. 7. As per now there is no interface between the F&G- and CCTV systems, meaning that additional time is needed to display the area on the monitors in the CCR. Integrating these systems is recommended to reduce time needed to diagnose a gas leak. 8. The alarm list is not available on the Large Screen Display (LSD). Implementing the alarm list for higher priority alarms (priority 1 & 2) on the LSD may lead to increase situation awareness and have positive impact.
3	Some different work practices were identified in terms of how work is organized in the CCR and how decisions are made. This could contribute to increased response time	9. Ensure that all shifts have a common practice in how work is organized and further emphasize that personnel are empowered to make own decisions so response time is not delayed in situations where the shift supervisor may be unavailable.

Part 3
Background Information for The Petro-HRA Method

4 Background to the Petro-HRA Method: Introduction

A human reliability analysis is defined as: "*Any method by which human reliability is estimated*" (Swain, 1990, p.301). The result of an HRA is a quantitative estimate of the likelihood of one or several human errors. A human error is an action, or lack of expected action, that results in an irreversible failure of a component, system, or function. Note that the definition of human error is in no way a definition that "blames the human", as an operator might be "forced" to the action, or inaction, by the presence of unfavourable conditions. Therefore, Petro-HRA, as most contemporary HRA methods, shifts the focus from the intrinsic reliability of an operator performing a task to the performance conditions for the task. An HRA is usually performed within a larger quantitative risk analysis such as probabilistic risk analysis (PRA), quantitative risk analysis (QRA) or total risk analysis (TRA). The purpose of the quantitative estimate is usually to estimate if risk is within acceptable range and to estimate where risk reducing effort is most needed.

5 Overview of the Petro-HRA Method

Table 19 gives an overview of the purpose, expected input and expected output from each step of the Petro-HRA. This table can be used as a checklist and look-ahead for analysts during the analysis process.

Table 19: Overview of the main steps in a Petro-HRA

Step Number	Main step (and sub-steps)	Purpose of the step	Expected Inputs	Expected Use of Outputs
Step 1	Scenario Definition • Initial meetings • Document review • Hazard identification • Establish scenarios for analysis	• To define the context, scope and boundary of the HRA and the analysis scenario(s). • To start familiarizing with details of the scenario, such as the role and responsibilities of the operator. • To identify potential HFEs (e.g., in the QRA and/or HAZID, etc.)	Inputs from the QRA team, process or systems experts, site contact, other relevant SMEs.	Outputs will determine the focus of the qualitative data collection activities (Step 2).
Step 2	Qualitative Data Collection • Site visit • Workshop	• To collect information about the event sequences, timings and operator tasks in the scenario. • To collect information about factors that may affect human performance. • To start to identify potential human errors.	Inputs from site personnel such as operating staff, shift supervisors, training personnel, technical disciplines, and from additional documentation collected at site.	Outputs will be used to inform the task analysis (Step 3), HEI (Step 4) and human error modeling (Step 5). Outputs will also inform the PSF assessment in Step 6.
Step 3	Task Analysis • Define the goal of the operator in the scenario. • Define the task steps required to achieve the goal.	• To describe the task steps that are carried out by human operators in the scenario.	Inputs primarily from the qualitative data collection (Step 2). Some inputs may also come from the information collected during preparation (Step 1) (for example, initial meetings and documentation review)	Outputs will be used to inform the HEI (Step 4) and human error modeling (Step 5). Outputs will also be used to inform which operator actions should be quantified (Step 6).

Step 4	Human Error Identification • Review significant task steps. • Identify potential human errors.	• To identify the potential human errors that could occur in the scenario. • To identify likely consequences and recovery opportunities.	Inputs primarily from the task analysis (Step 3) and the qualitative data collection (Step 2).	Outputs will be used to inform the human error modeling (Step 5) and the human error quantification (Step 6). Outputs will also inform the human error reduction (Step 7).
Step 5	Human Error Modelling • Define the HFE • Develop event/fault trees • Model recovery • Model dependency	• To define the human failure events (HFE) to be quantified. • To represent graphically the sequence/logic of events/faults which lead to the HFE(s) occurring. • To show how human failures interact with system failures in the scenario.	Inputs primarily from the HEI (Step 4) and the task analysis (Step 3).	Outputs will be used to inform the human error quantification (Step 6) and human error reduction (Step 7).
Step 6	Human Error Quantification • Assign nominal value • Assign PSF weights • Calculate HEP for the HFE	• To quantify the probability of the HFE(s) occurring, given the presence of factors that may positively or negatively affect human performance.	Inputs from all the former steps.	Outputs will be used to update the QRA. Outputs may also be used to inform human error reduction (Step 7).
Step 7	Human Error Reduction • Impact assessment • Error reduction analysis • Develop recommendations	• To develop recommendations to reduce the risk in the scenario.	Inputs from all the former steps.	Outputs will be provided to the site for consideration as part of their normal risk reduction processes.
N/A	Document the HRA	• To present the results of the HRA for use by the QRA, the site and other relevant parties. • To provide evidence of a structured approach to human reliability assessment for the given scenario(s). • To provide a clear and unambiguous record of the activities and analyses performed, and their results, for future consultation (e.g., as part of a periodic update of the QRA).	Inputs from all previous steps of the HRA.	Outputs will be provided to the QRA team for inclusion in the Total Risk Assessment (TRA) document package.

6 Background to the Petro-HRA Method

This section provides some background and history to QRA in the Petroleum industry and the context within which a Petro-HRA might be commissioned. The section also provides guidance on performing Petro-HRA for a design project.

6.1 QRA in the Petroleum Industry

QRA has been performed in the petroleum industry for a number of years. It is somewhat striking that it has taken almost 40 years to include HRA as part of QRA, while the Nuclear Industry has been doing this from the very beginning in the mid-1970s. Even to this end HRA is only rarely integrated with QRA; however, there has been some recent studies using HRA, both as input for QRA and other special safety studies. In order to understand this and then be able to improve it, we must understand the background and basic methodology for QRA.

Quantitative risk assessment (QRA) is a formalised specialist method for calculating individual, environmental, employee and public risk levels for comparison with regulatory risk criteria (DNV GL, 2014). Although it may be demonstrated that the calculated risk is below a given risk criterion, the QRA still constitutes valuable decision support for making decisions about safety throughout the lifecycle of an installation/facility. Continuous improvement and risk reduction are required even if a certain risk criterion is met. In principle, this applies for human as well as hardware reliability improvements.

QRAs are typically made and updated in several project phases, including the design phase (design risk analysis – DRA), construction phase (construction risk analysis – CRA) and the operation phase (usually just termed QRA)[1]. The main differences between a DRA, a CRA, and an as-built QRA are the level of information available at the time of analysis. Simple assumptions made in early phases may be explicitly modelled when sufficient information is available. The modeling of HFEs is most relevant when sufficient information is available. This will be the case in late stages of the design phase (to the extent modeling of HFE during design is feasible) and in the operation phase, which are the phases that have been focused on in the Petro-HRA project.

The QRA methodology originated from the Reactor Safety Study in the US (WASH-1400), which developed the methods used in the Nuclear Power Industry's Probabilistic Risk Assessment (PRA) or Probabilistic Safety Assessment (PSA). However, the development of QRA within the Petroleum Industry has been different from PRA/PSA within the Nuclear Power Industry in many ways. Some of the differences are important for us since the Petro-HRA method developed for the Petroleum Industry, which need to be integrated with the QRA, is based on the SPAR-H method developed for integration with the Nuclear Power Industry PRA/PSA.

PRA is mainly a tool used during operation of nuclear power facilities (NPPs), not for the design of NPPs, whereas QRA mainly has been a tool during design of the petroleum installations/facilities. More recently there have been some efforts to make the QRAs more "operational". One challenge is that the QRAs (or CSEs) developed for the early project phases are very coarse, and even with more explicit modelling in the operations phase, a QRA in the Petroleum Industry is far less detailed compared to a PRA in the Nuclear Power Industry. A PRA is maybe ten to twenty times as comprehensive as a QRA. This is one reason why HFE and the use of HRA within PRA have been in place since day one (i.e., THERP as part of WASH-1400); whereas HRA within QRA has been absent (HFEs have not been explicitly modelled).

[1] Also other terms like Concept Safety Evaluation (CSE) and Total Risk Analysis (TRA) are used.

Another important difference, when we try to integrate HRA in QRA, is the difference in methodology between PRA and QRA. The backbone of a PRA is the combination of event trees and fault trees, which makes it possible to calculate risk through the sum of minimal cut sets. One of the types of parameters included in the minimal cut sets are HFEs, which makes it fairly easy to assess the importance of an HFE, e.g., for the purpose of conducting screening analyses.

The QRA is also based on event trees; however, the branch probabilities in the event trees are not necessarily calculated using fault tree models. Quite often the branch probabilities are calculated through empirical equations, for which it is not possible to express risk in terms of the sum of minimal cut sets. Thus, the integration of HRA in QRA is not through HFEs included in minimal cut sets; it has to be adapted to the existing QRA methodology. It could be part of an equation for the calculation of event tree branch probability, part of a fault tree, or directly as a branch probability in the event tree.

6.2 Understanding the Context of HRA

The context within which the HRA has been commissioned will have implications with respect to the most appropriate approach to take, because this may affect the amount of information available and the time available for the overall analysis. Some examples of the different context within which the HRA is likely to be required are listed below:

- **Design HRA**. The HRA may be commissioned as part of a TRA for a new facility that has not yet been built. In this case, there will be no existing documentation to review (such as operating procedures, system descriptions, previous analysis reports, event reports, etc.) and no experienced operators to interview. The HRA analyst will have to make a lot of assumptions about human actions in the major accident scenario and the HRA will include a lot of uncertainty.

- **HRA for an operating facility**. The HRA may be commissioned as part of a QRA of an existing facility. In this case, there is likely to be lot of documentation available to the HRA analyst for review, and there will be experienced operators that the analyst can interview as well as fewer assumptions and uncertainties.

    - *Update to an existing analysis*: The HRA may be commissioned to assess the human contribution to risk of a change to an existing operation as a result of the introduction of new equipment, an upgrade of existing equipment, or a change to the way operators perform a task, etc.
    - *Validation of an assumption in the QRA*: The HRA may be commissioned to validate an assumption regarding a human action in the existing HRA.
    - *Periodic review of the QRA*: The QRA may be subject to a period review (for example, every 5 years) and this may include a review of human actions modelled in the QRA. In this case, the HRA analyst will investigate the previous claims on human actions to assess whether anything has changed over time and whether this affects the claimed Human Error Probability (HEP).

It is important for the HRA analyst to understand the context of the HRA from the beginning, as this will shape the approach used.

6.3 Performing Petro-HRA for a Design Project

HRA is usually thought of in terms of predictive analysis of the factors that influence human performance in systems that are already built and/or in operation. However, HRA can also be used to

provide valuable input to the design of systems, as part of the overall HF engineering activity. It is important that HF and HRA are implemented early enough in the design process when they can still influence the system design (i.e., to assess and select designs that will decrease the likelihood of human error). If implemented too late in the process, where the design is very mature and/or already finalized, it may be too costly or impractical to alter the design and so the real value of performing an HRA or HF analysis is lost.

HRA should be performed on an iterative basis throughout the design process, however the analyst should be aware that it might not be possible to perform any quantification until later in the design process. In the early stages of designing a system, there is typically a lot of uncertainty about, for example, the roles and functions of the human operator, the system interfaces, etc. Qualitative analysis techniques are more suitable here: for example, performing a high-level task analysis to inform other design activities such as function allocation, HAZOP, etc. Detailed task analysis or quantification may not be possible or practicable at this point due to the lack of information available. As more detail about the design becomes available, and as the design options stabilize, then the level of uncertainty should reduce and the possibility to perform detailed qualitative and quantitative analysis is increased. The HRA can be updated based on this new information, and the calculated HEPs can be refined further.

Some benefits of performing Petro-HRA for design projects:

- Qualitative analysis can provide valuable early input to other HF engineering activities such as function allocation, HMI design, procedure development, etc.
- Quantitative analysis can be used to compare the likelihood of human error in different designs concepts, to enable ranking of designs for particular errors or ranking of recommendations for improvements to the design

Important considerations for Petro-HRA for design projects:

- Uncertainties must be clearly documented and communicated to the design team, reviewers and/or other relevant personnel to ensure transparency and traceability of the HRA and any recommendations made to the design team.
- The rationale for any assumptions made must also be clearly documented. Assumptions should be checked periodically with the design team or other knowledgeable personnel to ensure that they remain reasonable.

If performing quantification, the substantiation for the weighting of PSFs should also be clearly documented so that the PSFs can be adjusted at a later date if any of the documented conditions change.

7 Background to Step 1: Scenario Definition

One of the most important activities in an HRA is to define the scope of the analysis, i.e., to identify what is to be analysed. This will shape the remainder of the HRA, for both the qualitative and quantitative analyses. It can be difficult because it is unlikely that the HRA analyst will be provided with a well-defined HFE at the beginning of the analysis. It is more likely that they will be provided with a general description of a major accident scenario (for example, "hydrocarbon leak") or will simply be instructed to perform an HRA for a facility. In both cases, the analyst must do some preparation to identify a credible scope and clarify the purpose of the analysis.

There are four main activities in this step:

- **Participate in initial meetings**. The analyst should participate in the general QRA kick-off meeting and the general HAZID meeting to ensure that HRA is represented and to assist with the identification of HFEs and human-related hazards. The analyst should also arrange an HRA-specific meeting and scenario meeting to discuss and agree the scope of the HRA, confirm and talk-through the scenario(s) to be analysed and start collecting information about the scenario.

- **Perform a document review**. The analyst should next review available documentation to gather additional information to define the analysis scenario. The document review may be ongoing throughout the whole HRA as additional documentation is identified.

- **Develop the scenario description**. The analyst should now have enough information to develop a description of the scenario, setting the boundaries and scope for the HRA and documenting assumptions made about the scenario.

- **Perform an initial task identification**. The analyst should then use the information collected to date to identify the key operator tasks in the scenario, and to check whether there are any knowledge gaps about the operator response. This information is used as the basis for further discussion and talk-through of tasks with operators during the qualitative data analysis step.

7.1 Guidance on Participating in Initial Meetings

The HRA analyst should participate in the general QRA kick-off meeting to discuss the scope of work for the project and identify the role and place for HRA. A good starting point is to discuss what the scope of the QRA is, which hazardous events are analysed, and where in the QRA the HRA may be relevant. Subsequent discussions (e.g., in the general HAZID meeting, or the scenario meeting) may target the role of operators in accident scenarios, what operators typically do to monitor and control safety systems/ barriers, and how this can be modelled in the QRA event tree. These discussions can then work as a preliminary identification of which events operator actions and potential HFEs can have a significant impact on the facility's risk level.

The HRA kick-off meeting should as a minimum include the HRA analyst, one person with competence in or responsibility for QRA, one person with competence in or responsibility for technical safety, one person with competence in or responsibility for operational safety and the person who commissioned the HRA. At least one of the people in the kick-off meeting should be from the facility where the analysis will take place, to act as a main site contact for the qualitative data collection activities.

In addition, it is necessary to discuss and agree on the ambitions and resources of the analyses. This depends highly on whether or not there is an existing QRA available, and to what extent the team is

familiar with the facility. In QRAs for which event trees have already been developed, a review, such as Hazard Identification (HAZID), of the existing model should be planned for to identify which events warrant further analysis.

If event trees have not been developed, an approach may be chosen where the HFEs are explicitly modelled as branches in the event tree or where the HFEs are combined with system failure events to form a pivotal event in the event tree sequence.

7.2 Guidance on Participating in a HAZID Meeting

If the HRA is conducted as part of a QRA, a HAZID is commonly within the scope of work, either as an entirely new activity in the early design phases of the facility, or as an update of existing versions. The HAZID often involves a dedicated meeting where various stakeholders and disciplines meet to discuss the hazards, consequences and safeguards present at the facility. This is the main arena for agreeing on whether an HRA should be performed, and if so, what scenarios should be included in the scope of work.

From the HRA analyst's point of view the objectives of the HAZID meeting are:

- To gain further understanding about the operator(s) role in preventing or mitigating hazardous events, as indicated through initial discussions with the QRA team and document reviews.
- To use this understanding to verify whether the operator actions and potential HFEs are (to be) modelled in the QRA risk model and thus require quantification of HEPs.

Before the actual meeting takes place the HRA analyst should discuss and agree with the HAZID meeting facilitator how HRA-related topics shall be addressed, such as:

- Safety systems dependence on operator actions.
- Operator responses (monitoring, detection, diagnosis, decision and action).
- Time available.
- Personnel involved.

The HRA analyst and HAZID facilitator should also agree on a set of HRA-specific guidewords to use during the HAZID meeting. A common approach is to ask these guidewords for each hazard and associated safety system (i.e., barrier). Keep in mind that HRA related topics are just a small part of the HAZID scope, which also is often pressed on time, so keep things short and simple.

In the actual meeting, HRA should be introduced to ensure other participants are aware of the purpose of discussing HRA guidewords and considering operator hazards. This is especially true if HRA has not previously been considered in HAZID meetings. The introduction should include:

- The scope of the HRA within the QRA
- A short explanation of the HRA process
- The HRA objectives in the HAZID meeting
- The HAZID guidewords for discussing HRA topics
- The expected outcome and way forward

The expected outcomes from the HAZID meeting are:

- High-level identification of HFEs and operator tasks that are critical for facility safety.
- Decision about whether or not the HFEs and operator tasks should be modelled in the QRA model, and thus quantified.
- Establishment of representative scenarios which form the context and assumptions for the HFEs that are to be included in the QRA.
- Consideration of whether HFEs should still be investigated and quantified even if this is not required by the QRA.

If the conclusion is that it is not feasible or practical to model the HFEs in the QRA risk model, consider whether the task is safety critical and should be analysed as a separate activity, outside of the QRA. There are several ways to assess criticality, but the easiest and most common method is to assess it based on the severity of potential consequences resulting from human errors. This can be discussed initially during the HAZID meeting and then elaborated on when studying the topic closer by re-visiting documentation. For more information on this subject the Energy Institute's guidance on Safety Critical Task Analysis can be read (Energy Institute, 2011). The HRA analyst should discuss this with the client/facility representative, QRA team members and other technical safety experts.

For HRAs not modelled in the QRA a decision should be made about whether or not it is beneficial (to the client/facility) to perform HEM and quantification, i.e., only perform HEI and Safety Critical Task Analysis. There are advantages and disadvantages to this approach. The obvious benefit is that it takes less time. In particular, activities related to human error modeling (such as generating fault trees), can be very time consuming. Human error quantification also takes some time, depending on the complexity of the chosen quantification method. One of the disadvantages of not performing any HEM is that it is difficult to identify how combinations of errors represent vulnerabilities in task execution. This is especially true for well-defended, complex systems.

The most apparent disadvantage of not performing the HEP calculation is that relative quantitative probabilities (derived from PSFs) cannot be used to assess and prioritize human error reduction strategies, which will instead depend on the qualitative analysis. Furthermore, there are other applications besides QRA that can benefit from including HEPs, such as Layers of Protection Analysis (LOPA). Consequently, such needs should be discussed when deciding whether or not to perform a full HRA including HEP quantification. More information about whether to choose a qualitative or fully quantitative analysis can be read in the Energy Institute's guidance on HRA (Energy Institute, 2012).

7.3 Guidance on Performing a Document Review

The document review alone will not provide sufficient information about the scenario and tasks and must be supplemented with a site visit and/or workshop with operators before the analyst will have enough information to perform the qualitative and quantitative analyses. There is often a wealth of reports, manuals and system descriptions available, so it is important to carefully select the most relevant documents to read. Based on initial discussions with the customer, QRA analysts and other technical disciplines, browse through reports and identify key topics to narrow down on. The documents are reviewed throughout the HRA process, according to information needs.

A recommended list of documents is provided in Table 1.2. This list is not exhaustive and there may be additional relevant documents available that are useful for the HRA. Similarly, all of the documents on the list might not be available, or they may be called by different names at different sites. However, the list should be used as a starting point for requesting documentation for review.

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. Any questions, knowledge gaps, areas of uncertainty or assumptions should be documented for incorporation into the later data collection activities.

In addition to reviewing the documentation for information about the major accident scenario, the analyst should also try to become familiar with the terminology and acronyms used in the documents. This will facilitate later discussions and interviews with SMEs. The analyst should be aware that terminology and acronyms may differ between sites, or the same terms may be used to refer to different things.

7.3.1 Representation of Scenarios

As a minimum the scenario should be described in prose; using a table format also gives a good overview. There are also several ways to illustrate the scenario graphically using, for example, a Sequential Time Event Plotting (STEP) diagram or Operational Sequences Diagram (OSD; Stanton et al. 2013). Such techniques are especially useful for visual communication of event sequences, time, and relationships between different actors (both technical and human).

7.3.2 Verification of the Scenarios' Relevance to the QRA

For QRA-driven HRAs, the scenarios are defined by the QRA event tree model. That is, a scenario can be made by following a specific event sequence from the initiating event to the outcome (i.e., impact or consequence). Each branch in the event tree represents the probability of success or failure for a safety system/ barrier to be realized or for an undesired event to occur. When developing a scenario, it is important that it captures the details and assumptions for each event to ensure that it correctly illustrates which safety systems/barriers are involved and how they function, especially with regards to time. The scenario should therefore be verified by QRA analysts and/or other relevant technical disciplines such as technical safety, process technology, well control, and Dynamic Positioning (depending on the scenario).

Site visits and feedback from operators (e.g., in an HRA workshop) can be used to verify that the scenario correctly captures details about task context, location and external environment. However, keep in mind that the operators may be concerned about events and circumstances which deviates from how the scenario is defined by the QRA event tree. Such "What-If" concerns can be addressed and recorded but must not make the scenario description invalid. The consequence may be that the HEP for the HFE integrated in the event tree is incorrect.

7.4 Guidance on Defining Success and Failure for HFEs in the QRA

One of the most important criteria for a good integration of HRA into a QRA is to have a clear and concise definition of what is meant by HFE "success" and "failure". While this can be considered part of verifying the scenario's relevance for the QRA event sequence, its importance makes it necessary to emphasize it in a dedicated and separate section. As an overall principle, the definition should derive from the QRA model. Examples of HFEs in QRAs are "ESD failure" or "blowdown failure". Then, for ESD, it needs to be defined what success and failure refers to in terms of number of ESD valves closing or not closing, if the failure is a partial close or none at all, what segment is affected, and the location of the valve(s). Similarly for blowdown, success or failure needs to be defined with regards to pressure levels, time frames, and segments. For example, does the QRA consider blowdown to be successful regardless of time? If no, when can it be considered a success? Are there degrees of success

e.g., reflected in different risk levels? Such questions need to be answered before continuing with task analysis, error identification and modelling.

The scenario description should also include a definition of what is considered HFE success and failure, including a consideration of time. If it is not possible to conclude on a final definition, a preliminary version should be made and later verified in the HRA workshop and or further meetings with the QRA analysts.

7.5 References

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

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.

8 Background to Step 2: Qualitative Data Collection

Qualitative data collection is rarely a linear process, and it is unlikely that the analyst will collect all of the necessary information in a single site visit/workshop. A more likely situation is that the analyst will identify additional questions or knowledge gaps after the site visit/workshop, when they are collating and organizing the information, and working through the Task Analysis (Step 3), HEI (Step 4), Human Error Modeling (Step 5) and even Quantification (Step 6). The analyst may need to perform more than one site visit or workshop to collect all of the information they need, and/or make arrangements to follow up (e.g., by telephone or email) with site contacts after the main data collection activity to collect additional information.

Whenever possible, it is recommended to conduct two site visits – one for general familiarization and a second visit at a later date to collect specific information, once the analyst has had some time to think about what is needed for the HRA. Another alternative is to conduct a site visit for familiarization and hold an operator workshop at a later date, again giving the analyst some time to consider and interpret the learnings from the site visit and identify specific information needs for the workshop.

8.1 Guidance on Conducting a Site Visit

Most of the published literature on collecting qualitative data for HRA agrees that the most important data source is the facility itself. Therefore, a visit to the petroleum facility should always be conducted whenever possible. The site visit aims to gather operational data for the scenarios under analysis through interviews, observations, scenario walk/talk-throughs, etc. The site visit is an important activity in that it provides a rich amount of data to be used for analyses performed earlier in the HRA process. Therefore, it is important that the scope of the visit is clarified with the QRA team such that the interviews and observations can focus on obtaining relevant data for the HRA and QRA.

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. Regardless, interviews and discussions with operating personnel are essential to understand the “as operated” context of the human operator actions contained within the major accident scenario.

The analyst should aim to meet with experienced and knowledgeable personnel either at the facility or in a workshop to explore their thoughts and insights on the analysis scenario. However, the most experienced and knowledgeable people are often the busiest, and so it is important that the analyst (i) contacts the site as soon as possible at the beginning of the project to secure time for site interviews or the workshop and (ii) is appropriately prepared to maximise their time at the site/in the workshop and to avoid wasting the time of the busy facility personnel.

The analyst should discuss the intentions for the qualitative data collection with a site contact in advance of the visit, to allow time for both the analyst and the site contacts to prepare. The following topics should be discussed:

- **Agree a date and set an agenda for the site visit/workshop.** What data collection activities does the analyst wish to carry out, and how much time will be needed?

- **If going to the site, identify the areas of the facility to visit**. Does the analyst need to visit specific areas of the facility, or will the data collection take place primarily in the control room (if permitted) or a meeting room? Does the analyst need to visit any administrative personnel (e.g., engineering, training, HR) or a training simulator (if available)?

- **Clarify the purpose of the site visit/workshop and set expectations.** The analyst should emphasize that the purpose of the visit/workshop is to collect data to inform the HRA and to observe/discuss task conditions so that the analysis can provide more accurate predictions for human performance (i.e., the analyst is not assessing individual performance).

- **Identify personnel to observe and/or interview.** The analyst should clarify which personnel they would like to interview/observe/participate in the workshop. This may be based on task types, job roles or responsibilities identified during the preparation step. The site contact may also suggest people for the analyst to talk to.

- **If going to the site, determine security and/ or access requirements and constraints.** The analyst should determine whether there are any site access requirements, such as safety training, which must be conducted in advance of the visit, and make the necessary arrangements. The analyst should also ask whether there are any constraints on bringing and using recording media on site (e.g., camera, video recorder, microphone, laptop).

If the analyst is using the workshop as the primary qualitative data collection opportunity, then the analyst should bring additional materials to support the discussions. These materials should be available to the analyst from the initial document review (in Step 1). For example:

- A description of the analysis scenario(s).
- The preliminary HTA.
- A copy of the HAZID or HAZOP report that was used to identify potential HFEs.
- A copy of relevant operating or emergency operating procedures for the analysis scenarios.
- Facility layout and control room layout diagrams.
- Photographs or pictures of the control room and/or relevant facility systems in the field.
- Photographs or pictures of relevant HMIs and operator screens.

