Petro-HRA

En ny metode for å analysere vurdere menneskelig pålitelighet i kvantitative risikoanalyser

Metodebeskrivelse og casestudie

Claire Taylor, Sondre Øie,

ESRA, 08 September 2016

PetroHRA · The Research Council of Norway · Statoil · IFE · NTNU – Trondheim Norwegian University of Science and Technology · DNV·GL · SINTEF · INL Idaho National Laboratory

Contents

General introduction

- Why does QRA need HRA?

The Petro-HRA method

- Background & overview
- The 7 steps in the Petro-HRA method

(*Illustrative examples throughout the presentation)*

Glossary of terms

- HRA – Human Reliability Assessment
- QRA – Quantitative Risk Assessment
- HFE – Human Failure Event
- HEP – Human Error Probability
- PSF – Performance Shaping Factor
- DP – Dynamic Positioning

Why does QRA need HRA? -1

- Risk informed decision-making
- Problem definition;
  - Drilling on shallow waters using Dynamic Positioning (DP)
  - Avoid costs associated with mooring assistance
  - How do we know this is safe (enough)?
  - Uncertainties associated with critical DP operator actions

Why does QRA need HRA? -2

- Quantitative Risk Assessment (QRA)
  - Typically uses event trees to model system failures that could lead to a Major Accident Scenario
  - Some differences in how human-initiated failures are represented in QRA
  - Human Failure Events (HFEs) may be explicitly represented at the top level of the even tree, or may be implicit in other top level failures

Why does QRA need HRA? -3

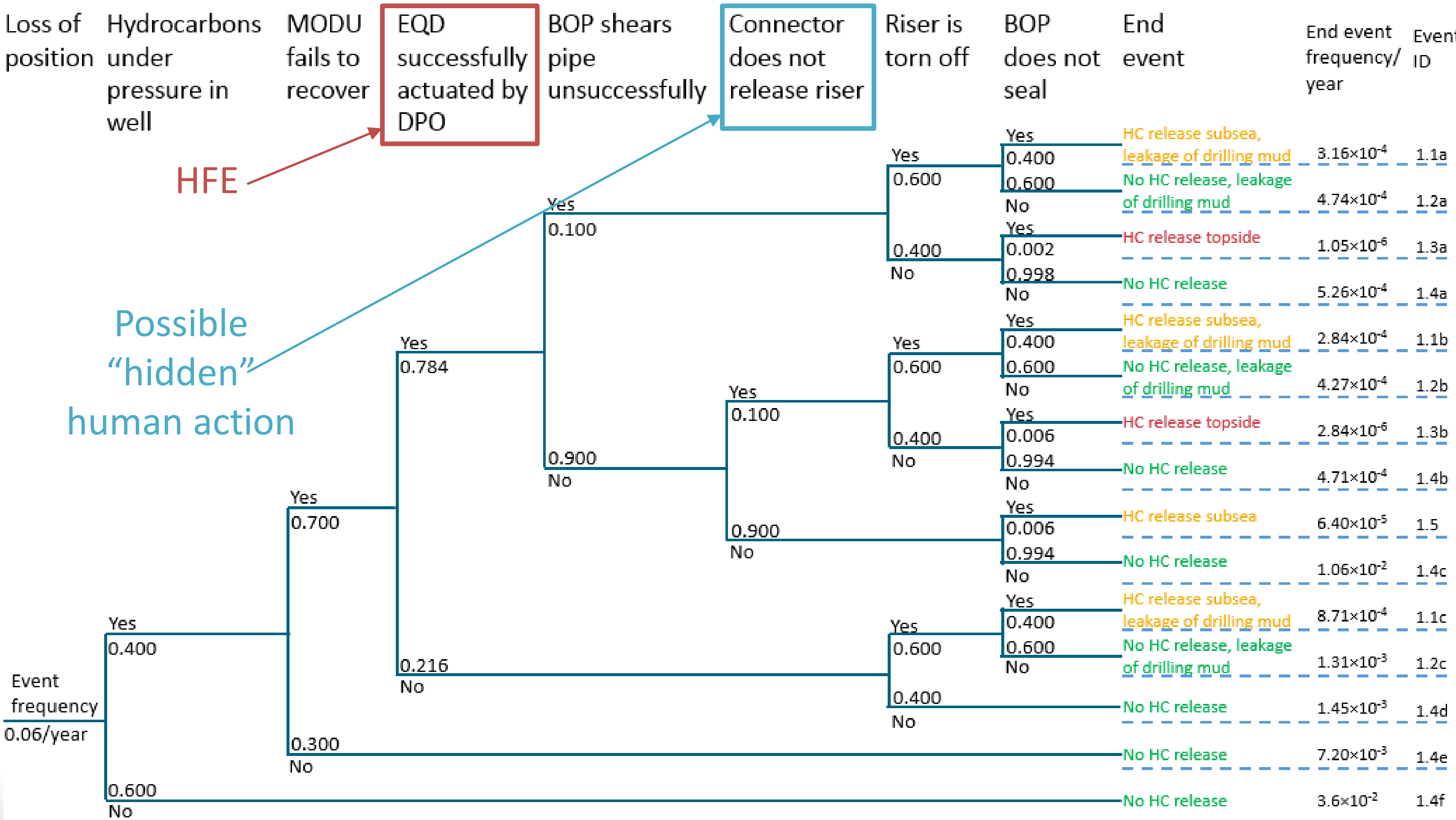


Figure from: Pedersen, R. N. (2015). QRA Techniques on Dynamic Positioning Systems During Drilling Operations in the Arctic: With Emphasis on the Dynamic Positioning Operator. University of Tromsø.

PetroHRA The Research Council of Norway Statoil IFE NTNU – Trondheim Norwegian University of Science and Technology DNV·GL SINTEF INL Idaho National Laboratory

The Petro-HRA project

- Established in 2012 as a joint industry/research project, sponsored by Statoil and the Research Council of Norway (RCN), with contribution from DNV-GL

- The main goal was to evaluate and adapt an existing nuclear HRA method to a petroleum context
  - The Standardized Plant Analysis Risk-Human Reliability Analysis (SPAR-H) method was originally developed for analysis of human actions in a nuclear control room
  - The SPAR-H method has been used quite extensively in the US for human reliability analysis in the nuclear industry
  - The SPAR-H method was chosen for the Petro-HRA project based on a previous study which concluded that it was the most promising for evaluating petroleum events

- The Petro-HRA guideline will be completed by end of 2016.

Development of the Petro-HRA method

- Much of the focus was on:
  - Evaluating and adapting SPAR-H nominal values and PSF descriptions & levels, to make them more suitable for petroleum activities & tasks
  - Documenting the qualitative analysis process, including task and error analysis, to make Petro-HRA a "complete" method

- Many HRA methods do not describe how to do qualitative analysis
  - Causes uncertainty amongst less experienced analysts
  - Increases variability between analysts in their approach and results

- The Petro-HRA method includes guidance on qualitative analysis, therefore is considered a "complete" method

SPAR-H and Petro-HRA: key differences -1

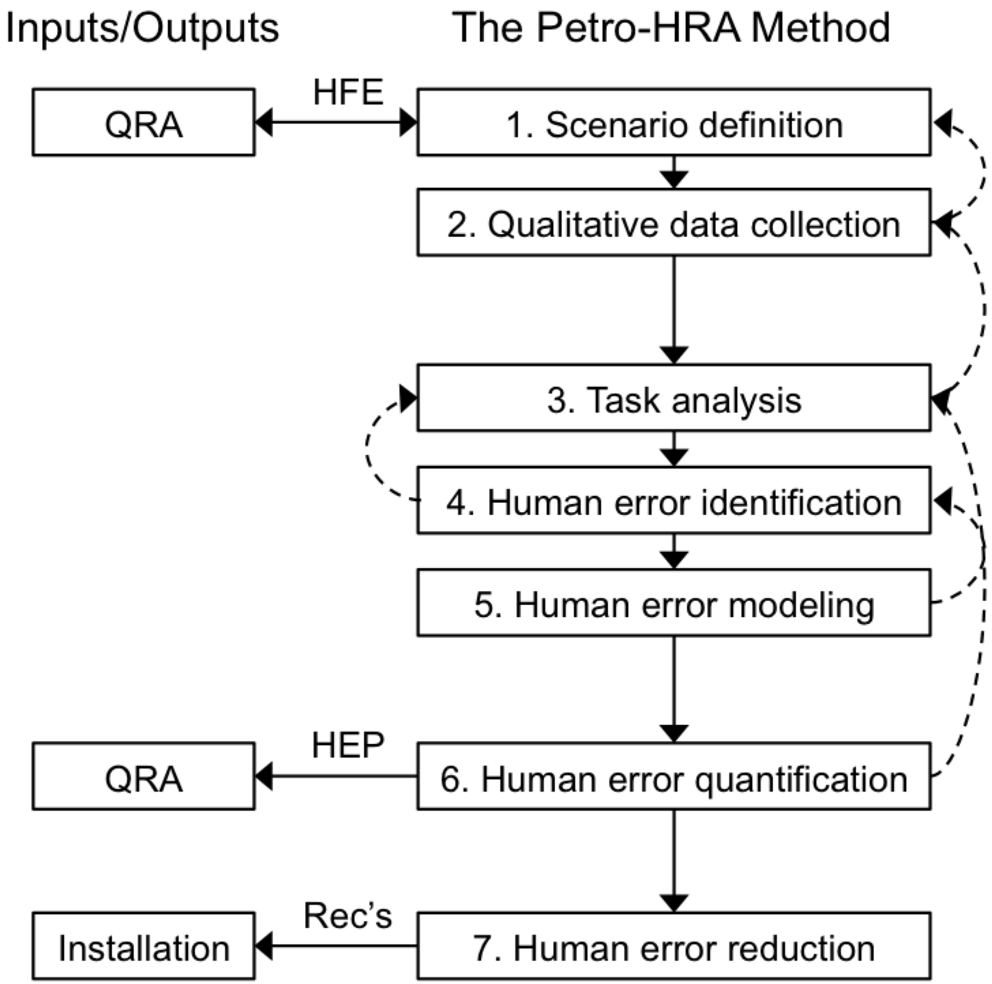
SPAR-H method	Petro-HRA method
Nominal Human Error Probability (HEP)	
• Nominal HEP = 0.01 for diagnosis tasks and 0.001 for action tasks	• Nominal HEP is set at 0.01
• *Analyst must decide whether the task is a diagnosis or action task (or both)*	• *No separation between diagnosis (cognition) and action tasks because there are no tasks in petroleum that are purely diagnosis or action*
Performance Shaping Factors (PSFs) *(and descriptions)*	
• Available time • Stress and stressors • Experience and training • Complexity • Ergonomics (including HMI) • Procedures • Fitness for duty • Work processes	• Time • Threat stress • Task complexity • Experience/Training • Procedures • Human-Machine Interface (HMI) • Adequacy of Organization • Teamwork • Physical working environment

