RAPPORT

HFC – forum for human factors in control

Postadresse: 7465 Trondheim
Besøksadresse: S P Andersens veg 5
7031 Trondheim
Telefon: 73 59 03 00
Telefaks: 73 59 03 30

TITTEL

Safety analysis and major accidents – how to include human and organisational elements;
resultater fra HFC forum, 17. til 18.oktober 2012. (Møte nr 16)

FORFATTER/REDAKTØR

Stig Ole Johnsen

OPPDRAGSGIVER(E)

HFC forum

RAPPORTNR.	GRADERING	OPPDRAGSGIVER	
SINTEF A23545	Åpen	Arne Jarl Ringstad/Statoil ASA	
GRADER. DENNE SIDE	ISBN	PROSJEKTNR.	ANTALL SIDER OG BILAG
Åpen	978-82-14-05508-5	60S011	194
ELEKTRONISK ARKIVKODE		PROSJEKTLEDER (NAVN, SIGN.)	VERIFISERT AV (NAVN, SIGN.)
eRoom/civil/504017CRIOPUserGroup/0_2ffb7		Stig Ole Johnsen	Lars Bodsberg
ARKIVKODE	DATO	GODKJENT AV (NAVN, STILLING, SIGN.)	
	26/10-2012	Arne Jarl Ringstad/Statoil ASA	

SAMMENDRAG

Denne rapporten dokumenterer presentasjoner, relevante artikler, agenda og deltakerliste fra HFC forum møtet den 17. til 18.oktober 2012 i Halden. Det er møte nummer 16 i regi av HFC forum. De vedlagte presentasjonene er fra:

A. Bye	Introduction, safety analysis in complex industries.
P. LeBot	HRA in the human factor engineering process.
A. Balfour	Introduction to Human Factors, methods and theory.
K. Gould; K.van de Merwe	Human reliability analysis in major accident risk analyses in the Norwegian petroleum industry: applying SPAR-H.
Ø. Lauridsen	Barrier Management - Technical, operational and organizational barrier elements, is it possible to define performance requirements? A regulators perspective.
R. Boring	Lessons learned from HRA in the US space program.
K. Hansen	The Petroleum Safety Authority has accused Statoil for lacking the ability to learn - are they right?
U.Kahlbom	Lessons and experiences from applying human reliability analysis in the Swedish nuclear industry.
J.E. Vinnem	Reflections on the recent serious events in the offshore oil and gas sector from a risk assessment perspective with focus on human and organizational factors.
S. Hauge	Barrier management in the PDS project.
K. Lauman	Informasjon om vårt prosjekt i Petromaksprogrammet

STIKKORD	NORSK	ENGELSK
GRUPPE 1	Menneskelige faktorer	Human factors
GRUPPE 2	ISO 11064	ISO 11064
EGENVALGTE	Sikkerhet	Safety

INNHOLDSFORTEGNELSE

1 Evaluering av møtet og innspill fra møtedeltakerne

1.1 Innledning

I denne rapporten gis en oppsummering av HFC møtet den 17.-18.oktober i Halden med presentasjoner, relevante fagartikler (”papers”), oppsummering av evaluering fra deltakerne og liste over alle deltakere.

I det nedenstående har vi oppsummert fra de skriftlige evalueringene som deltakerne leverte inn.

1.2 Evalueringer

Valg av tema og foredragsholdere ble positivt mottatt ut fra en deltakelse på over 60 påmeldte. Samlet sett ble presentasjonene positivt motatt. Balansen mellom diskusjoner, presentasjoner og pauser synes å være bra. Første dag ble litt lang, men fra tilbakemeldingene synes seminaret under ett å være et godt møte, selv om HRA metodene oppfattes som tunge og utfordrende å bruke. Det var derfor nyttig med en viss temabredde i presentasjonene.

Det virker som om formen på møtene, dvs over to dager med hyppige pauser mellom forelesningene, fungerer bra. De fleste forelesningene, paneldiskusjonen og muligheten for å diskutere i et fagnettverk ble trukket frem positivt. Studentene satte stor pris på å kunne delta. Det ble oppfattet som noe uheldig at et marginalt antall personer (2) ikke forstår norsk, så må over 60 deltakere fra Norge bruke engelsk. Det gir en demper i engasjement og innlevelse fra sal og foredragsholdere.

Paneldiskusjonen ble oppfattet som spennende.

Forumet er bredt med mange forskjellige deltakere, og utfordringen er å gi alle noe. Vi får derfor mange forskjellige innspill, alle konstruktive og gode kommentarer som bidar til å påvirke møteform og møteinnhold.

1.3 Formen på HFC møtene

Tilbakemeldingene er generelt positive til formen på møtene. Det ble påpekt at det var viktig med tid til debatterog pauser slik at det blir tid til å utveksle erfaring med andre. Sunn mat i de fleste pausene var et ønske, dvs frukt og noe som kan gi energi.

1.4 Samarbeid med HFN i Sverige

Det norske HFC forumet har et godt løpende samarbeid med human factors nettverket (HFN) i Sverige. Medlemmer fra HFN deltar aktivt på HFC møtene og de inviterer medlemmer i HFC til sine seminarer og møter. Aktuelle HFN samlinger kan være:

- "HFN-CRM-seminarium", Linköpings universitet, Sverige 18-19. oktober. For ytterligere informasjon se http://www.humanfactorsnetwork.se

1.5 Tema og forelesere til de neste HFC møtene

Av tema som ble trukket frem som spesielt interessante til neste møte, kan nevnes:

- Etikk og sikkerhet – kanskje et innlegg fra J.E.Vinnem. Et tilgrensende område er risikokommunikasjon – hvor Prof. B.M.D.Sjøberg kan være aktuell.
- Mer om kvalitative metoder som kan benyttes innen Human Factors området.
- Erfaringer fra fjernstyring av bemannede og ubemannede plattformer. Bl.a. Human factors utfordringer knyttet til økt grad av ubemannede platformer og fjernstyring - bruk av CCTV.
- Mer om Crew Resource Management (CRM) – hva er viktige områder – hva er erfaringene og hva bør vi fokusere på videre? Delt situasjonsforståelse i distribuerte tverrfaglige team - hva er konsekvenser for organisering, trening (CRM), utforming av kontrollrom og løsninger. Diskusjon av CRM kompetanse for alle innen Olje.
- Hvordan ulike disipliner tilnærmer seg oppgaven å designe for sikkerhetskritiske miljø. Tema som går på tvers av disipliner– det blir ofte enten et rent teknisk perspektiv eller et psykologisk perspektiv.
- Utforming av interaksjon mellom menneske og maskin – Human Machine Interface (HMI). Spesielt fokus på utforming av informasjonssystemer og utforming av alarmer.
- Grensesnitt mellom full automatikk og menneskelig intervensjon. Bruk av Cognitive engineering.Ledelse og styring (etterlevelse av regelregime) – diskusjoner av flere dilemma knyttet til sikkerhet. Hvordan påvirker ledelse or organisatoriske forhold ytelsen til barrierene?
- Human factors standarder utenfor kontrollrommet.
- Foreslår et opplegg fra Keil-senteret. De har hatt et todagerskursopplegg for Statoil med vekt på HF metoder. Jeg forstår at det evt vil bli et annerledes opplegg, men tror det vil være veldig spennende og aktuelt for mange.
- Gjennomgang av noen gode "case" - Hva skjedde på Scarabeo 8 høsten 2012 da den fikk slagside, var det en feiloperasjon i forbindelse med ballastering? I den sammenheng trekk inn erfarne operatører som har vært med på noen hendelser og som kan fortelle hva som gikk bra/dårlig – og hvordan/hvorfor operatørene tar feil valg/beslutninger i en kritisk situasjon. Det hadde vært veldig interessant perspektiv og ikke bare fått teori.