The participants will be away from their normal working environment during the course of the workshop and so it is important to have photographs, diagrams and documentation that they can point to and use to prompt thinking, to help them describe how they would respond in the analysis scenario and to illustrate any points they wish to make.

8.1.1 Conducting an HMI Evaluation

The main concern with HMIs is the usability of the systems in relation to the tasks that the operators must perform in response to the scenario; for example, can the operators easily get the information that they need when they need it, does the system support decision making, etc.? In addition to interviewing operators about their experience of using the HMIs, the analyst should also perform an independent evaluation of the HMI, particularly if the operators indicate that there may be some issues present.

The System Usability Scale, developed by John Brooke (1996), is a short questionnaire that can be used to quickly collect information from operators about the perceived usability of the systems. It is based on 10 questions, which the operators rank from “Strongly Agree” to “Strongly Disagree”. The questions and a scoring template can be accessed from the following link: http://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html.

The “10 Usability Heuristics for User Interface Design” (Nielsen and Mack, 1994) contains a list of ten general principles or “rules of thumb” for design of HMIs that can help to identify usability problems.

The analyst uses this method to examine the interface directly and judge whether it is compliant with the general principles. The ten heuristics can be found at the following link: http://www.nngroup.com/articles/ten-usability-heuristics/, along with a guide on how to conduct a heuristic evaluation, which can be accessed directly at the following link: http://www.nngroup.com/articles/how-to-conduct-a-heuristic-evaluation/.

If the analyst identifies significant problems with the HMI, either through discussion with operators and/or through a usability assessment, it may be useful to perform a more in-depth evaluation. If possible, this should be performed as part of the HRA so that the findings can be incorporated into the later PSF evaluation and the final HEP calculation. Rajan, Wilson and Wood (2005, pg. 421) have developed a detailed evaluation checklist for control room interfaces.

8.2 Guidance on Conducting a Scenario Walk-/Talk-Through

One of the first activities that the analyst should perform on site or in the workshop is a scenario walk-/talk-though. This is a relatively simple activity in which one or more experienced operators demonstrate or discuss step-by-step how they would respond in the event of the scenario. A walk-through is typically performed in the location where the operator is likely to be working in the event of the scenario occurring, for example, the control room. A talk-through is typically performed in a different “offline” location, such as a meeting room, to avoid disturbing or distracting workers in the actual location or due to restrictions on access.

Depending on time and availability of personnel, the analyst may wish to perform both activities: a walk-through in the actual location to obtain an initial understanding of how the scenario would unfold and how the operator would respond, and a talk-through later in an “offline” location (such as a meeting room) to discuss aspects of the scenario in more detail.

The purpose of the walk-/talk-through is to investigate any tasks that are not fully understood by the analyst (e.g., due to the complexity of the task), to determine how long tasks are likely to take and to evaluate the working environment and the interfaces used by the operator (Kirwan, 1994). The walk-/talk-through also provides an opportunity for the analyst to confirm any judgements and assumptions remaining from the scoping phase of the analysis, and to obtain a more informed understanding of the context for the tasks and scenarios under analysis (Kolaczkowski et al., 2005).

The main steps in performing a walk-through are listed below (adapted from Kirwan and Ainsworth, 1992):

1. **Prepare for the walk-/talk-through**. Prepare a description of the analysis scenario to present to the operators. The scenario needs to be realistic and credible, with detailed system behaviour (including operation modes), event descriptions, time of day, description of the external environment (e.g., weather), operator responses, etc. However, the description should not include the outcome of the scenario to avoid biasing the operator’s thinking about how they would respond.

2. **Perform the walk-/talk-through**. The walk-/talk-through should being with the analyst explaining the purpose of the activity (i.e., to understand how the operator would respond in this scenario, to allow for a more realistic analysis) and what is expected of the operator (i.e., to think about how they would respond, what systems and documentation they would use, etc.). The analyst should explain briefly how the data will be used and should explain that the walk-through is not a test of individual performance, but rather an activity to collect data about the task and scenario in general.

3. **Record the collected data**. The best way to capture all of the information from the walk-through is to video or audio record the session. However, the operators might not feel comfortable with being recorded whilst performing the task and/or there may be restrictions on the use of such equipment in the walk-through location; the analyst should check both of these aspects before beginning the walk-through. The analyst should be aware that the recording will generate a lot of data, which can be time-consuming to review and analyse afterwards. Therefore, the analyst should also make written notes during the walk-through, which can be later supplemented with information from the recordings (rather than relying on transcribing the recording).

4. **Review and debrief**. After the walk-/talk-through, the analyst should review the information they have collected to check whether the goal of the activity has been achieved. If not, it may be necessary to further discuss and/or walk-through certain aspects of the scenario to collect the missing information. The analyst should also hold a debriefing session with the operators to confirm any remaining assumptions and discuss uncertainties, and also to raise any issues that have been noted or discuss any particular difficulties that were identified during the walk-through. The analyst should also ensure to thank the operators for their participation and their time.

8.3 Guidance on Conducting an Interview

Interviews or discussions are one of the most commonly used approaches for collecting qualitative data, especially to supplement, investigate in more detail, or discuss data collected using other techniques. Interviews can take many forms, including structured, semi-structured or unstructured, and may be non-directive or focused (Cohen et al., 2007). Interviews can also be informational to collect a wide range of information on a particular topic or task, or they can take the form of a survey, to collect more specific data in a systematic way (Kirwan and Ainsworth, 1992).

As with all qualitative data collection techniques, the analyst must do some preparation upfront to enable a more efficient and effective process. When preparing for operator interviews, the analyst should consider the type of interview, the topics and the target population for the interviews:

- **Interview type**. A semi-structured approach is recommended for Petro-HRA as this allows the analyst to keep the interview loosely focused on a particular topic or task, but also allows for some flexibility to explore relevant issues that may arise during the course of the interview. The analyst should also carefully consider how much time will be needed for the interviews. It is unlikely that an interviewee will be available for more than about 2 hours maximum. Equally, the analyst should not drag out the interview for the full amount of time allocated if all the topics and questions have been covered – this will only cause irritation and may result in reluctance for others to be interviewed.

- **Interview topic(s)**. This will be determined by the scope of the analysis and the findings from the documentation review, preliminary HTA and/or the discussions, observations and scenario walk-throughs that have been performed up to now. The analyst should think about whether there are specific task steps, human errors, recovery actions, PSFs, etc. that they would like to explore in greater detail. Alternatively, the analyst may wish to talk through the scenario with the interviewee, discussing more generally how the interviewee would respond in that scenario and what PSFs could occur that might affect human performance.

- **Target population**. The analyst should consider who are the best people to interview, based on the topics that they wish to cover in the interview. In the case that the analyst is unsure,

they should consult with their site contact. It is also possible during an interview to ask if the interviewee knows of any other person(s) who may be available for interview. The analyst should consider how many interviews they wish to carry out; this may be limited by the duration of the site visit and the number of other activities that they wish to perform, but a general rule of thumb is to interview as many people as necessary to gain the information needed across a range of responses (to avoid bias). The analyst should be aware that they might not be in a position to choose the interviewee; often the "best" (i.e., most knowledgeable and experienced) people are the busiest, and so they might not be available for interview. However, the analyst should stress that the overall analysis will benefit greatly (in terms of efficiency and accuracy) if these people can be made available for interview (Kirwan, 1994).

The analyst should also take some time to prepare the interview questions before going to site so that they know what to ask during the interview. The benefit of using a semi-structured approach is that the analyst can decide to explore other topics or issues that have arisen during the course of the interview if they wish, and then return to the list of pre-prepared questions to get back on topic again. Firstly, the analyst must consider the type of information they wish to get, and therefore what type of question they should ask. Different question types can include (from Cohen et al., 2007): introducing a topic or idea; following up on a topic or idea; probing for further information; asking interviewees to specify and provide examples; directly asking for information; indirectly asking for information; or interpreting a previous response.

Next, consider the sequence of questions. Easier and less threatening questions should be addressed earlier in the interview to put the interviewees at ease (Cohen et al., 2007). A useful approach is to arrange the questions according to the task step sequence. At the end of the interview, the analyst should ask an open-ended question such as "Is there anything else you think we should know about the task or scenario that we have not yet covered?" or "Is there any more information that you think we need?" (Kirwan and Ainsworth, 1992).

Interviewing skills take time and practice to develop. The analyst should strive to make the interviewee feel comfortable and to establish good communication and a good rapport, whilst at the same time adhering to the interview objectives and purpose. Timekeeping is also important in interviews to ensure that the most important topics and questions are covered within the time available. Some general points to note when conducting interviews are listed below:

- **Pick an appropriate location**. An interview is best carried out near to the interviewee's place of work, to minimize inconvenience for them and to make them feel more comfortable. The analyst should arrange to use a meeting room or some other private place for the interview to minimize distractions and interruptions.

- **Explain the purpose of the interview and introduce the topic, task and/or scenario that you wish to cover**. Make sure the interviewee understands why they are being interviewed, what you are trying to find out, what will be done with the information they provide, and that they can end the interview or decline to respond if they wish.

- **Be confident (but humble) and relaxed**. The analyst should be confident and relaxed in their approach, as their demeanor will affect the interview. However, the analyst should also take care to be humble and to avoid asking questions in an overbearing, presumptuous or authoritarian manner.

- **Be flexibl**e. The analyst should be prepared to be flexible. Some people may not want to be interviewed at all; some people may not want to or may be unable to answer particular questions. Some people may be very conversational and keep wandering off topic, or may have a very specific issue that they wish to get off their chest. The analyst should be prepared to move on to another question and/or steer the interview back on schedule without getting irritated or angry.

- **Listen and be interested but non-judgmental**. The analyst should also pay attention to what is said; sometimes very interesting topics or issues can arise, seemingly from nowhere, and the analyst must make a quick decision whether to investigate these in more detail at the risk of not covering some other questions. The analyst should show that they are interested and avoid giving signs of approval or disapproval, as these could bias the interviewee's subsequent answers.

- **Give the interviewee time to answer**. Do not try to answer the question for the interviewee. Give them time to think and reflect on the question. However, if the interviewee appears uncomfortable and if there is a long pause, this may indicate that they do not wish to answer; in this case, move on to the next question.

- **Prompt for clarification and probe for more information**. The analyst should prompt for clarification if they do not understand some aspect of the interviewee's response (for example, simply ask "Can you explain what … means?" or "Can you explain how … works?"). The analyst should also probe for more detail if needed (for example, simply ask "Why?" or "How?" questions).

- **Take notes and/or record the interview**. Taking notes during an interview is not an easy task. The analyst may wish to audio record the interview so that they can focus on asking questions, listening and responding to the interviewee. Appropriate permission should be sought from the interviewee in advance (see Section 4). Alternatively, the analyst may wish to bring a second person to act as a note-taker during the interview. If this is not possible, then the analyst should try to take short hand notes throughout and review these immediately after the interview to include any additional information.

- **Review the interview data**. Before ending the interview, the analyst should quickly check back to make sure that all of the important interview questions and topics have been covered. After the interview has ended, the analyst should make a more detailed review of the interview to see if there are any information gaps or additional information needed.

- **Thank the interviewee for their time and participation**. After the interview has ended, the analyst should thank the interviewee for their time and participation. The analyst may also wish to ask if the interviewee would be happy to be contacted again in the future (for example, by telephone or email) in case any clarification or further information is needed.

8.3.1 Additional Guidance on Collecting Information to Assist PSF Evaluation

The analyst may wish to do some more in-depth assessment of particular PSFs if there are indications that these factors have a significant impact on the successful outcome of the scenario. It is important that the analyst has sufficient information to evaluate and substantiate the PSFs during Step 6 of the HRA (quantification step).

Providing qualitative evidence to show how the PSFs have been evaluated is necessary to ensure that the process is transparent and traceable, and that there are no hidden assumptions or misunderstandings that could cast doubt over the evaluation of the PSFs and their subsequent impact on the HEP. Providing qualitative substantiation of how the PSFs were evaluated also provides valuable input into the human error reduction process (Step 7) because it is easier to see which PSFs are considered dominant in the overall HRA scenario, why these are considered dominant, and how these could be improved to reduce the likelihood of human error.

8.3.2 Additional Guidance on Discussing Human Error with Operators

A common challenge for HRA analysts is learning how to talk to operating personnel about human error. This can often be a sensitive subject and so it is a challenge to discuss it in an objective, non-personal and non-judgmental way. This may be particularly true if the analysis scenario is one that the operators are regularly trained on and where there is a high expectation that they would succeed in this scenario, or if the scenario has occurred before at the facility and the outcome was problematic. It is understandable that operators would take pride in their work and in their ability to successfully handle any scenario that they may find themselves in.

It can be difficult to break operators out of the mind-set of “that would never happen here” to get them to consider potential errors they could make during the scenario. The analyst may find that some people will speak more freely about potential errors while others will not. If an operator appears very reluctant to discuss human error, then the analyst should not push the issue, but should move on with the data collection activity.

It is important for the analyst to try to make the operator feel comfortable so that they will be more willing to talk about what could go wrong. Instead of directly asking “What errors could you make?” try a more indirect approach, such as “What would happen if you didn’t open that valve/shut down that system/etc.?” or “What are the things that could happen/go wrong that could prevent you from performing that task successfully?” or “What could happen if a less experienced operator was in this situation?”

It is also useful to read relevant event reports, either from that site or from other facilitys, to understand the kind of events that have happened before and why. These can be discussed with operators during the site visit and/or the workshop to explore whether similar errors have or could happen at this site. However, it is important to keep the interview focused and to make sure that the entire time is not taken up by trading anecdotes of previous events.

8.4 Guidance on Identifying Deviation Scenarios

A deviation scenario can be defined as a scenario that deviates from the nominal conditions normally assumed for the QRA sequence of interest, which might cause problems or lead to misunderstandings for the operating crews (adapted from Forester et al., 2007). For example, the case study in Part 2 of this guideline describes the analysis of a drive-off scenario on a drilling rig. The nominal scenario in this test case was a “fast” drive-off, in which the time from initiating event to detection and operator response was quite short (less than one minute). The nominal operator response was to stop all active rig thrusters and disconnect the rig from the wellhead. However, during the operator workshop, a deviation from this nominal scenario was identified – a so-called “slow” drive-off. This deviated from the nominal scenario in that the time from initiating event to detection and operator response could be as much as several hours as the drilling rig slowly moved out of position. The discussion with operators during the workshop revealed that the scenario also deviated from the nominal in terms of the anticipated operator response; in this case, the operator would have much more time available to

try to correct and maintain the position of the rig, rather than disconnecting from the wellhead. This example of a deviation scenario is not included in Part 2: Case Study Example of this guideline as it was considered outside the scope of the case study at that time.

According to the ATHEANA (A Technique for Human Event Analysis) HRA method (Forester et al., 2007, pg. 3-45), failure to successfully control and mitigate the scenario, in the way that it is modelled in the QRA, is mostly likely due to deviations in operator expectations of facility conditions, created by procedures, operator training, and facility and industry experience. The ATHEANA user guide states that "deviations from what is generally expected, if sufficiently different, can cause serious mismatches between the actual situation and the operators' expectations, their performance aids, their usual approach to implementing the procedures, and so forth."

The ATHEANA method includes detailed guidance for how to identify and screen deviation scenarios; however, this approach can be very time- and labour-intensive and may not be necessary for every Petro-HRA. The key points from this approach are summarized below and should be sufficient for most Petro-HRAs. If the analyst is requested to perform a more detailed investigation of potentially risk-important deviations, then the full ATHEANA approach may be more appropriate, as described later in this section.

It is important that deviation scenarios are maintained as credible and relevant to the QRA, as well as risk significant. The analyst should be clear as to why they should look for deviation scenarios. Screening and analysis of deviation scenarios can take some time, and so the analyst should not try to identify deviation scenarios just for the sake of it. The analyst should look for certain keywords in the interviews and discussions that might indicate the existence of a deviation scenario. For example:

- When asked how an operator would respond to a scenario, or perform a task step, the operator says, "Well, that depends…" This might mean that different conditions would require different courses of action, and hence a deviation scenario.
- Different operators or different operating crews give different answers when asked how they would respond to an initiating event. This may particularly be the case if there are no formal written procedures or instructions detailing the expected operator response.

The ATHEANA method provides useful guidance on how to identify deviation scenarios. Figure 22 (next page, from Forester et al., 2007, pg. 3-48) shows the recommended process for identifying such scenarios. The analyst should first use a set of guidewords to identify plausible facility conditions that could give arise to deviation scenarios. In some cases, the guidewords might lead to overlapping suggestions of deviation scenarios, but this is considered acceptable because it helps to ensure that no potentially significant conditions are missed.

The guidewords are shown in Figure 23 (from Forester et al., 2007, pg. 3-48). The guidewords are applied to both the initiating event and to the scenario evolution as a thought exercise to consider plausible changes from the nominal context of the scenario.

The ATHEANA method also provides two tables (shown as figures in this guideline) that can be used to consider the different facility conditions that could result in a deviation scenario. These tables can be used alongside the guidewords in the thought exercise. Figure 24 and Figure 25 (from Forester et al., 2007, pg. 3-51) describes some scenario characteristics that could cause operators to have problems in detecting, understanding or responding to a situation. Figure 26 and Figure 27 (from Forester et al., 2007, pg. 3-53) describes some additional parameter characteristics and questions to consider that could result in problems for the operator.

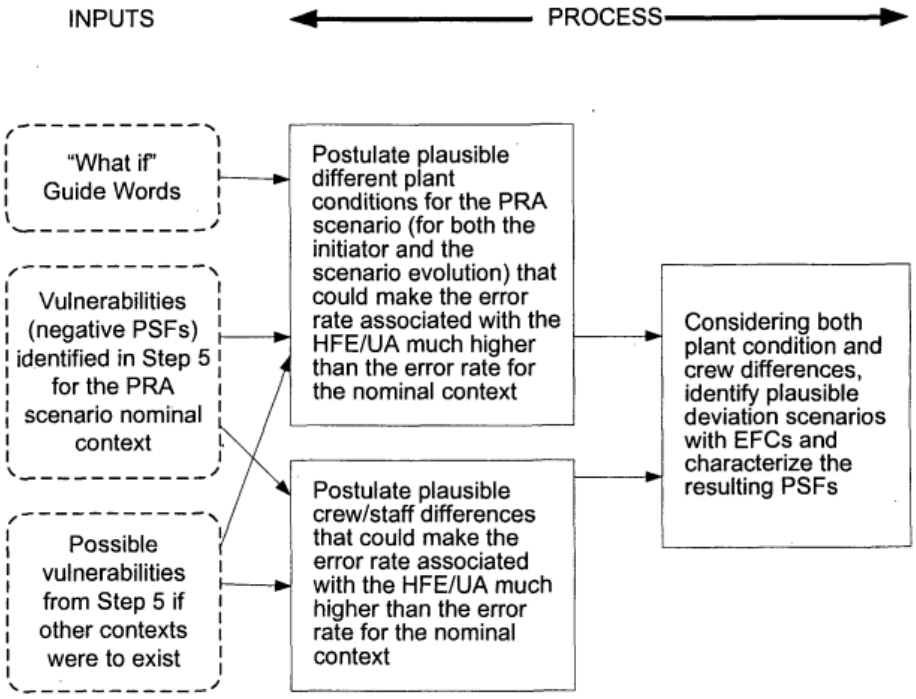

Figure 22: Process for identifying deviation scenarios

No or Not	A deviation in which something normally expected per the nominal context does not happen (e.g., what if the expected automatic low-level safety injection actuation did not occur?)
More or Greater or Larger	A deviation that represents a quantitative increase from that expected in the nominal context (e.g., what if the size of the breach were to be somewhat larger than that assumed in the nominal context?)
Less or Smaller	A deviation that represents a quantitative decrease from that expected in the nominal context (e.g., what if less flow than expected were available from the one operable train of injection such as if the train were operating in a degraded state?)
Early or Late or Never	A deviation that represents a change in the expected timing of events per the nominal context (e.g., what if the loss of injection occurred later in time, as a result of a room cooling fault, for example, rather than as a failure to start as assumed for the nominal context?)
Quicker or Slower	A deviation that represents a change in the expected speed or rate from that assumed in the nominal context (e.g., what if the vessel depressurization occurred much slower than that assumed for the nominal context?)
Shorter or Longer	A deviation that represents a change in the expected duration from that assumed in the nominal context (e.g., what if the battery power depleted in a shorter time than that assumed for the nominal context?)
Part of or Partial	A deviation in which only part of what is expected occurs (e.g., what if the stuck-open valve were only partially open rather than full open as assumed in the nominal context?)
In addition or As Well As	A deviation in which something additional occurs that is beyond what is assumed for the nominal context (e.g., what if other extraneous equipment faults and associated alarms were to also occur as well?)
Reversed	A deviation that is the logical opposite of that assumed for the nominal context (e.g., what if the stuck-open valve were to suddenly close on its own as a change to the nominal context?)
Repeated	A deviation that represents a repeated event (e.g., what if the relief valve was to open in a repeated fashion such as a second time during the scenario?)

Figure 23: Guidewords for identifying deviation scenarios

Scenario Characteristics	Description
Garden path problems	Conditions start out with the scenario appearing to be a simple problem (based on strong but incorrect evidence) and operators react accordingly. However, later correct symptoms appear, which the operators may not notice until it is too late.
Situations that change, requiring revised situation assessments	Once operators have developed a situation assessment and have started acting on it, it is often very difficult for them to recognize that there is new information or new conditions that requires them to change their situation assessment
Missing information	Key indicators may be missing as a result of failed sensors, lack of sensors, or lack of informants in the plant.
Misleading information	Misleading information may be provided as a result of inherent limitations of reports (e.g., stale information, inherent limitations of predictions, distortions resulting from indirect reports, secondary sources, translations).
Masking activities	Activities of other agents, or other automated systems may cover up or explain away key evidence.
Multiple lines of reasoning	Situations can occur where it is possible to think of significantly different explanations or response strategies, all of which seem valid at the time, but which may be in conflict (or a source of debate and disagreement by the operating crew).
Side effects	Situations can arise where the effects of human or automated system actions, or effects of the initial failure, have side effects that are not expected or understood.
Impasses	The scenario contains features where, at some point, it is very difficult for the operators to move forward, such as when procedures or the operators' situation model no longer matches the conditions, or assumed personnel or resources are not available.

Figure 24: Scenario characteristics that can cause problems for operators (cont. on next page)

Scenario Characteristics	Description
Late changes in the plan	The scenario is being managed according to a prepared plan, and then for some reason changes are required late in the scenario. Operators can become confused as to next steps; the plan is no longer well tested and can contain flaws, or the whole "big picture" gets lost by those managing the event.
Dilemmas	Ambiguity in the plan or in the situation (the event looks somewhat like two or more different accidents) can raise significant doubt in the operators' minds about the appropriate next steps.
Trade-offs	Operators must make impromptu judgments about choices between alternatives, such as when to wait to see if a problem develops (and may get out of control) versus jumping in early before it is clear what has caused the problem (just one of many examples).
Double binds	Conditions exist where operators are faced with two (or more) choices, all of which have undesirable elements.
High tempo, multiple tasks (Sub- or related categories are escalating events, cascading problems, and interacting problems)	The operators simply run out of resources (mental or physical) to keep up with the task demands. In escalating events, the problem keeps getting harder and harder or more complex. Cascading problems are those where the effects of one problem (or an attempt to solve it by the operators) create new problems. In interacting problems two or more faults interact to create complex symptoms that may have never been foreseen.
Need to shift focus of attention	As the scenario unfolds, the operators may need to move attention from one particular aspect of the problem to another, yet they remain focused on the initial problem area, which may be minor.

Figure 25: Scenario characteristics that can cause problems for operators (cont.)

Parameter Characteristics	Question
No indication	Does this scenario involve failed indicators? Does this scenario involve indications calculated from other failed instruments (e.g., subcooling based on RCS pressure)?
Small change in parameter	Within this scenario and with the existing human-machine interface design, is there a relevant parameter change small enough that it might be overlooked (i.e., not detected) such as a non-alarmed change in a valve position? Does this scenario involve small or significantly smaller-than-expected changes in any indication? Can the operators be led to a state of complacency by this small change? Within this scenario and with the existing human-machine interface design, is it likely that the operators will be misled by a small change as to the kind of situation they face (e.g., does it now resemble another scenario that is more familiar)? Does this scenario involve smaller-than-expected changes in an important parameter used as a cue or caution in the procedures, or used in training as a basis for actions? What is the likely effect of the operators misapplying this cue or caution? Can the operators be led to apply informal rules by this deviation? Can the operators be led to a state of complacency or forgetfulness by this small change?
Large change in parameter	Within this scenario and with the existing human-machine interface design, is there a relevant parameter change so large or out of range that it might be overlooked (e.g, indicator pegged at the top or bottom of a meter and not noticed). Does this scenario involve a large or significantly larger-than-expected changes in any indication? Can the operators be led to a state of anxiety by this large change? Within this scenario and with this interface design, is it likely that the operators will be misled by a large change as to the kind of situation they face (e.g., does it now resemble another scenario that is more familiar)? Does this scenario involve larger-than-expected changes in an important parameter used as a cue or caution in the procedures? Can the operators be led to apply informal rules by this deviation? Can the operators be led to a state of stress or anxiety by this large change?

Figure 26: Parameter characteristics that can cause problems for operators (cont. on next page)

Parameter Characteristics	Question
Lower or higher than expected value of parameter	Does this scenario involve indications that are lower or higher than would be expected? Does this deviation correspond with expected values for non-accident conditions, so that the deviation might not be detected as anomalous? Does this deviation correspond with expected values for other (different) accident conditions? Does this scenario involve lower or higher-than-expected values in an important parameter used as a cue or caution in the procedures? Can the operators be led to apply informal rules by this deviation? Can the operators be led to a state of complacency or forgetfulness by the lower change or a state of anxiety by the higher change?
Slow rate of change in parameter	Does this scenario involve slow or significantly slower-than-expected changes in any indication? Within this scenario and with the existing human–machine interface design, is it likely that the slow rate of change might be overlooked? Can the operators be led to a state of complacency or forgetfulness by this slow change? Within this scenario and with this interface design, is it likely that the operators will be misled by a slow change as to the kind of situation they face (e.g., does it now resemble another scenario that is more familiar)? Does this scenario involve slower-than-expected changes in an important parameter used as a cue or caution in the procedures? What is the likely effect of the operators mis-applying this cue or caution? Can the operators be led to apply informal rules by this slower deviation?
High rate of change in parameter	Does this scenario involve rapid changes in any parameter that, with the existing human-machine interface design, may be overlooked (e.g., fleeting changes, briefly appearing alarms or indications, or an indicator pegged at the top or bottom of a meter and not noticed)? Does this scenario involve rapid or significantly more rapid-than-expected changes in any indication? Can the operators be led to a state of anxiety by this rapid change? Does this scenario involve rapid changes in any parameter that, with this interface design, may be discounted or assumed to be anomalous (such as fleeting changes or briefly appearing alarms or indications)? If overlooked or ignored, is the absence likely to confuse the operators as to the kind of situation they face (e.g., does it now resemble another scenario that is more familiar)? Does this scenario involve faster-than-expected changes in an important parameter used as a cue or caution in the procedures? Can the operators be led to apply informal rules by this deviation?