PSFs	PSF Levels	Multiplier for Diagnosis
Available Time	Inadequate time	P(failure) = 1.0
	Barely adequate time (≈2/3 x nominal)	10
	Nominal time	1
	Extra time (between 1 and 2 x nominal and > than 30 min)	0.1
	Expansive time (> 2 x nominal and > 30 min)	0.01
	Insufficient information	1
Stress/ Stressors	Extreme	5
	High	2
	Nominal	1
	Insufficient Information	1
Complexity	Highly complex	5
	Moderately complex	2
	Nominal	1
	Obvious diagnosis	0.1
	Insufficient Information	1
Experience/ Training	Low	10
	Nominal	1
	High	0.5
	Insufficient Information	1
Procedures	Not available	50
	Incomplete	20
	Available, but poor	5
	Nominal	1
	Diagnostic/symptom oriented	0.5
	Insufficient Information	1
Ergonomics/ HMI	Missing/Misleading	50
	Poor	10
	Nominal	1
	Good	0.5
	Insufficient Information	1
Fitness for Duty	Unfit	P(failure) = 1.0
	Degraded Fitness	5
	Nominal	1
	Insufficient Information	1
Work Processes	Poor	2
	Nominal	1
	Good	0.8
	Insufficient Information	1

RA: ke … -2

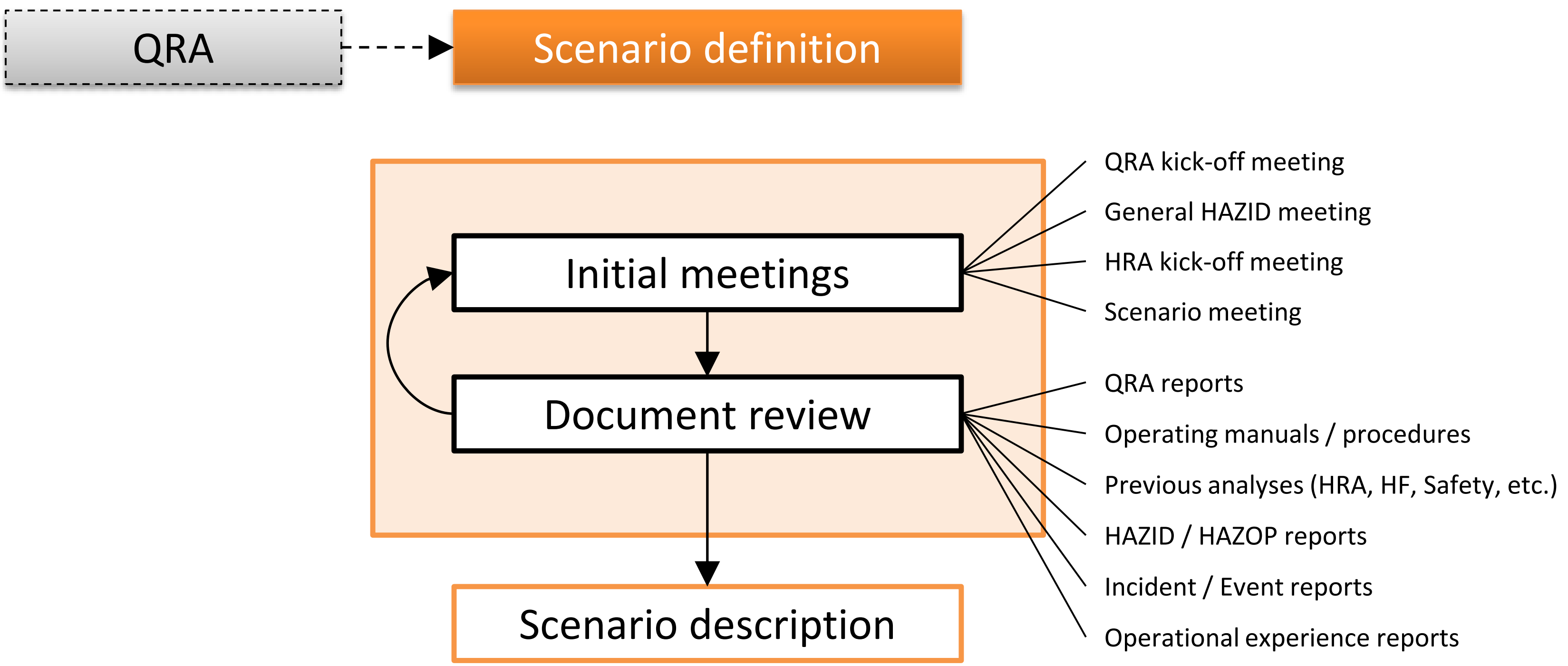
PSFs	PSF levels	Multiplier
Available time	Extremely high negative	HEP=1
	Very high negative	50
	Moderate negative	10
	Nominal	1
	Moderate positive	0.1
	Not applicable	1
Threat stress	High negative	25
	Low negative	5
	Very low negative	2
	Nominal	1
	Not applicable	1
Task complexity	Very high negative	50
	Moderate negative	10
	Very low negative	2
	Nominal	1
	Moderate positive	0.1
	Not applicable	1
Experience/training	Extremely high negative	HEP=1
	Very high negative	50
	Moderate negative	15
	Low negative	5
	Nominal	1
	Moderate positive	0.1
	Not applicable	1
Procedures	Very high negative	50
	High negative	20
	Low negative	5
	Nominal	1
	Low positive	0.5
	Not applicable	1
Human-machine interface	Extremely high negative	HEP=1
	Very high negative	50
	Moderate negative	10
	Nominal	1
	Low positive	0.5
	Not applicable	1
Adequacy of organization	Very high negative	50
	Moderate negative	10
	Nominal	1
	Low positive	0.5
	Not applicable	1
Teamwork	Very high negative	50
	Moderate negative	10
	Very low negative	2
	Nominal	1
	Low positive	0.5
	Not applicable	1
Physical working environment	Extremely high negative	HEP=1
	Moderate negative	10
	Nominal	1
	Not applicable	1

The Petro-HRA method

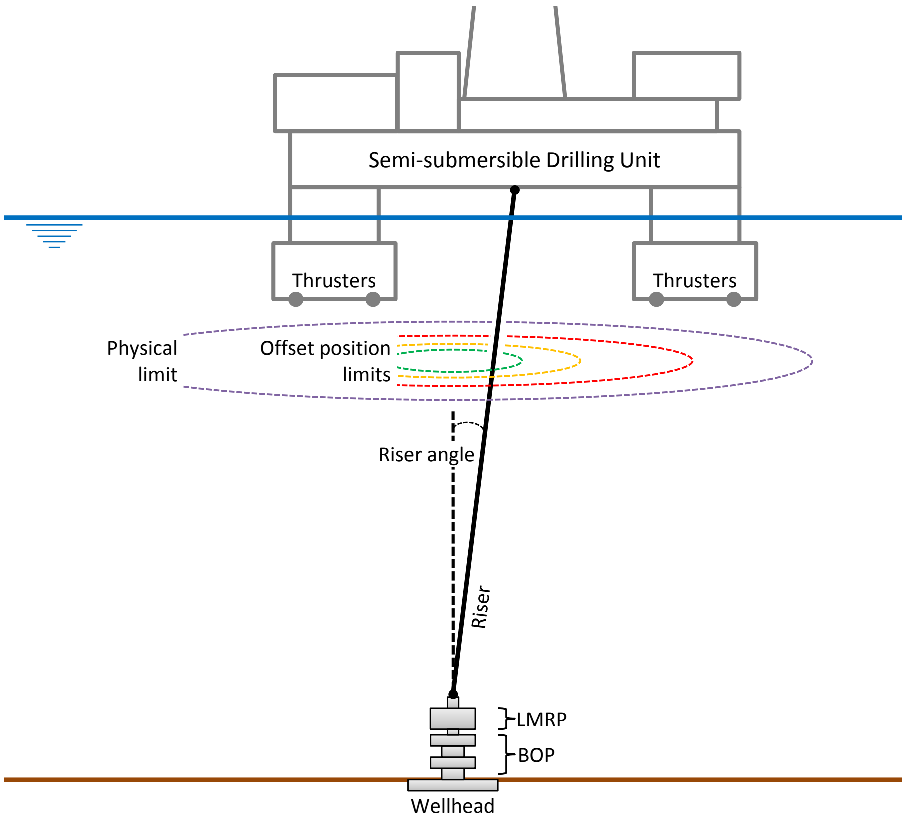


- 7 steps in the method
- Non-linear – iteration between & within steps
- May include inputs from the QRA in the form of a HFE, HEP and/or scenario information
- Outputs an updated HEP to the QRA
- Outputs recommendations for improvement measures to the installation itself

Step 1 - Define the scenario



Example: loss of position of a drill rig



- Position of the rig above the wellhead is maintained autonomously by Dynamic Positioning (DP) through the action of a set of thrusters
- A Dynamic Positioning Operator (DPO) located in the Marine Control Room (MCR) is responsible for constant monitoring of DP panels and screens and carrying out emergency procedures if needed
- In a drive-off scenario, the DPO must stop the thrusters and initiate emergency disconnection of the rig from the wellhead

