Statoil

Human Reliability Analysis of safety critical actions in high-risk scenarios – an introduction

Jan Tore Ludvigsen, Statoil

Xuhong He, Scandpower

April 10, 2013
ESRA Norge

Content

- Human as a Safety Barrier

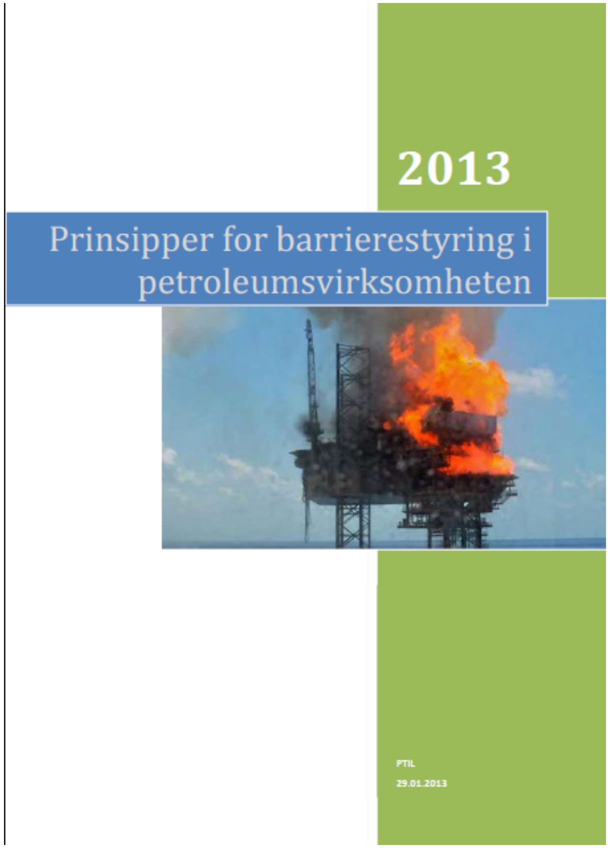
- Human Reliability Analysis

- Case Study
  - Dynamic Positioning Operator in the Drive-off Scenarios

PSA priority, 2013

Constant challenges are faced in relation to well integrity, gas leaks, and aging installations and plants:

- Ensure robust **technical, operational and organisational barriers**. This is crucial for preventing accidents and reducing risk.
- The PSA sees a need for better understanding of the interaction between operational, organisational and technical elements in barriers.