Figure 27: Parameter characteristics that can cause problems for operators (cont.)

The ATHEANA user guide lists some PSFs that might be particularly relevant when considering crew differences that could result in deviations scenarios (Forester et al., 2007, pg. 3-57):

- Differences in some tendencies and information rules among the different crews.
- Differences in the crew communication protocols.
- Differences in crew characteristics such as degree of independence allowed among the operators and preferences regarding the use of indications and computer screens.
- Differences in the strategies used among the crews as to how methodical the procedures are used and how often crew-wide checks of facility status are or are not used.
- Differences in the staffing levels for the different shifts, etc.

The search for deviation scenarios may produce a large, or even unmanageable, number of possible deviation scenarios. The ATHEANA User's Guide (Forester et al. 2007, page 3-58) suggests the

following screening criteria for selecting the most important deviation scenarios to be analysed further:

- Is the perceived strength of the combined negative PSFs for the postulated deviation scenario very high, such that the context is potentially among the most error-forcing of those considered?
- Is the recovery potential judged to be low so that if the initial error represented by the HFE were to be made, it does not seem likely that the operator(s) would recover from the mistakes before undesired consequences occur?
- Is the likelihood of the postulated deviation scenario and its associated error-forcing context (the combination of PSFs and facility conditions that increase the likelihood of human error or unsafe actions) sufficiently high that it is worthy of being carried forward in the analysis rather than being so low that even with a corresponding high HEP, the overall contribution to risk will be insignificant?
- Are there similarities among the postulated deviation scenarios and their associated error-forcing contexts so that some can be combined thereby lessening the number of contexts to be addressed?

The purpose of the screening exercise is to ensure the analyst is selective regarding how many and which deviation scenarios are taken forward for further analysis, and to ensure the analyst does not accidentally screen out a unique and potentially risk-important deviation.

8.5 References

Cohen et al. (2007). Research Methods in Education. Routledge: London. 6th Edition

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.

Kirwan, B. (1994). A Guide to Practical Human Reliability Assessment. CRC Press: London. 1st Edition.

Kirwan, B. and Ainsworth, L. K. (1992). A Guide to Task Analysis. CRC Press: London. 1st Edition, 1992.

Kolaczkowski, A., Forester, J., Lois, E. and Cooper, S. (2005). Good Practices for Implementing Human Reliability Analysis. NUREG-1972, U.S. Nuclear Regulatory Commission.

9 Background to Step 3: Task Analysis

9.1 Understanding Goals versus Tasks

Embrey (2000) distinguishes between action-oriented and cognitive approaches for task analysis. Action-oriented approaches involve observable behaviors (such as visible tasks), while cognitive approaches look primarily at problem solving and decision making. HTA is primarily action-oriented, but it may also be used to capture cognitive activities that manifest in decisions. Tasks may entail taking an action or making a decision, while the steps to support those tasks may involve actions or information gathering (i.e., perceptual tasks).

An important consideration is that most actions and decisions are governed by overarching goals. Whether procedurally driven or based on the expertise of the operator, a series of goals guide behavior. Goals are therefore a useful way to group sets of actions together. Also, since the precursors to actions—namely the decisions operators make—are not always as readily observable as actions, understanding goals can help the analyst determine what decisions might be necessary for the operators to make. During data collection, the analyst should ask questions of the operators and other SMEs to identify goals.

Further, goals are broken down into subgoals or tasks necessary to accomplish the goals. For example, if the high-level goal is to stop a gas leak, subgoals or tasks might include closing a valve and stopping the process that is producing the gas. These subgoals shape the actions the operator takes, including the possible ways to mitigate the problem. Goals are also important to understanding the type of errors that are possible. In the parlance of Reason (1990), if the operator has the right understanding of the problem at hand, the errors that might occur would include slips (doing the wrong thing despite a good understanding) and lapses (failure to do the right thing). If the operator does not have proper understanding of the problem at hand, the potential error would be a mistake. Such error taxonomies are helpful to anticipating the types of errors that might occur for different situations.

9.2 Selecting a Task Analysis Approach

There are numerous methods for task analysis (see Stanton et al., 2013), and a full review is beyond the scope of this report. Many task analysis methods are simply refinements of basic, established approaches. Still other task analysis methods that were designed for particular human factors applications may not prove suitable for HRA applications. Kirwan (1994), in discussing task analysis specifically for HRA, limits his discussion to a handful of methods, but highlights in particular HTA. HTA is a task analysis method that decomposes tasks hierarchically according to goals at the top level and the tasks at the lower levels that are required to accomplish the goals. This approach is very widely used for both human factors and HRA applications, and it represents a simple yet flexible approach. It is in many ways the logical task analysis counterpart to SPAR-H, which similarly represents a simple yet flexible method.

Embrey (2000), in his discussion of task analysis for HRA, outlines the key advantages of HTA (p. 2):

- “HTA is an economical method of gathering and organizing information since the hierarchical description needs only to be developed up to the point where it is needed for the purposes of the analysis.
- The hierarchical structure of HTA enables the analyst to focus on crucial aspects of the task which can have an impact on facility safety.

- When used as an input to design, HTA allows functional objectives to be specified at the higher levels of the analysis prior to final decisions being made about the hardware. This is important when allocating functions between personnel and automatic systems.
- HTA is best developed as a collaboration between the task analyst and people involved in operations. Thus, the analyst develops the description of the task in accordance with the perceptions of line personnel who are responsible for effective operation of the system.
- HTA can be used as a starting point for using various error analysis methods to examine the error potential in the performance of the required operations."

The Petro-HRA approach has adopted the HTA and TTA approaches, but analysts should not be limited to these techniques when other techniques are warranted. A variant of TTA—operational sequence diagrams (OSDs)—represent similar information graphically as the TTA do in a table. While the many variants on task analysis may provide additional insights to the analyst while completing the HRA, it should be noted that most such techniques add layers of complexity and time onto the analysis. The resources required for such an analysis may be justified, especially in the face of complex, difficult to understand, and highly risk significant activities. Otherwise, the analysts should strive to be efficient in completing the analysis in a cost effective and timely manner. HTA and TTA can help ensure this objective.

9.3 Representing an HTA in Outline Format

The goals and tasks in an HTA can also be represented in outline format. The outline format simply lists the goal first and then sub-bullets the tasks required to achieve that goal. See the example in Table 20. For example, the overarching goal to manually activate blowdown is numbered 0. Successful activation of blowdown requires four tasks, numbered 1 – 4 in the outline. These tasks, in turn, require several steps (e.g., Steps 1.1 – 1.2). The outline format is the most effective way to build the HTA initially, since it can be easily modified as new insights are added.

Table 20: Example HTA in outline format (derived from Øie et al., 2014)

0.	Manually activate blowdown
1.	Detect leakage
1.1	Detect auditive alarms
1.2	Detect visual alarms
2.	Diagnose event
2.1	Examine leakage location
2.2	Examine leakage size
2.3	Examine status of safety barriers
2.4	Examine presence of personnel in the area
3.	Decide on blowdown
3.1	Decide if blowdown is necessary
3.2	Decide which segment to blowdown first
4.	Activate blowdown
4.1	Ensure button is in correct position; if not, turn in correct position
4.2	Push blowdown button on CAP

10 Background to Step 4: Human Error Identification

10.1 Alternative Error Taxonomies

A number of error taxonomies exist that support task analysis, e.g., SHERPA (Embrey, 1986), the Technique for the Retrospective and Predictive Analysis of Cognitive Errors (TRACEr; Shorrock and Kirwan, 1999), or even the recent so-called proximate causes (error mechanisms) in the Integrated Decision-tree Human Error Analysis System (IDHEAS; Whaley et al., 2012b). The SHERPA and TRACEr error mode taxonomies, among numerous others (see Stanton et al., 2013 for a review), are functionally fairly similar and may be used interchangeably as desired. The TRACEr approach is a bit more complex, featuring a total of eight taxonomies to cover the error context, the production of the error, and the recovery of the error for both predictive and retrospective analysis (Shorrock and Kirwan, 2002). In practice, however, TRACEr covers most of the same errors as SHERPA, with the addition of gradations of scale. Whereas SHERPA is relatively absolute in terms of an error occurring or not occurring, TRACEr scales the errors (e.g., too little action or action too long). TRACEr also delineates internal and external error modes, corresponding to cognition (internal) and action (external), although this distinction is implicit in SHERPA. IDHEAS is actually an HRA method in itself, but it includes a generic psychological taxonomy as part of the method. The taxonomy behind IDHEAS includes a number of cognitive errors but very few action error modes. Whereas it may be easier to identify and catalog action errors in SHERPA, IDHEAS provides a more complete way to identify and catalog cognitive errors.

These taxonomies are found in the tables below. Table 21 presents the external error modes in TRACEr, which are centered on action and communication (called information) errors. Figure 28 (next page) provides the internal error modes in TRACEr, which step through errors that can occur during perception; memory; judgment, planning, and decision making; and action execution. Note that the action execution errors embedded in the internal error modes overlap considerably with the external error modes, with the key difference being that the internal error modes specify cognitive causes underlying the action execution errors. Finally, Table 22 outlines the proximate cause error taxonomy in IDHEAS. The failure types are based on the situation awareness framework but essentially map identically to the internal error modes in TRACEr.

Table 21: The external error modes in TRACEr

Selection and quality	Timing/sequence	Communication
Omission	Action too long	Unclear information transmitted
Action too much	Action too short	Unclear information recorded
Action too little	Action too early	Information not sought/obtained
Action in wrong direction	Action too late	Information not transmitted
Wrong action on right object	Action repeated	Information not recorded
Right action on wrong object	Mis-ordering	Incomplete information transmitted
Wrong action on wrong object		Incomplete information recorded
Extraneous act		Incorrect information transmitted
		Incorrect information recorded

Cognitive Domain	Cognitive Function	Relevant Keywords	Example IEM
Perception	Vision – Detection	None, late, incorrect	Late detection
	Vision – Identification	None, late, incorrect	Misidentification
	Hearing – Recognition/ Comparison	None, late, incorrect	Hearback error
Memory	Recall perceptual information	None, incorrect	Forget temporary information
	Previous actions	None, incorrect	Forget previous actions
	Immediate/current action	None, incorrect	Forget to perform action
	Prospective memory	None, incorrect	Prospective memory failure
	Stored information (procedural and declarative knowledge)	None, incorrect	Misrecall stored information
Judgement, Planning and Decision Making	Judgement	Incorrect	Misprojection
	Planning	None, too little, incorrect	Underplan
	Decision Making	None, late, incorrect	Incorrect decision
Action Execution	Timing	Early, late, long, short	Action too early
	Positioning	Too much, too little, incorrect, wrong direction	Positioning error: overshoot
	Selection	Incorrect	Typing error
	Communication	None, unclear, incorrect	Unclear information transmitted

Figure 28: The internal error modes in TRACEr

Table 22: The IDHEAS proximate cause error taxonomy

Failure Type	**Proximate Cause**
Failure of Detecting and Noticing	Cues/information not perceived
	Cues/information not attended to
	Cues/information misperceived
Failure of Understanding and Sensemaking	Incorrect data
	Incorrect integration of data, frames, or data with a frame
	Incorrect frame
Failure of Decision Making	Incorrect goals or priorities set
	Incorrect pattern matching
	Incorrect mental simulation or evaluation of options
Failure of Action	Failure to execute desired action
	Execute desired action incorrectly
Failure of Team Coordination	Failure of team communication
	Error in leadership/supervision

11 Background to Step 5: Human Error Modelling

Human activities of interest to HRA do not generally occur in isolation but rather in interaction with hardware systems. Hardware systems modelled in the QRA feature reliability curves for systems and components to address the mean time before failure. A failed hardware system can cause humans to fail at their prescribed task, or a human error can cause a hardware system to fail. Likewise, a hardware system may be designed as a failsafe backup for human actions that fail, e.g., an automatic pressure venting valve can mitigate system damage should the human fail to manually regulate a pressurized system properly. Perhaps often overlooked, humans are often the key to saving a failed hardware system: positive human intervention can prevent the escalation of a hardware failure. In HRA, human activities are modelled as part of an event or fault tree to show the interaction of human activities with the hardware system functioning.

11.1 Defining the Human Failure Event

HRA depicts a cause-and-effect relationship of human error. The causes are typically catalogued in terms of qualitative contributions to a human error, including the processes that shaped that error and the failure mechanisms. The processes—cognitive, environmental, or situational—that affect human error are typically treated through PSFs. The resultant effect is the manifestation of human error—often called the HFE. This failure mode is treated quantitatively and has an associated failure probability, the HEP.

The term human error is often considered pejorative, as in suggesting that the human is in him- or herself the cause of the failure mode (Dekker, 2006). This belies the current accepted understanding that human error is the product of the context in which the human operates. In other words, it is not the human as the ultimate cause of the error but rather the failure mechanisms that put the human in a situation in which the error is likely to occur. The colloquial term, human error, is further challenged in that a human error may manifest but have little or no risk consequence. Human errors may be recovered or may simply not have a direct effect on event outcomes. Such risk insignificant occurrences are typically screened out of the HRA model.

Thus, to denote a risk significant human error, the term HFE has been posited. According to the American Society of Mechanical Engineers (ASME), a human failure event is “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” (2009). The HFE is therefore the basic unit of analysis used in the QRA to account for HRA. While an HFE may be incorporated as a simple node in a fault tree or a branch in an event tree, the documentation supporting the HFE represents an auditable holding house for qualitative insights used during the quantification process. These insights may be simple to detailed, depending on the analysis needs and the level of task decomposition.

In the PSAs used in the nuclear industry, as per the ASME definition, HFEs are determined as a subset of hardware failures, namely those hardware failures that could be triggered by human action or inaction. This approach is top-down, starting with hardware faults and deducing human contributions to those faults. Elsewhere, there is a bottom-up approach. More traditionally human factors driven approaches would tend to look at opportunities for human errors first in a task analysis and then model them in terms of potential for affecting safety outcomes. The order of identifying vs. modeling HFEs may be seen as changing depending on the approach. A top-down approach would tend to model the opportunity for HFEs and only then identify the sources of human error. In contrast, a bottom-up approach would first identify sources of human error and then model them in the QRA.

The intersection of top-down and bottom-up approaches to defining HFEs has not been carefully studied. Ideally, both approaches should arrive at the same set of HFEs. This question is crucial, however, because the HFEs used in nuclear PSAs tend to be top-down—defined as a subset of the PSA hardware faults—whereas the HFEs used in petroleum QRAs may also be bottom-up—derived from a task analysis conducted by human factors experts, especially in cases where an older QRA is used that does not extensively model human error. The marriage of these approaches is necessary in order to ensure that HRA methods developed for top-down HFEs are also sufficient for bottom-up applications. Figure 29 (from Boring, 2014) depicts the top-down and bottom-up approaches to defining HFEs. As can be seen, it is possible that both approaches arrive at the same solution. However, the solution set for the top-down and bottom-up approaches should be seen in terms of two circles in a Venn diagram. The problem is not that the HFEs may indeed overlap; the problem is that these HFEs may not always be identical.

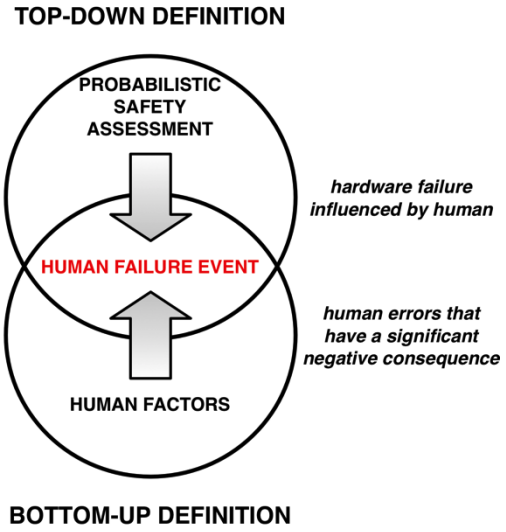

Figure 29: Two approaches to defining human failure events

Additionally, some HFEs used in a petroleum context are derived from barrier analysis and are prospective in nature, designed to identify how the defense in depth of a system may be increased to ensure the safety of a system to be built. This approach may emphasize the evolving timescale of barrier effectiveness, whereas most conventional PSAs represent a static snapshot of an HFE. The barrier analysis approach is rarely used in contemporary PSAs for the nuclear industry where most guidance on HFEs has been developed to date.

As depicted in Figure 29, there are areas covered in the bottom-up approach that are not necessarily covered by the top-down approach (and vice versa). Of interest, the top-down approach to defining HFEs begins by modeling those hardware systems that can fail and whose failure can be influenced by human actions or inactions. For example, if a particular electrical bus is a risk significant vulnerability to the overall system safety, the risk analyst would identify the failure of the bus as the starting point. He or she would next determine if the system is controlled by human operators. If yes, and if the human action is a significant subset of the overall risk of the bus failure, an HFE is modelled. The risk analyst must then determine what types of human errors are possible. This is often accomplished by referencing operating procedures and identifying which steps could be performed incorrectly. It is easier to identify a failure to execute particular required procedural steps than it is to postulate all the possible deviation paths the operator could follow that aren't encompassed by the procedure. In other words, the steps omitted (i.e., errors of omission) are more readily modelled than extra steps performed beyond the procedures (i.e., errors of commission). Thus, the top-down approach has

exhibited far greater success in including relevant errors of omission than in anticipating possible errors of commission. We argue that the bottom-up approach, which considers all aspects surrounding task performance, provides better opportunity to incorporate these commonly omitted types of human error.

HRA methods do not have a consistent level of task decomposition. This lack of consistency can result not only in different qualitative analyses but also different HEPs. The level of task decomposition affects the dependency between tasks, which may have a further effect in driving the HEP. The issue is not that different HRA methods necessarily produce different results for the same HFE; rather, different HRA methods may decompose the HFE to different levels. Thus, the quantification of the same HFE may entail different assumptions and, to some extent, different groupings of tasks across HRA methods. In other words, because of a lack of a common task decomposition framework, HRA methods may not be using the same unit of analysis when producing the HEP.

Defining an HFE for use in Petro-HRA still remains somewhat elusive. Although general guidance exists for the top-down approach, there remains a large element of skill of the craft in actually decomposing groups of subtasks into an HFE suitable for inclusion in the PSA or QRA. While approaches exist for bottom-up definitions, these still do not adequately address topics such as errors of commission.

Nonetheless, several candidate principles of HFE modelling have emerged from the review to date:

- Until clear guidance is available to identify commonalities and differences between the top-down and bottom-up approaches, it is desirable to employ a combination of both approaches to define the HFE.
- When adopting the top-down approach, the definition of the HFE should start broad, identifying those human actions and inactions that may trigger the unavailability of components, systems, or functions.
- These broad HFEs should be screened to determine the risk significant activities. Parts of this might be done in the QRA. The risk significant activities are the primary HFEs that are modelled in greater detail in the HRA.
- Task analysis of these risk significant activities may reveal additional sources of failures that may not be anticipated in the initial definition of the HFE. This represents the bottom-up approach. The definition of the HFE and screening should be an iterative process to arrive at a complete and relevant model of the human contribution to the overall system risk.
- Bottom-up approaches should consider errors of commission in crafting the HFEs.
- Subtasks may reasonably be grouped into a single HFE provided that they are logically related (such as sharing a common goal); that they do not represent different tasks, personnel, or equipment; and that they do not mask dependencies that need to be accounted for.
- The earliest HRA methods used a simple equipment-level task decomposition. This is the level of flipping a switch. As interfaces have progressed in complexity, the interaction of the human with the equipment may represent a much higher level of decomposition that includes more cognitive or diagnostic activities. It is insufficient to define HFEs in terms of simple tasks—it should include a significant cognitive component as well.

Ultimately, one key goal of the Petro-HRA project is to bridge the gap in existing SPAR-H guidance and application to the petroleum domain. Current practice in SPAR-H follows a somewhat vague top-down approach of using predefined HFEs from the PRA/PSA. By referencing the steps in the guideline on task analysis and HEI, the Petro-HRA analyst is poised to be able to define bottom-up HFEs as needed. If the bottom-up identified HFEs are on the level that is relevant for the PRA or the QRA, these should be fed back into the PRA or QRA to update the overall risk analysis. In that case one may perform sensitivity analyses, etc.

12 Background to Step 6: Human Error Quantification

12.1 Additional Guidance on Analysing the Time PSF

When people have little time, many types of behaviour may occur. One may think of a continuous scale from very high time pressure to extensive time: With high time pressure people may be rushed into taking uncontrolled, incorrect and desperate actions; become incapacitated and passive; or attempting to perform the task without being able to complete it within the time available. There may be different time available for considering alternative solutions for how to handle the event, double-check parameters, troubleshoot or verify the outcome of their actions. With extensive time there may be plenty of time to discuss possible strategies and break for discussion meetings. However, it is difficult to couple these kinds of behaviour to specific categories. This is also interconnected with their training and conduct of operations. For the analysis of Time, it is important for the analyst to get to know whether they objectively have a time margin or not, and how big this margin is.

After the occurrence of an initiating event there is limited time for safety systems and barriers to act before undesired consequences no longer can be prevented or mitigated. In cases where these safeguards rely on operator actions to perform their intended function, this duration is referred to as available time. Relative to the available time there is also the required time by the operator(s) to successfully execute and complete the necessary actions. The difference, or margin, between available time and required time determines the effect of time on task performance and human error probability.

The Time PSF (see Section 6.3.1) therefore considers the influence on human error probability as a result of the margin, or absence of margin, between two different measures of time: available time and required time.

This influence results from the degree of time pressure created by the time margin. For example, if there is inadequate time (i.e., a negative time margin) to perform all the necessary actions the operator(s) will fail in completing the task. In other words, failure is certain despite having performed all previous actions correctly. If there is limited available time (i.e., a small time margin) the operator(s) may complete the task itself but fail to achieve a successful outcome due to human errors induced by time pressure (incorrect or omitted actions). If there is extra or expansive available time (i.e., large time margin) the operator can perform the required actions in a controlled and calm manner, thus reducing the probability of failure.

When considering the difference between required time and available time it is normal practice to do so for the entire task, e.g., from detection of a critical alarm and all the way until the necessary safety valves have been closed (i.e., successful accomplishment of the task goal). This is illustrated in Figure 30.

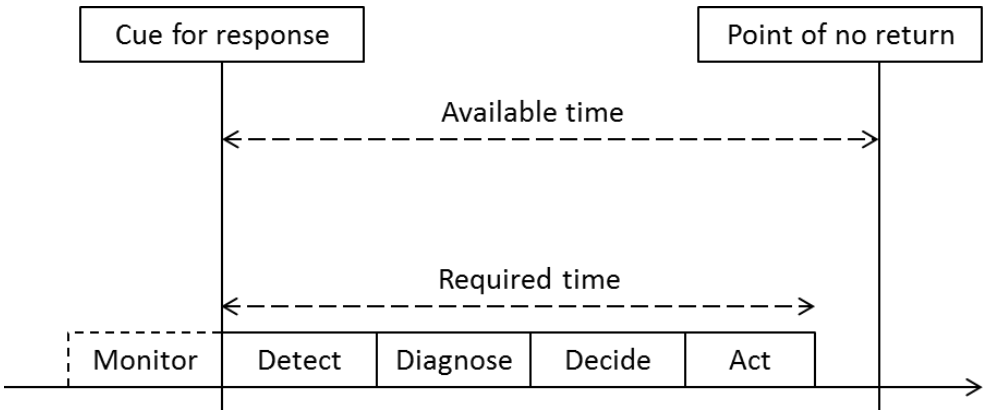

Figure 30: Relationship between available time and required time

12.1.1 Important Considerations for Analysing Time

While Figure 30 is useful for illustrating the relationship between available time and required time, it is at the same time an oversimplification on two accounts:

- In some cases, there may be expansive time to perform a task from start to finish, but at the same time there may be limited time margins within the task itself. For example, important information, such as an alarm, may only be available for a brief moment. If such actions are crucial for successful completion of the task, this needs to be addressed. However, to avoid overcomplicating the overall time assessment, it can be beneficial to account for such influences through other PSFs. In the case of an alarm being missed due to brief availability, this can be accounted for in the HMI PSF.
- In Figure 30 both available and required time is indicated to start from the "cue for response". While this is correct for required time, available time must be measured from the initiation of the event itself, and not from the cue presented to the operator(s). In most scenarios the initiating event and subsequent cue will be very close in time. This may however not always be the case, and in time critical scenarios with small time margins, not differentiating between these two times may have a significant impact on the analysis of Time.

12.1.2 Examples from the Petroleum Industry

The concept of available time and required time is already in use in the petroleum industry. For process safety incidents, available time translates into what is commonly referred to as process safety time (PST): "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 (SIF) is not performed" (p. 81, IEC 61511-02, 2004). PST is used to determine whether a SIF has sufficient response time.

An example could be to determine if a process safety valve closes fast enough upon a signal from the programmable logic controller (PLC) triggered by tank level indicator. If the SIF relies on manual activation by an operator the assessment of response time also have to include a measure of required time. Such evaluations may be part of or derive from the conclusion of a Safety Integrity Level (SIL) Allocation Study, such as LOPA. For more information about applying HRA in LOPA, an article titled Layer of Protection Analysis – Quantifying human performance in initiating events and independent protection layers (Myers, 2013) is recommended reading.

Table 23 lists relationships between various initiating events, required time and available time to perform the necessary actions, and the adverse consequences if the correct actions are not taken

within the time available. Note that the table is only meant to provide a list of general examples from the petroleum industry and is not meant to be exhaustive and complete. The relationships between the various bullet-points may vary depending on the scenario and technology involved.

Table 23: Initiating events, required time and consequences

Event categories	Initiating event/ cue for response	Response time/ time required	Point of no return/ time available	Adverse consequences
Process disturbances	• Pump failures • Valve failures	• Trip/ shut off pumps • Control valve position	• Overfilling of tanks • Vessel rupture capacities	• Loss of containment/ spillage
Loss of containment	• Hydrocarbon leaks • Blowouts, incl. shallow gas	• Emergency shutdown and depressurization • Seal off well • Relocate rig	• Hydrocarbon ignition probability • Potential explosion pressure limits	• Fire & explosion • Injuries & fatalities • Environmental damage • Loss of facility
Loss of position	• Dynamic positioning failure (drive-off) • Ship on collision course (force-off) • Loss of power/ blackout (drift-off)	• Disconnect rig from well • Avoid collision • Regain position	• Angle of marine riser • Collision speed and force too high	• Damage to wellhead & subsea equipment • Damage to rig structures & equipment • Vessel collisions
Loss of stability	• Water ingress (e.g., due to ship collision)	• Stabilize floating installation (rig, ship, FPSO or platform)	• Breaching listing angle limits • Floating capacity exceeded	• Capsize and loss of buoyancy
Loss of well control	• Unintentional flow of well fluids to surface or into wellbore	• Shut in well • Kill well	• Gas enters the marine riser • Kick tolerance exceeded	• Loss of well • Well release • Blowout (topside or subsea)

The following sections explain how to perform the analyses necessary for obtaining estimates of required time and available time, or where to look for already available and representative estimates.