Av nye forelesere ble følgende ønsket til neste møtet. (Listen inneholder navn som har vært trukket frem tidligere uten at de har fått plass):

- En operatør, eksempelvis en plattformsjef som presenterer sin hverdag.
- Ron Westrum - Two faces of resilience - requisite imagination & the human .issues.
- M.Endsley (Situational awareness).
- E. Hollnagel, R. Woods, J. Reason, C. Weick, K. Haukelid, Cato Bjørkli, Frode Heldal eller Stig O. Johnsen. Fra Telenor eller DNV f.eks Nalini Suparamaniam-Kallerdahl fra DNV.
- Presentasjoner fra andre industrier
- Gary Klein, Gorry, (Decision Making)
- J.Frohm (f.eks. automasjon eller lean production).
- G.R. Hockey fra Univ of Leeds, Mark Young.
- Fra miljøer som: Fraunhofer FKIE (Tyskland) eller MIT User Interface Design Group (USA).
- Interessant å utvide HF mot community of practice og praksisfellesskap som J.S.Brown, P.Duguide - eks. hvordan mobiliserer man et praksisfellesskap?

1.6 Kurs og forelesninger innen human factors

Ved NTNU arrangeres et innføringskurs innen human factors i vårsemesteret 2013, se: videre.ntnu.no/link/nv13119

1.7 Kontakt opp mot Human Factors fagnettverket i Europa og USA

For de som er interessert i faglig kontakt opp mot Human Factor nettverket i Europa og USA viser vi til: *www.hfes-europe.org* – som er den europeiske Human Factors and Ergonomics Society. HFES er tilknyttet den internasjonale Human Factors and Ergonomics Society, Inc. Se *www.hfes.org*.

1.8 Noen bilder fra HFC møtet

Vedlagt følger noen bilder fra møtet.

P. Le Bot/ EDF

K.Hansen/IRIS

Paneldiskusjonen

IFE HAMMLAB

2 Agenda og deltakerliste

2.1 Agenda for HFC møtet

Vedlagt ligger agenda for HFC møtet.

Dag 1	Innlegg og diskusjon	Ansvar
11.00-12.00	Lunsj.	IFE
12.00-12.30	Velkommen til seminaret og runde rundt bordet.	
12.30-13.00	Introduction, safety analysis in complex industries.	A. Bye/ IFE
13.00-13.45	HRA in the human factor engineering process.	P. LeBot/ EDF
13.45-14.15	Diskusjon og pause.	
14.15-14.30	Kursinfo – Introduksjon til Human Factors	A. Balfour/ HFS
14.30-15.00	Human reliability analysis in major accident risk analyses in the Norwegian petroleum industry: applying SPAR-H	K. Gould/ Statoil; K. van de Merwe/ DNV
15.00-15.30	Diskusjon og pause.	
15.30-16.00	Barrier Management - Technical, operational and organizational barrier elements, is it possible to define performance requirements to operational and organizational barrier elements? A regulators perspective.	Ø. Lauridsen/ Ptil
16.00-16.15	Diskusjon og pause	
16.15-16.45	Lessons learned from human reliability applications in the US space program.	R. Boring/ Idaho National Laboratory
16.45-17.15	Diskusjon og pause.	
17.15-17.45	The Petroleum Safety Authority has accused Statoil for lacking the ability to learn - are they right?	K. Hansen/ IRIS
17.45-18.00	Diskusjon og pause.	
18.00-18.30	Lessons and experiences from applying human reliability analysis in the Swedish nuclear industry.	U.Kahlbom/ Riskpilot
18.30-18.45	Diskusjon og pause.	
19.30-	Middag - Haldens Klub.(Kart lagt ut i auditoriet)	

Dag 2	Innlegg og diskusjon	Ansvar
08.30-09.00	Kaffe og noe å bite i.	
09.00-09.45	Reflections on the recent serious events in the offshore oil and gas sector from a risk assessment perspective with focus on human and organizational factors.	J.E. Vinnem/ UiS
09.45-10.00	Diskusjon og pause.	
10.00-10.30	Barrier management in the PDS project, PDS- Reliability of safety instrumented systems.	S. Hauge/ Sintef
10.30-10.45	Diskusjon og pause.	
10.45-11.45	Paneldiskusjon: What does quantification add to other types of safety analysis? How can broader, organisational or industry-specific factors be included?	Le Bot, Gould, Vinnem, Boring, Lauridsen, ordstyrer: A. Bye
11.45-12.00	Diskusjon og pause.	
12.00-12.30	Informasjon om Petromaks, avslutning og oppsummering.	K. Laumann/NTNU,HFC
12.30-13.30	Lunsj.	IFE
13.30-14.00	Omvisning Future Lab v/IFE.	IFE

2.2 Påmeldte og deltakere

Nedenstående tabell lister opp påmeldte og deltakere i HFC møtet.