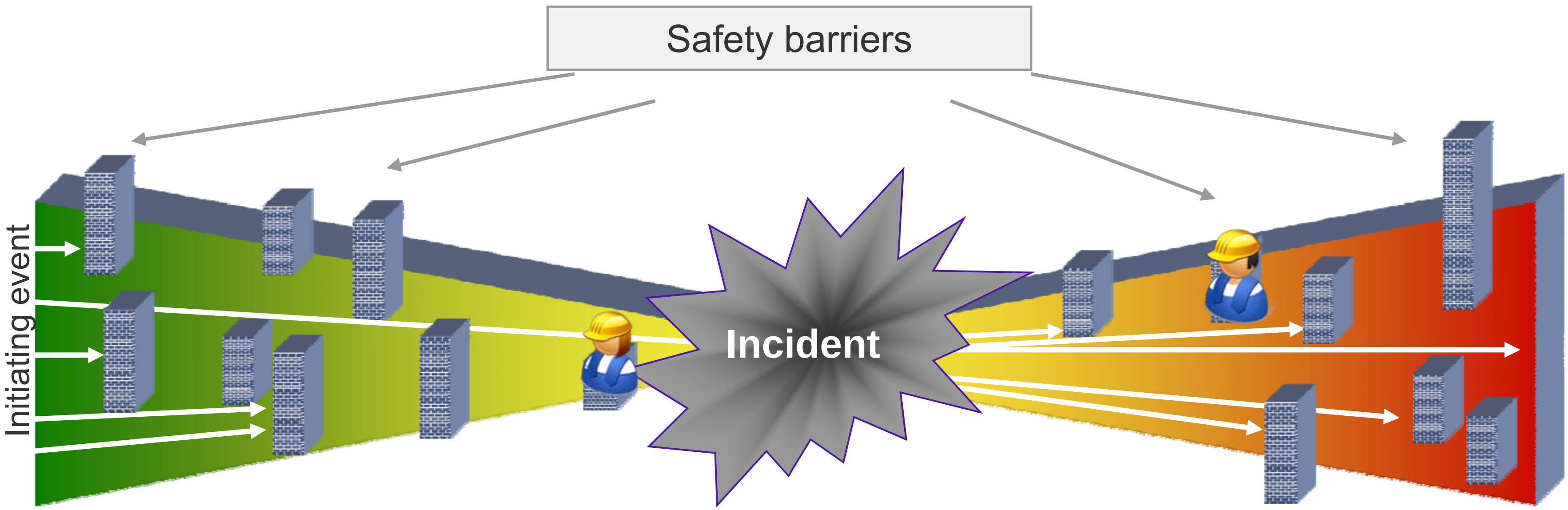
Industry need

- The concept of technical safety barriers is well established within the petroleum industry (PSA, 2012)

- Lack of proven concepts and methods to assess, quantify and manage human contribution to safety barriers

- Explore Human Reliability Analysis (HRA) as a tool to identify, assess and quantify “safety critical actions in high-risk scenarios”

Human reliability in high-risk scenarios



Barriers to ***prevent***

Barriers to ***reduce the consequence***

Ref. OGP report, 2011 p6: “*Critical human tasks are defined as those activities people are expected to perform as barriers against the occurrence of an incident, or to prevent escalation in the event an incident does occur. They include activities required to support or maintain physical and technological barriers”.*

Human Reliability Analysis

- **Aim**: to assess and predict the reliability of human performing safety critical tasks
- **Origin**: Human Reliability Assessment (HRA) originally developed for nuclear Probabilistic Risk Assessment (PRA) or Probabilistic Safety Assessment (PSA)
- **Steps**:

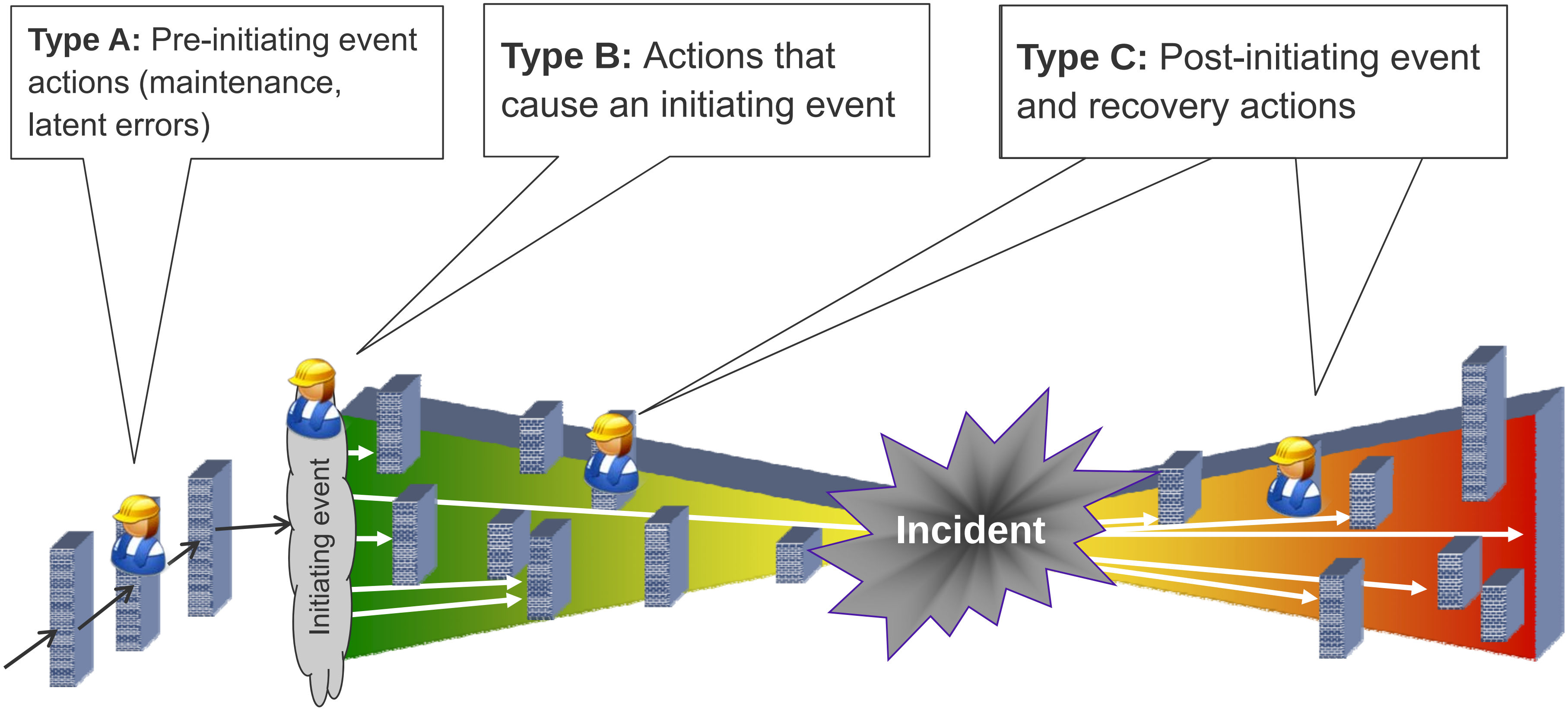
Identity risk scenario and safety critical human tasks