Input to scenario definition from QRA

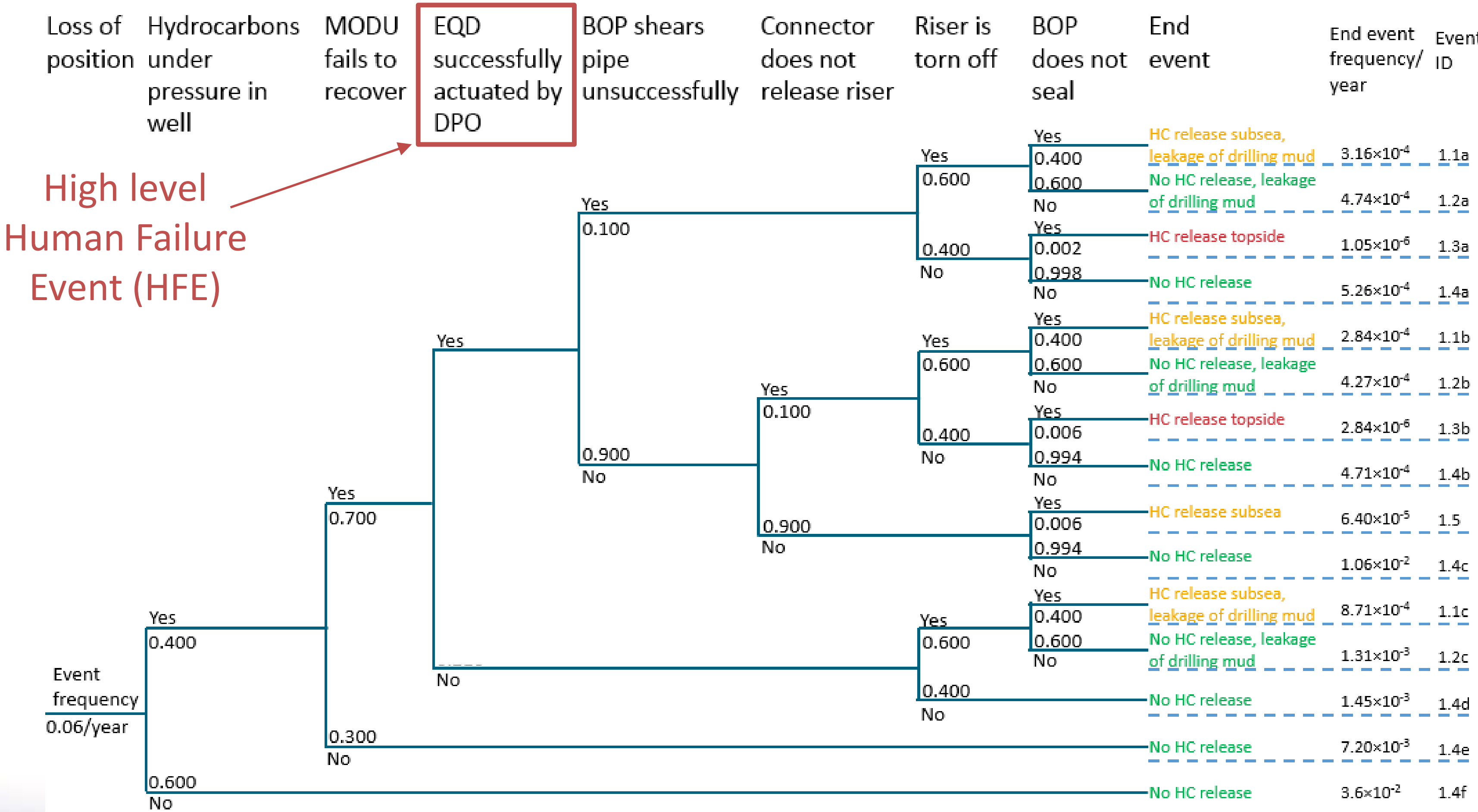
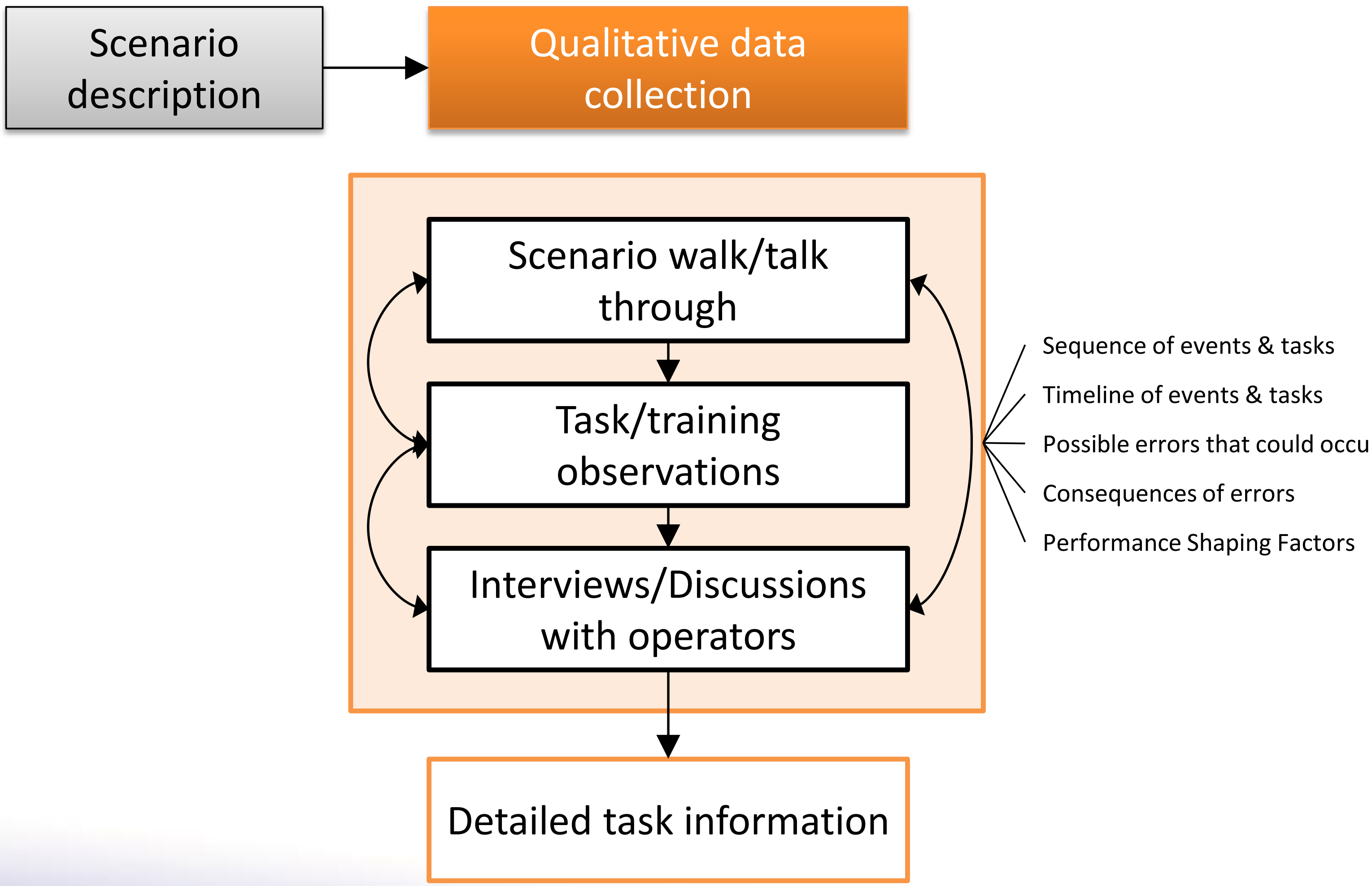


Figure from: Pedersen, R. N. (2015). QRA Techniques on Dynamic Positioning Systems During Drilling Operations in the Arctic: With Emphasis on the Dynamic Positioning Operator. University of Tromsø.

The Petro-HRA scenario description template

Topic	Description	Comments
Initiating event	An undefined DP failure initiates the drive-off. All thrusters 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. 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	Operator: • Detect drive-off • Diagnose the situation • Decide the next steps • Activate emergency thruster stop (bringing the rig into a drift-off) • 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 well-head. The rig 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."* 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.	There is no direct feedback in the system for successful disconnection. However CCTV images from the ROV and Moon Pool camera may show if the LMRP is disconnected and whether there is tension on the riser (i.e. slip joint is moving).
End of event sequence	For this scenario the Automatic EDS is enabled with a safety margin to prevent damage to the well and rig. As	

Step 2 - Collect qualitative data



Collecting qualitative data

Scenario talk-through / walk-through

- This should be one of the first activities in the data collection
- Gain a detailed understanding of how the operator would respond in the scenario
- Understand local contexts and constraints that could affect operator response

Observations of Task Performance / Training

- Understand how the operators work and interact with each other and the I&C systems around them
- Observe normal working conditions to collect general qualitative data
- Observe training exercise to collect scenario-specific qualitative data

Interviews / Discussions with Operators

- Most commonly used data collection technique
- Should always interview more than one operators to ensure a more balanced view
- Also consider interviewing shift managers, trainers, site QRA analyst/end user, HSE advisor, etc.