Bedrift	Etternavn	Fornavn	E-post
ABB AS	Graven	Tone Grete	tone-grete.graven@no.abb.com
Adept Solutions	Lindaas	Ole A.	ole.a.lindaas@gmail.com
Adept Solutions	Sætre	Tor Inge	toringe@adeptsolutions.com
Agility Group	Borén	Maria	mbo@agilitygroup.no
Agility Group	Moe	Anne Katrine	akm@agilitygroup.no
Aker Solutions MMO AS	Hovstad	Frøydis H.	froydis.hovstad@akersolutions.com
BG Norge	Heber	Hilde	hilde.heber@bg-group.com
Chalmers Tekniska Högskola	Salomonsson	Eva	evas@chalmers.se
CIRiS, NTNU Samfunnsforskning	Danielsen	Brit-Eli	brit-eli.danielsen@ciris.no
CIRiS, NTNU Samfunnsforskning	Fossum	Knut R.	knut.fossum@ciris.no
CIRiS, NTNU Samfunnsforskning	Stene	Trine M.	trine.stene@ciris.no
ConocoPhillips	Gunvaldsen	Bjørn V.	bjoern.v.gunvaldsen@conocophilips.com
ConocoPhillips - Drift	Lid	Øystein	Oeystein.Lid@conocophillips.com
Denmark Technical University	Duijm	Nijs Jan	nidu@dtu.dk
Det Norske Veritas	Hellesøy	Bjørn Tore	bjorn.tore.hellesoy@dnv.com
Det Norske Veritas	Sæternes	Snorre	snorre-saternes@dnv.com
Det Norske Veritas	van de Merwe	Koen	koen.van.de.merwe@dnv.com
Det Norske Veritas	Walsøe Pettersen	Solveig	solveig.pettersen@dnv.com
Det Norske Veritas	Øie	Sondre	sondre.oie@dnv.com
EDF France	Le Bot	Pierre	pierre.le.bot@edf.fr
Future Subsea AS	Røed	Bjarte	bjarte@futuresubsea.no
HF and UI Standards	Andersen	Heidi	heidi.andersen@nov.com
HMS Design & Utvikling AS	Holter	Anne	anne.holter@hms-du.no
HMS Design & Utvikling AS	Liu	Yuanhua	yuanhua.liu@hms-du.no
Human Centred Design	Green	Mark	mark.green@hcd.no
Human Centred Design	Green	Marie	marie.green@hcd.no
Human Factor Solutions	Balfour	Adam	adam@hfs.no
Idaho National Laboratories	Boring	Ronald	ronald.boring@inl.gov
INERIS	Fabre	Damien	damien.fabre@ineris.fr
Institutt for energiteknikk	Bye	Andreas	andreas.bye@htrp.no
Institutt for energiteknikk	Collier	Steve	steve.collier@hrp.no
Institutt for energiteknikk	Laumann	Karin	karin.laumann@svt.ntnu.no
Institutt for energiteknikk	Massaiu	Salvatore	salvatore.massaiu@hrp.no
IRIS	Hansen	Kåre	kaare.hansen@iris.no
Lundin Norway AS	Halden	Ola Vebjørn	ola.halden@lundin-norway.no
MTO Säkerhet AB/HFN Sverige	Obenius Mowitz	Aino	aino.mowitz@mto.se
NTNU	Rasmussen	Martin	martin.rasmussen@samfunn.ntnu.no
NTNU	Standal	Martin Inge	martinin@stud.ntnu.no
NTNU. Psykologisk Institutt	Sætren	Gunhild	gunhild.saetren@svt.ntnu.no
Petroleumstilsynet	Lauridsen	Øyvind	oyvind.lauridsen@ptil.no
Petroleumstilsynet	Løland	Grete	grete-irene.loland@ptil.no
Risk Pilot MTO AB	Kahlbom	Ulf	ulf.kahlbom@riskpilot.se
Safetec Nordic	Hynne	Tuva	tuva.hynne@safetec.no
Safetec Nordic	Krasniqi	Luftar	lkr@hrgroup.se
Safetec Nordic	Westvik	Astrid L.	astrid.lovise.westvik@safetec.no
Scandpower AS	Giskegjerde	Georg	ggi@scandpower.com
Scandpower AS	Sørensen	Linda	lso@scandpower.com
Scandpower AS	van de Merwe	Fenna	fvn@scandpower.com
Scandpower AS	Aaen-Stockdale	Craig	Craig.Aaen-Stockdale@akersolutions.com
Siemens	Aarskog Lund	Endre	endre-aarskog.lund@siemens.com

Siemens Oil & Gas Offshore	Gundersen	Pål	p.gundersen@siemens.com
SINTEF	Hauge	Stein	stein.hauge@sintef.no
SINTEF	Johnsen	Stig Ole	stig.o.johnsen@sintef.no
Sintef	Paltrinieri	Nicola	nicola.paltrinieri@sintef.no
SINTEF	Tinmanssvik	Ranveig K.	ranveig.k.tinmannsvik@sintef.no
Sintef	Wærø	Irene	irene.waro@sintef.no
SMSC AS	Aursø	Egil	egil@smsc.no
SMSC AS	Sund	Pål	paal@smsc.no
Statoil	Fröde	Anna Karin	annaf@statoil.com
Statoil	Glittum	Eli	elgl@statoil.com
Statoil	Gould	Kristian	kgou@statoil.com
Statoil	Pont	Arno	apon@statoil.com
Statoil	Ringstad	Arne Jarl	ajri@statoil.com
Universitet i Stavanger	Vinnem	Jan Erik	jan.e.vinnem@uis.no

HFC

Introduction, safety analysis in complex industries

A. Bye, IFE

Mer informasjon:

Forester J A, Lois E, Dang V N, Bye A, Boring R L. "Conclusions on Human Reliability Analysis (HRA) Methods from the International HRA Empirical Study." PSAM11&ESREL2012, June 25-29, 2012, Helsinki, Finland.

Vinh N. Dang, John Forester, Ronald Boring, Helena Broberg, Salvatore Massaiu, Jeff Julius, Ilkka Männistö, Huafei Liao, Pamela Nelson, Erasmia Lois, Andreas Bye: ”The International HRA Empirical Study – Phase 3 Report – Results from Comparing HRA Methods Predictions to HAMMLAB Simulator Data on LOFW Scenarios”, HWR-951, September 2011. To be issued as NUREG/IA-0216, Volume 3.

Andreas Bye, Erasmia Lois, Vinh N. Dang, Gareth Parry, John Forester, Salvatore Massaiu, Ronald Boring, Per Øivind Braarud, Helena Broberg, Jeff Julius, Ilkka Männistö, Pamela Nelson: ”The International HRA Empirical Study – Phase 2 Report – Results From Comparing HRA Methods Predictions to HAMMLAB Simulator Data on SGTR Scenarios”, HWR-915, February 2010. NUREG/IA-0216, Volume 2.

E. Lois, V.N. Dang, J. Forester, H. Broberg, S. Massaiu, M. Hildebrandt, P.Ø. Braarud, G.W. Parry, J. Julius, R. Boring, I. Männistö, A. Bye: ”International HRA Empirical Study - Phase 1 Report”. NUREG/IA-0216, Volume 1, November 2009. Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001 (HWR-844)

Safety analysis in complex industries

Human Factors in Control 17-18 Oct 2012

Safety analysis and major accidents – how to include human and organisational elements

Andreas Bye
Institutt for energiteknikk
OECD Halden Reactor Project

Outline

- Risk-informed decision making
- Nuclear examples, towards petroleum applications
- Probabilistic Risk/Safety Analysis (PRA/PSA)
- Human Reliability Analysis (HRA)
  - Human Failure Events
  - Human error
  - Barriers, event trees and bow-tie
  - Resilience and HRA
- Organisational factors
- Recent work at IFE

Risk informed decision making, nuclear industry

- One of several angles of attack in regulation and operation
  - Risk informed, not risk based
- Diversifies technical safety specifications, deterministic, normative rules, barriers and defense-in-depth
- Implemented by Probabilistic Risk/Safety Assessment (PRA/PSA)
  - Human Reliability Analysis (HRA) analyses the human actions involved in the operation of a plant, answers to PRA

What is HRA?

- Human Factors safety analysis
- Purpose of HRA[1]:
  - To ensure that the key human interactions are systematically identified, analysed and incorporated into the safety analysis in a traceable manner;
  - To quantify the probabilities of their success and failure.
  - To provide insights that may improve human performance. Examples include: improvements of man-machine interface, procedures and training, better match between task demands and human capabilities, increasing prospects for successful recovery, minimising the impact of dependencies between human errors etc.