Assess: qualitative task analysis & performance shaping factors

Quantify: Human Error Probability

Mitigate: if risk for human error is unacceptable, compensating measures to be implemented

Safety critical human actions

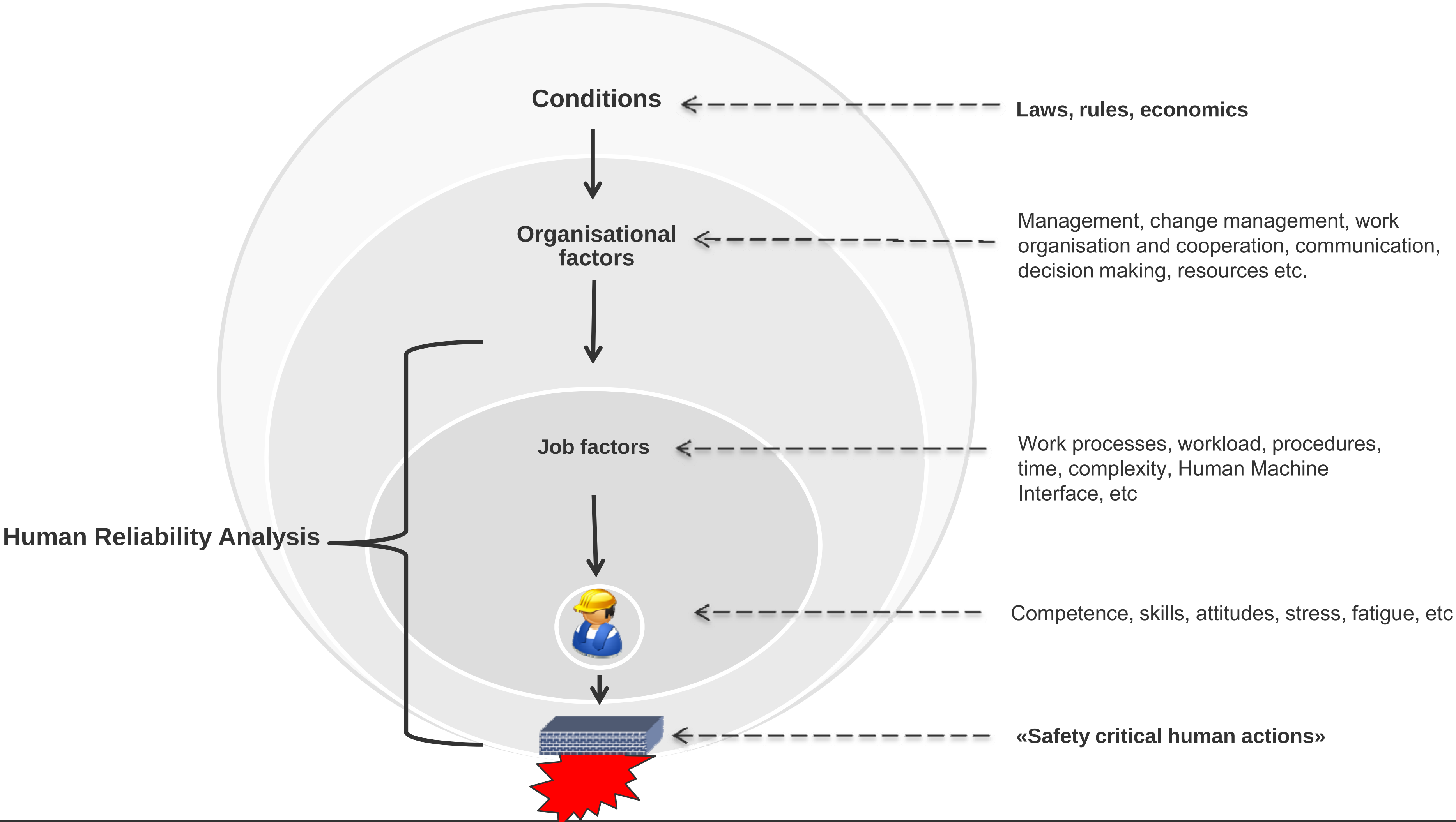


HRA in petroleum

- HRA applied to safety cases or scenarios where human performance are safety critical
  - Examples: flotel operations, drilling, well control, LNG fillling operations, stability scenarios, manual depressurisation
- SPAR-H (Standardized Plant Analysis Risk-Human Reliability Analysis, 2004) considered a reliable, easy-to-use method for human reliability analysis. (Boring & Blackman, 2007)
- HEART (Human Error Assessment and Reduction Technique, 1988)

Statoil

Human and organisational factors



There's never been a better time for good ideas

Jan Tore Ludvigsen
Principal Consultant,
Human Factors & Organisational Safety
Department for Technical and Operational Safety

Human Reliability Analysis of safety critical actions in high-risk scenarios - A Case Study

Xuhong He, Scandpower
Jan Tore Ludvigsen, Statoil

April 10, 2013
ESRA Norge

SCANDPOWER
Risk Management
A member of the Lloyd's Register Group

Lloyd's Register
LIFE MATTERS

History for HRA

- HF study: designer concerned with people how to read instruments accurately
- HF study: Radar stations operators distinguish transcontinental rockets from disturbances, Atomic bomb production
- 1975, WASH 1400 - 1st PRA where HRA was included
- 1980, draft ‘Handbook’ THERP approach
- 1981, 1st IEEE conference on human factors in nuclear power plants
- 1983, Final Version of ‘Handbook’ included TRC
- 1984, SLIM (David Embrey et al.), based on PSFs
- 1985, HEART(Jerry Williams), based on PSFs and error prediction coefficients
- 1985, HCR (Hannaman, Spurgin and Lukic), based on simulator