12.1.3 How to Analyse Required Time

Required time can be deducted with the help of various data sources, such as use of simulators, on-site observations, and incident reports. While representing realistic, relevant and often accurate estimates, such data can however be challenging and costly to obtain. A practical and more feasible approach is to estimate required time based on a structured review of the task analysis. This method is referred to as a timeline analysis and is commonly performed close in time to the task analysis (e.g., during the same data collection workshop). How to do a timeline analysis is therefore explained in the following section.

Timeline analysis: The objective of a timeline analysis is to assess the time required by the operator(s) to carry out the actions needed to successfully accomplish the task being analysed in the HRA.

The following input can be used as part of the timeline analysis:

- A complete task analysis, including all the required task steps (i.e., actions).

- Information gathered as part of walk and talk through during a site visit or workshop.
- Input from operating personnel with experience from actual (or similar) events.
- Data from relevant drills or training activities, e.g., emergency preparedness exercises.
- Incident reports and investigations in which time has been part of the evaluation.

Timing: Information about time required can be gathered already from the initial document review. However, the timeline analysis itself cannot be finalized before the scenario has been defined and the task analysis is complete. This is because the scenario context and actions identified determine how much time the operators need to successfully accomplish the task. It is therefore useful to include the timeline analysis as part of the HRA workshop after having verified the task analysis, see Sections 2.4 and 2.5.

If any actions are added, altered or removed in the task analysis, the timeline analysis should be reviewed and updated if found necessary. Results from the timeline analysis provide input to the evaluation of the Time PSF and must therefore be completed prior to performing the human error quantification.

Approach: An easy and practical way of doing a timeline analysis is to draw a diagram similar to the one illustrated in Figure 31. This can be done as part of the HRA workshop using a whiteboard or post-it notes based on thorough discussion between various key personnel, such as operators, supervisors, technicians and engineers. Note that this type of analysis provides an estimate of the time required for the operator(s) to perform a task. Unless other means are available to estimate time (e.g., simulator or detailed accident data), timeline analysis is often the only means at the analysts' disposal given the budget and time available.

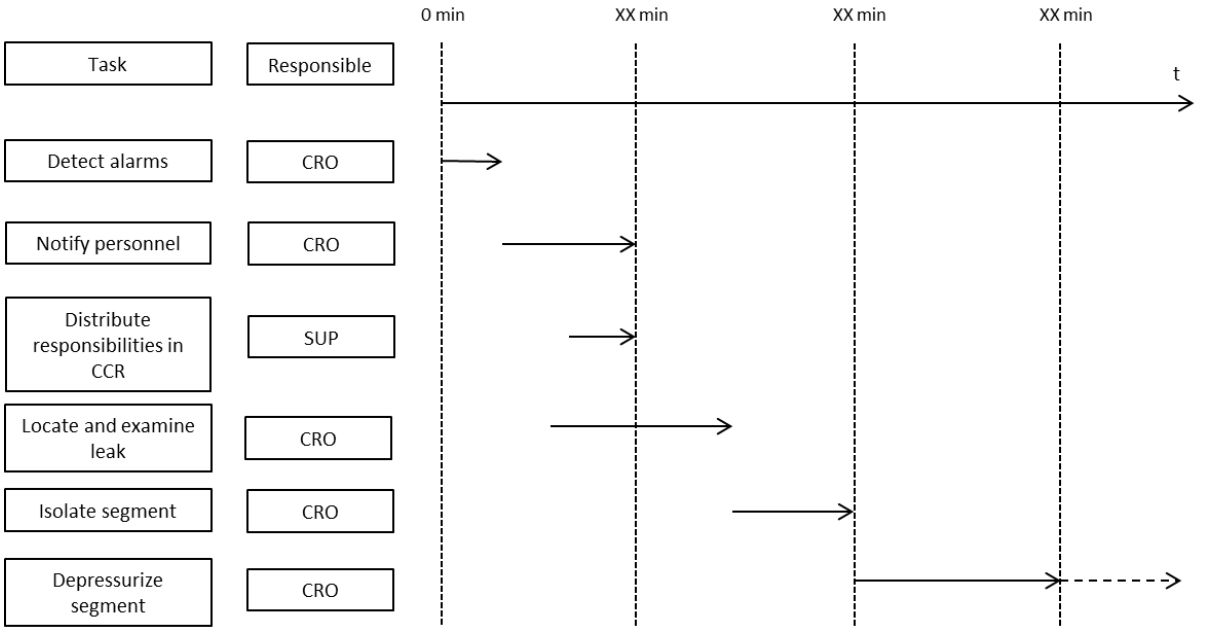

Figure 31: A typical timeline diagram

The following approach can be applied:

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 in Table 31):
    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, or when
    d. The rig is disconnected from the lower marine riser package.

Table 24: Example of 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.

Output: The output from the timeline analysis is an estimate of the time required to perform the task being analysed in the HRA. Substantiation for this estimate is documented in the timeline diagram and table.

Good practices: In addition to the suggested approach, the following good practices apply:

- **Check for uncertainties**. For some tasks, or parts of tasks, it may be difficult to obtain an accurate and reliable estimate of time required. Data collected via interviews and group discussions may contain uncertainties produced by differing opinions and experiences of the people providing input. The analyst should try to facilitate discussions and interviews in ways such that the level of uncertainty is minimized. Uncertainties must be highlighted together with potential impact on the risk and recommendations about how to reduce the uncertainty. The uncertainty should be recorded with a "conservative" upper and an "optimistic" lower boundary, so the practical outcome of this is an interval for expected time required.

- **Avoid input biases**. It is recommended not to reveal the available time to personnel providing input to the timeline analysis, such as operators participating in a workshop. This may make them biased towards this estimate and may influence their perspective on how much time is required. If revealing the available time is inevitable, this bias effect can be mitigated by presenting alternative time estimates for time required from for example incident reports and accident investigations.

- **Triangulate perspectives**. The workshop participants' perspectives on time may be significantly different and it is therefore important to triangulate this discussion so that all viewpoints are challenged and considered systematically. One way of doing this is to gather inputs individually first, and then present them as part of a plenary discussion.

- **Control unrealistic optimism**. While the input from operators responsible for performing the task is valuable, they also have a tendency to be optimistic about how much time is required to perform the task. This is especially relevant for operators who have not experienced the actual event, but have maybe trained for it, or discussed it as part of desktop exercises. To outbalance such optimism, it can be useful to present data from similar events.

- **Consider contextual factors**. Beyond the duration of performing the necessary cognitive and physical actions, time required must include time passed due to expected various disturbances and distractions. The analyst must however be careful not to double-count influences present in other PSFs. For example, if the design of a control panel is poor with regards to being time consuming to use, this should be accounted for in the Time PSF as time required.

- **Reflect average performance**. As far as possible, the time required should be estimated according to what is expected given the circumstances of the accident scenario. It should not (for example) reflect the shortest time possible, as performed by the most experienced and well-trained operator on the facility. Instead, time required should reflect the time it takes an average operator to perform all the necessary actions in a controlled manner, but without hesitation and unnecessary pauses.

Pitfalls: The following pitfalls should be avoided:

- Inconsistent assessment – Not being consistent in the manner each task step is assessed may result in an inaccurate estimate of the overall time required.
- Deviation from scenario – The task analysis reflects how the operator(s) will perform in a specific scenario. Deviating from the scenario's context may therefore invalidate the results from the timeline analysis.

12.1.4 How to Analyse Available Time

How to obtain measures of available time depends on what accident scenario is being addressed and the data available to the analyst. In summary, two main approaches can be applied; an analytical approach and a prescriptive approach.

Analytical Approach: The analytical approach suggest that available time is calculated after scrutinizing the physical parameters which characterises the accident scenario being analysed. The analyst starts with establishing a specific definition of the consequence which the operator(s) are trying to prevent or mitigate. To do this the end events for relevant branches in the QRA event tree must be examined. "Relevant" here means the branches in the event tree which includes the HFEs. Examples of an end event can be damage to the subsea wellhead when the maximum riser angle is exceeded in a loss of position scenario for a semi-submersible drilling rig.

The next step is to determine the available time – i.e., the point in time for when the task (and the associated safety system/ barrier) no longer has the desired effect on the adverse consequence for the end events. It is considerably easier to estimate available time for some accident scenarios than others. For example, in case of DP failure causing a drilling rig to drive off position, the available time can be calculated as a product of relatively accurate and obtainable parameters such as water depth, equipment tolerances, thruster force and environmental conditions. In addition, it is fairly straight forward to define the consequence for which timely and preventive actions are required (here: damage to wellhead).

For other scenarios, however, this picture can be far more complicated. For a gas leak, the available time can be considered for a larger number of intermediate and end events, as well as for a wider range of consequences. For example, isolating and depressurizing the leaking segment can be critical for:

- Reducing size of gas cloud, probability of ignition and explosion pressures.
- Avoiding escalation to other areas and making escape and evacuation means unavailable.
- And reducing potential fire loads on main safety functions, such as piping and ESD valves.

The available time may be different for each of these mitigations. In addition, the QRA can be run to account for differences in leak sizes and in different areas. This produces a large number of combined parameters and cases, each with potentially unique estimates of available time. Furthermore, reliable estimates of available time can be challenging to define due to the inherent uncertainties of the various parameters involved (e.g., the behaviour of gas clouds in various weather conditions and geometries). As such it can be troublesome to determine how quick the operators must respond for the risk to be acceptable based on physical parameters.

Suggestions for how to calculate available time in loss of containment scenarios are provided in Section 18.1.5. For other accident scenarios the analyst has to solve this on a case-by-case basis. It is

important that available time is discussed, clarified and defined in collaboration between the HRA team, QRA team and client to ensure a common understanding and definition.

Note 1: In any case, care must be taken not to confuse available time with the point in time for when unacceptable harm or losses occur. For example, the DP operator has to stop the thrusters and activate the emergency quick disconnect (EQD) soon enough. This is because the disconnect sequence has to be complete before an excessive riser angle jeopardizes a successful disconnection and causes damages to the wellhead.

Note 2: Be careful to ensure that the available time [and required time] is based on and follows the scenario description. If deviations from the scenario and task analysis are required to represent available time for several end events and consequences, these must be recorded and made traceable.

Prescriptive Approach: The prescriptive approach suggests available time based on (inter-)national industry standards and/or requirements. Some companies may also have internal requirements. Since such data is not facility-specific, agreement is needed to ensure there is a common understanding amongst the relevant parties of what is considered to be an acceptable available time limit for the scenario(s). To this end, a meeting should be set up with SMEs to collect a coherent set of qualified judgements using a suitable and systematic approach. Preferably, the final choice(s) should be backed up by trustworthy substantiation and evidence, such as reference to incident reports, full scale testing, simulations or similar source of information.

12.1.5 Analysis of Available Time for Process Accidents

In order to estimate the available time, it is important to define how the consequence should be reduced. An escalated fire or explosion event is the last part of a chain of event typically starting with a hydrocarbon leakage. Each step in the chain of event will normally be associated with a more or less increased consequence, i.e., it could be defined as an escalation of the event. Also, each step in the chain of events could in principle be avoided with an adequate measure in place, or if an action was performed soon enough. Available time has to be related to the action potentially avoiding a specific next step in the chain of event.

For a large process facility, a hydrocarbon leakage may occur in several different places within any of the process modules, the event scenario is also decided by the release rates, direction, distance to adjacent process segment or adjacent fire area, module, or main area. Hydrocarbon leakage scenarios are likely to follow similar chains of events, however the duration between steps in the events chain could vary significantly from case to case.

Clearly it is a coarse approach to establish a generic available time for which the risk related to process events are eliminated. With increased operator response time the risk is bound to rise because for one or more of the cases modelled the increased time is likely to allow the event to reach the next step in its chain of events.

Considering the complexity of the problem three approaches are suggested here:

1. Identify one available time for the QRA model, or per scenario, by investigating one or a few specific available times suitable for one or more defined initiating events (e.g., main risk contributors). This approach is detailed and time consuming but may provide a good insight into the scenario specific factors for which the specific initiating event available time(s) should be considered.

2. Apply a distribution of available times, i.e., a pre-defined number of time steps. This approach should be suitable for applying HRA on overall QRA risk results by using available times, e.g., times to initiate blowdown, without detailed analysis of suitable available times per end event. This approach is less scenario oriented, and less sensitive to inaccuracies in the defined available time(s) but requires that the QRA model can accommodate more than one blowdown time. The accuracy of this approach will increase by increasing the number of time steps, and may therefore also require increased computational power. However, introducing a limited number of time steps should give an indication of the influence of HRA results on the overall QRA risk results by influencing each end event frequency where HRA is applicable.

3. Identifying one available time based on running sensitivities for a number of specific times, and choose the available time based on how the risk results vary with the input time value.

The approaches described above are based on a hypothesis that the risk as a function of time to initiating a certain operator action will increase constantly, however not linearly. The purpose of the first and the third approaches described is essentially to identify the shape of the curve and more specifically the area of the curve where the risk is most sensitive to the increase in time (i.e., the steepest area of the curve). In the first approach this should typically be identified by detailed investigation of the largest contributor(s) to the risk.

Instead of investing time for detailed analysis and defining specific available times, e.g., for initiation of blowdown, the second and third approach considers a selected set of varying times available to initiate blowdown to be applied. Without detailed knowledge of any specific process event cases the sensitivity in the risk results related to the time to initiation can be obtained.

The second approach is presented as a new concept for including several blowdown times in one QRA event tree model.

The third approach is less conceptual and suggests running sensitivities over one single available time parameter in the study. As a simpler methodology, the available time is defined thanks to several runs of sensitivities that vary the available time parameter and the related HEP for the whole study. This methodology ensures that the identified available time reflects in terms of risk results the entire risk picture and not only a limited set of worst cases. It will however not provide the detailed understanding of the scenario and chain of events as may be obtained applying the first methodology. For many event tree models used in QRAs there are typically two outcomes (branches) for each potential factor influencing a scenario. For initiation of blowdown this is success or failure in initiating blowdown at a specific time (the available time) after the initiating event. There are only two analytical outcomes and thus the complete range of consequence outcomes must be categorised within either of these. In this case the result of the analysis is strongly affected by the selection of the available time.

By allowing the QRA to accommodate for more than one time to blowdown, multiple available times can be suggested (as suggested in the second approach listed above). As the number of increments increases, and the size of the increments decreases, the uncertainty related to the expected outcome corresponding to an available time (i.e., within the increment) will be reduced and thus it becomes less and less important to define the most accurate available times. The error margin and uncertainty related to choice of available time will therefore decrease. The justification for this is similar to the selection of categories for leak rates or hole sizes in the QRA.

12.1.6 Methodology 1: Detailed Available Time Analysis

The objective of the detailed analysis is to estimate reasonable available times for a pre-defined initiating event and selected related end events. Prior to any available time calculations the analyst should define for which specific initiating event detailed calculations will be performed.

The available time would typically be estimated for the modelling case with the highest contribution to the risk, i.e., the highest probability of occurrence or the scenario associated with the most severe consequences. In order to further strengthen the estimated available time values one or more of the modelling cases with large contribution to the risk could be also be analysed.

Limitations of this methodology: This approach will establish available times for the specific case analysed in more detail. Although it can be expected that the available time estimated for one case will also be a good estimate for many of the large number of less severe or less frequent cases, this may however not always be true. Running the QRA applying the estimated available time as the assumed time to perform the action, is one option to verify this.

Input to the detailed available time analysis: The following inputs can be used as part of the detailed available time analysis:

- Identified initiating event – ETA
- Input from safety personnel to identify which end event the analysis should focus on
- Select critical element specifications for example: design load for firewalls and blast walls, critical overpressure thresholds for pressurized vessel, TR fire integrity duration, etc.

Timing of the analysis: The detailed available time analysis can be performed after the event tree model of initiating events has been established. The initiating events will be reviewed and a selection of the estimated main risk contributors will be done for the detailed available time analysis.

For each selected initiating event, one or a few available times should be calculated by the detailed analysis in order to build-up the HEP for the event tree model. The number of the defined available times for one initiating event depends on the end events that the available time can prevent if the action (e.g., blowdown initiation) has been successful within this time frame. Calculations of available times take place after screening and selection of each initiating event main undesired outcomes (e.g., impairment of barrier preventing escalation of fire or explosion).

Available times are determined for the selected end events, either based on a standard (e.g., fire wall integrity for A or H-rated fire walls) in which case no calculation is needed, or they can be defined by process equipment failure in which case more detailed calculations should be performed in order to estimate the applicable available time. These calculations will be based on the agreed parameters e.g., expected releases rate and threshold load for the barrier or equipment to withstand (like radiation level).

Approach to the analysis: The following approach can be applied, using the example of a gas leak in a process module as an initiating event to illustrate each step.

Reviewing the outcomes of the selected initiating event: Outcomes from a specific initiating event will vary with regards to the initiating event itself and parameters defined in the event tree, for example isolation, ignition, and blowdown. Similar end events can appear several times and can be grouped in end event categories.

Example: How to regroup similar associated available time outcomes:

- Category 1 Immediate ignition outcomes
  - Jet fire / Pool fire escalating to other areas
  - Jet fire / Pool fire escalating to equipment
  - Local Jet fire / Pool fire
- Category 2 Delayed ignition outcomes
  - Explosion escalating to other areas
  - Explosion escalating to equipment
  - Delayed jet fire / Pool fire
- Category 3 No ignition outcome
- Unignited release

The purpose of the analysis is not to calculate one specific available time for each end event category. This could theoretically be done, but it could be considered excessively time consuming. The analyst has to choose the available time applicable for the scenario categories which would assure the end event will be avoided.

Selecting governing available times: Prior to the calculations, the analysts should assess the consequence associated with the end event categories. By reviewing the consequences, the analysts can select the end event that will define the governing available time to be evaluated. The governing end event can be selected according to the level of severity of consequences and/or because the end event is found to be the one associated with the shortest required time to initiation in order to be avoided. Given the event tree model, one available time may cover different end events.

In case of similar level of severity for more than one end event, the calculation may be performed for all end events and the shortest duration could be chosen. The governing available time should be agreed and should reflect the client's concerns.

Table 25: Example of how to select governing available times

		Consequences evaluation (qualitative)	Available time before undesired consequences	Representative available time
Category 1	Jet fire / Pool fire escalating to other areas	TR is an adjacent area and could be impaired by the fire	TR can withstand fire for 5 min	Yes – shortest duration
	Jet fire / Pool fire escalating to equipment	Pressurized vessel present in the module. BLEVE escalating scenario could occur	Mechanic failure of the vessel leading to BLEVE considering jet fire radiation is expected to take place within 10min	No
	Local Jet fire / Pool fire	Confined fire in the module	Escalation of the fire to other areas expected to take place within 20min	No
Category 2	Explosion escalating to other areas	TR is an adjacent area and could be impaired by the explosion	TR can withstand a specified level of overpressure	Yes
	Explosion escalating to equipment	Pressurized vessel in the module could be impaired by the overpressure	Pressurized vessel can withstand a specified level of overpressure	Yes
	Delayed jet fire / Pool fire	Same consequences as category 1	Same available time as category 1 time to delayed ignition could be added	As for category 1 time to delayed ignition could be added

Category 3	Unignited release	Explosive atmosphere in the module	Gas migrating and exposing other modules	No

Resulting from the analysis one or more available times could be identified. Fire events will e.g., be governed by avoiding TR collapse. For explosion the worst case may be governed by the filling level of the module volume that will lead to a stoichiometric cloud size with potential of an escalating explosion.

Calculating selected available times: Available times for specifics end events are calculated using defined parameters for the case. The initiating event should be sufficiently defined before calculating the related available time. After selecting the governing end event, the analyst can refer to design values for specific identified target and use the provided times as reference. The calculated available time is thus dependent on the parameters defined for the potential chain of events.

The available time applied for the fire case is assessed given the duration the TR can be exposed to fire before collapse, e.g., 5 min. In order to include the time needed for blowdown to be efficient the associated available time for initiating blowdown could be within 1 or 2 minutes depending on the defined initiating event and the efficiency of the blowdown system.

12.1.7 Methodology 2: Multiple available times in one model

The objective of this approach is to establish multiple available times in order to have a better representation of the consequence outcomes corresponding to the available times. Consequences will be distributed according to probabilities allocated to the available times. This approach will consider a selected number of system specific available times.
This approach can be tailored to the HRA result in terms of probability of successful human intervention within the time steps used as available times.

Limitations of this methodology: The overall approach assumes that a selected number of systems specific available times can be defined. The number and the values of the analysed available times e.g., associated to blowdown initiation, could be part of the discussion.

This approach is proposed mainly if the event tree in the QRA tool applied accommodates for multiple times to successfully conclude an action, e.g., to initiate blowdown.

Input to the multiple time approach: The following inputs can be used as part of the multiple blowdown initiation times approach:

- Times for blowdown valve to fully open.
- Typical times for operators to initiate blowdown given situation complexity.
- HEP for event tree models.

Timing of the analysis: The selection of available times using this methodology should be integrated with building the event tree models. These two activities are closely related because systems specific blowdown time steps may be defined at this stage, and the HEP should be integrated in the frequency analysis in this part of the QRA process. After the blowdown time steps have been defined with their respective frequencies, analysts can run the QRA model and proceed to results analysis.

Approach to the analysis: The overall approach is to divide the scenarios into more events than just successful and unsuccessful blowdown. The available times are the durations until initiation of

blowdown, and the corresponding HEPs will decide the likelihood of initiating blowdown within the defined available times.

The approach should start by defining how many blowdown initiation times to be included in the event tree model. An example could be four times to initiate blowdown, e.g., after 25 seconds, 60 seconds, 5 minutes, and 15 minutes, which can be associated with a gradually declining degree of successful intervention in terms of avoiding the escalation within the chain of events.

By increasing the number of time steps, the uncertainty related to the accuracy of the representative available times will decrease and the definition of the risk picture will increase. However, as a high number of steps will significantly increase the calculations required to run the QRA model, a level of detail should be chosen which matches the overall requirements of the QRA.

The available times might not be directly related to process issues but they should be more related to typical values for operating personnel to activate blowdown given situation complexity. This approach enables to associate HEPs to the overall frequency analysis and has an impact on the total risk results. The QRA model will reflect the results for each outcome given the time to initiating blowdown. The results can show the optimized blowdown initiation to be applied by operating personnel in order to get the lower risk results considering escalating events.

- Assessing HEP for each blowdown initiation time in the event tree model.
- Running the QRA model with several blowdown initiation times.
- Compiling results and identifying which blowdown duration(s) could be used as inputs for HRA analysis.

For example if risk results with initiation of blowdown after 25 seconds or after 60 seconds are almost identical, while there is a more significant increase after 5 minutes, then the HRA should use these results to improve the required time with a target of 5 minutes.

12.1.8 Methodology 3: Identifying a single available time by running sensitivities

The objective of this elementary methodology is to identify one applicable available time for the whole study and ensure that the entire risk results are represented as basis for this selected available time. This methodology is applicable for studies that enable only one time to successfully conclude an action, e.g., to initiate blowdown.

Limitations to this methodology: The overall approach is to select a wide range of values for an available time sensitivity analysis. This could be foreseen as blind runs changing the applicable available time and analysing the risk results.

In order to ensure that the identified available time is an appropriate value to represent the whole risk results, several runs and associated available times values should be applied. By increasing the number of runs and available times values the influence of the applied available time will be better reflected in the results.

Input to the sensitivity analysis: The following inputs can be used as part of the available time sensitivity analysis:

- Times for blowdown valve to fully open.
- Typical times for operators to activate blowdown given situation complexity.
- HEP for event tree models.

Timing of the analysis: The identification of available time by running sensitivities is performed either when building the event tree models or during later runs of the QRA model. The QRA model has to be run for each selected time value for initiation of blowdown and risk results shall be extracted.
This approach does not require a large amount of time to investigate the appropriate available time to be applicable. However the computational processing and results post processing time will increase according to the number of sensitivities runs.

Approach to the analysis: The overall approach is to define one available time applicable for the whole study. This approach does not consider a probability distribution of several available times but tries to reach the most relevant available time to be applicable to the whole study by varying it and analysing the sensitivities in the risk results.

Analysts will have to run the event tree model multiple times with a selected range of potential available time values. Parameters influencing consequences extracted from the QRA model (i.e., release durations) will vary according to each event tree model input. The influence on risk results for the various input values should be assessed in order to identify an available time value with a strong influence on the total risk level.

12.1.9 Overall Limitations

It is important to note that although changing the value used in the QRA for the time to initiating a certain human intervention will affect the QRA results, the actual risk will not be affected unless it can be substantiated that the value applied is realistic in terms of human reliability. The approaches described previously are based on a hypothesis that the risk as a function of time to initiating a certain human intervention will increase constantly, however not linearly, and the purpose is essentially to identify the shape of the curve and more specifically the area of the curve where the risk is most sensitive to the increase in time (i.e., the steepest area of the curve). The real value in estimating the available time is to provide a time input to the HRA, i.e., a “goal” which the HRA can aim towards. This goal should be related to the benefit of risk reduction, and with this estimated time to human intervention it is possible to re-visit the HRA and identify critical PSFs, e.g., stress factors, design, training, in order to meet the available time.

12.2 Examples of PSFs Evaluated But Not Included in Petro-HRA

Examples of PSFs that we have evaluated, but that are not included in the Petro-HRA method are:

- **Fatigue** was not included because the multipliers are too low compared to the other PSFs. Folkard and Tucker (2003) found that Fatigue increased accident rates by 30 percent when controlling for all other factors that separate day work and night work. This gives a multiplier of 1.3. The HRA method, Human Error Assessment and Reduction Technique (HEART; Williams, 1988, 1992) has an error producing condition (EPC) with a similar content to Fatigue called “Disruption of normal work sleep cycles”, with a multiplier of 1.1. HEART also has another EPC with similar content to Fatigue: “Prolonged inactivity or highly repetitious cycling of low mental workload tasks,” with a multiplier of 1.1 for the first half hour and x1.05 for each hour thereafter. Our suggestion is that if a scenario also could happen at night, the analysts should consider the scenario to be a deviation scenario, because night work might affect PSFs other than fatigue, such as the number of people at work, which again might affect several PSFs including Available Time, Experience/Training, and Teamwork. There might also be other issues at night, for example, darkness might make the Closed-Circuit Television (CCTV) difficult to see. The analyst should evaluate during the data-collection whether the

PSFs are different at night than during day. If differences are found in PSFs that affect the HEP(s) one should consider night work to be a deviation scenario.