1: CSNI Technical Opinion Papers No. 4, Human Reliability Analysis in Probabilistic Safety Assessment for Nuclear Power Plants, OECD NEA 2004

What is PRA?

- Decomposed analysis of the plant based on a set of predefined scenarios
- Major accidents
  - Not occupational safety
- Scenarios modeled by event trees, clearly defined end states
- PRA level 1, 2 and 3

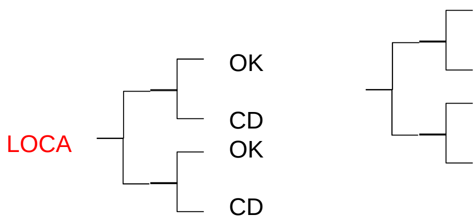
PRA level 1, 2, 3

Level 1
Plant model

Level 2
Containment model

Level 3
Site/Consequence model

Initiating Events → Plant damage states: Core Damage → Release states: How much release to the environment → Final damage states: Public health effects

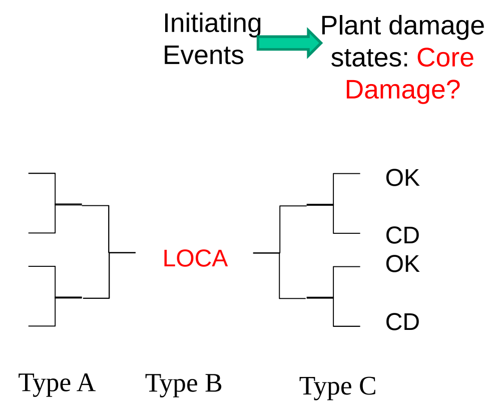


Human action types

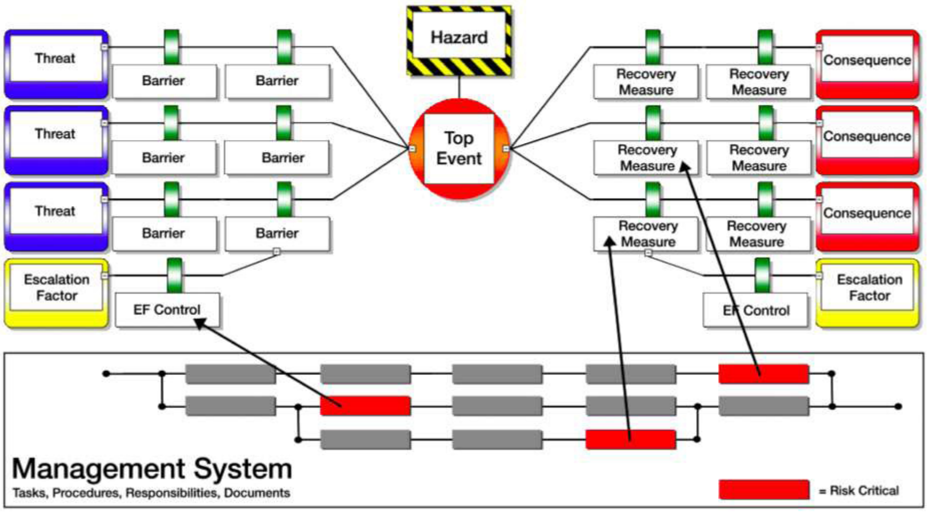
- PRA level 1
- Type A: Pre-initiating event actions
  - Maintenance, latent errors
- Type B: Actions that cause an initiating event
- Type C: Post-initiating event actions
  - Emergency Operating Procedures

Human action types in PRA level 1

Level 1
Plant model



Bow Tie

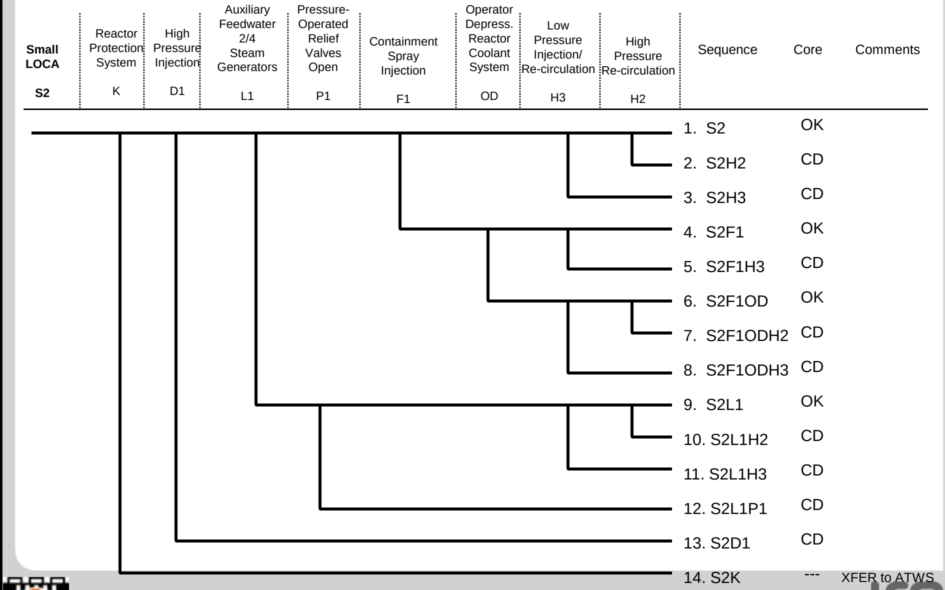


(Patrick Hudson, Delft University of Technology)

Event tree and Barriers

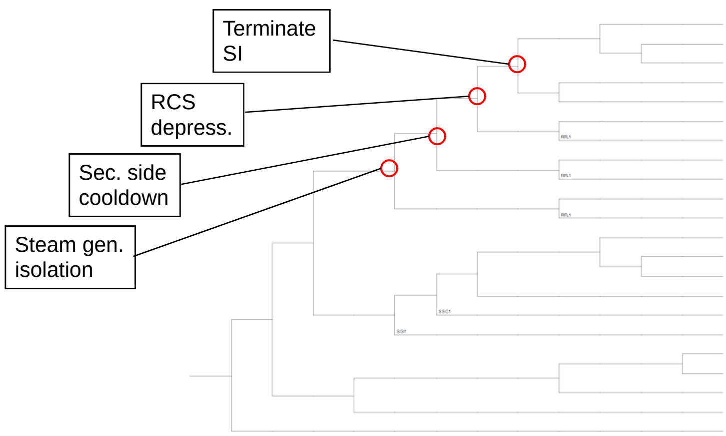
- A Human Failure Event constitutes a functional barrier

Event Tree for S_2 - Small LOCA



(Curtis Smith, INL)

An event tree, Major actions in procedure for Steam Generator Tube Rupture



12

HRA steps

- Human error identification and event tree modeling
  - Part of PRA modeling or specific HRA work
  - Some HRA methods include this step, e.g., ATHEANA
- Quantification
  - Many HRA methods only cover this part, e.g., SPAR-H

Observations

Human failure event modeling

- The nature of the modeling of the Human Failure Events depends on the frames for the human actions
  - Nuclear post-initiating event: Emergency Operating Procedures and safety systems (core cooling pumps etc)
  - Pre-initiators: Strict procedures? More human actions? Less strict frames?