- 1988, ASEP method
- 1990, HCR/ORE, EPRI simulator data collections
- 1990, Cause-based Decision Tree(EPRI)

1990s Birth of 2nd generation HRA Techniques

- 1998, CREAM by Hollnagel Erik
- 1999, MERMOS by LeBot et al, EFD
- 2000, ATHEANA by USNRC

HRA In Railway

- Focus on the qualitative HF studies:
  - Scandpower (UK, Norway, Sweden, etc.) performed many studies, e.g.
    - Human Machine Interface (HMI) assessments
    - Alarm management and rationalization
    - Physical and environmental ergonomics
    - Workload and stress related to safety critical roles - to assess staff workload and work-related stress within the operational organization
    - Assessment of shift work rosters and fatigue - to assess shift rosters and the incidence of fatigue across operational and maintenance departments
- Some HRA quantification studies were performed, e.g.
  - British Rail Standards and Safety Board (Gilroy & Grimes 2007) adapted the generic HEART (Williams 1985) method for the railway domain
  - HEART method was performed in the driver actions in the collision accident.
- On-going PhD project supported by LR Foundation in Imperial College London: A Human Reliability Analysis (HRA) Technique to improve Railway Safety

Case Study: Dynamic positioning (DP) operator response to the drive-off scenario in DP Vessel

- A situation where active thruster forces driving the vessel away from its target position.
  - a wrong target position being used in DP-controller, so that the DP-controller demands *abnormal* thrust to drive vessel to a wrong target posi-tion.
  - one or several failed thrusters which generate *abnormal* thrust

- Once drive-off happens, the DP operator should detect the situation, and perform evasive maneuvering to arrest the vessel movement.