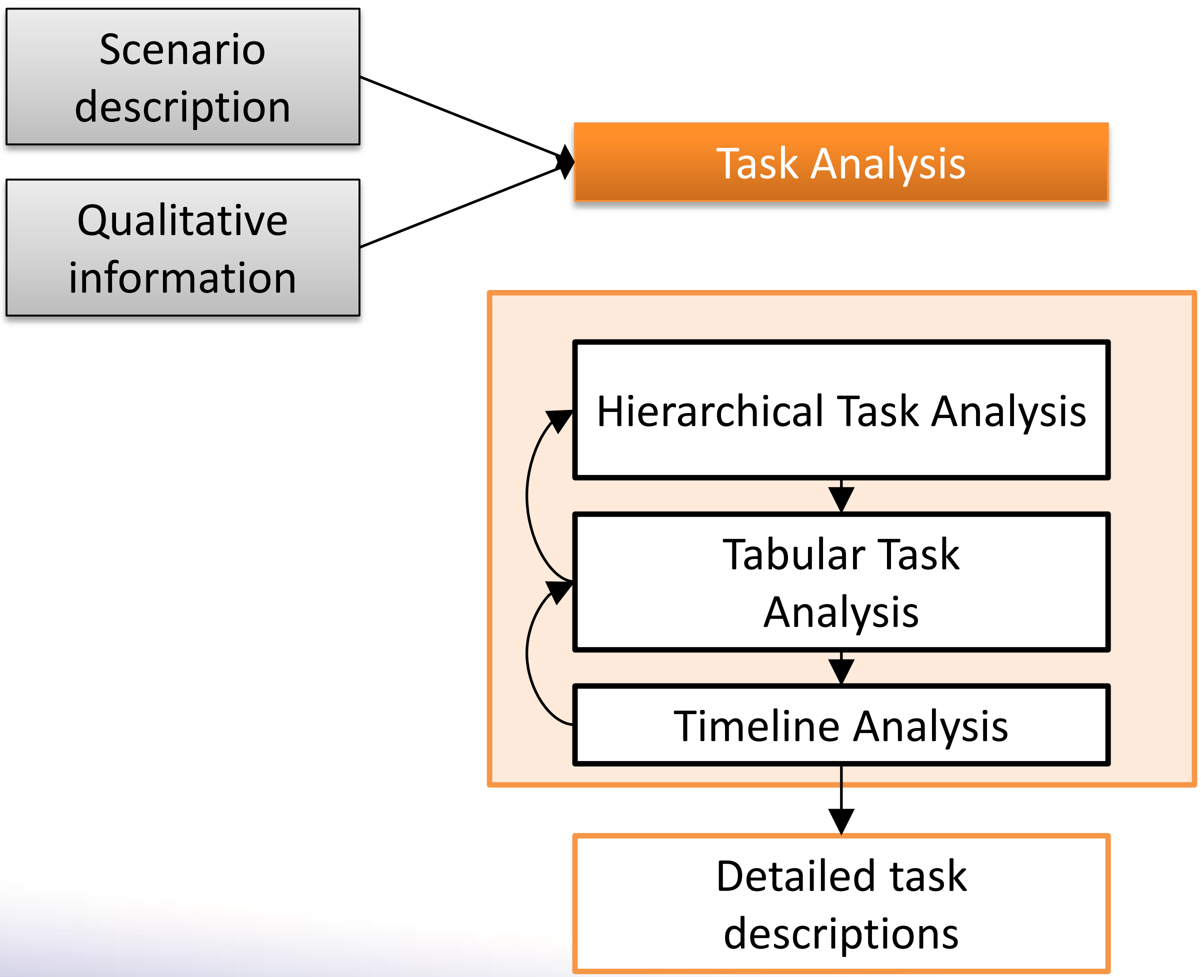
Identify deviation scenarios

- Deviations to the main scenario might also exist, and should be considered for analysis

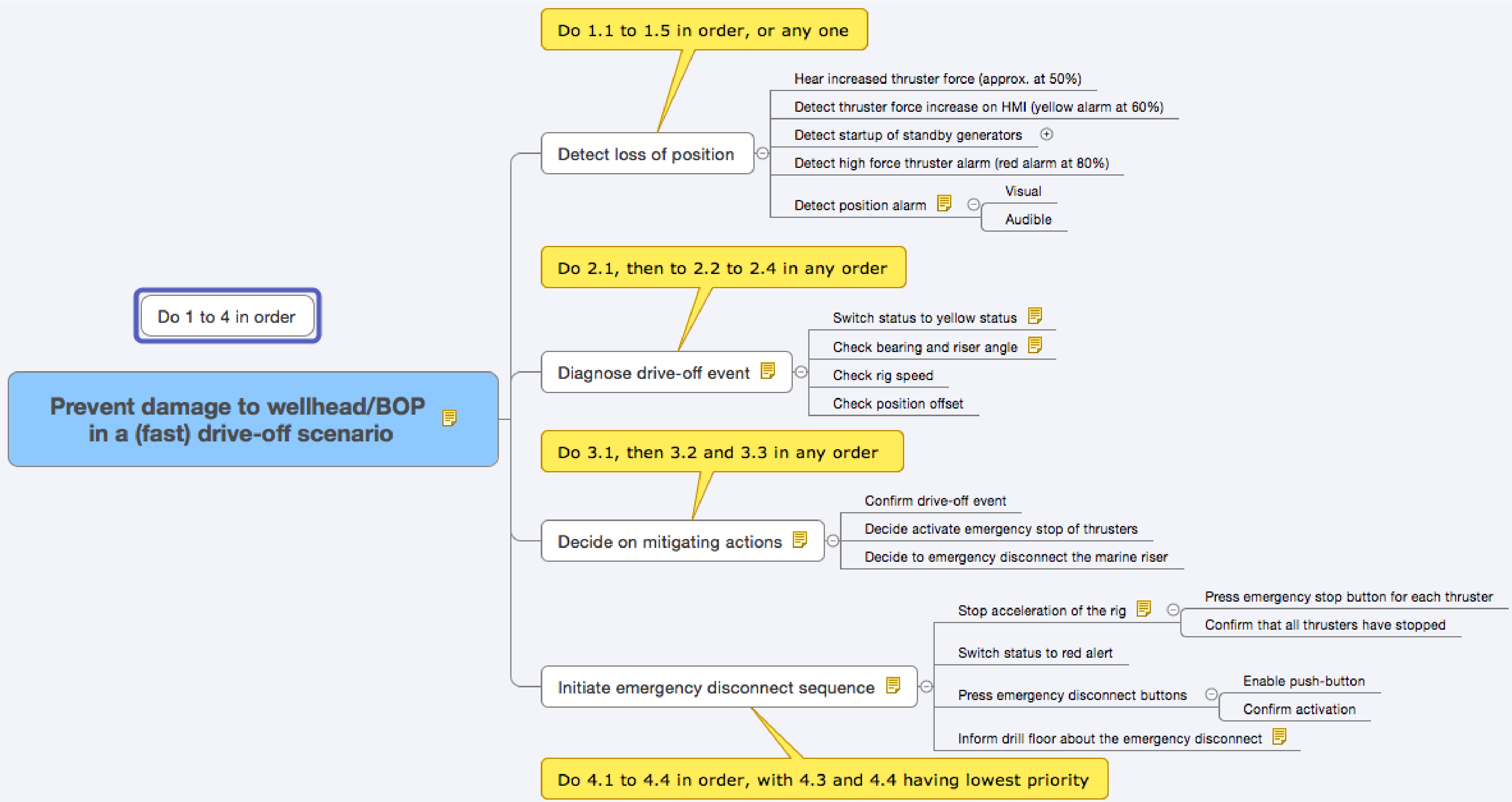
  - *[A deviation is] a scenario that deviates from the nominal conditions normally assumed for the QRA sequence of interest, which might cause problems or lead to misunderstandings for the operating crews (adapted from Forester et al., 2007)*

  - *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 procedures, and so forth (from Forester et al., 2007)*

Step 3 - Develop the task analysis



Hierarchical Task Analysis (HTA) example

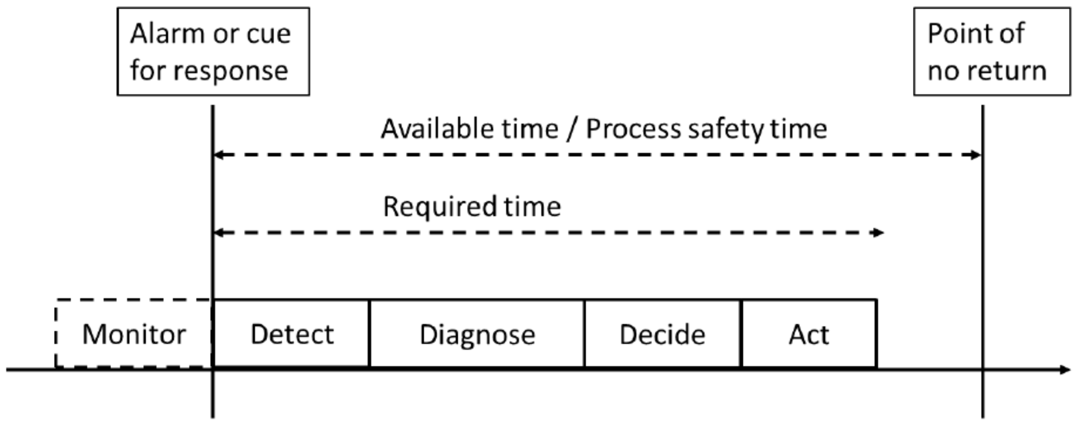


Tabular Task Analysis (TTA) example

Table 10.1 TTA for the task "Diagnose drive-off event"