Human error – HRA and blaming

- System view, not "blaming"
  - Classical HF
- The Human Error Probability (HEP) is the probability of Human Error of a Human Failure Event (HFE)
  - An HFE can be "diagnose and isolate ruptured steam generator within x minutes"
  - This could in principle be physically impossible
    - Too short time?
    - Still defined as human error
  - From a safety perspective, who's to blame is not interesting

Only study what can go wrong?

- One must study accidents in order to study safety and risk
- On the level of human actions, also success is studied (within an accident sequence)
  - Part of an accident can be “heroic” actions, improvisations
- Success of mitigation actions is the core thing to study in a safety analysis (PRA level 1)
- What can one take credit for in a safety evaluation?

Error of Omission and Commission

- Error of Omission (EOO)
  - Omitting a (required) procedure step
  - Compliance
- Error of Commission (EOC)
  - “Decision” error

Resilience and HRA

- Does HRA only study compliance?
- The analyst has to find out: How difficult is this task?
  - How much does it impact the HEP of the HFE?
  - Procedure example:
    - Execution of steps, but the procedure does not fit the situation
    - If there is no way to comply with the procedure, the operator should behave "resilient" (or robust). However, the HRA analyst still has to evaluate the probability of the operator not managing to reach the goal of the human failure event (e.g., diagnose the situation)
- Both compliance and resilience are relevant issues for safety analysis

Organisational factors in safety analysis

- In after-the-fact-analysis:
  - Interested in causes
  - Can count effects as many times as we like, if we find them
- In predictions, especially for probabilistic estimates
  - Should not double count effects
  - Do organisational factors influence sharp operations directly? Or through other factors already included in the analysis? (e.g., work processes)
- Last HFC meeting: Idea by Patrick Hudson
  - Bow-tie (or event tree) with PSFs
  - Organisational factors influence PSFs, not directly on barriers

Work at IFE later years

- Experiments in HAMMLAB to inform HRA
- International cooperation to compare strengths and weaknesses of HRA methods
  - International HRA Empirical Study

International HRA Empirical Study

- Compared 13 HRA methods to simulator results in HAMMLAB
- Quantitative and qualitative comparison
  - Qualitative most important
- Drivers of performance (PSFs) and operational expressions

International HRA Empirical Study

HRA teams

Scenarios
SGTR
LOFW

HAMMLAB experiments (14 crews)

Predictions
- HEP
- Driving PSFs
- Operational expression

Assessment team
- Separate analysis for each method
- Summary of method prediction
- Assessment of fit between method predictions and empirical data
- Additional comments
  - Insights for error reduction
  - Sensitivity to driving factors
  - Guidance and traceability

Analysis
- Failure rates
- PSFs per crew
- PSF drivers
- Op. summary
  - per crew
  - overall

Conclusion

- HF can contribute to Safety analysis through HRA

HFC

HRA in the human factor engineering process

P. Le Bot, EDF

Mer informasjon:
HRA Society (www.hrasociety.org)

Human Reliability Analysis in the engineering process

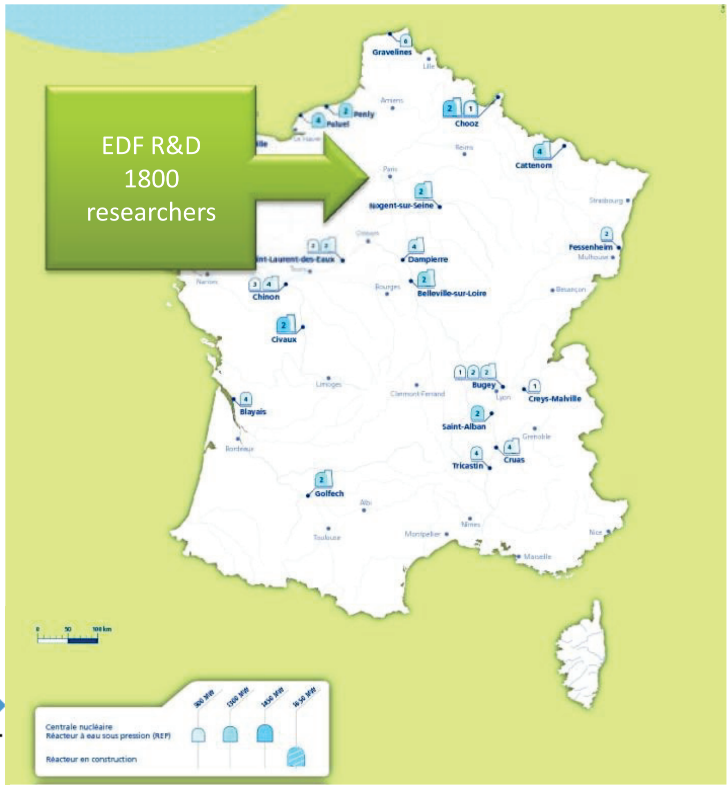
Human Factors in Control / Safety Analysis and Major Accident
How to include Human and Organisational elements

All sections to appear here

R&D

- Pierre Le Bot
- Mastered in engineery and sociology
- EDF R&D (since 1993)
  - Department MRI (Industrial Risk Management)
  - Group: « Organizational and Human factors for Socio-Technical Systems »
- Expert researcher in Human Reliability

- installated capacity: 128,200 GW
- 156.500 employees in the world
- In France 58 nuclear units at 19 plants – all PWR (4 main series)
- 1100 reactors.years cumulated experience
- High level of standardization within a series



Nuclear operator

On-going projects

- HRA Methods extension and industrialisation (PSA)
  - Agressions
  - MERMOS Catalogue
- Data collection
  - HF Data technical group
  - Simulations
- Tools
  - IDAFH
- Human Factors Engineering
  - French EPR organisation evaluation
  - EPR UK
  - NUREG 711 implementation
- Modelisation
  - Model of Resilience in Situation
  - Fukushima impact
  - EOS profiling
- HRA Society (www.hrasociety.org)

HRA in the engineering process (NUREG-0711)