Drive-off Scenario

Drive-off → Technical system responses / Human responses → Consequences

SCANDPOWER
Risk Management

A member of the Lloyd's Register Group

Lloyd's Register
LIFE MATTERS

DP console

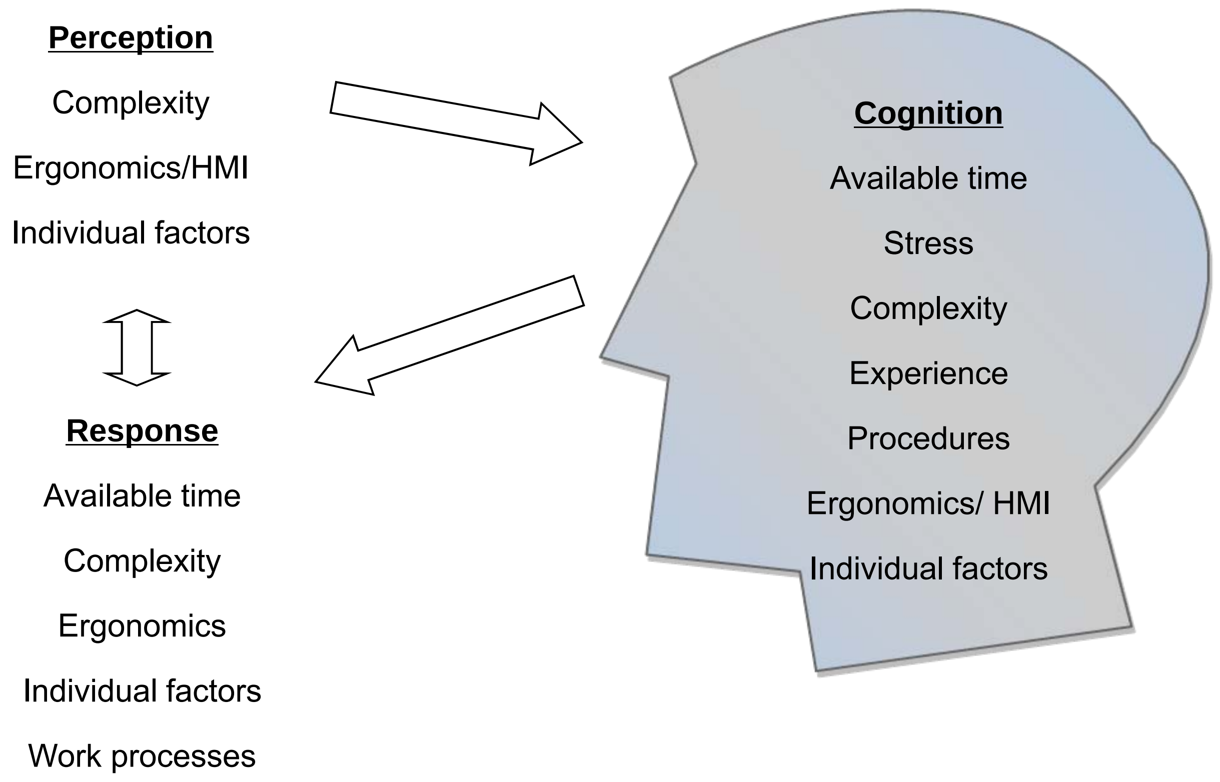
HRA Process

- The main purpose of the human reliability analyses is to estimate the human error probabilities (HEPs) of the DP operator actions not being taken when needed in the drive-off and drift-off scenario.
- As an important part of the HRA, a qualitative task analysis is performed to evaluate the contexts under which the operator actions are taken. The task analysis includes both the time lines of the scenario, human actions, and the 'driving' performance shaping factors (PSFs).
- Recommendations are made to improve the human performance in these scenarios.