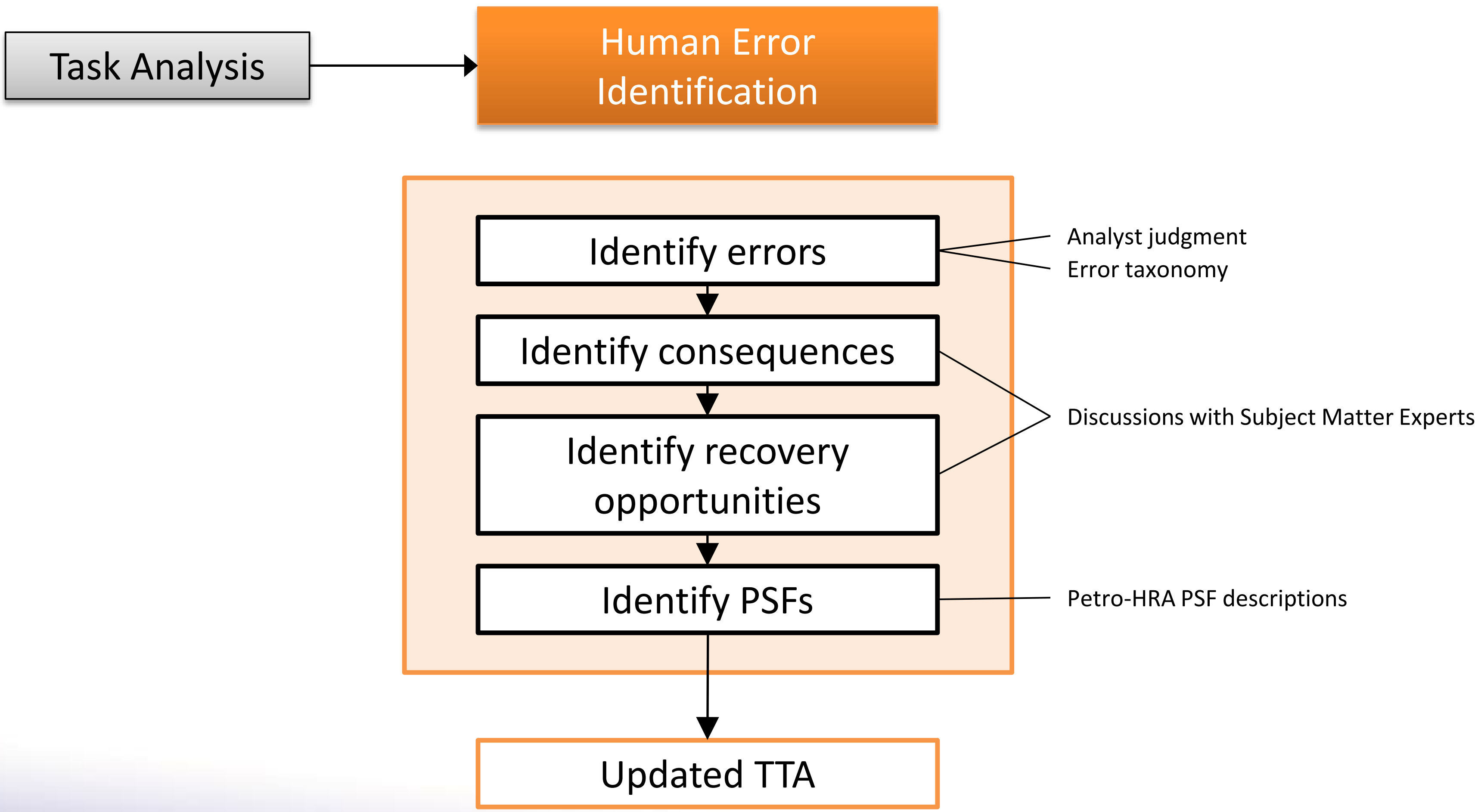
Step No	Task	Cue	Feedback	HMI	Responsible	Assumptions	Notes
2	DIAGNOSE DRIVE-OFF EVENT						
PLAN 2	*DO 2.1 to 2.3 in any order, then DO 2.4*						
2.1	Check riser angle	One or several loss of position indicators detected as part of task step 1.0 – most likely increase in thruster sound. In addition, previous task steps in 2.0 will be cues for subsequent diagnosis steps.	Noticeable increase in riser angle displayed in degrees.	DPOS	DPO 1	The DPO on duty monitors parameters continuously through the watch and will quickly notice deviation in trends and values.	Automatic EDS initiates when the riser angle exceeds 2°. To be successful (safe) the disconnection must occur before the riser angle exceeds 8°.
2.2	Check rig speed	Same as for task step 2.1.	Noticeable increase in speed on HMI displayed in knots.	K-Pos – DPOS.	DPO 1	Same as for task step 2.1.	
2.3	Check position offset	Same as for task step 2.1.	Noticeable position offset on HMI displayed in meters and with a rig position diagram.	K-Pos – DPOS.	DPO 1	Same as for task step 2.1.	It could take up to 5 seconds from the thrusters starting up before he will see any change in rig position on the HMI. The DPO would therefore have to check the position offset a few times to be sure that a drive-off is occurring.

Conducting a timeline analysis



- Time is often a critical factor in petroleum events; operators often have only minutes, or even seconds, to respond and intervene to control and mitigate the consequences of an event.
- Operators and other SMEs can give good insights into the time required to complete tasks, which tasks can be performed in parallel, where time pressure might exist, etc.

Step 4 - Identify and describe errors



Human Error Identification example

Table 10.3 Human error identification for the task "Diagnose drive-off event"

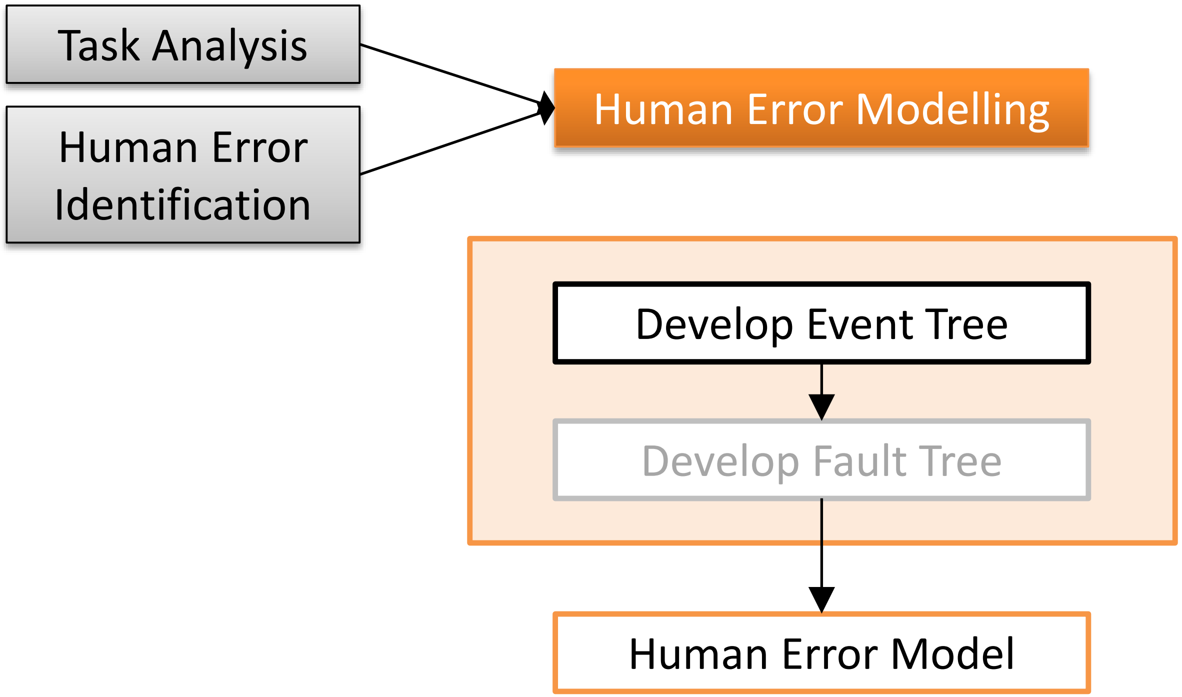
Step No	Description	Potential error	Likely consequences	Recovery opportunity	Further analysis	PSFs
2	DIAGNOSE DRIVE-OFF EVENT				Y	
PLAN 2	DO 2.1 to 2.3 in any order, then DO 2.4					
2.1	Check riser angle	DPO omits to check riser angle	DPO has an incomplete awareness of drive-off situation and must rely only on information about rig speed and position offset. This may cause delay or omission of thruster stop and EDS activation.	Additional checks in Steps 2.2 and 2.3	N	
		DPO misreads / misdiagnoses riser angle degrees (being less than actual)	DPO may experience less urgency something which in turn may delay subsequent required actions, i.e. thruster stop and EDS activation.	Additional checks in Steps 2.2 and 2.3	Y	
		DPO checks riser angle too late/ or spends too much time checking	DPO has less time available to check other loss of position indicators. DPO has an incomplete awareness of drive-off situation and must rely on checking rig speed and position offset alone. This may cause delay or omission of thruster stop and EDS activation.	No recovery	Y	

Identify Performance Shaping Factors (PSFs)

- The Petro-HRA method quantifies errors by considering the effects of PSFs
- Therefore the analyst must also consider what PSFs exist that may contribute to the identified errors by considering "*what if…?*", e.g.
  - *Is time a factor for the error potential in this task?*
  - *Could the quality of procedures affect the potential errors in this task?*

- The Petro-HRA method includes nine PSFs:
  1. Time
  2. Threat Stress
  3. Task Complexity
  4. Experience / Training
  5. Procedures
  6. Human-Machine Interface
  7. Adequacy of Organization
  8. Teamwork
  9. Physical Working Environment