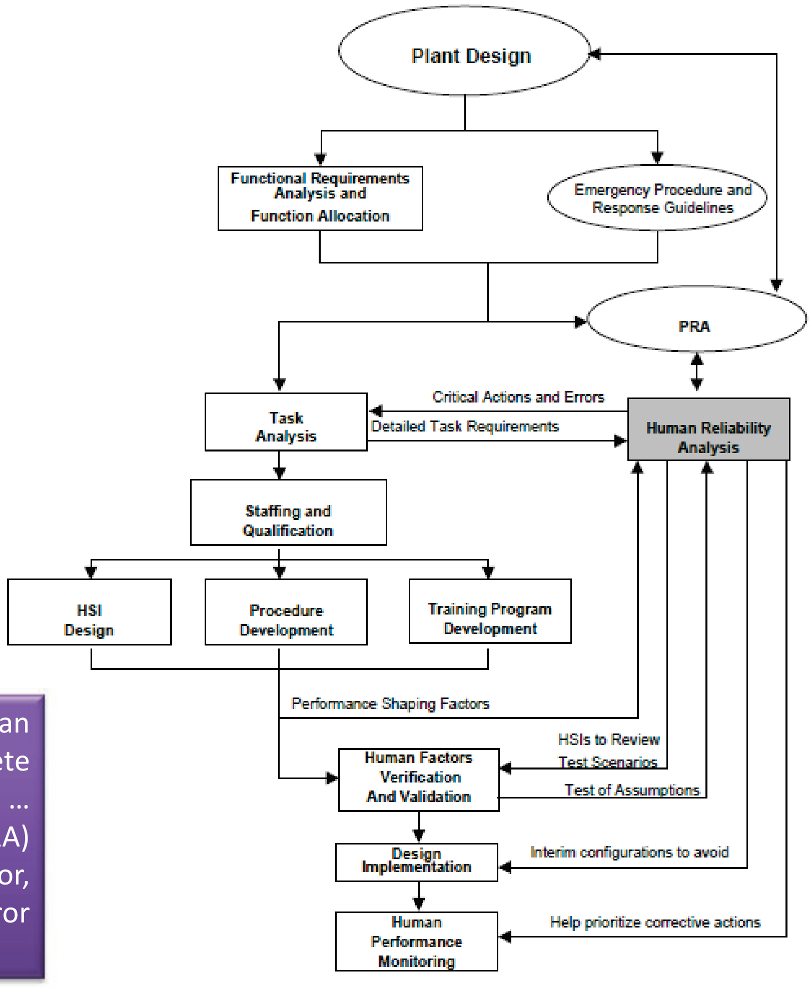


Figure 7.1 The role of human reliability analysis in the HFE program

Human reliability analysis (HRA) is an integral activity of a complete probabilistic risk assessment (PRA) … Human reliability analysis (HRA) seeks to evaluate the potential for, and mechanisms of, human error that may affect plant safety.

Definitions of HRA (Human Reliability Analysis)

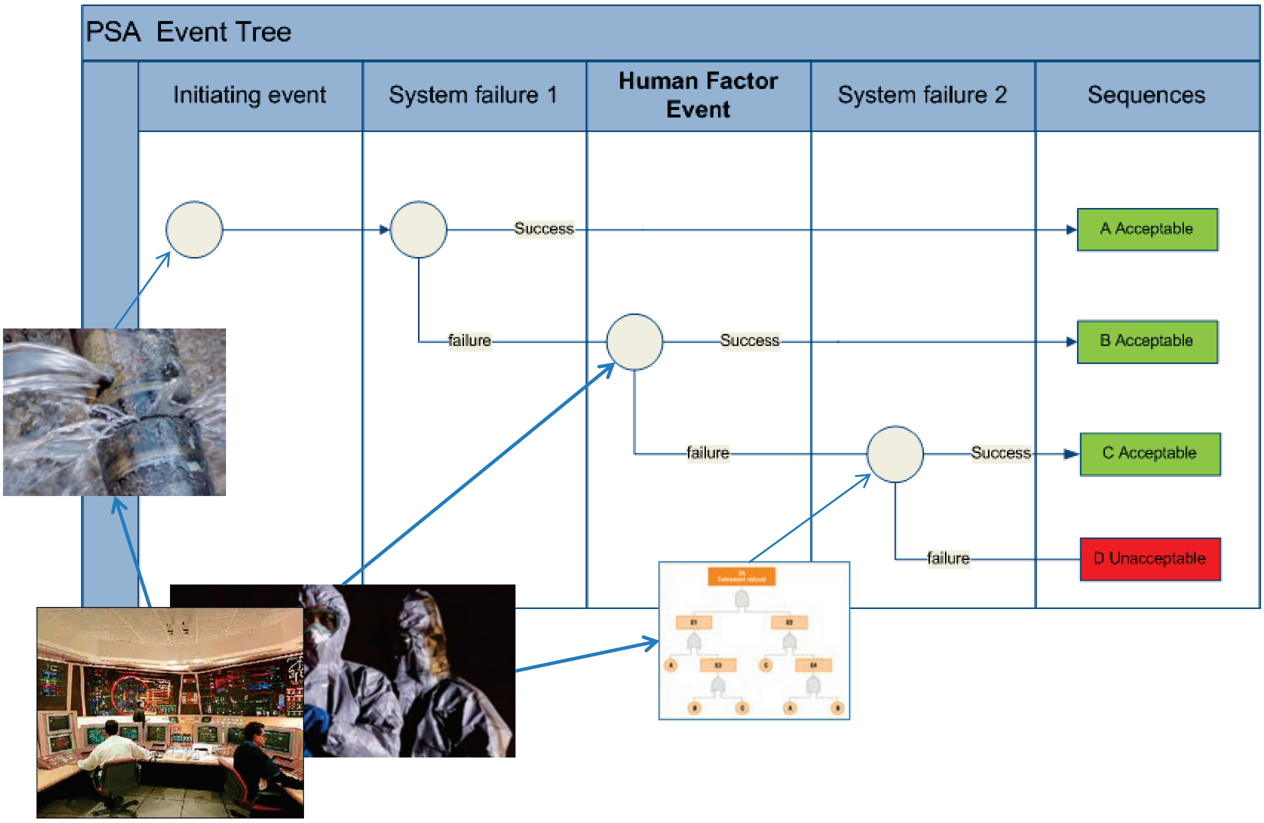
Science of human failure (Swain 1983)

Characteristic of the operator related to his task (Leplat 1985)

Knowledge related to prediction, analysis and reducing of human error (…) (EEC norm 1988)

Risk Management approach based on the evaluation of the performance of processes in which the human part is essential (Le Bot, 2000)

HRA within a PSA (PRA)