Time Line Task Analysis

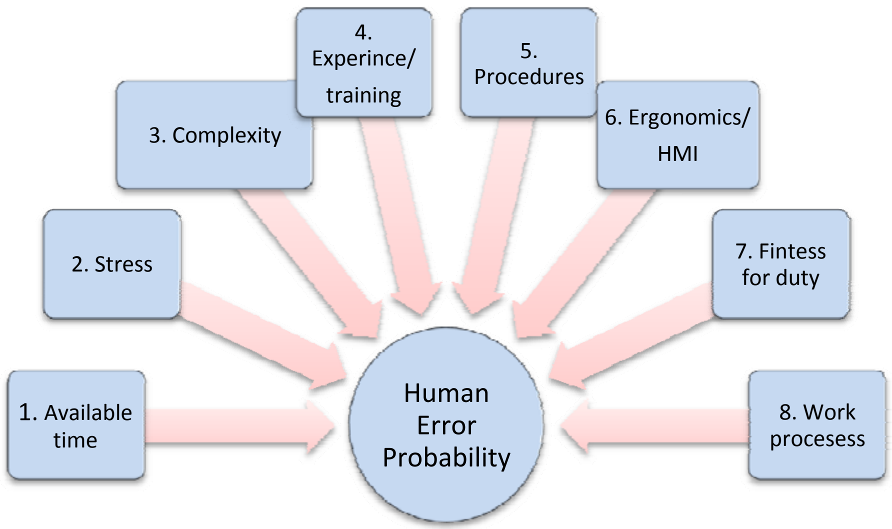
Time [s]		Position [m] from normal	Alarms/indicators	How	DP Operator tasks
			Most or all thrusters aligning to the same direction as external forces		As usual situation: DP operators are always on duty to monitor the DP system
			Insufficient thruster¤	Warning	
0*	0**	0	Power demand reduced alarm¤	Red with audible	
11*	16**	2	Out of position warning	Yellow with audible	1. Recognize the drive-off. Try to stop vessel movement and restore position. 2. If drive-off is severe enough, walk over to the K-trust panel 3. Change operation to the C-joy (IJS-Independent Joystick System) by pushing double button 4. Enable the C-joy (if system is in stand-by mode) by pushing double button 5.Put thrusters in reverse 6. Advisory to OIM/Client, by the DPO not operating the DP system Note: The C-joy incorporates all the levers on one joystick. The C-joy is independent of the DP system.
17*	23**	3	Out of position alarm	Red with audible	
20*	25**	4	Gangway with predefined warning	Warning	
22*	27**	5	Gangway red alarm	Red light + audible alarm	
24*	29**	6.5	DP exceeding fatal limits	Red with audible	
25*	31**	7	Gangway autolift	view through the window	
45*	58**	40			

Human Reliability Analysis (HRA): SPAR-H



SPAR-H (Standardized Plant Analysis Risk-Human Reliability Analysis)

- Calculation of human error probability (HEP) rates is straightforward, starting with pre-defined nominal error rates:
  - *Processing/Diagnosis:* Nominal HEP = 1E-2
  - *Response/Action:* Nominal HEP = 1E-3
- Eight PSFs with multipliers typically corresponding to degraded or enhanced human performance for individual PSFs.



SPAR-H Worksheet

Diagnosis

PSFs	PSF Levels	Multiplier for Diagnosis	Please note specific reasons for PSF level selection in this column.
Available Time	Inadequate time	P(failure)=1	Nominal diagnosis time is 20 seconds until the Floatel moved away from original position 4 meters in bad weather condition. The available time for diagnosis is about 30-35 seconds.
	Barely adequate time（=2/3 x nominal）	10	
	Nominal time	1 √	
	Extra time(between 1 and 2 x nominal and >30 min)	0.1	
	Expansive time(>2 x nominal and >30 min)	0.01	
	Insufficient information	1	
Stress/Stressors	Extreme	5	Stress is high. Several alarms indicate that something very rare and serious is happening.
	High	2 √	
	Nominal	1	
	Insufficient Information	1	
Complexity	Highly complex	5	Obvious to recognize the drive-off situation with several alarms and the visual view of the gangway to the nearby platform.
	Moderately complex	2	
	Nominal	1 √	
	Obvious diagnosis	0.1	
	Insufficient Information	1	
Experience/Training	Low	10	DP operators have been through the formal training process and been certified from the authorized institute. It is also anticipated that it will be an experienced DP operator that is working in the Floatel when the situation occurs, so even though will not be a routine situation this is what the DP operator are there for, to supervise that nothing unusual happens and to take actions if it does.
	Nominal	1 √	
	High	0.5	
	Insufficient Information	1	
Procedures	Not available	50	Procedures are not considered to be a driving PSF for diagnosis for this scenario since it requires diagnosis to take place within a very short time frame.
	Incomplete	20	
	Available, but poor	5	
	Nominal	1 √	
	Diagnostic/symptom oriented	0.5	
	Insufficient Information	1	
Ergonomics/HMI	Missing/Misleading	50	Several screens and alarms are available in the close vicinity of the DP operator. This together with the visual view of the gangway and nearby platform motivates that this PSF is considered to be nominal.
	Poor	10	
	Nominal	1 √	
	Good	0.5	
	Insufficient Information	1	
Fitness for Duty	Unfit	P(failure)=1	Active DP operator is shifted every hour. No fatigue is noticed by the DP operator.
	Degraded Fitness	5	
	Nominal	1 √	
	Insufficient Information	1	
Work Processes	Poor	2	Not a driving PSF in the scenario. Safety culture is considered as good. The active DP operator also has some back-up by the stand-by DP operator who is not allowed to leave the bridge except for very short brakes.
	Nominal	1 √	
	Good	0.8	
	Insufficient Information	1	