Step 5 – Human error modelling

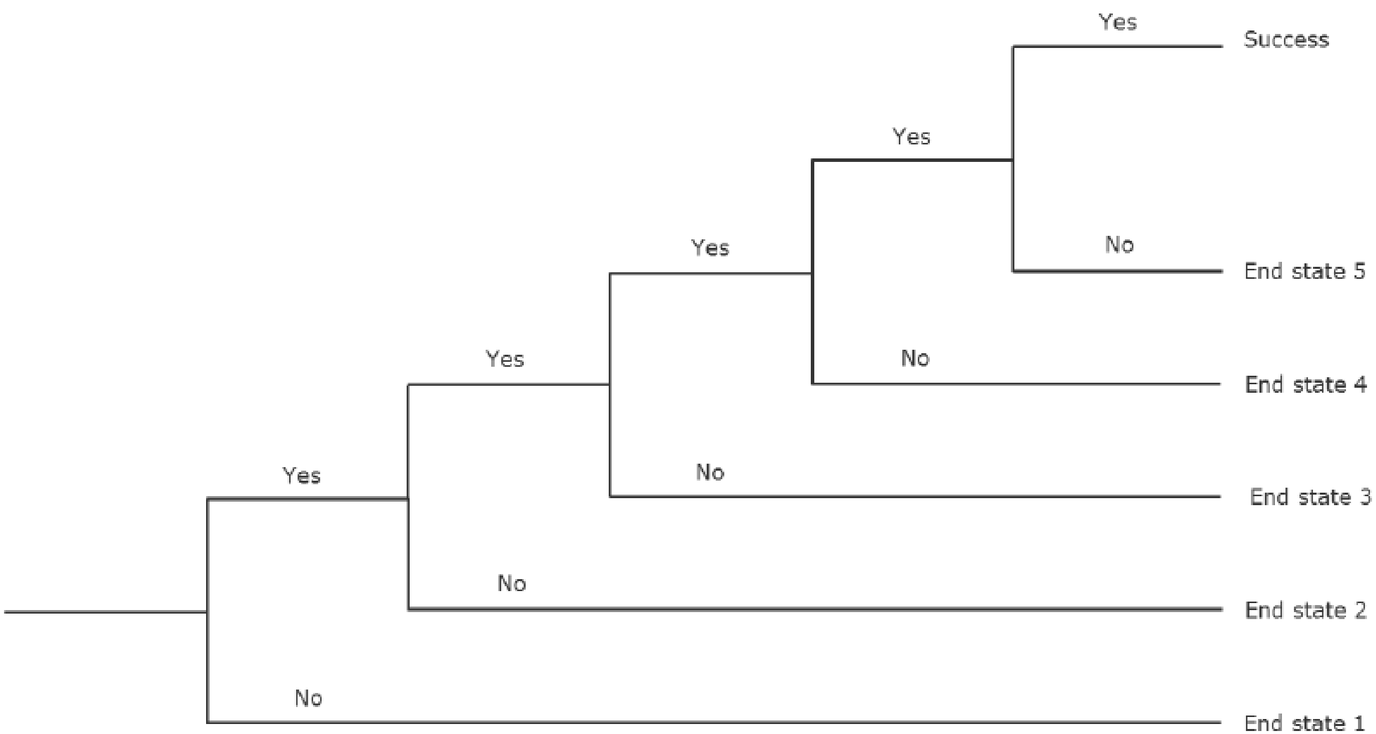


Human Error Modeling for Petro-HRA

- Event trees most commonly used in QRA, and therefore it is the recommended approach for Petro-HRA
  - Event trees provide a good high-level description of the post-initiating event scenario
  - It may be easier to integrate the results into the QRA event tree if a similar format is used

Event Tree model example

Drive-off occurs	DPO detects abnormalities in rig behaviour	DPO diagnose situation as a drive-off	DPO decides to disconnect rig from well	DPO stops all running thrusters	DPO activates emergency disconnect seq.	Final outcome / end state



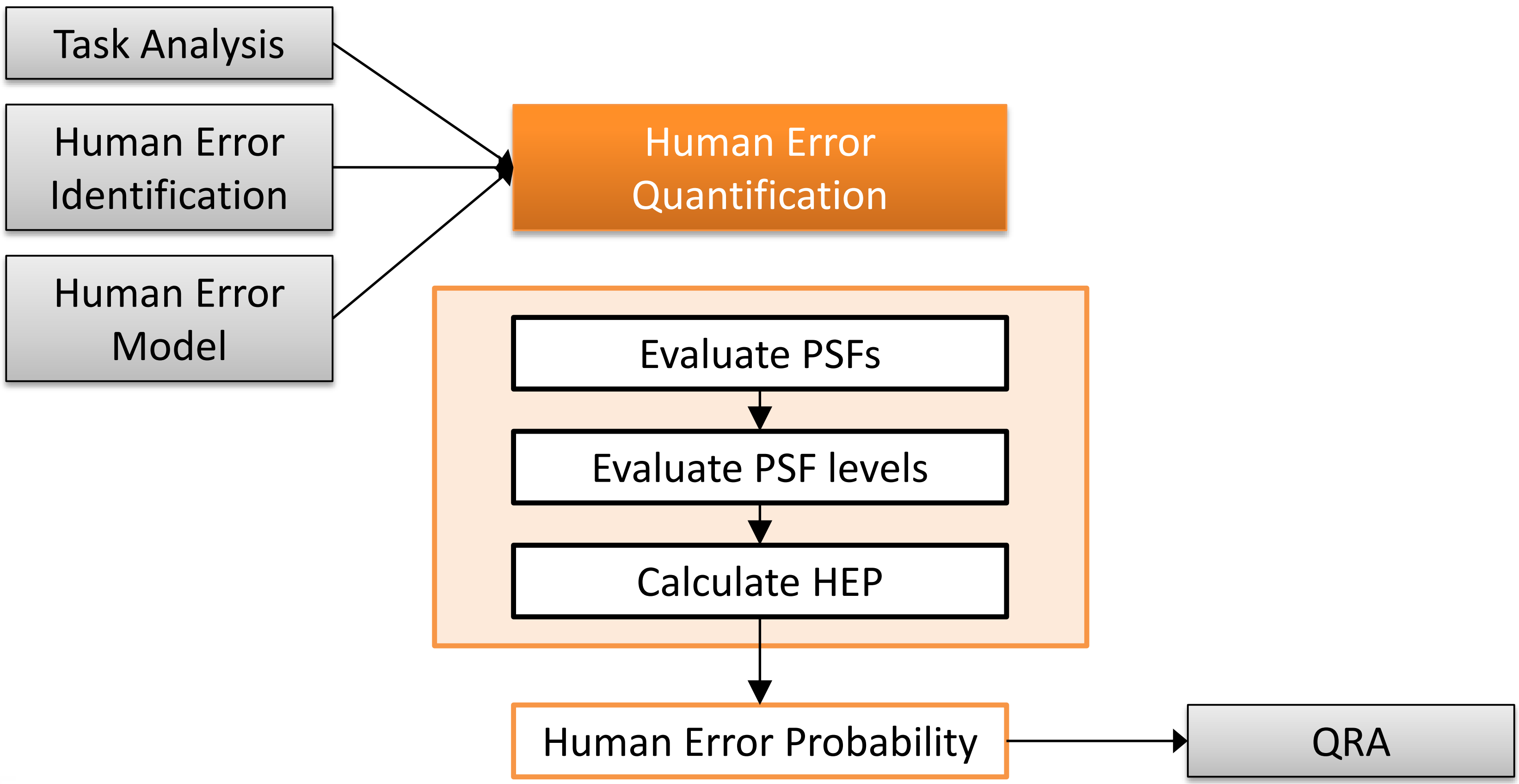
PetroHRA
The Research Council of Norway
Statoil
IFE
NTNU – Trondheim Norwegian University of Science and Technology
DNV·GL
SINTEF
INL Idaho National Laboratory

Event Tree table example

Table 10.5 Operator action event tree table for a drive-off scenario

ID	Event	Failure Event	Potential errors (from HEI)	HEP	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. Ref. Task 1.0	Failure to detect DP abnormalities. The drive-off is not detected or detected too late by the DPO, making him or 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 hear sound of thrusters increasing. DPO does not detect increase in thrusters force on HMI.	0.x	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 diagnose situation as drive-off. Ref. Task 2.0	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 or she fails to recognize the type of event or its severity.	DPO does not diagnose that this is a drive-off event. See additional associated human errors marked (Y) in the HEI, Table 11.3.	0.x	See ID 1 (above).
3	DPO decides to disconnect rig from well.	Failure to decide on correct mitigating actions.	DPO does not realise that thrusters should be stopped first before initiating EDS.	0.x	See ID 1 (above).

Step 6 – Human error quantification



Petro-HRA PSF sheet

- One for each event
- Select multipliers
- Document justification
- Identify ‘performance drivers’
- Avoid ‘double counting’
- Calculate HEP for event (see next slide)

- The example is fictional and only for illustration purposes

Petro-HRA PSF summary worksheet			
Plant/installation	Mobile Offshore Drilling Unit	Date	17.03.16
HFE ID/code	2.0		
HFE scenario	Fast drive-off		
HFE description	Failure to prevent wellhead damage by disconnecting from well		
HFE sub-event	Failure to diagnose situation as drive-off		
Analysts	Sondre Øie, Claire Taylor		
HEP	HEP = 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 EQD.
	Very high negative	50	
	Moderate negative	10	
	Nominal	1	
	Moderate positive	0.1	
	Not applicable	1	
Threat stress	High negative	25	At this stage, when starting to realize that the event is in fact a drive-off, the DPO is beginning to experience some degree of threat stress. However it is not considered to have a significant effect on the performance of this event/ task step.
	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 parameters.
	Moderate negative	10	
	Very low negative	2	
	Nominal	1	
	Moderate positive	0.1	
	Not applicable	1	
Experience/training	Extremely high negative	HEP=1	The DPOs have a lot of general training in DP systems and navigation, as well as some desktop discussions and draw on experiences from previous events. But they do not train specifically on 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 scattered across several documents.
	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 for diagnosing the drive-off parameters (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	
Adequacy of organization	Very high negative	50	Adequacy of organization is not considered a performance driver for this event/ task step.
	Moderate negative	10	
	Nominal	1	
	Low positive	0.5	
	Not applicable	1	
Teamwork	Very high negative	50	The event/ task step is only carried out by the DPO on watch. It is standard procedure that performing the disconnection is the on-duty DPOs responsibility.
	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	

How to calculate Human Error Probabilities (HEPs)

Nominal HEP	x	PSFs	with	PSF Levels	=	HEP
0.01		Time		Extremely High Negative		
		Threat Stress		Very High Negative		
		Task Complexity		High Negative		
		Experience/Training		Moderate Negative		
		Procedures		Low Negative		
		HMI		No Effect		
		Adequacy of Organization		Low Positive		
		Teamwork		Moderate Postive		
		Physical Working Environment				