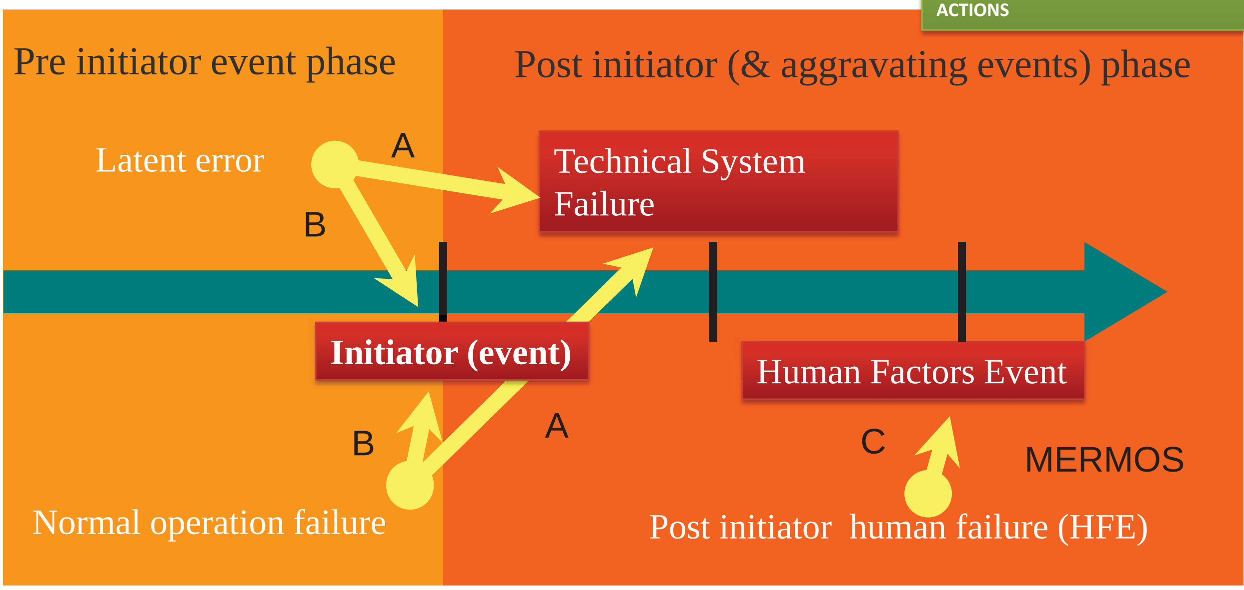
9

HRA for NPP's PSA

TYPE A: PRE-INITIATING EVENT ACTIONS

TYPE B: ACTIONS THAT CAUSE AN INITIATING EVENT

TYPE C: POST-INITIATING EVENT ACTIONS



Normal operation
Maintenance

Emergency operation

Steamline Break + SGTR, auto-isolation of the break (complex scenario)

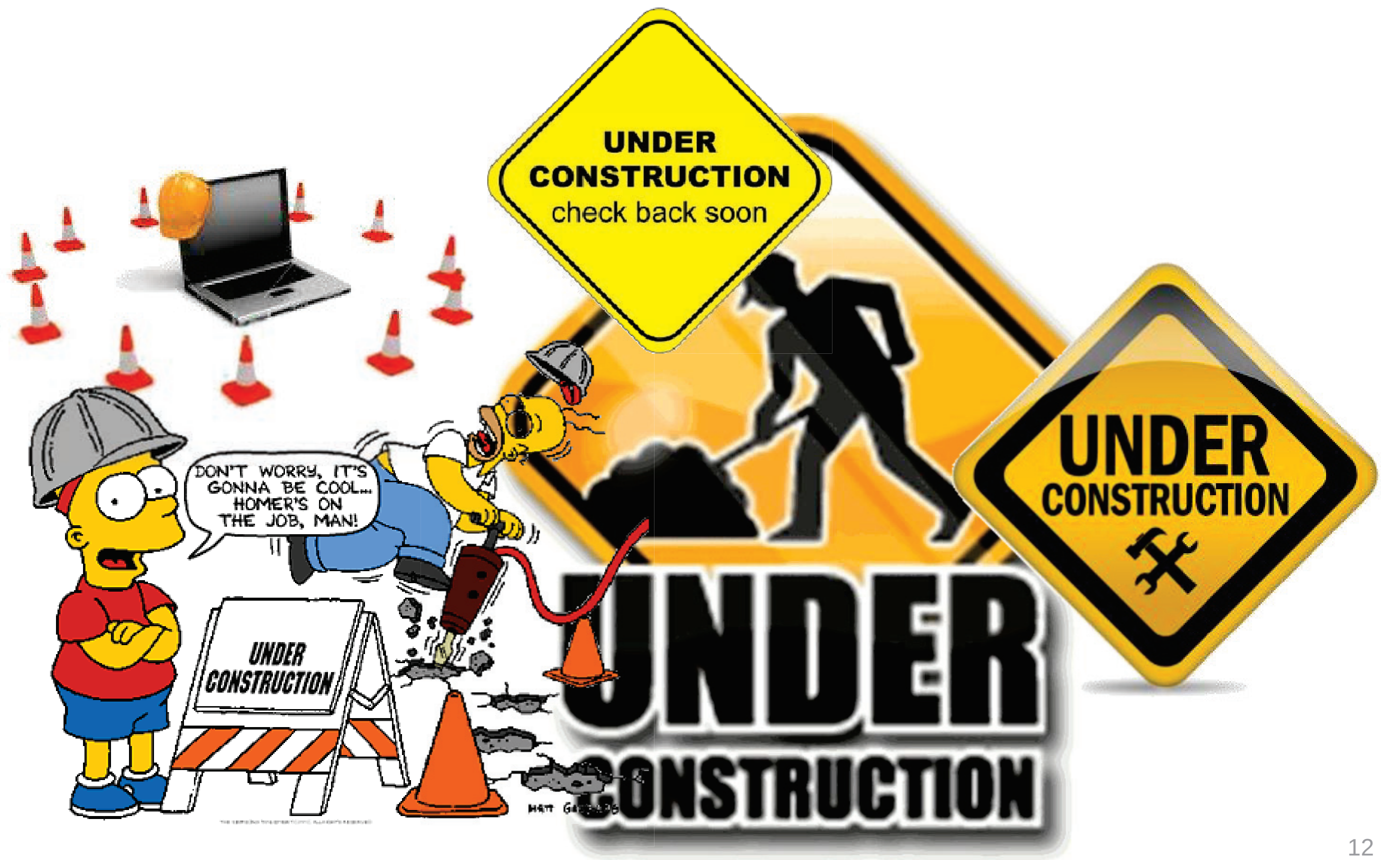
Cooldown the RCS within 15 minutes from E-3 step 7

Probability of mission failure (HEP):	1.0 E-2
Uncertainty:	3.7 E-4 to 3.7 E-2

N°	Scenarios	Prob.
1	The system hesitates about the means and does not operate the cooldown early enough	8.1 E-3
2	Before operating the cooldown, the system wants to make sure that the SG has been well locally isolated	7.3 E-4
3	The system tries first to reach ruptured SG level > 17% narrow range, and starts the cooling too late	0
4	The team does not choose the expeditious cooldown given a reading error of the level of the SG	8.1 E-5
5	the system interrupts too early the cooling given a reading error on a parameter that governs the stopping of the cooling, and does not restarts on time	2.4 E-4
6	the system is cooling too much and overtakes the limit of subcooling margin	9 E-5
7	the system operates an unsufficient cooling because of an error of rating and of lack of communication	8.1 E-4
Pr	-	6 E-5

Example of an HFE HRA analysis (with MERMOS)