- **Workload** is not included as a PSF since workload is a multi-construct that overlaps with several other PSFs. For example, National Aeronautics and Space Administration Task Load Index (NASA-TLX; (Hart & Staveland, 1988) included the following subscales to measure Mental Demands, Physical Demands, Temporal Demands, Own Performance, Effort, and Frustration. These subscales overlap with Complexity (Mental Demands and Effort), Time (Temporal Demands), and Physical working environment (Physical Demands). Since workload overlaps with other PSFs, workload is evaluated through them, but it is not included as a PSF in its own.

- **Frustration and emotions**. These PSFs are studied in Psychology. However, they are internal factors and difficult for the analyst to assess in a method like Petro-HRA. Also it is the other PSFs (for example Complexity, Teamwork) that often are the cause of frustration, and the effect of frustration is counted though the other PSFs. We consider that the most relevant part of emotions and frustration is covered by Threat Stress and the other PSFs.

12.3 Practical Advice on Quantification

Petro-HRA includes thorough data collection from interviewing, observing and analysing subject matter experts (SMEs) in workshops or training and simulations, see Section 2 on qualitative data collection. The succeeding steps; the task analysis (Step 3), human error identification (HEI; Step 4) and human error modelling (HEM; Step 5), are all based on this data collection. In addition, the analyst should check back with the SMEs interviewed for clarification, confirmation and verification throughout these steps.

Having arrived at the quantification step, the analyst(s) have acquired a considerable knowledge about the scenarios and events, and about which PSFs that impact the tasks and the probable errors involved. The detailed knowledge about how and to which extent these PSFs affect performance of each task is the key to choosing the multipliers for the PSFs. In Petro-HRA, this judgement must be done by the analyst(s). It is not only a matter of evaluating whether conditions in the form of PSFs are present in the scenario or not, it is a matter of judging whether a PSF is present to the extent that it will actually affect human performance. The whole process of collecting data; analysing tasks; identifying the way in which people may perform or not perform tasks (HEI); and modelling the details of the scenario, including recovery opportunities, in the HEM; and throughout this process identifying and evaluating PSFs, should now enable the analyst to judge whether a PSF would impact task performance or not.

This section outlines a few alternatives for the practical quantification, dependent on the number of analysts and the access to SMEs.

12.3.1 Number of Analysts

In some cases the analyst may be performing the HRA alone. In this case, the evaluation of the PSFs would have to be done alone but with the best help possible from SMEs (see below).
In many cases there should be more than one analyst, especially for the data collection. If two or more analysts are available for the quantification, the following procedure may be applied. For each of the nine PSFs:

- Compare the collected information with the PSF level description/definition.
- Determine PSF level and corresponding multiplier value.
- Determine PSF level individually (each analyst).
- Compare results and decide on a consensus level.
- Document concurrent and divergent individual assessments.
- Document selected level / multiplier value and provide substantiation in summary worksheet.

It is advantageous to use two or more analysts for the quantification. Of course, these should be the ones that have joined the whole process. Especially, it is also advantageous to be two analysts during the qualitative data collection (one facilitator and one scribe) to obtain all relevant information about the PSFs.

12.3.2 Contribution from Subject Matter Experts

Subject matter experts (SMEs) consulted throughout the analysis must be knowledgeable of the facility under analysis. It is not sufficient to consult with a domain expert who has not worked at or know the facility. The best SMEs are typically operators who know the current operation and actual conditions at the facility, not only its design. If other experts are consulted, they should know the facility in detail. In the following, the term SME is used about people with such detailed knowledge of the facility analysed.

For quantification, there are a number of specific activities that should be supported by one or more SME. The analysts base their judgements of PSFs on a number of analysis steps. Before the analyst evaluates the PSF levels, it is invaluable to get SMEs involved in the following:

- Verify the task analysis (TA). The TA should be verified by the SME in order to check that the analyst has understood the tasks correctly, and understood the links between various tasks. Included is a check that the assumptions and preconditions for the tasks are understood and properly represented in the TA.
- Verify the HEI. This should be verified by the SME to check that the descriptions of the way in which tasks can fail and the corresponding influencing factors (PSFs) are fully understood by the analyst.
- Verify the modelling (HEM). The SME can check that the events modelled in the HEM represent the events and scenarios in a plausible way.

For all these steps, the SME should verify the descriptions of how the PSFs impact tasks, errors and events. In this way one may assure that the relation between the PSFs and the tasks are correctly understood by the analyst.

There are various ways of consulting the SMEs at this point of the analysis. The best alternative would be to gather SMEs in a workshop again, to get their full attention for a day. The SMEs should be given the opportunity to read and judge the material individually before a group discussion takes place.
When all assumptions are verified, the analyst(s) can perform the quantification by choosing multiplier levels for the PSFs for each task. After the quantification is done, SMEs should be involved in the reasonableness check of the results, as described in the next section.

12.4 References

Myers, P.M. (2013). Layer of Protection Analysis – Quantifying human performance in initiating events and independent protection layers. Journal of Loss Prevention in the Process Industries, 26, pp. 534-546.

13 Background to Step 7: Human Error Reduction

One of the main incentives for quantifying the probability of human error is to obtain a numerical measure of how human actions influence the plant's risk level and safety performance. After the HEP calculations have been performed they can be integrated into the overall risk model, such as a QRA event tree. This provides an opportunity to quantitatively demonstrate the contribution (i.e., impact) of human error on the risk level. The quantification provides, via the impact assessment, justification for how much effort to put into the ERA in terms of scope, depth and level of detail.

Resources put into developing and implementing risk reducing measures can be kept to a minimum in cases where the contribution is considered to be negligible. Conversely, if the contribution is considered to be high, or if the results contain a high degree of uncertainty, the analyst has to demonstrate how the risk can be reduced down to an acceptable or desired level.

13.1 The Purpose of Human Error Reduction

Developing ERMs and ERSs is ultimately a product of how the analyst understands the system, task and scenario being analysed. Consequently, the quality of risk reducing measures depends greatly on the scope, format and level of detail of the preceding analyses. To finalize this part of the HRA process it is therefore necessary that all preceding analyses are more or less complete. In particular, the following topics and outputs must be re-visited:

- How PSFs are considered performance drivers for various parts of the task, or across the task – documented in the task analysis (Step 3).
- Which human errors are targeted as critical and how PSFs can contribute to their occurrence – documented in the HEI (Step 4).
- How a HFE results from unsuccessful task outcomes caused by one or a combination of several human errors – documented in the HEM (Step 5).
- Which parts of the task is the most error prone, and how do the PSFs influence task performance – documented in the human error quantification (Step 6).

ERMs and ERSs are in practice identified and developed throughout most of the HRA process, starting with preparations such as document reviews and ending with modelling and quantification of human errors. Risk reduction should therefore be considered an iterative process starting from the onset of the HRA by utilizing information gathered from the various analyses steps. However, it is not until after the human error quantification is done that this process can be finalized.

Several of the considerations and calculations done as part of the impact assessment require QRA expertise. It is therefore important that such activities are performed in close collaboration between the QRA analysts, the HRA analyst and relevant stakeholders (e.g., facility management). Furthermore, the facility management, who often also is the "risk owner", should determine the preferred level of accuracy.

13.2 Additional Guidance on Performing an Impact Assessment

This section describes how to perform an impact assessment consisting of the following steps:

- Integration of HEP into overall risk model.
- Consideration of impact assessment criteria:
    - Risk acceptance criteria.

    - Size of HEP value(s).
    - Degree of HEP uncertainty.
    - Severe QRA end states.
- Assessment of HEP contribution.

13.2.1 Impact Criteria

The following four impact criteria need to be examined to determine whether or not to further assess HEP contribution to the overall risk level and/or perform an ERA.

Risk acceptance criteria – Having performed the necessary QRA calculations the risk can be compared against a set of pre-defined risk acceptance criteria. These are typically put forth by regulatory bodies, international standards, and/or companies own internal requirements. One example is the Norwegian Petroleum Safety Authorities guidelines for Facility Regulations §11 which stipulate a risk acceptance level of 1 x 10 -4 as the annual limit to the probability of loss of main safety functions for offshore facilities.

If the QRA fails to meet the risk acceptance criterion the analyst will typically first scrutinize the model for inaccuracies, errors, etc., adjust if necessary, and then re-calculate parts of the model to check if the risk level changes. If the risk level still exceeds (or is unacceptably close to) the criterion, the analyst initiates a process to determine which parts of the QRA constitute significant contributions. This includes the HFEs which then may become subject for further assessment.

High HEP value – A high HEP value should encourage the analyst and decision-makers to assess HEP contribution, regardless of whether the QRA fails to meet the risk acceptance criteria or not. What constitutes a high (or conservative) HEP can be determined by use of expert judgement, statistics, or other types of industry experience. However, it is considered good practice to conduct an ERA any time the HEP of a HFE equals or is larger than 0.1 (Kirwan, 1994). As such, it can be recommended that HEP contributions should be quantitatively assessed for HEPs larger than 0.01 (i.e., one order of magnitude down).

HEP uncertainties – A third consideration for whether or not to perform a more in depth ERA is the degree of uncertainty in the input data and results from the HRA. The HEP of a HFE may be low or appear to have an insignificant contribution to the risk level, but if the analyst has noted one or several uncertainties in the analysis this may produce an incentive for developing ERMs and ERSs. This will first become relevant after attempts to remove the uncertainty have proved to be unfeasible.

There is currently no standardized approach available for how to evaluate uncertainty in a HRA. Conclusions made about uncertainty are therefore a result of the analyst's judgement about the quality and characteristics of input data, such as accuracy, relevance and more. The analyst therefore should continuously make note of potential areas of uncertainty throughout the HRA process and include them in the decision basis used to conclude on the need for an ERA.

Severe QRA end states – The QRA may have revealed that the end state for one or several of the event sequence pathways are associated with particularly severe consequences. If these event sequences include HFEs it may become relevant to examine effects of HEP contribution.

13.2.2 Selecting Events for Error Reduction Analysis

Fault trees – For fault trees, basic events are selected based on two combined considerations: 1) The HEP for each basic event; and 2) the relative contribution of the same HEP if combined with other

basic events. It is important that the analyst does not consider the failures as separate and isolated basic events. The analyst must first check whether the basic event has to occur together with one or several other basic events in order to cause the TOP event. A single basic event may have a high HEP without contributing significantly to the overall HEP for the HFE. This is illustrated in Figure 32.

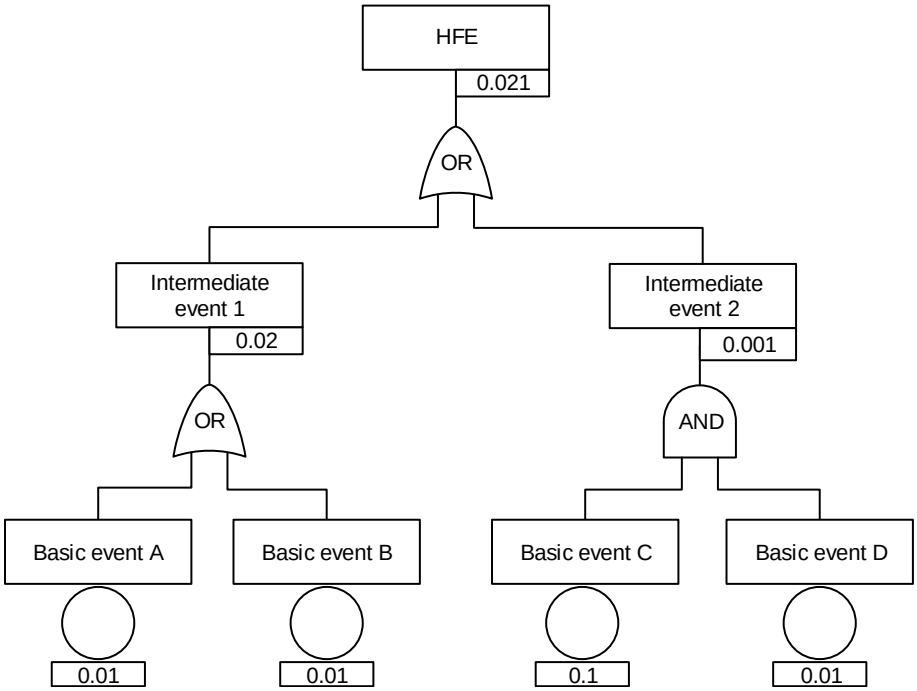

Figure 32: Fault tree with example quantifications

In Figure 33, because they are solely connected to the TOP event via OR-gates, either Basic event A or B can result directly in HFE 1. The HEPs for these basic events are therefore added together to produce the HEP for Intermediate event 1, which is again connected to the TOP event via an OR-gate together with Intermediate event 2. Basic event C and D, on the other hand, are initially connected via an AND-gate and must therefore occur together for Intermediate event 2 to happen. The HEPs for these basic events are therefore multiplied to produce the HEP for Intermediate event 2. As can be seen, although Basic event C has the highest HEP – because it has to occur together with Basic event D, it has a smaller contribution to the overall HEP of the HFE than both Basic event A and B. In the case of Figure 33 both Basic events A and B should therefore be prioritized over Basic events C and D.

For slightly more complex fault trees it is recommended to perform what is referred to as a minimal cut set analysis. This is a mathematical technique for manipulating the logic structure of a fault tree to identify all combinations of basic events that result in the occurrence of the TOP event. These basic event combinations, called cut sets, are then reduced to identify those “minimal” cut sets, which contain the minimum sets of events necessary and sufficient to cause of the TOP event. For minimal cut set analysis it is recommended that the HRA analyst confers reliability engineers or other experts on fault tree analysis (FTA).

13.3 Additional Guidance on Developing Error Reduction Measures

Error mechanism prevention – An effective error reduction technique is finding ways to prevent various error mechanisms (or causes) from triggering specific internal and subsequently external error modes (i.e., ways to err). Error mechanisms can be psychological or contextual. Psychological error mechanisms (PEM) are the cognitive biases known to affect (human) performance, such as

"expectation bias", "perceptual confusion" or "cognitive preoccupation". Contextual error mechanisms (CEM) are external conditions (social or physical) likely to produce errors, such as incorrect procedure, alarm floods or poor HMI. CEMs are external PSFs identified to affect specific aspects of human (task) performance. Internal error modes (IEM) refer to cognitive (i.e., psychological) ways of erring, while external error modes (EEM) are the behavioural (i.e., physical) manifestations. Preventing error mechanisms therefore involves understanding how humans' characteristics interact with the social and physical environment in ways that provoke operator failures. For example, a poor HMI (CEM or PSF) may present the operator with a large amount of information causing memory overload (i.e., a PEM). This makes the operator forget information (i.e., an IEM) about how to correctly perform a subsequent action (i.e., an EEM). In this example several different ERMs can be implemented. A starting point would be considering ways of re-designing the HMI to reduce the amount of information and/or improve its quality. If this is considered too costly or not practical, other ways of reminding the operator of what to do can be introduced. Examples include checklists, procedures, collegial support or supervision.

Error mechanism prevention is perhaps the most advanced error reduction technique and requires in-depth knowledge about the task, its contextual factors and cognitive psychology. The HEI technique presented in Petro-HRA is developed to be an easy-to-use and simple approach. For error mechanism prevention it can therefore be useful to draw upon guidewords, definitions, and other methodological principles from more advanced HEI techniques, such as TRACEr (Shorrock & Kirwan, 2002).

Error pathway blocking – While preventing error mechanisms attempts to reduce the likelihood of errors to occur in the first place, another approach is to block error pathways. The HEI technique in Petro-HRA includes guidewords for describing EEMs such as »operation mistimed« or »operation incomplete«. Such an analysis may reveal potential unsafe actions, such as opening a critical valve which should be left closed, entering an incorrect pressure parameter, or setting a too high alarm limit.

Example of ERMs could be to make it physically impossible to unintentionally open a valve e.g., by use of interlocks. Another example is to introduce upper and lower limits for which values can be entered via the HMI. This also gives the operator an opportunity to immediately detect and correct the error (see also error recovery enhancement). Such solutions should be strengthened by providing the operator with feedback about the error (i.e., error messages). If the operator understands the error and its potential consequences this may also prevent intentional unsafe actions, such as overriding safety systems.

Measures to block error pathways should be assessed in terms of their effectiveness. Signs and posters for warning or information purposes can easily be ignored, overlooked or misread, both in routine and abnormal situations. Interlocks and similar solutions are effective, but care should be made to make sure that the system functions are made unavailable in situations where they are required.

Error recovery enhancement – Trying to either prevent or block all human errors is neither feasible nor practical. For critical tasks it can therefore be necessary to consider ERMs aiming at enhancing error recovery. Here, recoveries refer to operator actions which detect and correct a human error before it has a significant effect on facility safety. For tasks having a potentially immediate effect on the facility, opportunities for recovery can be intentionally designed into the system. By using visual or audible cues the operator is provided with the required feedback, such as alarms, messages, visual indications (e.g., valve status).

Another measure is to use procedures or checklists which include steps for reminding the operators to check for correct performance of previous tasks. This may also be used to enhance recoveries for

error associated with cognitive or interpersonal tasks, such as poor decision-making or misdiagnosis (i.e., IEM). While such errors do not necessarily have an immediate impact on the overall system performance, recoveries should be considered due to potentially delayed effects. Last, recoveries can be enhanced by use of interpersonal or “non-technical” skills, such as buddy-checks, supervision, and read-backs.

As with other ERMs the effectiveness of recovery measures should be thoroughly considered. For example, if a recovery involves the supervisor recording a log of actions taken in an emergency, this should not be given credit if it is mainly a paper exercise and not sufficiently trained for.

Error consequence reduction – A last way of using HEI techniques for error reduction is not to actually reduce the error itself, but instead to reduce its consequences in case it is not prevented, blocked or recovered. Consequence reduction here refers to minimizing the effects of human errors which have a direct effect on facility safety (i.e., interactions with the facility's systems and functions). ERMs aiming at reducing such consequences typically involve changes in design and can therefore be expensive if not discovered at an early stage as part of an engineering process.

Examples can be various use of automation with an aim of making the system less reliant on operator performance, e.g., having an automatic sequence for disconnecting a drilling rig from the well in case of a drive-off event. Another example is having automatic emergency shutdown and depressurization in case of a confirmed gas leak. Introducing automation may lead to other unforeseen events and situations, so it is important to evaluate the human-automation collaboration before such systems are introduced. Other ERMs besides automation can be to make a system more robust, e.g., designing a flare system strong enough to handle any amount of gas the operators may decide to blow down.

13.4 Additional Guidance on Developing Error Reduction Strategies

Overall task re-design – The task analysis can be used effectively to determine risk reducing measures by closely examining task execution times, task sequences, and task requirements, etc.

Most TAs include plans that describe in what sequence the tasks shall be executed. Plans may be linear (»do task one, two then three«), cyclical (»do task one to five, then repeat«) or may include requirements for which task to execute when (»do task one, then two, if pressure level is above 20 PSI, then continue with task three«), etc.. A plan depicts the sequence a task is executed in and may reveal, for example, the complexity of the task. That is, a plan can reveal that there are conflicting cues for task execution, or show that multiple tasks need to be executed simultaneously. In such a case, risk reducing measures may be implemented that aim to simplify the task sequence or that offloads some of the tasks to the system or to other operators.

Task analysis can be used to determine the time operators require for executing their tasks in the response sequence (see Section 18.1.3). As time is an important performance driver, the analysis may therefore also be used to identify which tasks are time consuming and where and how time may be saved in order to improve operator response time. For example, the task analysis can be used to:

- Identify which tasks may be offloaded to the system (i.e., by changing the allocation of functions).
- Offloaded to other operators (i.e., changing the allocation of responsibility).
- Facilitated by improved information presentation (i.e., implementing user friendly interfaces).
- Facilitated by improved operator support (i.e., implementing decision support tools)

Risk reduction by re-designing the task can be demonstrated by several different PSFs depending on how the improvement is being implemented and correlations between different PSFs.

Overall PSF improvement – Already during the initial data collection it may become evident that several PSFs can be improved on a general basis. In many cases it can be argued that human reliability can be increased by implementing improvements targeting the overall task performance. Examples of ERSs targeting overall PSF improvement are:

- Poor quality of procedures; recommend to update procedures using Human Factors principles.
- No explicit task training; recommend to train explicitly on different varieties of the task and scenario.
- Inconsistent work practices; recommend sharing knowledge about good working practices across shifts.
- Missing alarm philosophy; recommend updating the alarm system using one common alarm philosophy.

Furthermore, some ERSs can be related to uncertainties identified in the data collection phase, such as verifying time required by operators to perform a task by using simulator facilities.

14 Arguments for Changes in Definitions of PSFs, PSF Levels and PSFs Multipliers from SPAR-H to Petro-HRA

This section presents arguments for the changes to the performance shaping factors (PSFs) between the SPAR-H and Petro-HRA methodologies.

14.1 Available Time -> Time

PSF no	SPAR-H name	Available time	Version	Date
1	**Petro-HRA name**	**Time**	1	08.05.14
SPAR-H Definition: The SPAR-H Human Reliability Analysis Method (Gertman *et al.,* 2005)				
Available time refers to the amount of time that an operator or a crew has to diagnose and act upon an abnormal event. A shortage of time can affect the operator's ability to think clearly and consider alternatives. It may also affect the operator's ability to perform. Multipliers differ somewhat, depending on whether the activity is a diagnosis activity or an action.				
SPAR-H Definition: Step-by-Step Guidance (Whaley et al., 2011)				
Available time as a PSF term can be misleading. In the assessment of the Available Time PSF, SPAR-H does not look solely at the amount of time that is available for a task. Rather, it looks at the amount of time available relative to the time required to complete the task. In the existing SPAR-H documentation (Gertman et al., 2005) this PSF is evaluated by comparing the time required to the time available. Although the exact definitions for the various PSF levels differ between those for Diagnosis and those for Action, both have a basically consistent definition for the nominal level. Namely, nominal is defined as some extra time is available beyond that minimally required. (Nominal time for Diagnosis is actually defined as "on average, there is sufficient time to diagnose the problem," which implies more than the minimum requirement.) Additionally, while it was not part of the original SPAR-H guidance for this PSF, it is useful to include the time margin in this discussion, which is the difference between the required time and the available time (US Nuclear Regulatory Commission, 2009). Nominal time includes some small but important time margin over the minimum amount of time required. For Diagnosis, the analyst must recognize that the amount of time needed to make a decision (i.e., formulate a diagnosis) is highly dependent on the individual, and significant variability among operators should be expected. Hence the nominal time should be assessed in terms of how the average operator is estimated to perform. Another way to look at this is to estimate the time needed by a better-than-average operator (i.e., the minimum time required) and add some small but significant time margin for the nominal time. While the use of time margins can simplify the assessment of the Time Available PSF, it does not remove the facility and operations expertise required to determine the overall available time and the time required to complete the task. These parameters must also be considered in the context of time required for the Diagnosis and Action parts of a task. Before a judgment can be made about the effect of time on the HEP, the time issue needs to be reconciled with whatever choice the analyst made on how Diagnosis was treated. As mentioned above, it is only in rare cases that Diagnosis is not factored into the HEP calculation. Therefore, the obvious question here is how the available time is allocated between the event Action and the event Diagnosis. To apportion the available time between Diagnosis and Action, the analyst should first estimate the nominal time (i.e., the minimum time needed plus some time margin) to perform the action. If there is sufficient time to perform the action,				

then the available time PSF for the Action is judged to be nominal and the remainder of the time is assigned to the Diagnosis part of the event. This might mean that the available time for Diagnosis is not nominal. Additionally, if a time apportionment is done without specifically estimating the time required for Diagnosis, then time available for Diagnosis is either “nominal” or “barely adequate” no positive adjustment should be used.

There are many influences that can drive the amount of time required and the analyst is cautioned against being too pessimistic by allowing a single influence to affect multiple PSF estimates. For example, a particular action might be very complex, which can extend the amount of time needed to execute that particular action. An analyst might be inclined to then estimate the Time Available PSF as less than nominal and also assess the Task Complexity PSF as worse than nominal in the quantification of the Action component of the HFE. This would result in a “double counting” of that particular influence. The analyst should decide whether available time or complexity is the primary performance driver, and model a negative influence of only one of these PSFs. For example, if the primary hurdle for a crew 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 crew has to deal with multiple system malfunctions, multiple procedures, inexplicable facility response, and multiple indication errors, then the primary performance driver is the complexity of the situation. Analysts should only include a negative assessment of multiple PSFs if there is reason to believe that each of the respective PSFs is a separate performance driver in its own right, and not merely a side effect of one of the other PSFs. Also note that the two PSFs might influence performance in opposite directions in some situations, with a complex task being performed in the context of a substantial time margin. In such cases, modeling one PSF as a negative driver and the other as a positive driver is justified.

Again, note that the Available Time PSF descriptions for Diagnosis and Action events differ. The assumption is that when necessary, decisions can be made very quickly. However, when judging the nominal time for Diagnosis, the analyst should consider the amount of time needed to make a systematic and thoughtful decision as to the nominal time. That is, what information needs to be gathered and reviewed to support the decision-making process? What permissions or concurrences need to be obtained? The characterizations of the Available Time PSF for Diagnosis are intended to be best estimate descriptions and are not deliberately conservative. Hence the analyst should likewise make a deliberate effort to be realistic and comprehensive in estimating the nominal time requirement for Diagnosis and not assume there is any conservative margin built into the PSF quantification process as a rationale for not being as thorough as possible. Again, the intent here is not to simply assume the time required is only the (virtually instantaneous) time needed to decide upon a course of action, it also includes the observation of indicators, the gathering of information, processing of the information and any group interactions (among team members or between supervisor and subordinate).

Once the time required has been estimated, it is then compared to the time available to quantify the Available Time PSF. Again, the intent is to be realistic and make a best estimate of this time window. However, uncertainty pervades this process and it should be recognized that hard and fast discrimination among the different PSF Levels (in particular, among Nominal Time, Extra Time, and Expansive Time) is not feasible.

Therefore, the analyst is cautioned against relying on overly precise estimates that lead to threshold effects from the Available Time PSF. The description of Extra Time (for Diagnosis) in Gertman et al., 2005 is between 1 and 2 times nominal time AND greater than 30 minutes. The 30-minute criterion should be evaluated in the context of the time required for Action (i.e., after accounting for the Action portion). Therefore, if the time available is estimated in the 25 to 30 minute range, then the PSF (for Diagnosis) should be assigned the Nominal level despite the fact that it would

otherwise meet the criterion for Extra Time (i.e., be 2 times nominal). Use of the time margin described above might help reduce the over literal reliance on the 30 minute criterion.

Note that the Available Time PSF does not consider aspects of perceived time pressure by the operator or crew. Actual and perceived time pressure induces stress and should therefore be considered under the Stress/Stressor PSF.