Final Diagnosis HEP	2.00E-02

SPAR-H Worksheet

Action

PSFs	PSF Levels	Multiplier for Action	Please note specific reasons for PSF level selection in this column.
Available Time	Inadequate time	P(failure)=1	The required action time is about 5-10 seconds. Total available time for diagnosis and action is about 40 seconds based on the drive-off scenario No.38. Taken into account that the diagnosis time will be ~20 seconds this gives that the available time will sufficient for the DP operator to move to the control panel where the C-joy is located and perform the necessary actions.
	Time available is =the time required	10	
	Nominal time	1 √	
	Time available>=5x the time required	0.1	
	Time available is >=50x the time required	0.01	
	Insufficient Information	1	
Stress/Stressors	Extreme	5	Stress is high with several alarms and a very serious situation. However, once the diagnosis has been made there are no questions about what action that should be taken; neither does any conflict of interest prevail.
	High	2 √	
	Nominal	1	
	Insufficient Information	1	
Complexity	Highly complex	5	The actions are not complex, comparable to a few simple maneuvers in sequence (walk to K-trust panel, change operation to C-joy, enable C-joystick and put in reverse)
	Moderately complex	2	
	Nominal	1 √	
	Insufficient Information	1	
Experience/Training	Low	3 √	The DP operator has good knowledge and skills to manipulate the C-joy and lever. However specific training or experience to response quickly in a short time frame is missing.
	Nominal	1	
	High	0.5	
	Insufficient Information	1	
Procedures	Not available	50	DP Operation manual contains specific faults and required operator actions. Switch-over to C-joy is covered in the operating manual. However a short and clear specific procedure on what kind of actions should be taken would also helps in this situation.
	Incomplete	20	
	Available, but poor	5 √	
	Nominal	1	
	Insufficient Information	1	
Ergonomics/HMI	Missing/Misleading	50	The layout of the display screens, push buttons and C-joy stick is general good. However during the workshop there were discussions about the C-joystick is quite small, maybe not easy to manipulate rapidly in this situation. It is not a driving PSF.
	Poor	10	
	Nominal	1 √	
	Good	0.5	
	Insufficient Information	1	
Fitness for Duty	Unfit	P(failure)=1	Active DP operator is shifted every hour. No fatigue is noticed by the DP operator.
	Degraded Fitness	5	
	Nominal	1 √	
	Insufficient Information	1	
Work Processes	Poor	5	Not a driving PSF in the scenario. Safety culture is considered as good.
	Nominal	1 √	
	Good	0.5	
	Insufficient Information	1	

Final Action HEP	2.92E-02

HRA-based safety insights

- Once drive-off happens, the failure probability of the DP operator (barrier) can be high
  - The available time is a key driving factor
- HRA results were used as inputs to the QRA to check the risk level
- Recommendations were made
  - Better estimate the available time and the required time
  - Collect operator response information through simulators
  - Develop a specific training program and include in the regular training
  - Develop a symptom based emergent procedure for drive-off scenario

Based on the study, it is necessary to consider to introduce an additional technical barrier for drive-off situation

Human reliability in barrier management?

- We are relying upon successful human performance of safety critical actions to prevent or reduce the escalation of unwanted events or accidents
- HRA can be applied to identify, asses and quantify these safety critical human actions
- Without addressing human factors as part of management of safety barriers, risk control is not accomplished

⇒ The potential use of HRA in the management of safety barriers should be explored further

Discussions

- HRA is a relatively new approach within oil & gas industry, and is still under development
- No available methods are tailor made for the industry, thus HRA has its limitations with regard to precision level
  - SPAR-H method was developed for nuclear industry
- HRA is an essential part of the quantitative risk analysis
- HRA should be considered as one of the several tools that can improve our understanding of human as a barrier / barrier management

For more information, please contact:

Xuhong He
Principal Consultant

Scandpower AB

T +46 703771447
E xhe@scandpower.com
W www.scandpower.com
www.lr.org

SCANDPOWER
Risk Management

A member of the Lloyd's Register Group

Lloyd's Register
LIFE MATTERS