Quantify HEP for overall HFE

Petro-HRA PSF summary worksheet			
Plant/installation	Mobile Offshore Drilling Unit	Date	17.03.16
HFE ID/code	2.0		
HFE scenario	Fast drive-off		
HFE description	Failure to prevent wellhead damage by disconnecting from well		
HFE sub-event	Failure to diagnose situation as drive-off		
Analysts	Sondre Øie, Claire Taylor		
HEP	HEP = 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 EQD.
	Very high negative	50	
	Moderate negative	10	
	Nominal	1	
	Moderate positive	0.1	
	Not applicable	1	
Threat stress	High negative	25	At this stage, when starting to realize that the event is in fact a drive-off, the DPO is beginning to experience some degree of threat stress. However it is not considered to have a significant effect on the performance of this event/ task step.
	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 parameters.
	Moderate negative	10	
	Very low negative	2	
	Nominal	1	
	Moderate positive	0.1	
	Not applicable	1	
Experience/training	Extremely high negative	HEP=1	The DPOs have a lot of general training in DP systems and navigation, as well as some desktop discussions and draw on experiences from previous events. But they do not train specifically on 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 scattered across several documents.
	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 for diagnosing the drive-off parameters (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	
Adequacy of organization	Very high negative	50	Adequacy of organization is not considered a performance driver for this event/ task step.
	Moderate negative	10	
	Nominal	1	
	Low positive	0.5	
	Not applicable	1	
Teamwork	Very high negative	50	The event/ task step is only carried out by the DPO on watch. It is standard procedure that performing the disconnection is the on-duty DPOs responsibility.
	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	

Nominal HEP x PSF Level = HEP

0.01 x 5 x 5 x 0.5 = 0.125

Experience / training
(low negative)

Human-machine
interface
(low positive)

Procedures
(low negative)

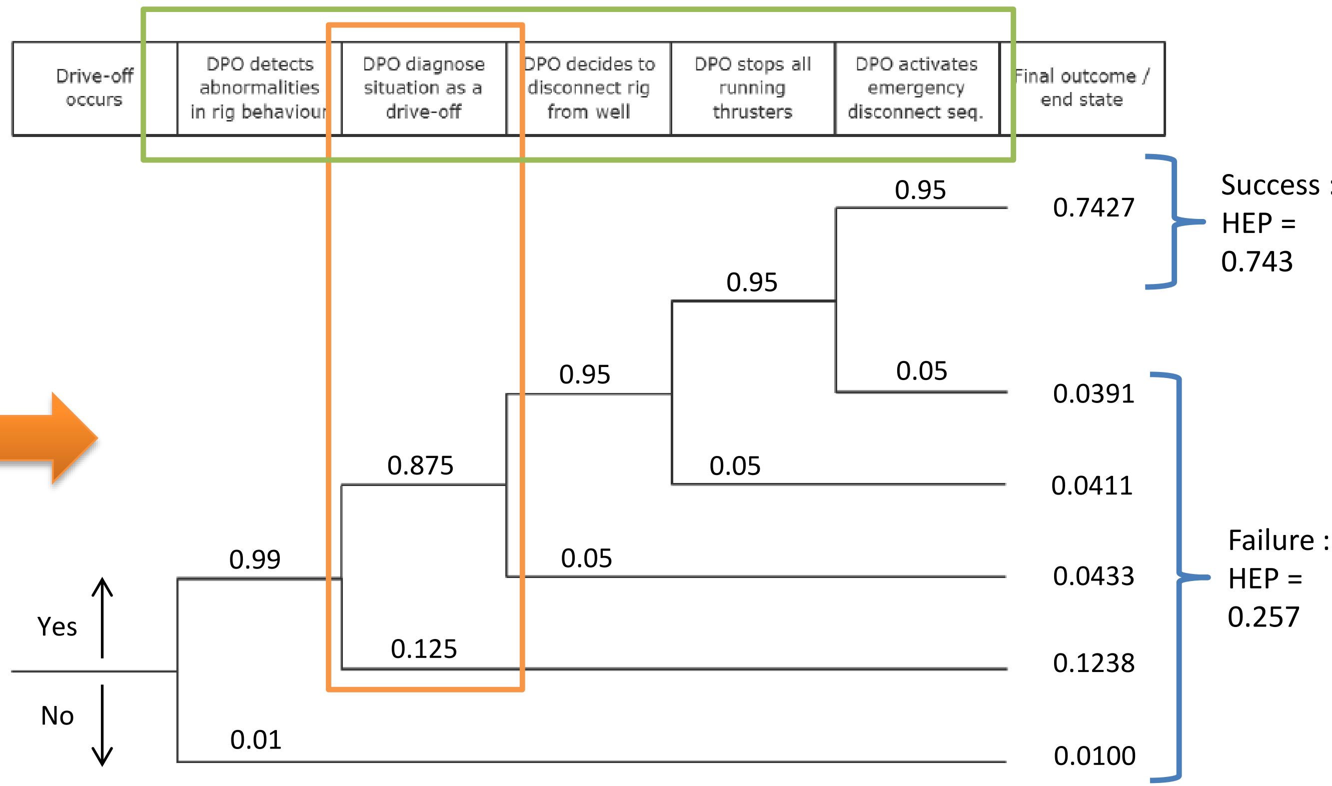
Update the PSF sheet with the calculation and HEP

Update the human error event tree

Calculate the HEP for each PSF sheet and update the event tree

Do this for each event in the event tree model

Petro-HRA PSF summary worksheet			
Plant/installation	Mobile Offshore Drilling Unit	Date	17.03.16
HFE ID/code	2.0		
HFE scenario	Fast drive-off		
HFE description	Failure to prevent wellhead damage by disconnecting from well		
HFE sub-event	Failure to diagnose situation as drive-off		
Analysts	Sondre Øie, Claire Taylor		
HEP	HEP = 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 EQD.
	Very high negative	50	
	Moderate negative	10	
	Nominal	1	
	Moderate positive	0.1	
	Not applicable	1	
Threat stress	High negative	25	At this stage, when starting to realize that the event is in fact a drive-off, the DPO is beginning to experience some degree of threat stress. However it is not considered to have a significant effect on the performance of this event/ task step.
	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 parameters.
	Moderate negative	10	
	Very low negative	2	
	Nominal	1	
	Moderate positive	0.1	
	Not applicable	1	
Experience/training	Extremely high negative	HEP=1	The DPOs have a lot of general training in DP systems and navigation, as well as some desktop discussions and draw on experiences from previous events. But they do not train specifically on 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 scattered across several documents.
	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 for diagnosing the drive-off parameters (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	
Adequacy of organization	Very high negative	50	Adequacy of organization is not considered a performance driver for this event/ task step.
	Moderate negative	10	
	Nominal	1	
	Low positive	0.5	
	Not applicable	1	
Teamwork	Very high negative	50	The event/ task step is only carried out by the DPO on watch. It is standard procedure that performing the disconnection is the on-duty DPOs responsibility.
	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	

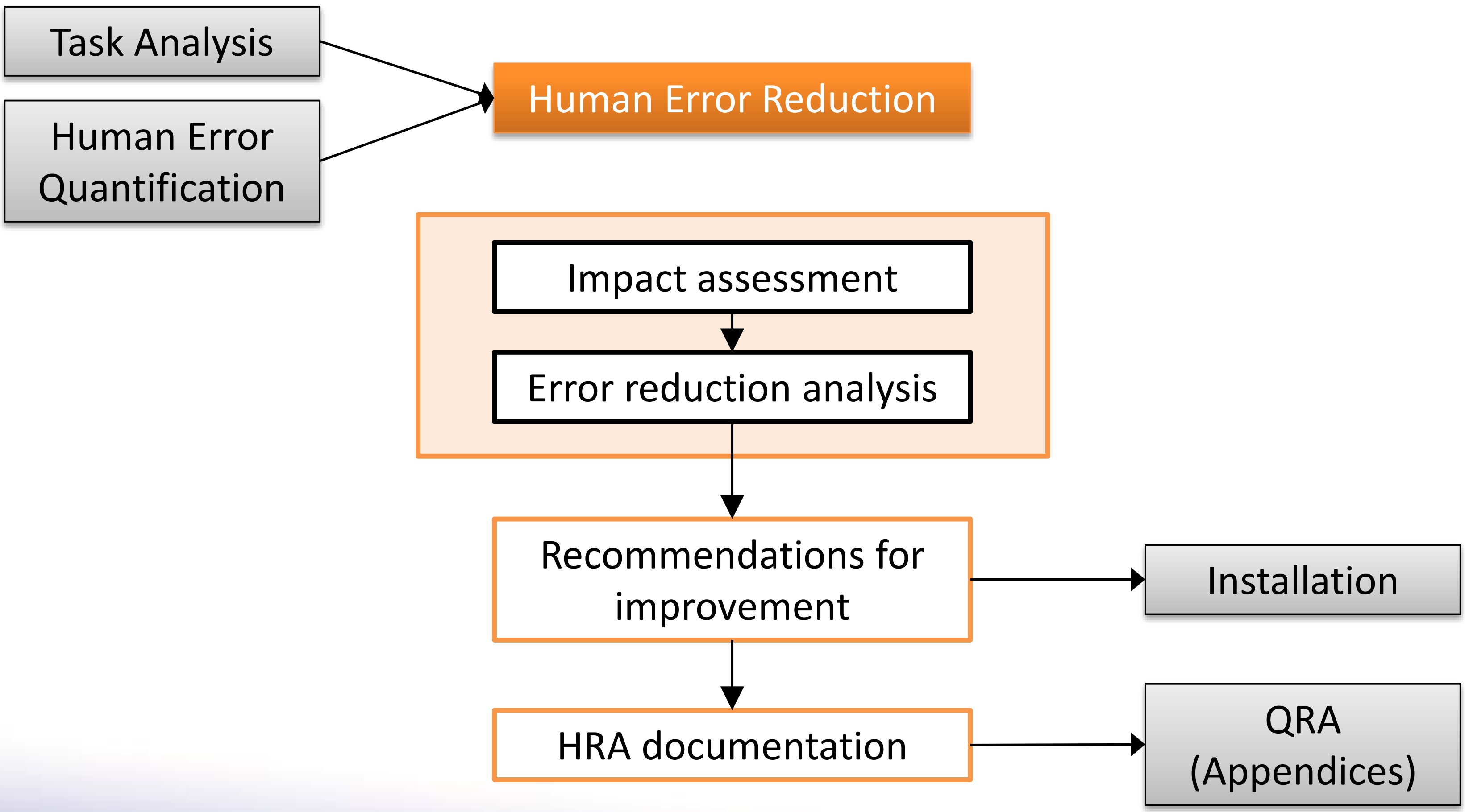


The example is fictional and only for illustration purposes

Deciding the level of quantification

- Similar issues to task analysis decomposition
  - If at a too high level, then the quantification may be overly simplistic, not capturing important nuances or the influence and impact of particular task steps on human performance
  - If at too low a level, then the quantification may become too detailed, resulting in an overly conservative HEP
- There is no “rule of thumb” for the level at which to quantify; there are pros and cons with each