Petro-HRA short explanation of changes (need for change)

The description of the Available Time PSF should emphasize context (such as competing tasks, distractions, teamwork, time to communicate, time on procedures, etc.) and how the context could influence Available Time. This PSF should focus on the objective time available. If the operators experience time pressure without real time pressure (subjective time pressure) this should be considered as an aspect of Training/Experience since the operators then do not have a realistic experience of the available time for the task or scenario. 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.

References (for change)

Kolaczkowski, A., Forester. J., Lous, E., & Cooper S. (2005). Good practices for implementing human reliability analysis. Washington DC. U.S. Nuclear Regulatory Commission.

Reer, B., & Sträter O. (1996). Evaluation of new developments in cognitive error modeling and quantification: Time reliability correlation. In Probabilistic Safety Assessment and Management (pp. 645-650). London: Springer.

Swain, A., & Guttmann, H. (1983). Handbook of human-reliability analysis with emphasis on nuclear power facility applications, Final report (NUREG/CR-1278). Washington, DC: U.S. NRC.

Petro-HRA (full) description

Time refers to the difference between the time it takes to complete the task, here called required time, and the time to consequence, here called available time. The analyst has to evaluate if the operator has enough time to complete the task. If there is not enough time, 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. If there is extra time available, this PSF is expected to improve operators' performance. In determining the appropriate PSF level the analyst should evaluate:

1) How much time does the operator(s) have to complete the task before the task no longer gives the desired result?
2) How much time will the operator(s) use to complete the task? In deciding the time required for an operator it is important to not only analyse the time required to perform the task itself, but also how contextual factors might affect the time required. The contextual factors could, for example, be distractions (communication, other tasks), time to read procedures, time spent on teamwork/communication, and how the operator is trained to respond to the task (fast or slow).
3) Select the level (see level description) based on the difference between the available time and time needed to complete the task.

PSF levels			
SPAR-H levels	**SPAR-H multipliers**	**Petro-HRA levels**	**Petro-HRA multipliers**

Inadequate time	P (failure)=1.0.	Extremely high negative effect on performance	P (failure)=1.0
Barely adequate time	Multiplier=10	Very high negative effect on performance	Multiplier=50
		Moderate negative effect on performance	Multiplier=10
Nominal time	Multiplier=1	Nominal effect on performance	Multiplier=1
Extra time	Multiplier=0.1	Moderate positive effect on performance	Multiplier=0.1
Expansive time	Multiplier=0.01		

SPAR-H guidance/criteria for PSF levels		**Petro-HRA guidance/criteria for PSF levels**	
P=1	*Inadequate time:* If the operator cannot diagnose the problem in the amount of time available, no matter what s/he does, then failure is certain.	P=1	Extremely high negative effect on performance: Operator(s) does not have enough time to perform the task.
		50	Very high negative effect on performance: The available time is the minimum time to perform the task. In this situation the operator(s) experiences very high time pressure or that they have to speed up very much to do the task in time.
10	*Barely adequate time*—2/3 the average time required to diagnose the problem is available.	10	Moderate negative effect on performance: The operator(s) has limited time to perform the task. However there are more time than the minimum time required. In this situation the operator(s) experiences high time pressure or that they have to speed up much to do the task in time.
1	*Nominal time*—on average, there is sufficient time to diagnose the problem.	1	Nominal effect on performance There is enough time to do the task. The operator(s) only experiences a low degree of time pressure or 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	*Extra time*—time available is between one to two times greater than the nominal time required, and is also greater than 30 minutes.	0.1	Moderate positive effect on performance - there is good time/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.
0.01	*Expansive time*—time available is greater than two times the nominal time required and is also greater than a minimum time of 30 minutes; there is an inordinate amount of time (a day or more) to diagnose the problem.	-	

Arguments/references for changing levels, multipliers or criteria

1) Item 2 in THERP Table 20-1 (Swain & Guttmann, 1983) was not included in SPAR-H. Item 2 is 10 minutes after annunciator and a HEP of .50. It could be argued that the term "Barely adequate time" seems to fit more with 10 minutes and a multiplier of 50 than with 20 minutes and a multiplier of 10 especially in the petroleum industry where the time aspect is shorter than in the nuclear industry. There is no argument in NUREG/CR-6883 or in Boring and Blackman (2007) why the 10 minutes, item 2, and a HEP of .50 was left out.
2) The definitions of the multipliers/levels for Available time for diagnosis in SPAR-H are ambiguous. The term "Barely adequate time" is defined as "2/3 the average time required to diagnose", which implies that the operator(s) do not have enough time to diagnose. This level seems to be very similar to the level "Inadequate time" which is defined as operator cannot diagnose the problem in the amount of time available no matter what s/he does, and then failure is certain. The level "Nominal" in SPAR-H is not well defined. The descriptions of the levels in SPAR-H need to be changed.
3) From comparison of the THERP and the other data based methods presented by Reer and Sträter (1996) the multiplier for the level "Barely adequate time" in SPAR-H seems to be debatable. The multiplier in SPAR-H is 10 (for both Diagnosis and Action). In comparisons with THERP, and Reer and Sträter (1996) this multiplier could be 50.
4) It is suggested to remove the "expansive time" level because in the "Good Practices for Implementing Human Reliability Analysis" (Kolaczkowski, Forester, Lous, & Cooper 2005). it is said that (pp. 5-15): "The total combined probability of all the HEPs in the same accident sequence/cut set should not be less than a justified value. It is suggested that the value should not be below ~0.00001 since it is typically hard to defend that other dependent failure modes that are not usually treated (e.g., random events such as even a heart attack) cannot occur. Depending on the independent HFE values, the combined probability may need to be higher. If the expansive time multiplier and another positive PSF multiplier is chosen one can get a HEP into the ~0.00001 area. It also seems debatable that performance will improve if the operators have "expansive time"."

14.2 Stress/Stressors -> Threat Stress

PSF no	SPAR-H name	Stress/Stressor	Version	Date
2	**Petro-HRA name**	Threat Stress	1	08.05.14

SPAR-H Definition: The SPAR-H Human Reliability Analysis Method (Gertman *et al.*, 2005)

Stress (and levels of arousal) have been broadly defined and used to describe negative as well as positive motivating forces of human performance. Stress as used in SPAR-H refers to the level of undesirable conditions and circumstances that impede the operator from easily completing a task. Stress can include mental stress, excessive workload, or physical stress (such as that imposed by difficult environmental factors). It includes aspects of narrowed attentional field or muscular tension, and can include general apprehension or nervousness associated with the importance of an event. Environmental factors often referred to as stressors, such as excessive heat, noise, poor ventilation, or radiation, can induce stress in a person and affect the operator's mental or physical performance. It is important to note that the effect of stress on performance is curvilinear—some small amount of stress can enhance performance, and should be considered nominal, while high and extreme levels of stress will negatively affect human performance.

Common measures of stress have included galvanic skin response (GSR), heart rate (HR), blood volume pulse (BVP), numerous self-report inventories, and the measurement of chemical markers. For example, lowered levels of s-IgA, an immune response marker present in saliva, have been linked to increased risk of ill health inindividuals. When applying SPAR-H, the analyst will not have the above physical measures available. Assignment of the specific stress level will therefore involve making an interpretation based on operational knowledge and human factors as to the expected level of stress for a particular scenario or context.

SPAR-H Definition: SPAR-H Definition: Step-by-Step Guidance (Whaley et al., 2011)

Stress (and level of arousal) has been broadly defined and used to describe negative as well as positive motivating factors in predicting human performance. However, stress as used in SPAR-H specifically refers to the level of undesirable conditions and circumstances that impede the operator in completing a task. Stress can include mental stress, excessive workload, or physical stress such as that imposed by environmental factors. Consequently, stress could manifest on both Diagnosis and Action performance. Environmental factors, often referred to as stressors, such as excessive heat, noise, poor ventilation, or radiation, can induce stress in a person and affect mental or physical performance. It is important to note that the effect of stress on performance is curvilinear—that is, some small amount of stress can enhance performance, and in the context of SPAR-H should be considered nominal, while high and extreme levels of stress will negatively affect human performance. It is the degradation of performance that is the key point when assigning high or extreme stress levels. Typically, this will occur when the context of a situation deviates from what is anticipated (leading to confusion, uncertainty, fear or overloading the capabilities of the human operator). Situations that are expected, even though they might result in some anxiety in the human operators, should be judged nominal. Remember, some enhanced level of stress can be good in that it can help the operators stay focused. The analyst is cautioned against being too analytical in assigning a stress level. Even if we could predict the specific individual subjected to the context of interest (which we can't), everyone handles stress a little differently. Therefore, the focus here (for High or Extreme Stress) is on those situations outside of what the operator(s) have experienced or trained for.

It is important to note that stress is not independent of other PSFs. Often stress results from limited time, high complexity, poor procedures, poor training, poor work processes, or poor crew dynamics. However, the analyst should make an effort to avoid any "double counting" of specific influencing factors. If time constraints are being accounted for in the Available

Time PSF, then the effect of time on the Stress/Stressors PSF should be minimized (note that other details of the context, not explicitly accounted for in other PSFs might still need to be accounted for in the Stress/Stressors PSF). While high or extreme stress does increase the probability of an error, it does not guarantee failure; people can and have succeeded during high-stress scenarios.

The key to assigning a level to this PSF is the distinction between high and extreme stress. Extreme stress is qualitatively different from high stress, and is likely to occur if a problem is prolonged, such as multiple equipment failures, if the crew has had prolonged difficulties controlling facility parameters, or in situations where there is a severe threat to personnel or facility safety.

Petro-HRA short explanation of changes (need for change)

Salas et al. (1996) have summed up the different definitions and meanings of the concept of stress and have developed a four stage model of stress and performance. The model sums up the literature on stress and seems consistent with the most influential stress theories.

The four steps are:

a) An environmental stimulus becomes salient;

b) It requires a positive and negative valence through the appraisal process;

c) This leads to the formation of performance expectations;

d) These in turn determine a number of physiological, cognitive, emotional, and social consequences.

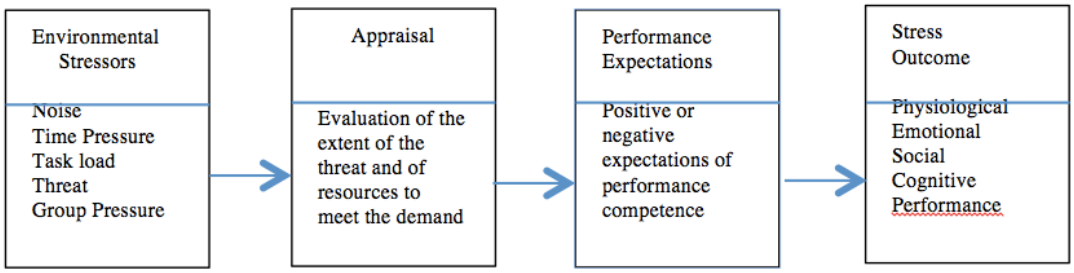

Figure 33: Salas et al.'s (1996) Four stage model of stress and performance

From this model (Figure 19.3) it is difficult to separate the Stress/Stressor PSFs as it is defined in SPAR-H, from the other PSFs included in SPAR-H. Every other PSF (e.g., Available Time, Complexity, Ergonomics /HMI) is an environmental stressor. Most of what is included in the Stress/Stressor PSFs in SPAR-H is covered by other PSFs. Time pressure could be included into the Available Time PSF, noise and temperature seems to better fit into Ergonomics/HMI PSF. However there is one part of the Stress/Stressor PSF in SPAR-H that is not covered by another PSF and that is Threat Stress. Salas et al. (1996, p. 23) define threat as the "anticipation of fear of physical or psychological harm". Thus, a threat-provoking situation is one in which dangerous and novel environmental events pose the potential for pain or discomfort.

Since it is the external PSFs that cause arousal it is not necessary to include arousal in the definition of the PSFs. It is enough to count the effect of a PSF once.

The problem with having overlapping definitions of the PSF is that the same factor might be counted more than once, and then become double counted. With overlapping definitions of the PSFs it is difficult for an analyst to decide which PSF to choose. Since the PSFs have different levels with different multipliers, this will reduce inter-rater reliability.

References (for change):

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.

Swain, A. & Guttmann, H. (1983). Handbook of human-reliability analysis with emphasis on nuclear power facility applications, Final report (NUREG/CR-1278). Washington, DC: U.S. NRC.

Petro-HRA (full) description

Threat Stress is defined as the anticipation or fear of physical or psychological harm (Salas et al., 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). An example of a situation that might cause Threat Stress is a situation where the operator(s) life is in danger or other people's lives are in danger. Another example of Threat Stress might be a threat to self-esteem or professional status if performing a wrong decision or action. The analyst should evaluate:

1) Does Threat Stress affect performance of this task?
2) What is the level of Threat Stress?

PSF levels

SPAR-H levels	SPAR-H multipliers	Petro-HRA levels	Petro-HRA multipliers
Extreme	5	High negative effect on performance	25
High	2	Low negative effect on performance	5
		Very low negative effect on performance	2
Nominal	1	Nominal effect on performance	1

SPAR-H guidance/criteria for PSF levels		Petro-HRA guidance/criteria for PSF levels	
5	Extreme—a level of disruptive stress in which the performance of most people will deteriorate drastically. This is likely to occur when the onset of the stressor is sudden and the stressing situation persists for long periods. This level is also associated with the feeling of threat to one's physical well-being or to one's self-esteem or professional status, and is considered to be qualitatively different from lesser degrees of high stress (e.g., catastrophic failures can result in extreme stress for operating personnel because of the potential for radioactive release).	25	High negative effect on performance: The operator experiences very high threat stress. In this situation the operator's own life or other person's life is in immediate danger.
2	High—a level of stress higher than the nominal	5	Low negative effect on performance: The operator(s) experiences moderate threat stress.

	level (e.g., multiple instruments and annunciators alarm unexpectedly and at the same time; loud, continuous noise impacts ability to focus attention on the task; the consequences of the task represent a threat to facility safety).		The operator experiences that there is a threat to their own life, others' lives, or a very high threat to their self-esteem or professional status.
		2	Very low negative effect on performance: The operator(s) experiences some threat to their self-esteem or professional status.
1	Nominal—the level of stress that is conducive to good performance.	1	Nominal effect on performance: Operator(s) does not experience threat stress. Threat stress has not a negative effect on performance.
Arguments/references for changing levels, multipliers or criteria			
For the multipliers for this PSF we have chosen to follow THERP (Swain & Guttmann, 1983). SPAR-H multipliers deviate from THERP. The multipliers found in THERP better represent the studies that have been performed. The level for high threat stress in THERP Table 20-16: For diagnosis and extremely high stress/ skilled person, HEP=.25, Extreme high stress/novice HEP=.50. For step by step, extreme high stress/skilled, multiplier=5 and high stress/novice, multiplier=10. For moderate stress in THERP Table 20-16 for diagnosis, skilled has a multiplier=5, novice has a multiplier of 10. For step by step, skilled has a multiplier=2, novice has a multiplier=4. We also chose to include the multiplier 2 from SPAR-H for a very low negative effect on performance. It was found in the user test that the analysts chose to be conservative and chose a low negative effect on performance for a very small influence of Threat stress (multiplier 5). To avoid that the analyst selected a multiplier of 5 for this situation we included SPAR-H multiplier 2 for this level. To include this level also gave more flexibility to the analysts.			

14.3 Complexity -> Task Complexity

PSF no	SPAR-H name	Complexity	Version	Date
3	**Petro-HRA name**	Task Complexity	1	08.05.14

SPAR-H Definition: The SPAR-H Human Reliability Analysis Method (Gertman *et al.*, 2005)

Complexity refers to how difficult the task is to perform in the given context. Complexity considers both the task and the environment in which it is to be performed. The more difficult the task is to perform, the greater the chance for human error. Similarly, the more ambiguous the task is, the greater the chance for human error. Complexity also considers the mental effort required, such as performing mental calculations, memory requirements, understanding the underlying model of how the system works, and relying on knowledge instead of training or practice. Complexity can also refer to physicalefforts required, such as physical actions that are difficult because of complicated patterns ofmovements. Figure 19.4 illustrates typical contributing factors to complexity. Identification of these complexity factors may be found in Braarud (1998), EPRI TR-100259 (1992), Gertman and Blackman (1994), and NUREG-1624 (2000). The SPAR-H analyst may wish to refer to these factors when evaluating the complexity PSF. It is recognized that a single complexity factor can result in different levels of influence on HSI. For example, mental calculations required of operators may be slight or, given aspects of the event, may prove to be overwhelming. The same is true for combinations of factors. Because of this, assignment of the specific complexity levelassociated with a HEP is left to the analyst to determine. At the current time, there is no algorithm for inferring levels of influence based on which combination of factors is selected.

For analysts who wish to differentiate between rule- and knowledge-based diagnosis, in most cases the former would present less complexity and would often be associated with a positive rating on the procedures PSF. Knowledge-based diagnosis and decision-making will often present the operator with greater complexity and often be associated with more negative ratings on procedures, including incomplete or misleading procedures or lack of procedural guidance. In general, a task with greater complexity requires greater skill and comprehension to successfully complete. Multiple variables are usually involved in complex tasks. Concurrent diagnosis of multiple events and execution of multiple actions at the same time is more complex than diagnosing and responding to single events.

Figure 34: Contributing factors to complexity

SPAR-H Definition: Step-by-Step Guidance (Whaley et al., 2011)

Complexity refers to how difficult the task is to perform in the given context; it considers both the task and the environment. The more difficult the task is to perform, the greater the chance for human error. Similarly, the more ambiguous the task is, the greater the chance for human error. Complexity also considers the mental effort required, such as performing mental calculations, memory requirements, understanding the underlying model of how the system works, and relying on knowledge instead of training, practice or procedures. Complexity can also refer to physical efforts required, such as physical actions that are difficult because of complicated patterns of movements. In general, a task with greater complexity requires greater skill and comprehension to successfully complete. Multiple variables are usually involved in complex tasks. Concurrent Diagnosis of multiple events and execution of multiple actions at the same time is more complex than diagnosing and responding to single events.

A crew or operator's understanding of the situation can influence complexity. If the crew does not have an adequate understanding of the nature of the problem, solving it becomes more complex, as the facility parameters often do not respond as expected. Key to assigning a level for this PSF is determining how challenging the situation is to the operator/crew. Obviously, complexity is a relative issue. As with all other PSFs, there is the potential to double count the effects of complexity. To a well-trained and experienced operator/crew, a particular situation might be simple, whereas for those poorly trained or inexperienced it might be very complex. As a general rule, the analyst should avoid double counting the effects of a PSF. If the Experience/Training PSF is assessed negatively, the analyst should avoid including the effects of experience/training in the Complexity PSF.

Petro-HRA short explanation of changes (need for change)

We chose to use the name Task Complexity rather than Complexity because we are focusing on the complexity of the task and not characteristics covered by other PSFs such as Experience/Training. Complexity is rather poorly defined in SPAR-H. The figure that is used to define complexity shows that complexity in SPAR-H overlaps to a large extent with several of the other PSFs such as:

- System interdependencies not well defined and misleading or absent indicators seem to belong to the Ergonomics/HMI PSF
- Transition between multiple procedures seems to belong in the Procedure PSF
- Large amount of communication required and task requires coordination with ex-control room activities; both seem to belong in the Work Processes PSF.

We suggest that Task Complexity should be limited to six factors—goal, size, step, dynamic, connection, and structure complexity. There seems to be a problem in that some analysts chose Complexity and some analysts chose HMI for the same situation. Since there is a large difference in multipliers for these PSFs it reduces inter-rater reliability.

References (for change)

Braarud, P. Ø. (1998). *Complexity factors and prediction of crew performance (HWR-521)*. Halden, Norway: OECD Halden Reactor Project.

Ham, D-H., Park, J., & Jung, W. (2011). A framework-based approach to identifying and organizing the complexity factors of human-system interaction. *IEEE Systems Journal*, *5*, 213-222. Doi: 10.1109/JSYST.2010.2102574.

Liu, P., & Li, Z. (2012). Task complexity: A review and conceptualization framework. *International Journal of Industrial Ergonomics*, *42*, 553-568. Doi: 0.1016/j.ergon.2012.09.001.

Lois, E., Dang, V. N., Forester, J., Broberg, H., Massaiu, S., … Bye, A. (2009). *International HRA empirical study – pilot phase report. Description of overall approach and first pilot results from comparing HRA methods to simulator data (HWR-844).* Halden, Norway: OECD Halden Reactor Project.

Kim, J. W., & Jung, W. (2003). A taxonomy of performance influencing factors for human reliability analysis of emergency tasks. *Journal of Loss Prevention in the Process Industries*, *16*, 479-495. Doi: 10.1016/S0950-4230(03)00075-5.

Park, J., & Jung, W. (2008). A study on the validity of a task complexity measure for emergency operating procedures of nuclear power facilitys – Comparing task complexity scores with two sets of operator response time data obtained under a simulated SGTR. *Reliability Engineering & System Safety*, *9*3, 557-566. Doi: 10.1016/j.ress.2007.02.002.

Rasmussen, M., Standal, M. I., & Laumann, K. (In review). Task complexity as a performance shaping factor: A review and recommendations in SPAR-H adaption. *Safety Science.*

Xing, J., & Manning, C. (2005). *Complexity and automation displays of air traffic control: Literature review and analysis.* Federal Aviation Administration. Oklahoma, OK: Civil Aeromedical Institute.

Petro-HRA (full) description

Task Complexity refers to how difficult the task is to perform in the given context. More complex tasks 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. Task Complexity factors include goal complexity, size complexity, step complexity, connection complexity, dynamic complexity, and structure complexity.

Goal complexity refers to the multitude of goals and/or alternative paths to one or more goals. The complexity of a task will increase with more goals/paths, and 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 refers to the size of the task and the number of information cues. This also includes task scope, which is the sub-tasks and spread of faults to other tasks. The complexity of a task will increase as the amount and intensity of information an operator has to process increases.

Step complexity refers to 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 increase, even more so if the steps are continuous or sequential.

Connection complexity refers to 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 refers to 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 refers to 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.

In determining the appropriate PSF level the analyst should evaluate:

1) Identify which of the Task Complexity factors are present in the task and affect performance.
2) 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.
3) Set the Task Complexity PSF multiplier level based on the severity and presence of the various Task Complexity factors present in the task.

PSF levels			
SPAR-H levels	**SPAR-H multipliers**	**Petro-HRA levels**	**Petro-HRA multipliers**
Highly complex	5	Very high negative effect on performance	50
Moderately complex	2	Moderate negative effect on performance	10
		Very low negative effect on performance	2
Nominal	1	Nominal effect on performance	1
Obvious diagnosis	0.1	Low positive effect on performance	0.1

SPAR-H guidance/criteria for PSF levels		**Petro-HRA guidance/criteria for PSF levels**	
5	*Highly complex*—very difficult to perform. There is much ambiguity in what needs to be diagnosed or executed. Many variables are involved, with concurrent diagnoses or actions (i.e., unfamiliar maintenance task requiring high skill).	50	Very high negative effect on performance: The task is highly complex. One or several of the complexity categories are highly present and influence performance very negatively.
2	Moderately complex—somewhat difficult to perform. There is some ambiguity in what needs to be diagnosed or executed. Several variables are involved, perhaps with some concurrent diagnoses or actions (i.e., evolution performed periodically with many steps).	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 is expected to have a low negative effect on performance.
1	Nominal—not difficult to perform. There is little ambiguity. Single or few variables are involved.	1	Nominal effect on performance: The task is not very complex and task. Task complexity has neither a negative nor a positive effect on performance
0.1	Obvious diagnosis—diagnosis becomes greatly simplified. There are times when a problem becomes so obvious that it would be difficult for	0.1	Moderate 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

	an operator to misdiagnose it. The most common and usual reason for this is that validating and/or convergent information becomes available to the operator. Such information can include automatic actuation indicators or additional sensory information, such as smells, sounds, or vibrations. When such a compelling cue is received, the complexity of the diagnosis for the operator is reduced. For example, a radiation alarm in the secondary system, pressurized heaters, or a failure of coolant flow to the affected steam generator are compelling cues. They indicate a steam generator tube rupture (SGTR). Diagnosis is not complex at this point; it is obvious to trained operators.		sensory information such as clear visual and auditory cues.

Arguments/references for changing levels, multipliers or criteria

The origin for the multipliers for complexity in SPAR-H does not seem to be well founded. The origin is Table 20-23 in THERP which shows errors according to the number of alarms, which is only one aspect of the Complexity PSF. The Task Complexity multiplier 50 in Petro-HRA is based on an assumption from ATHEANA where Complexity is considered as one of the strongest PSFs in deviation scenarios and therefore is compared to the other highest PSF levels. HEART has a Generic task (Task C) which contains complexity: “Complex task requires high level of comprehension and skill” with a proposed nominal human unreliability of 0.16. The strongest EPC in HEART that contains a Task Complexity element is EPC 3: A low signal-noise ratio with a multiplier of x10. SPAR-H has x5 as the highest multiplier for complexity. Based on these multipliers a multiplier of 10 was chosen for the level “Moderate negative effect on performance”. After a user analysis of the Petro-HRA method we discovered that the analyst chose the level moderate negative effect on performance if the complexity factors were slightly present. We chose therefore to include the level: Very low negative effect on performance with the lowest multiplier in SPAR-H which is 2. To include this level gives the analyst more flexibility.

14.4 Experience/Training -> Experience/Training

PSF no	SPAR-H name	Experience/Training	Version	Date
4	**Petro-HRA name**	Experience/Training	1	08.05.14

SPAR-H Definition: The SPAR-H Human Reliability Analysis Method (Gertman *et al.*, 2005)

This PSF refers to the experience and training of the operator(s) involved in the task. Included in this consideration are years of experience of the individual or crew, and whether or not the operator/crew has been trained on the type of accident, the amount of time passed since training, and the systems involved in the task and scenario. Another consideration is whether or not the scenario is novel or unique (i.e., whether or not the crew or individual has been involved in a similar scenario, in either a training or an operational setting). Specific examples where training might be deficient are guidance for bypassing engineered safety functions, guidance for monitoring reactor conditions during reactivity changes, and guidance for monitoring facility operation during apparently normal, stable conditions for the purpose of promoting the early detection of abnormalities.

SPAR-H Definition: Step-by-Step Guidance (Whaley et al., 2011)

This PSF refers to the experience and training of the operator(s) involved in the task. Included in this consideration are years of experience of the individual or crew, and whether or not the operator/crew has been trained on the type of accident, the amount of time passed since training, the frequency of training, and the systems involved in the task and scenario. Another consideration is whether or not the scenario is novel or unique (i.e., whether or not the crew or individual has been involved in a similar scenario, in either a training or an operational setting). Specific examples where training might bedeficient are guidance for bypassing engineered safety functions, guidance for monitoring reactor conditions during reactivity changes, and guidance for monitoring facility operation during apparently normal, stable conditions for the purpose of promoting the early detection of abnormalities.

If Training/Experience has been judged to be a performance driver, then this PSF might also include the quality of the training provided. If the simulator training does not match facility response, training might be judged as low. If the training does not cover the given situation, training might be judged as low, as would be the case if training were incomplete or incorrect. If the training for a particular situation is infrequently conducted, to the extent that important skills and concepts are not regularly rehearsed and refreshed, training might be considered low. Note that the threshold of 6 months of experience and/or training for the Low level should not be viewed as a firm rule; an activity that is well trained over fivemonths may find the operator more qualified than one which is infrequently trained over multiple years.

Petro-HRA short explanation of changes (need for change)

There is little consistency between the description of the PSF and the description of the levels in SPAR-H. The low level is only described as time in position. Quinones *et al.* (1995) had done a meta-analysis of experience and job performance. They found that a task or amount based definition of job experience predicted job performance best. Time in job does not predict performance as much.

The description of training is very nuclear oriented.

From the literature, training is described as one of the most important factors organizations can control to increase task performance. The multipliers for Experience/Training seem to be very low compared to the other PSFs.

The SPAR-H definition says nothing about knowledge and skills that are outcomes of Experience/Training.

References (for change)

Quinones, M. A., Ford, J. K., & Teachout, M. S. (1995). The relationship between work experience and job performance: A conceptual and meta-analytic review. *Personnel Psychology, 48*(4), 887-910.

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.

Williams, J. C. (1988, June). A data-based method for assessing and reducing human error to improve operational performance. In Human Factors and Power Facilitys, 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. Nuclear Electric plc. UK.

Petro-HRA (full) description

Experience is defined as how many times in the past the operator(s) has experienced the tasks 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 or scenario in question ((definition based on Salas et al., 2012). The outcome of experience and training is knowledge and skills that are necessary to be prepared for and to perform the tasks in the scenario being analysed. Research (Arthur *et al.*, 2009) has shown that 90 percent of training outcome is lost after one year if the knowledge and skill is not used. Type of training might vary, and some examples are simulator training, on the job training, classroom training, and mental training (mentally rehearsing the task steps). Experience and training is compensatory and the analyst should evaluate if the operator(s) have the necessary knowledge and skills to do the tasks in this scenario from either experience or training. The analyst should not only check that the operators have the necessary education and certificate, he/she should specifically look at the experience and training for the task(s) in the scenario being analysed.

In determining the appropriate PSF level the analyst should evaluate:

1) Does Experience/Training have an influence on the performance of this task? Are there some characteristics with this task(s) that makes Experience/Training on this task/scenario superfluous? If so the level nominal should be used. However, it is a general expectation that there should be training for highly safety critical tasks and scenarios.
2) If Experience/Training has an influence on performance on this task, the analyst has to decide which level of relevant Experience/Training the operator(s) has for the task in this scenario.

To evaluate which level for experience/training PSF for a particular task(s) or scenario the HRA analyst could a) investigate what experience and training the operators have and if the experience/training have provided operators with the knowledge and skills to do the tasks or scenario, and/or b) investigate the operators' actual knowledge and skills to handle the scenarios. Since it might be difficult to get a complete overview of the operators' experience and training or the operators' knowledge and skills, the analyst will have more information on which to base the selection of a level for experience/training if both aspects are investigated.

To assess if the operators have the necessary knowledge and skills the analyst first needs to define: what knowledge and skills are necessary for the task(s) or scenario(s) under analysis. The task analysis could also be extended to include an analysis of the necessary knowledge and skills to do each task step.

It might be challenging for an HRA analyst to access information about which knowledge and skills are needed for a scenario. The analyst should be careful not to base this analysis on interviews only with operators, since it is not certain whether they know all the necessary knowledge and skills required to perform a task. Information about the necessary

skills could in addition be obtained from available documentation, procedures, training programmes and interviews with trainers.

After defining the necessary knowledge and skills the analyst needs to decide if the operators' have them. Kraiger et al. (1993) have described methods for how to evaluate learning outcomes, and their suggestions for evaluation methods could be relevant for evaluating if operators have the necessary experience and training or knowledge and skills for an HRA task or scenario., Kraiger et al. (1993) suggest paper-and-pencil tests (multiple-choice, true-false or free recall tests) to test declarative knowledge. To develop a paper-and-pencil test during an HRA might be too resource demanding. However, an advantage with this method is that it is possible to get information from many operators. A technique described by Kraiger et al. (1993) to test metacognitive skills or a person's understanding of a task is probed protocol analysis. With this analysis, the necessary steps in a task are first described (task analysis). The operators are next asked to describe how they would do each step. The subjects are also asked probing questions such as why they took a particular step or what would happen if they did it wrong. Another technique described by Kraiger et al. (1993) is self-report about knowledge, lack of knowledge and training needed.

To test skill-based learning outcomes (technical or motor skills), Kraiger et al. (1993) describe target behavioural observation. In HRA behavioural observation has to be done in a simulator, which is costly, time-consuming often not feasible to do. As an alternative technique, Kraiger et al. (1993) suggest a structured situational interview where operators would be asked to describe how they would perform a task. This method is also called a talk-through (Stanton et al. 2013). A similar method is to ask the operators to simulate how they would undertake a task either in the control room or in a workshop. This method is also called a walk-though (Stanton et al. 2013). Kraiger et al. (1993) describe that the structured situational interview has been found to correlate highly with performance.

There are some indications that Experience/Training levels have a very high negative effect on performance:

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

When the analyst(s) investigates if the operators have the necessary knowledge and skill from experience and training the analyst should also consider:

- Fidelity – how similar are the Experience/Training environment to the actual scenario and task?
- 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 the necessary knowledge and skills.
- How recent/updated is the Experience/Training?

PSF levels			
SPAR-H levels	**SPAR-H multipliers**	**Petro-HRA levels**	**Petro-HRA multipliers**
		Extremely high negative effect on performance	P=1
		Very high negative effect on performance	50

Low	10	Moderate negative effect on performance	15
		Low negative effect on performance	5
Nominal	1	Nominal	1
High	0.5	Moderate positive effect on performance	0.1

SPAR-H guidance/criteria for PSF levels		**Petro-HRA guidance/criteria for PSF levels**	
		P=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 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 at all have any experience or training and does not have the necessary knowledge and skills to be prepared for and to do the task(s) in this scenario.
10	Low—less than 6 months experience and/or training. This level of experience/training does not provide the level of knowledge and deep understanding required to adequately perform the required tasks; does not provide adequate practice in those tasks; or does not expose individuals to various abnormal conditions.	15	Moderate negative effect on performance: The operator(s) has low experience or training and does not have the complete necessary knowledge and experience to be prepared for and to do the task(s) in this scenario.
		5	Low negative effect on performance: The operator has experience or training, but there are some lacks in their experience/training and they do not have the complete knowledge and experience to be fully prepared for and to do the task(s) in this scenario.
1	Nominal—more than 6 months experience and/or training. This level of experience/training provides an adequate amount of formal schooling and	1	Nominal effect on performance: The operator(s) has experience and/or training on the task(s) in this scenario and has the necessary knowledge and experience to be prepared for and to do the task(s)

	instruction to ensure that individuals are proficient in day-to-day operations and have been exposed to abnormal conditions.		in this scenario. Experience/Training does not reduce performance nor to a large degree improve performance.
0.5	High—extensive experience; a demonstrated master. This level of experience/training provides operators with extensive knowledge and practice in a wide range of potential scenarios. Good training makes operators well prepared for possible situations.	0.1	Moderate positive effect on performance: The operator(s) has extensive experience and/or training on this task and the operator(s) have extensive knowledge and experience to be prepared for and to do the task(s) in this scenario.

Arguments/references for changing levels, multipliers or criteria

See explanation for change in this PSF above. We argue that if the operator is given improper training where a strong learned improper response tendency is the cause, one should expect P=1. We have also included the level no training which we think could be the case for some tasks or scenarios. If the operator has no training we think there is a 50/50 chance that they will do the task correctly. The new multipliers for Experience/Training are set in comparison to the multipliers for Procedures. The generic task in HEART (Williams, 1988, 1992) that is most similar to the content for Experience/Training is generic task A) "Totally unfamiliar, performed at speed with no real idea of likely consequences with a proposed Nominal Human Unreliability of 0.55." This value is close to the multiplier 50 which is chosen for the No Experience/Training level. The Error producing condition in HEART that has the highest multiplier is Error producing condition 1. Unfamiliar with a situation which is potentially important but which only occurs infrequently or which is novel, has a multiplier of x17. SPAR-H (Gertman et al. 2005) has only one negative multiplier which is 10 for diagnosis and 3 for action. We have split the one SPAR-H level and multiplier into two levels and multipliers with multipliers of 15 and 5 to differentiate between low training and some lacks in training. SPAR-H seems not to emphasize the PSF Experience/Training as much although this factor is emphasized in the literature as a way to improve reliability and operators' performance. Also, since we do not think that SPAR-H emphasizes enough the importance of Experience/Training we also think that this PSF could better improve performance and therefore have changed the positive level from 0.5 to 0.1.

14.5 Procedures -> Procedures

PSF no	SPAR-H name	Procedures:	Version	Date
5	**Petro-HRA name**	Procedures	1	08.05.14

SPAR-H Definition: The SPAR-H Human Reliability Analysis Method (Gertman *et al.*, 2005)

This PSF refers to the existence and use of formal operating procedures for the tasks under consideration. Common problems seen in event investigations for procedures include situations where procedures give wrong or inadequate information regarding a particular control sequence. Another common problem is the ambiguity of steps. PSF levels differ somewhat, depending on whether the activity is a diagnosis activity or an action. In situations where multiple transitions between procedures are required to support a task or group of tasks, SPAR-H suggests that the analyst adjust the PSF for complexity accordingly. If the procedures themselves are problematic, i.e., inadequate, then the HRA analyst should assess the procedures and determine whether they should be assigned an “inadequate” or “poor” rating.

SPAR-H Definition: Step-by-Step Guidance (Whaley et al., 2011)

This PSF refers to the existence and use of formal operating procedures for the tasks under consideration. Use of procedures and the assignment of a PSF level for Procedures can apply to either Diagnosis or Action (or both). Past problems seen in event investigations involving procedures include situations where procedures give wrong or inadequate information regarding a particular control sequence. Another problem that has been cited is ambiguity in procedure steps. PSF levels differ somewhat, depending on whether the activity is a Diagnosis activity or an Action. In situations where multiple transitions between procedures are required to support a task or group of tasks, SPAR-H suggests that the analyst adjust the PSF for complexity accordingly. If the procedures themselves are problematic, then the analyst should assess the procedures and determine whether they should be assigned an “Incomplete” or “Available but poor” rating. However, as with all PSFs in SPAR-H, a prerequisite to evaluating this PSF quantitatively is the qualitative determination of whether or not Procedures are in fact a performance driver for the subject HFE.

This PSF assesses the quality of procedures and other reference documents or information available to operators. If there is no procedure to cover the situation, then procedures are not available. The distinction between the levels “Incomplete” and “Available but poor” can be difficult to make, but generally, if a procedure is missing important information, it is “Incomplete”. If the procedure contains incorrect or inaccurate information, if it allows for or directs improper actions, or if it is difficult to use or understand, then it is “Available but poor”.

Contemporary control room operating procedures are written to be diagnostic or symptom oriented. There may be the temptation to credit this level automatically for the Procedures PSF. This has the effect of lowering the HEP by a factor of 10. The assignment of “Diagnostic/symptom oriented” for the Procedures PSF should only be undertaken when there is clear evidence that the procedures will quickly help the operators diagnose a situation that would otherwise be difficult or would take considerable additional effort to diagnose without particular procedural guidance. This is the exception, not the rule.

Petro-HRA short explanation of changes (need for change)

The SPAR-H definition does not give a definition of what a procedure is.

The SPAR-H Procedures PSF only contains whether procedures exist, not the use of procedures. Use of procedures is in the Work Processes PSF. These two factors are highly dependent: if a procedure does not exist it cannot be used; if a procedure has low quality it is also more likely not to be used. When the PSF is defined as it is in SPAR-H, some analysts

might choose the Procedures PSF, some might chose Work Processes PSF, and some will choose both. It seems more logical to include Procedures and use of Procedures within the same PSF and not split those two highly dependent aspects of Procedures into two different PSFs.

References (for change)

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.

Petro-HRA (full) description

"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" (O'Hara et al., 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 can be 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. It might be in this situation that the operators know the procedures so well that Procedures are not a performance driver. The analyst should evaluate if Procedures are a performance driver or not.

In determining the appropriate PSF level the analyst should evaluate:

1. Is there a formal written procedure available?
2. Will the operator follow the procedures for this task(s) or scenario?
3. What is the quality of the procedure(s)?
   a) Does the procedure(s) correctly and logically describe every task and task steps?
   b) Is the format of the procedure good (text, tables, matrices, etc.)?
   c) Is the language easy to understand for the operator?
   d) Does the operator(s) know where to find the procedure?
   e) Does the operator have to switch between several procedures to do the correct task?
   f) Does the procedure only include relevant information (and exclude irrelevant information)?

PSF levels

SPAR-H levels	SPAR-H multipliers	Petro-HRA levels	Petro-HRA multipliers
Not available	50	Very high negative effect on performance	50
Incomplete	20	High negative effect on performance	20
Available but poor	5	Low negative effect on performance	5
Nominal	1	Nominal effect on performance	1
Diagnostic/symptom oriented	0.5	Low positive effect on performance	0.5

SPAR-H guidance/criteria for PSF levels		Petro-HRA guidance/criteria for PSF levels	
50	Not available - the procedure needed for a	50	Very high negative effect on

	particular task or tasks in the event is not available.		performance: No procedures available or the procedures are not used. 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	Incomplete - information is needed that is not contained in the procedure or procedure sections; sections or task instructions (or other needed information) are absent.	20	High negative effect on performance: Very poor procedure. The procedure lacks steps and important information that is needed to do the task or the procedures are briefly used. 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	Available, but poor - a procedure is available but it is difficult to use because of factors such as formatting problems, ambiguity, or such a lack in consistency that it impedes performance.	5	Low negative effect on performance: Poor procedures. The procedures are complete but there are some human factors 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 or if here are some problems to navigate between different procedures.
1	Nominal - procedures are available and enhance performance.	1	Nominal effect on performance: The quality of the procedures is adequate and they are followed. Procedures do not reduce nor to a large degree increase performance.
0.5	Diagnostic/symptom oriented – diagnostic procedures assist the operator/crew in correctlydiagnosing the event. Symptom-oriented procedures (sometimes called function-orientedprocedures) provide the means to maintain critical safety functions. These procedures allow operators to maintain the facility in a safe condition, without the need to diagnose exactly what the event is, and what needs to be done to mitigate the event. There will be no catastrophic result (i.e., fuel damage) if critical safety functions are maintained. Therefore, if either diagnostic procedures (which assist indetermining probable cause) or symptom-oriented	0.5	Low positive effect on performance: Good procedure(s). Procedures are exceptionally good, they are followed, and they increase performance.

	procedures (which maintain critical safety functions) are used, there is less probability that human error will lead to a negative consequence. This being said, if the symptom-based procedure is found to be inaccurate or awkwardly constructed, then the procedures PSF should be negatively rated.		

Arguments/references for changing levels, multipliers or criteria

It is difficult to separate between “incomplete” and “available but poor” levels in SPAR-H.

In Petro-HRA Procedures not used are included in the description of the level.

The multipliers for Procedures in Petro-HRA are the same as in SPAR-H for all levels. Human Unreliability for a Generic task in HEART with a similar content as Procedures are Generic task B: Shift or restore a system to a new or original state on a single attempt without supervision or procedures=0.26. The highest Error producing condition in HEART with a similar content as for Procedures is no. 11: Ambiguity in the required performance standard with a HEP of x5.

14.6 Ergonomics/HMI -> Human-Machine Interface

PSF no	SPAR-H name	Ergonomics/HMI	Version	Date
6	**Petro-HRA name**	Human-Machine Interface	1	08.05.14

SPAR-H Definition: The SPAR-H Human Reliability Analysis Method (Gertman *et al.*, 2005)

Ergonomics refers to the equipment, displays and controls, layout, quality and quantity of information available from instrumentation, and the interaction of the operator/crew with the equipment to carry out tasks. Aspects of HMI are included in this category. The adequacy or inadequacy of computer software is also included in this PSF. Examples of poor ergonomics may be found in panel design layout, annunciator designs, and labelling.

When considering panel design layout, event investigations at U.S. commercial nuclear facilities have shown that when necessary facility indications are not located in one designated place, it is difficult for an operator to monitor all necessary indications to properly control the facility. If there is evidence that this is the case, a negative PSF value is assigned.

Examples of poor annunciator designs have been found where only a single acknowledge circuit for all alarms is available, which increases the probability that an alarm may not be recognized before it is cleared. Another problem exists where annunciators have set points for alarms that are too near the affected parameter for an operator or crew to react and perform a mitigating action.

Examples of poor labelling include instances where labels are temporary, informal, or illegible. In addition, multiple names may be given to the same piece of equipment. Ergonomics of the facility are also called the HMI or the human engineering aspects. Job performance aids can also be considered a special case of ergonomics. However, in SPAR-H, if the job performance deficiency is related to a procedure, then the preferred means of evaluating the situation is to apply this information to the Procedures PSF, as opposed to the Ergonomics PSF. For example, if the procedure does not match the equipment to be used, then the equipment procedure deficiency should be noted in the procedures, not the Ergonomics, PSF.

SPAR-H Definition: Step-by-Step Guidance (Whaley et al., 2011)

Ergonomics refers to the equipment, displays and controls, layout, quality, and quantity of information available from instrumentation, and the interaction of the operator/crew with the equipment to carry out tasks. Aspects of the human-machine interface (HMI) are included in this category. The adequacy or inadequacy of computer software is also included in this PSF. Examples of poor ergonomics might be found in the panel design layout, annunciator designs, and labelling. Facility instrumentation generally corresponds to the Diagnosis aspect of crew performance, while facility controls correspond to the Action aspect.

When considering the panel design layout, event investigations at U.S. commercial nuclear facilities have shown that when necessary facility indications are not consolidated in one location, it is difficult for an operator to monitor all such indications to properly control the facility. If there is evidence that this is the case, a negative PSF value should be assigned. Examples of poor labelling include instances where labels are temporary, informal, or illegible. Multiple names used for the same piece of equipment can cause confusion and create ambiguity in communication. Job performance aids can also be considered a special case of ergonomics. However, in SPAR-H, if the job performance deficiency is related to a procedure, then the preferred means of evaluating the situation is to apply this information to the Procedures PSF, as opposed to the Ergonomics PSF. For example, if the procedure does not match the equipment to be used, then the equipment-procedure deficiency should be noted in the Procedures, not the Ergonomics, PSF. During low power and

shutdown (LPSD) facility operations, certain information is assumed for the nominal ergonomics case. For Boiling Water Reactors this includes availability of reactor coolant system (RCS) level instrumentation and RHR system instrumentation. For Pressurized Water Reactors, this includes the availability of RHR system instrumentation, the availability of RCS temperature instrumentation, and the availability of RCS level instrumentation.

Included in Ergonomics and HMI is the quality and quantity of information available from displays and gauges, control sensitivity and panel layout, usability of tools and quality of materials, and control accessibility, among others. If instrumentation is inaccurate, incomplete, missing, or unavailable, then HMI is "Missing/Misleading". Issues such as poor panel displays or layouts, inadequate control sensitivity or accessibility are best assessed as "Poor". Note that although a typical control room console may not meet usability criteria for being intuitive or easy to use, the extensive training and experience of the crew allows them to interact with the system in an effective manner. They are able to get the information they need to monitor and diagnose facility states, and they are able to control all necessary parameters. Any deficiency in this basic functionality should be considered "Poor" or "Missing/Misleading".

Petro-HRA short explanation of changes (need for change)

We would recommend that this PSF should only focus on the interaction between the operator and the computerized system and leave out other ergonomic factors related to the physical working environment such as noise and temperature. This recommendation is based on: (1) the relatively weak impact these factors have shown in meta-studies, (2) to ensure that new challenges due to working in a computerized control room are covered, and (3) to reduce analyst difficulties in attributing a large area in one PSF. We also recommend that the PSF should be called "HMI". The description of the PSF needs to be adapted to the computerized control rooms found in the petroleum industry. Guidance on what should be evaluated and reference points on HMI quality could be taken from the standards used in the petroleum industry (e.g., NORSOK I-002 Rev. 2, 2001), existing HMI evaluation tools on usability (e.g., Dumas & Salzman, 2006), and current research.

We recommend that the Petro-HRA guidelines specifically state that what should be evaluated is how the HMI affects the operators' performance in the specific task that is being analysed. The general quality of the HMI or potential problems with the HMI that are outside this task should be added as an additional qualitative comment.

The other ergonomic factors outside of HMI are included as a separate PSF.

References (for change)

Dumas, J. S., & Salzman, M. C. (2006). Usability assessment methods. *Reviews of Human Factors and Ergonomics, 2*, 109-144.

Hickling, E. M., & Bowie, J. E. (2013). Applicability of human reliability assessment methods to human–computer interfaces. Cognition, technology & work, 15(1), 19-27.

NORSOK I-002 Rev. 2 (2001). *Safety and automation system (SAS)*, Rev. 2.

Petro-HRA (full) description

Human-Machine Interface 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 are: difficulties in obtaining relevant information or carrying out tasks through the safety and automation system; layout organization or colors that are not stereotypical; and communication difficulties due to the 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.

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:

1) Does the task rely on the HMI? If not, the Not Applicable level should be selected.
2) 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.

PSF levels			
SPAR-H levels	**SPAR-H multipliers**	**Petro-HRA levels**	**Petro-HRA multipliers**
		P=1	Extremely high negative effect on performance
Missing/Misleading	50	50	Very high negative effect on performance
Poor	10	10	Moderately negative effect on performance
Nominal	1	1	Nominal
Good	0.5	0.5	Low positive effect on performance

SPAR-H guidance/criteria for PSF levels		**Petro-HRA guidance/criteria for PSF levels**	
		P=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	Missing/Misleading—therequired instrumentation fails to support diagnosis or post-diagnosis behavior, or the instrumentation is inaccurate (i.e., misleading). Required information is not available	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

	from any source (e.g., instrumentation is so unreliable that operators ignore the instrument, even if it is registering correctly at the time).		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	Poor—the design of the facility negatively impacts task performance (e.g., poor labelling, needed instrumentation cannot be seen from a work station where control inputs are made, or poor computer interfaces).	10	Moderately 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—the design of the facility supports correct performance, but does not enhance performance or make tasks easier to carry out than typically expected (e.g., operators are provided useful labels; the computer interface is adequate and learnable, although not easy to use).	1	Nominal: 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 easily 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	Good—the design of the facility positively impacts task performance, providing needed information and the ability to carry out tasks in such a way that lessens the opportunities for error (e.g., easy to see, use, and understand computer interfaces; instrumentation is readable from workstation location, with measurements provided in the appropriate units of measure).	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.

Arguments/references for changing levels, multipliers or criteria

We consider it realistic that situations could occur where the HMI degrades performance to such a degree that it is unreasonable to expect that the operator will ever succeed. Therefore we recommend that the highest PSF level ("Missing/Misleading") in this PSF should give a HEP of one. It is important that this level is clearly described as a level that should be chosen only in situations where HMI alone is influencing the performance to such a degree.

If the impact of the "Missing/Misleading" PSF level is increased to always result in HEP equals one then the PSF will only include one PSF level ("Poor") that degrades performance without always ending in an error. The "Poor" PSF in the "Ergonomics/HMI" PSF in SPAR-H has a multiplier of 10, which would lead to a HEP of 0.1 for Diagnostic tasks and 0.01

for Action tasks (if no other PSFs are degrading or enhancing performance) (Gertman *et al.*, 2005). Hickling and Bowie's (2013) review found several studies where the "Poor" PSF level would probably have been chosen and underestimated the HEP, but also several where the "Poor" PSF level would have been chosen and the HEP would have been overestimated. A functional HRA method will never have the flexibility to predict the exact results of all HEP studies, but through adding one or two more levels of that decreased performance the analyst will be able to give a more nuanced description and calculation of the HEP influence from this PSF.

14.7 Fitness for Duty -> Fatigue (Removed)

PSF no	SPAR-H name	Fitness for Duty	Version	Date
7	**Petro-HRA name**	Fatigue (taken out)	1	08.05.14

SPAR-H Definition: The SPAR-H Human Reliability Analysis Method (Gertman *et al.*, 2005)

Fitness for duty refers to whether or not the individual performing the task is physically and mentally fit to perform the task at the time. Things that may affect fitness include fatigue, sickness, drug use (legal or illegal), overconfidence, personal problems, and distractions. Fitness for duty includes factors associated with individuals, but not related to training, experience, or stress.

SPAR-H Definition: Step-by-Step Guidance (Whaley et al., 2011)

Fitness for duty refers to whether or not the individual is physically and mentally suited to the task at hand. Issues that might degrade Fitness for Duty include fatigue, sickness, drug use (legal or illegal), overconfidence, personal problems, and distractions. Fitness for duty includes factors associated with individuals, but not related to training, experience, or stress (which are covered by other PSFs).

Fitness for Duty encompasses much more than fatigue, such as impairment due to drugs (prescription, over-the-counter, or illegal) or alcohol, distraction due to personal or family issues, whether a person is physically or mentally capable of performing a task, or boredom. These issues are rarely documented in event reports, however; so, the most common Fitness for Duty issue cited is fatigue. Time of day plays a role in Fitness for Duty. For example, it is not unusual for persons to become drowsy in the early afternoon, after lunch. For individuals accustomed to a night shift, cognitive functioning in the early hours of the morning is poorer than during the day. In circumstances such as this, a PSF assignment of "Degraded Fitness" might be appropriate. The type of task a person is working on also influences fitness for duty: it is well documented that people are bad at extended vigilance or monitoring tasks. Performance typically drops after about 30 minutes of continuous monitoring.

Petro-HRA short explanation of changes (need for change)

Fatigue seems to be the most relevant part of Fitness for Duty for a prospective analysis. We think there are enough mechanisms in high risk organizations that prevent factors such as drug abuse, illness or mentally upset operators that the effect on performance from these factors should be represented by the nominal failure rates. Also few organizations would admit that their workers are unfit for duty on a general basis. From the HRA analysts, it is said that this is a non-used PSF. There is much research on fatigue and human performance. However, when we investigated studies on the effect of Fatigue the multipliers are very much lower than for other PSFs and we decided that this PSF be removed because it has such low influence. In the Folkard studies (2003, 2006) it was found that Fatigue from night shift increased accidents by 30 percent, which gives a multiplier of 1.3. HEART has two Error producing conditions with a similar meaning as Fatigue: 35. Disruption of normal work-sleep cycles, multiplier=1.1; Error producing condition 34. Prolonged inactivity or highly repetitious cycling of low mental workload tasks, x1.1 for first half hour and x1.05 for each hour thereafter. Also these EPCs have very low multipliers.