Step 7 – Human error reduction

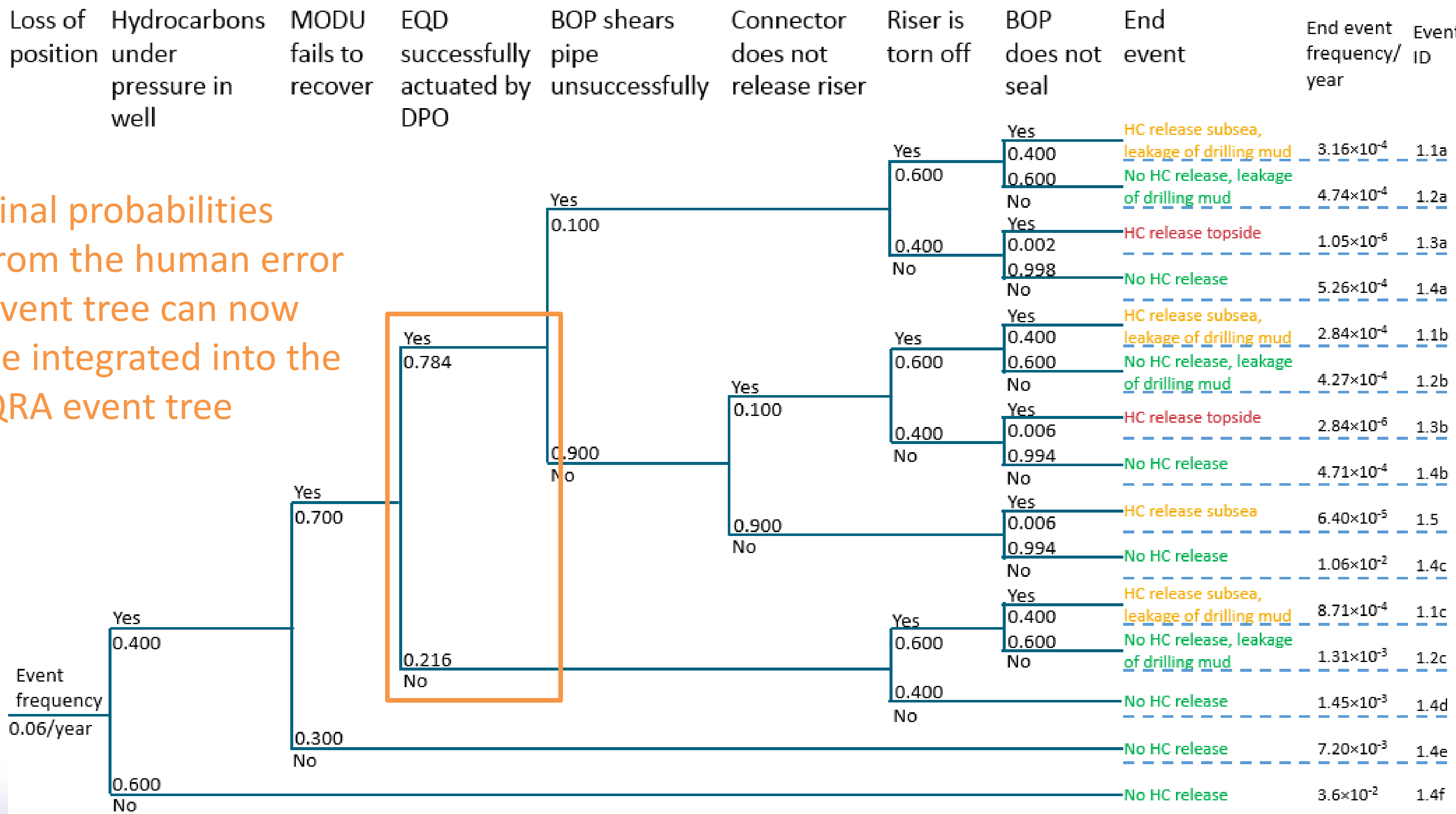


Impact assessment

- Integration of HEP into overall risk model
- Consideration of impact assessment criteria
  - Risk acceptance criteria
  - Size of HEP value(s), >0.1
  - Degree of HEP uncertainty
  - Severe QRA end states
- Assessment of HEP contribution

Integrate results into QRA

Final probabilities from the human error event tree can now be integrated into the QRA event tree



PetroHRA The Research Council of Norway Statoil IFE NTNU – Trondheim Norwegian University of Science and Technology DNV·GL SINTEF INL Idaho National Laboratory

Error reduction analysis

- Select events for risk reduction
- Re-visit performance shaping factors
- Develop ERMs targeting specific human errors
- Develop ERSs targeting overall task performance
- Recalculate HEPs based on updated PSF justifications

Select events for risk reduction

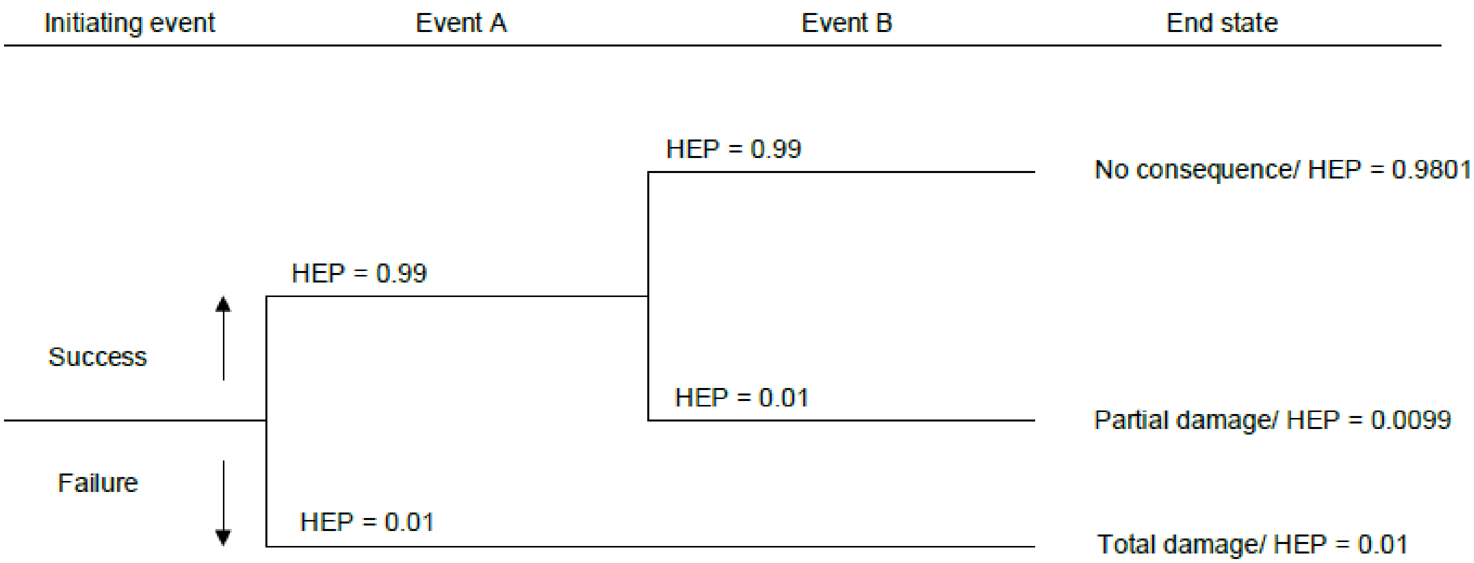


Figure 7.2 Event tree with example quantifications

For event trees, events are selected based on three combined considerations:

1) the HEP for each single event
2) the HEP for end states associated with each event sequence pathway
3) the severity of end states for each event sequence pathway the events are part of

Re-visit performance shaping factors

- Purpose is to demonstrate risk reduction
  - Establish traceability between the PSF evaluations, calculated HEPs and suggested ERMs and/or ERSs
- Re-check which PSFs are performance drivers
- Error Reduction Measures (ERM) and Error Reduction Strategies (ERS) can target (reinforcing) positive PSFs as well as targeting (improving) the negative PSFs

Develop ERM & ERS

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

} ERM

- Overall task re-design
- Overall PSF improvement

} ERS

Developing ERM & ERS - example

Loss of position (drive off) scenario – main performance drivers

Time

Problem: The whole scenario takes place in under 2 minutes but cannot “create” more time without redesigning the entire rig.
Long-term ERS: Provide feedback to engineers & designers for future installation builds.

HMI

Problem: Non-optimal design & layout of the workstation – esp. thruster shutdown.
Intermediate ERM: Add a single emergency stop button to shutdown all thrusters at the same time.
Long-term ERS: Provide feedback to engineers & designers for future installation builds.

Training

Problem: DPOs receive no continuous training on hos to respond to a drive off event.
Intermediate ERM: DPOs should receive simulator training at least X times per year .
Short-term ERM: DPOs should receive onsite training (desktop exercises) at least X/year

Procedures

Problem: No procedure detailing the appropriate order of response actions in a drive off scenario.
Short-term ERM: Develop an appropriate operating procedure to clarify the required response actions (reinforced by training).

Update HRA/QRA model

HRA

- Document justifications (Petro-HRA sheet)
- Re-calculate HEPs for each event and model

QRA

- Integrate HFE HEP in QRA model
- Re-calculate QRA to check for effects

Document the HRA

- All analysis outputs; ensure traceability
  - Scenario description
  - PSF assessment
  - Task and timeline analysis
  - Human error identification
  - Human error model, incl. summary table
  - Human error quantification, incl Petro-HRA sheets
  - Impact assessment and error reduction analysis

Thank you!

Sondre Øie (Sondre.Oie@dnvgl.com)
Claire Taylor (Claire.Taylor@ife.no)