References (for change)

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

Folkard, S., & Lombardi, D. A. (2006). Modelling the impact of the components of long work hours on injuries and "accidents". *American Journal of Industrial Medicine, 49*(11), 953-963.

Williamson, A., Lombardi, D. A., Folkard, S., Stutts, J., Courtney, T. K., & Connor, J. L. (2011). The link between fatigue and safety. *Accident Analysis & Prevention, 43*(2), 498-515.

14.8 Work Processes –> Attitudes to Safety, Work and Management Support

PSF no	SPAR-H name	Work Processes	Version	Date
8	**Petro-HRA name**	Attitudes to Safety, Work and Management Support	1	08.05.14

SPAR-H Definition: The SPAR-H Human Reliability Analysis Method (Gertman *et al.*, 2005)

Work processes refer to aspects of doing work, including inter-organizational, safety culture, work planning, communication, and management support and policies. How work is planned, communicated, and executed can affect individual and crew performance. If planning and communication are poor, then individuals may not fully understand the work requirements. Work processes include consideration of coordination, command, and control. Work processes also include any management, organizational, or supervisory factors that may affect performance. Examples seen in event investigations are problems due to information not being communicated during shift turnover, as well as communication with maintenance crews and auxiliary operators. Measures could include amount of rework, risk worth of items in utility corrective action program backlog, enforcement actions, turnover, performance efficiencies, etc.

The shift supervisor also plays a major role in work processes. Instances where the shift supervisor gets too involved in the specifics of the event—in contrast to maintaining a position of leadership in the control room—would indicate a breakdown in work processes.

Conditions with effects adverse to quality are also included in the work practices category, as are problems associated with a safety-conscious work environment. This includes retaliation by management against allegations as it pertains to the failure event under investigation. For example, the analyst must decide whether utility management actions against maintenance staff have any bearing on a particular control room action or maintenance action under evaluation. If the analyst believes there is such evidence, then the appropriate negative level for work practices PSF is assigned.

Additionally, any evidence obtained during the review of an operating event indicating inter-group conflict and decisiveness (e.g., between engineering and operations), or an uncoordinated approach to safety, is evaluated in SPAR-H as a work process problem. Schisms between operators and management are also considered work process problems.

SPAR-H does directly acknowledge potential problems between the regulator and licensee as it may affect operator and crew performance. It is assumed that problems in communication or adherence to enforcement actions or notices are indicative of work process problems. Finally, inadequacies in the utility corrective action program (CAP), such as failure to prioritize, failure to implement, failure to respond to industry notices, or failure to perform root cause as required by regulation, is considered in SPAR-H as a work process variable. Because there are so many potential areas of concern within the work process category that can be assigned to a potential PSF level, the analyst is directed to provide as much information as possible in the worksheet space provided, listing the reasons for assigning a particular work process PSF level, the analyst is directed to provide as much information as possible in the worksheet space provided, listing the reasons for assigning a particular work process PSF level.

SPAR-H Definition: Step-by-Step Guidance (Whaley et al., 2011)

Work Processes refer to aspects of doing work, including inter-organizational, safety culture, work planning, communication, and management support and policies. How work is planned, communicated, and executed can affect individual and crew performance. If planning and communication are poor, then individuals might not fully understand the work requirements. Work Processes include consideration of coordination, command, and control. Work Processes also include any management, organizational, or supervisory factors that may affect performance. Examples seen in event

investigations are problems due to information not being communicated during shift turnover, as well as communication with maintenance crews and auxiliary operators.

The shift supervisor also plays a major role in Work Processes. Instances where the shift supervisor gets too involved in the specifics of the event—in contrast to maintaining a position of leadership in the control room—would indicate a breakdown in Work Processes.

Conditions with effects adverse to quality are also included in the Work Processes category, as are problems associated with a safety-conscious work environment. This includes retaliation by management against allegations as it pertains to a failure event under investigation. For example, the analyst must decide whether utility management actions against maintenance staff have any bearing on a particular control room action or maintenance action under evaluation. If the analyst believes there is such evidence, then the appropriate negative level for Work Processes PSF might be assigned.

Additionally, any evidence obtained during the review of an operating event indicating inter-group conflict or indecisiveness (e.g., between engineering and operations), or an uncoordinated approach to safety, is evaluated in SPAR-H as a Work Process problem. Schisms between operators and management are also considered Work Process problems.

SPAR-H does directly acknowledge potential problems between the regulator and licensee as they might affect operator and crew performance. It is assumed that problems in communication or adherence to enforcement actions or notices are indicative of Work Process problems.

Work Processes is a “catch-all” PSF, encompassing organizational and management issues, cultural issues, safety culture, communications, crew dynamics, work planning and scheduling, supervision, conduct of work, and problem identification and resolution. The assignment of “Poor” or “Good” should follow from clear indications that aspects of work processes degraded or enhanced performance. For example, simply having a crew that communicates well is not sufficient reason to credit “Good” for Work Processes. If, on the other hand, good communication clearly helped to quickly diagnose an event at the facility, it would be appropriate to credit Work Processes as “Good”. Because so many factors are encompassed under Work Processes, it might be possible that a particular situation both features positive and negative aspects of the same PSF. In such cases, the most dominant factor should be considered as the main weighting factor. Precedence may be given to factors that degraded performance in such cases.

Petro-HRA short explanation of changes (need for change)

The Work Processes PSF is a very broad and poorly defined PSF in SPAR-H. It seems that Work Processes consists of: safety culture, teamwork/team dynamics/communication, and leadership/administrative control. Planning is also included which seems more to be a task in itself rather than a PSF. The last part of the definition is very nuclear oriented. Since this PSF is so poorly defined, a literature review was done on the topics of safety culture and teamwork to investigate what these topics include and how they could be more precisely defined. The result showed that an analysis of safety culture consists of factors that overlap with the other PSFs such as Procedures and Experience/Training. The factors from the safety culture domain that is not included in another PSF, and which affects post-initiation tasks is Attitudes to Safety and Work Conduct and Management Support which we have combined and named Attitudes to Safety, Work and Management Support. Teamwork is also a PSF that has been intensively studied for the last 20-30 years. Studies from the Halden Reactor Programme have shown that Teamwork is an important PSF in post-initiation tasks. We decided to split the Work Processes PSFs into Attitudes to Safety, Work and Management Support, and Teamwork. Teamwork also includes team leadership and communication. Use of procedures is moved to the Procedures PSF.

References (for change)

Flin, R., Mearns, K., O'Connor, P., & Bryden, R. (2000). Measuring safety climate identifying the common features. *Safety Science, 34*, 177-192.

Guldenmund, F.W. (2007). The use of questionnaire in safety culture research. An evaluation. *Safety Science, 45*, 376-387.

Guldenmund, F.W. (2010). (Mis)understanding safety culture and its relationships to safety management. *Risk Analysis, 30*, 1466–1478.

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

Petro-HRA (full) description

The Attitudes to Safety, Work and Management Support PSF consists of two related factors that have been found to predict safety outcomes in studies of safety culture. The two factors are: 1) Attitudes to safety and work conduct, 2) Management support.

Attitudes are defined as: The individual's positive or negative evaluation of performing the behavior (Ajzen, 1985).

Attitudes to safety and work conduct contribute to a safety conscious work environment. One example demonstrating how attitudes to safety and work conduct could negatively affect task performance can be given in the way 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 as, for example, not monitoring when they should. Another example of how attitude to safety and work conduct could negative affect safety is that the operators are not mindful of safety. The management of the organization is responsible for developing these attitudes.

Management support is defined as the operators' experiencing explicit support from management in performing the task(s) in question. An example is that the operators experience support from management to shut down production when appropriate even if this might have 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.

PSF levels			
SPAR-H levels	**SPAR-H multipliers**	**Petro-HRA levels**	**Petro-HRA multipliers**
Poor	2	Very high negative effect on performance	50
		Moderate negative effect on performance	10
Nominal	1	Nominal effect on performance	1
Good	0.8	Low positive effect on performance	0.5
SPAR-H guidance/criteria for PSF levels		**Petro-HRA guidance/criteria for PSF levels**	

2	Poor—performance is negatively affected by the work processes at the facility (e.g., shift turnover does not include adequate communication about ongoing maintenance activities; poor command and control by supervisor(s); performanceexpectations are not made clear).	50	Very high negative effect on performance: In this situation safety is not at all prioritized over other concerns when that 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. There could also, for example, be strong management pressure for production even if safety is clearly in question.
		10	Moderate negative effect on performance: In this situation it is unspecified 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. There is also low mindfulness regarding safety.
1	Nominal—performance is not significantly affected by work processes at the facility, or work processes do not appear to play an important role (e.g., crew performance is adequate; information is available, but not necessarily proactively communicated).	1	Nominal effect on performance. The operators have good attitudes to safety and work conduct and there is explicit management support to prioritize safety when that is appropriate. The operator(s) also shows mindfulness about safety.
0.8	Good—work processes employed at the facility enhance performance and lead to a more successful outcome than would be the case if work processes were not well implemented and supportive (e.g., good communication; well understood and supportive policies; cohesive crew).	0.5	Low 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.

Arguments/references for changing levels, multipliers or criteria

In SPAR-H the connection between the description of the PSF, the levels, and multipliers does not seem logical. If the organizational safety culture is evaluated to be poor, the highest multiplier possible is 2. There seems to be no relationship between the seriousness of the organizational conditions and the multipliers given. We do not yet have a good basis for the multipliers. Since the conditions in an organization that is described in this PSF are extremely serious organizational weaknesses that have been shown in accident reports like Deep Water Horizon to affect performance in a strong negative direction, this PSF should have high multipliers. The multipliers are set in comparison to the other multipliers.

There is no generic task in HEART (Williams, 1988, 1992) with a similarity to Attitudes to Safety, Work and Management Support . HEART has an error producing condition with a similarity to Attitudes to Safety, Work and Management Support :

18, a conflict between immediate and long-term objectives, with a multiplier of 1.8. This PSF does not seem to be a PSF that has received a lot of attention in HRA and it is difficult to find a good basis for the multipliers.

14.9 Work Processes -> Teamwork

PSF no	SPAR-H name	Work Processes	Version	Date
8	**Petro-HRA name**	Teamwork	1	08.05.14

SPAR-H Definition: The SPAR-H Human Reliability Analysis Method (Gertman *et al.*, 2005)

See above Work Processes

SPAR-H Definition: Step-by-Step Guidance (Whaley et al., 2011)

See above Work Processes

Petro-HRA short explanation of changes (need for change)

See above Work Processes

References (for change)

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

Williams, J. C. (1988, June). A data-based method for assessing and reducing human error to improve operational performance. In Human Factors and Power Facilitys, 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.

Petro-HRA (full) description

"Team is defined as two or more individuals with specified roles interacting adaptively, interdependently, and dynamically toward a common and valued goal" (Salas et al., 2005, p. 562). Teamwork is defined as a set of interrelated thoughts and feelings of team members that are needed 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 consisting of five core components (team leadership, mutual performance modelling, backup behavior, adaptiveness, and team orientation) and three coordinating mechanisms (shared mental models, achievement of mutual trust, and closed-loop communication).

A team in this analysis should be defined as everyone who is involved in the task(s) or scenario (also management).

In determining the appropriate PSF level the analyst should evaluate:

1) Is teamwork needed for this task? If teamwork is not needed the level not applicable should be chosen.
2) The analyst should use the form presented below and evaluate whether each of the teamwork factors has an effect on performance of the task. If the teamwork factors in the analysed scenario are evaluated and found to have an effect on performance the analyst should investigate whether they, for the task(s) in question, increase or reduce performance. The analyst has to perform a total evaluation of the factors when deciding on the levels. It might, for example, be that some factors are not important. In this case, they should be deemed neutral. Sometimes one factor might be evaluated as very important and then that factor might be the only basis for selecting a positive or negative level.

Strong antagonistic relationships are often indicative of issues with several of the teamwork factors.

Teamwork	*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 so as to achieve balance during periods of high 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 task 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 change. Identify opportunity for improving and innovation in habitual or routine practices. Remain vigilant to changes in the internal and external environment of the team.
Team orientation	Propensity to take others' behavior into account during group interaction and the belief in the importance of the goal 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	Anticipating and predicting each other's needs.

	engaged in and how the team members will interact.	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.

PSF levels			
SPAR-H levels	**SPAR-H multipliers**	**Petro-HRA levels**	**Petro-HRA multipliers**
Poor	2	Very high negative effect on performance	50
		Moderate negative effect on performance	10
		Very low negative effect on performance	2
Nominal	1	Nominal effect on performance	1
Good	0.8	Low positive effect on performance	0.5

SPAR-H guidance/criteria for PSF levels		**Petro-HRA guidance/criteria for PSF levels**	
2	Poor—performance is negatively affected by the work processes at the facility (e.g., shift turnover does not include adequate communication about ongoing maintenance activities; poor command.	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 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 this 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—performance is not significantly affected by work processes at the facility, or work processes do not appear to play an important role (e.g., crew performance is adequate; information is available, but not necessarily proactively communicated).	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.
0.8	Good—work processes employed at the facility	0.5	Low positive effect on performance: The team is good on one or more teamwork factors that have been identified as important for the task or scenario in question and teamwork increase performance.
Arguments/references for changing levels, multipliers or criteria			
See also Attitudes to Safety, Work and Management Support for explanations. Since we have changed the name of the PSF the descriptions of the levels had to be changed. A multiplier of 50 is chosen for the poor level because this seems appropriate compared to the other negative PSF levels. Good teamwork is expected to increase performance. We do not yet have a good basis for the multipliers since this is a PSF that has not yet received much attention in HRA, probably because the research on Teamwork is newer than the HRA methods developed. HEART does not have any Generic task that is similar to Teamwork. HEART has one Error producing condition with similar content to teamwork: 25, Unclear allocation of function and responsibility. HEP=1.6. The multipliers are set in comparison with the other PSF multipliers.			

14.10 Ergonomics/HMI – Physical Working Environment

PSF no	SPAR-H name	Ergonomics/HMI	Version	Date
10	**Petro-HRA name**	Physical working environment	1	

SPAR-H Definition: The SPAR-H Human Reliability Analysis Method (Gertman *et al.*, 2005)

Ergonomics refers to the equipment, displays and controls, layout, quality and quantity of information available from instrumentation, and the interaction of the operator/crew with the equipment to carry out tasks. Aspects of HMI are included in this category. The adequacy or inadequacy of computer software is also included in this PSF. Examples of poor ergonomics may be found in panel design layout, annunciator designs, and labelling.

When considering panel design layout, event investigations at U.S. commercial nuclear facilities have shown that when necessary facility indications are not located in one designated place, it is difficult for an operator to monitor all necessary indications to properly control the facility. If there is evidence that this is the case, a negative PSF value is assigned.

Examples of poor annunciator designs have been found where only a single acknowledge circuit for all alarms is available, which increases the probability that an alarm may not be recognized before it is cleared. Another problem exists where annunciators have set points for alarms that are set too near to the affected parameter for an operator or crew to react and perform a mitigating action.

Examples of poor labelling include instances where labels are temporary, informal, or illegible. In addition, multiple names may be given to the same piece of equipment. Ergonomics of the facility are also called the HMI or the human engineering aspects. Job performance aids can also be considered a special case of ergonomics. However, in SPAR-H, if the job performance deficiency is related to a procedure, then the preferred means of evaluating the situation is to apply this information to the procedures PSF, as opposed to the ergonomics PSF. For example, if the procedure does not match the equipment to be used, then the equipment procedure deficiency should be noted in the procedures, not the ergonomics, PSF.

During LP/SD, certain information is assumed for the nominal ergonomics case. For BWRs this includes availability of RCS level instrumentation and RHR system instrumentation. For PWRs, this includes the availability of RHR system instrumentation, the availability of RCS temperature instrumentation, and the availability of RCS level instrumentation.

SPAR-H Definition: Step-by-Step Guidance (Whaley et al., 2011)

Ergonomics refers to the equipment, displays and controls, layout, quality, and quantity of information available from instrumentation, and the interaction of the operator/crew with the equipment to carry out tasks. Aspects of the human-machine interface (HMI) are included in this category. The adequacy or inadequacy of computer software is also included in this PSF. Examples of poor ergonomics might be found in the panel design layout, annunciator designs, and labelling. Facility instrumentation generally corresponds to the Diagnosis aspect of crew performance, while facility controls correspond to the Action aspect.

When considering the panel design layout, event investigations at U.S. commercial nuclear facilities have shown that when necessary facility indications are not consolidated in one location, it is difficult for an operator to monitor all such indications to properly control the facility. If there is evidence that this is the case, a negative PSF value should be assigned. Examples of poor labelling include instances where labels are temporary, informal, or illegible. Multiple names used for the same piece of equipment can cause confusion and create ambiguity in communication. Job performance aids can also be considered a special case of ergonomics. However, in SPAR-H, if the job performance deficiency is related to a

procedure, then the preferred means of evaluating the situation is to apply this information to the Procedures PSF, as opposed to the Ergonomics PSF. For example, if the procedure does not match the equipment to be used, then the equipment-procedure deficiency should be noted in the Procedures, not the Ergonomics, PSF. During low power and shutdown (LPSD) facility operations, certain information is assumed for the nominal ergonomics case. For BWRs this includes availability of RCS) level instrumentation and residual heat removal (RHR) system instrumentation. For Pressurized Water Reactors, this includes the availability of RHR system instrumentation, the availability of RCStemperature instrumentation, and the availability of RCS level instrumentation. Included in Ergonomics and HMI is the quality and quantity of information available from displays and gauges, control sensitivity and panel layout, usability of tools and quality of materials, and control accessibility, among others. If instrumentation is inaccurate, incomplete, missing, or unavailable, then HMI is "Missing/Misleading". Issues such as poor panel displays or layouts, inadequate control sensitivity or accessibility are best assessed as "Poor". Note that although a typical control room console may not meet usability criteria of being intuitive or easy to use, the extensive training and experience of the crew allows them to interact with the system in an effective manner. They are able to get the information they need to monitor and diagnose facility states, and they are able to control all necessary parameters. Any deficiency in this basic functionality should be considered "Poor" or "Missing/Misleading".
Petro-HRA short explanation of changes (need for change)
In the discussions at the Gardermoen-meeting it was decided that the method should be applicable also to tasks outside the control room. To be able to attribute influences outside the control room this PSF has been added. Including both physical working environment and HMI in the same PSF had practical issues, so they were represented in separate PSFs.
References (for change)
Rasmussen, M., & Laumann, K. (2014). The Suitability of the SPAR-H "Ergonomics/HMI" PSF in a computerized control room in the petroleum industry. *Proceedings of the PSAM12 Conference,* Honolulu, HI.
Petro-HRA (full) description
Physical working environment refers to the equipment used by, accessibility, and the working conditions of the person performing the task. The ergonomic effects inside a control room are rarely large enough to have an affect large enough to be included in an HRA. This PSF should primarily be used for tasks outside the control room. Examples of ergonomic issues are: extreme weather conditions, work that should be performed in an inaccessible or hard to reach place, manually operated functions in the field that are physically demanding (e.g., hard to turn valve). Aspects of HMI are not included in this PSF. These are covered by a separate PSF: Human-Machine Interface.

PSF levels			
SPAR-H levels	**SPAR-H multipliers**	**Petro-HRA levels**	**Petro-HRA multipliers**
Missing/Misleading	50	Extremely high negative effect on performance	P=1
Poor	10	Moderate negative effect on performance	10

Nominal	1	Nominal effect on performance	1
Good	0.5		

SPAR-H guidance/criteria for PSF levels		Petro-HRA guidance/criteria for PSF levels	
50	Missing/Misleading—the required instrumentation fails to support diagnosis or post-diagnosis behavior, or the instrumentation is inaccurate (i.e., misleading). Required information is not available from any source (e.g., instrumentation is so unreliable that operators ignore the instrument, even if it is registering correctly at the time).	P=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	Poor—the design of the facility negatively impacts task performance (e.g., poor labelling, needed instrumentation cannot be seen from a work station where control inputs are made, or poor computer interfaces).	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—the design of the facility supports correct performance, but does not enhance performance or make tasks easier to carry out than typically expected (e.g., operators are provided useful labels; the computer interface is adequate and learnable, although not easy to use).	1	Nominal effect on performance. Physical working environment has neither a negative nor a positive effect on performance.
0.5	Good—the design of the facility positively impacts task performance, providing needed information and the ability to carry out tasks in such a way that lessens the opportunities for error (e.g., easy to see, use, and understand computer interfaces; instrumentation is readable from workstation location, with measurements provided in the appropriate units of measure).		

Arguments/references for changing levels, multipliers or criteria
The levels and multipliers used in Petro-HRA are the same as for Ergonomics/HMI in SPAR-H.

15 Task Analysis Library Template

The purpose of a task analysis library is to capture analysis details that can be reused in similar HRAs. One of the primary concerns with doing a detailed HRA, including a task analysis, is that it is resource intensive. The review of human actions requires extensive and often repeated input from operators and other SMEs as well as extensive time by the human reliability analysis team to complete the HRA. Yet, many aspects of this analysis are similar to other analyses. There are tremendous efficiencies to be won by identifying the overlap between analyses, allowing analysts to reuse relevant portions of the analysis.

This task analysis library template is not a database but rather an index of relevant pieces of the analysis. The key to reuse is for analysts to be able to identify significant areas of overlap between their current HRA and an existing HRA. As such, the indexing focuses on helping analysts find relevant information amid the archived documentation supporting the new analysis.

The library template indexes nine aspects of the HRA:

1. *A clear description of the type of systems and facilities being analysed*. To facilitate searches on this information, this index includes two levels of classification—both the general facility family and the specific facility. The general facility family includes:

    - On-shore facilities
    - Fixed production installations
    - Floating production installations
    - Mobile installations
    - Other

Specific facilities include:

- Fixed on the seabed
- Semi-subs
- Floating production storage and offloading
- Tension leg platform
- Bridged installations
- Wellhead installations
- Jackups
- Floatels
- Drilling rigs
- Transport vehicles
- Other

2. *A description of DSHAs that are implicated in the analysis.* These include:

    - Non-ignited hydrocarbon leak
    - Ignited hydrocarbon leak
    - Well incident / loss of well control
    - Fire/explosion in other areas (non-hydrocarbon)
    - Ship on collision course
    - Drifting objects
    - Collision with field related vessel

- Structural damage/stability/mooring/positioning failure
- Leakage from subsea systems/pipelines/risers/flowlines/loading buoy/loading hose
- Damage on subsea systems/pipelines/diving gear caused by fishery equipment
- Evacuation (precautionary/emergency evacuation)
- Helicopter accident
- Man over board
- Serious injury
- Serious illness/epidemic
- Blackout
- Non-operational control room (not in use)
- Diving accident
- Release of hydorcarbons
- Loss of control of radioactive source (not in use)
- Falling objects
- Other

3. *A listing of the HFEs* including the short title and a short but comprehensible description, including the systems affected and the consequences of the failure.

4. *Links to the task analysis and HEI for each HFE*. This may be included in any reasonable form (e.g., document or spreadsheet). As outlined in the body of this report, the task analysis and HEI should include documentation of all assumptions made during the analysis. This can include tasks that were not analysed because they were not risk significant. The reasons for exclusion should be clearly documented.

5. *Links to event and fault trees* showing integration of the HRA in the QRA.

6. *Links to the quantification worksheets* (see the worksheets in Section 11.3) completed for the HFEs. These should include any assumptions made that shaped the analysis. These assumptions should detail to a sufficient degree such that the analyst can reconstruct the quantitative portion of the analysis.

7. *A lessons learned synopsis from the analysis*. This lessons learned synopsis may take the form of insights into improving the process of conducting the analysis or specific information that was gathered and that proved instrumental in shaping the analysis.

8. *Links to source documents that supported the analysis*. These documents may be proprietary, and access rights may be limited to some source materials.

9. *A description of other analyses* that have made use of this information. If an analyst references or reuses an analysis, this new analysis should be "checked in" and cross-referenced to the source analysis.

Mostly, the library serves as a repository of information that should be included with any quality HRA. Specifically, documentation in the form of background information, workshop results, and assumptions that were made are crucial to understanding the HRA in the library. Many analyses fail to be standalone—they represent a shorthand that is difficult to understand and perhaps impossible to reconstruct later. The library aims to prevent HRA shorthand and instead ensure that all artifacts of the analysis are retained.

Such information is crucial if an analyst reuses the HRA at a later date. Reuse is actually a misnomer. Reuse does not mean simply copying the contents of an existing analysis verbatim. Rather, reuse means adapting the analysis to meet the needs of another facility or installation. Adaptation of an existing HRA means understanding all the assumptions that were made, because those assumptions may not hold to a new application. For example, tasks that were excluded because they were not risk significant may prove highly significant in another context. Adaptive reuse requires that parts of the HRA be reanalysed with updated information to fit the new application.

The library template is built using Microsoft OneNote, a resource for sharing and cataloging information. OneNote is the combination of a database (e.g., Microsoft SQL Server), a shared directory (e.g., Microsoft SharePoint), and an easy-to-use configuration management system (e.g., Microsoft Excel). It is included with Microsoft Office and is therefore a readily available resource for analysts. It is cross-platform, allowing it to be used across different computer platforms. It retains strict user access priviledges, allowing information to be safely stored on a server—a particular concern due to the proprietary nature of QRA and HRA information. Finally, it includes powerful built-in search tools, allowing analysts to find required information quickly yet in an organized fashion. A particular strength of OneNote is that as a native Microsoft Office application, it understands most common document formats and indexes them. Thus, searches, if desired, may not only reference the nine key indices of the library but may also reference the source documents embedded in the library.

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 Statoil Petroleum AS, and DNV-GL 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-GL[2], SINTEF Technology and Society, the Idaho National Laboratory and Statoil[3].

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, Statoil; Andreas Falck, DNV-GL; 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 Statoil 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 Statoil 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 Statoil, by Marius Fernander and Sondre Øie, DNV-GL. 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-GL 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 Statoil.

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.

[2] Now called DNV.

[3] Now called Equinor.

Major Updates to Revision 1

Since the publication of the method in 2017, it has been applied in several petroleum projects in Norway. Informal feedback has been collected from analysts, end-users and stakeholders during this time regarding potential improvements that could be implemented to enhance usability. In 2020, Equinor initiated a project with DNV and IFE to update the guideline to address these suggestions for improvement.

The guideline has now been split into two documents:

- Part 1 The Petro-HRA Method: Step-by-Step Instruction (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 majority of changes were made to Part 1, which included edits to the text for clarify as well as updated examples to illustrate the guidance.

A second case study of a gas leak scenario has been added to Part 2. This demonstrates the application of the Petro-HRA method to a more complex scenario, and is based on a real-life example.

Other changes to Parts 2 & 3 of the guideline include: updating the document template, removal of in-document cross-references that are no longer relevant, and correction of typographical and grammatical errors. The text, figures and tables are presented as they were in the original version of the Petro-HRA guideline.