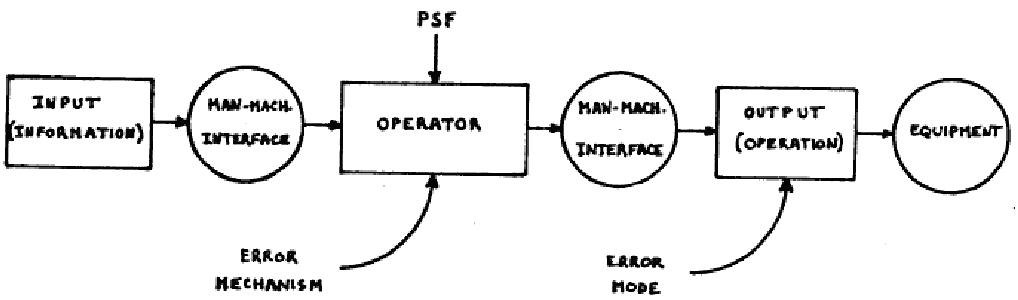
HRA and Organisational Factors



THERP and Simulation for PSA

- HRA used only for PSA
- PSA used only for as a verification of deterministic safety Approach
- US methods adapted cautiously:
  – Simplification
  – Use of full scope simulators

First Human Reliability paradigm at EDF (1986)



THE BASIS OF THE ERROR DESCRIPTION FORM : AN ELEMENTARY MODEL OF HUMAN BEHAVIOR

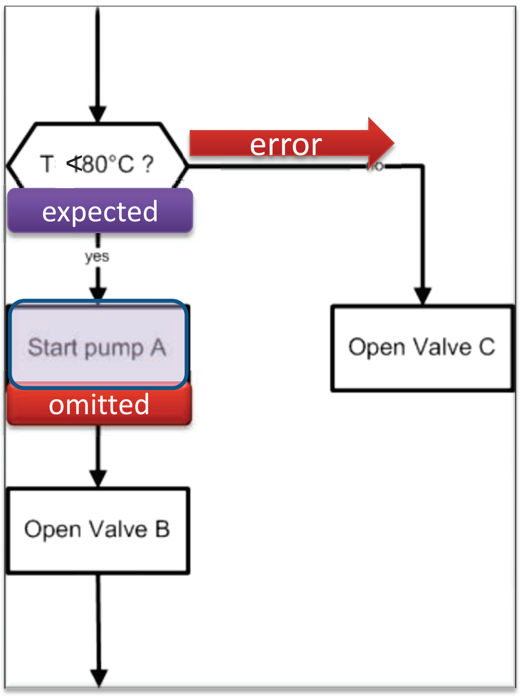
FIGURE 1

A. Villemeur, F. Mosneron-Dupin, M. Bouissou, T. Meslin *"A Human Factors Databank For French Nuclear Powerplants", Proceedings of the International Topical Meeting on Advances in Human Factors in Nuclear Power Systems, American Nuclear Society, Knoxville, TN.(1986)*

First VISION : unrationally, operator sometimes does'nt perform expected action

- Operator = machine
  - Without autonomy
  - With limited capacities
  - Very unreliable
- Human failure:
  - Individual
  - Operator informed and sollicitated by interface and procedure
  - If response is not as expected➔ **Error**

How to identify and assess potential Human Failure Event ? An engineering problem for HRA



- The classical engineer approach (1rst generation method):
  - Failure = the omission of the expected actions prescribed in the applicable procedure

  ➔Screening of the prescribed actions, depending on their consequences

  - **HFE of EOO (error of omission)** are easy to identify
  - No clear method for **EOC (error of commission)** or limited
    - Not easy to find out plausible potential unexpected output
    - No clear validation from operational feedback

Feedback

- Data collection on simulator is expensive but very rich:
  - Understanding of operation
  - Very few quantitative results, a lot of qualitative knowledge
  - Individual errors are observed but are very difficult to categorize and they have only an influence on the failure, they are not a cause (because of system tolerance)
- First HRA generation methods are limited:
  - They need expert judgment
  - They are not very sensitive to organizational factors
- No clear link between operation during actual events and HRA models

Issues

- The classic HRA model from the first vision of human contribution to safety has to be improved. We needed new paradigm and concepts :
  What is the role of humans in Safety ?
- Context drives the operation
  - PSFs influence is very difficult to observe
  - PSFs effect is context dependant (sense and intensity)
- Individual error is not the failure
  - Because of human, interface & procedure redundancy, failure is systemic and collective
  - Individual error taxonomy is not useful
- Emergency operation is performed by a cognitive distributed system: it is responsible for failure

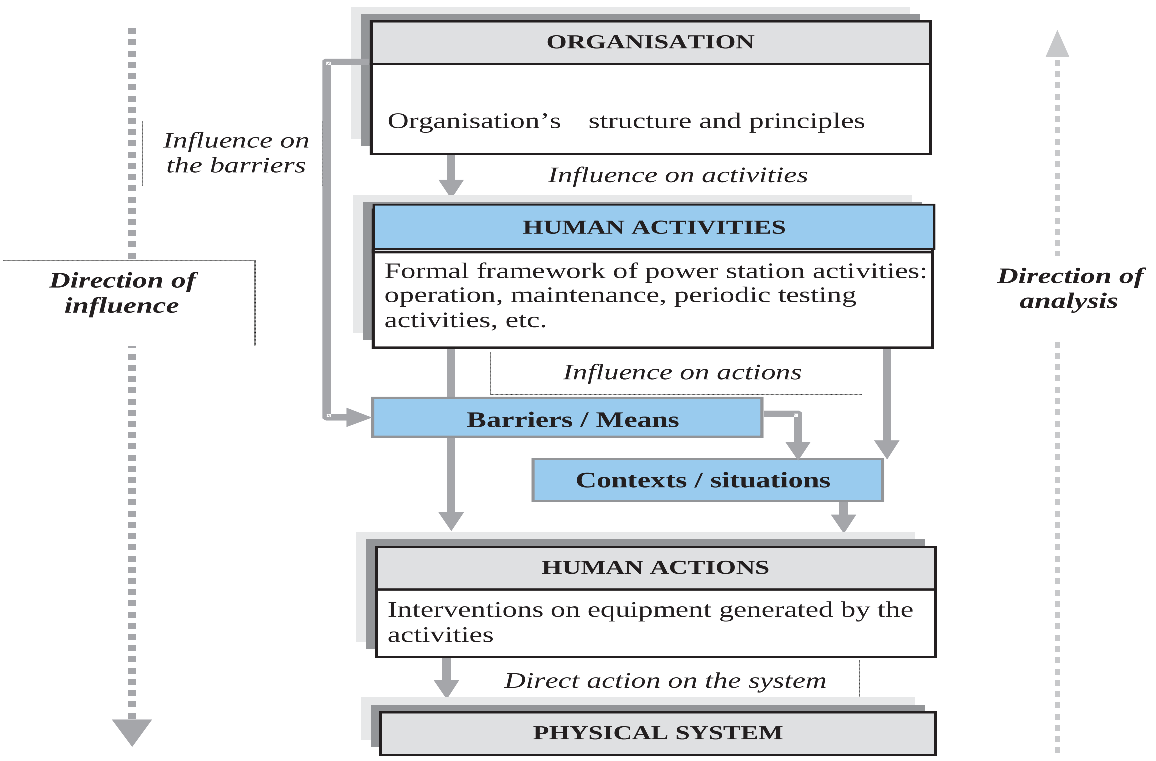
About organizational models

–In the field of safety, the existing organizational models are *”mostly devoid of theoretical underpinnings”* and they are rarely predictive (in a quantitative sense). *(Wilpert)*

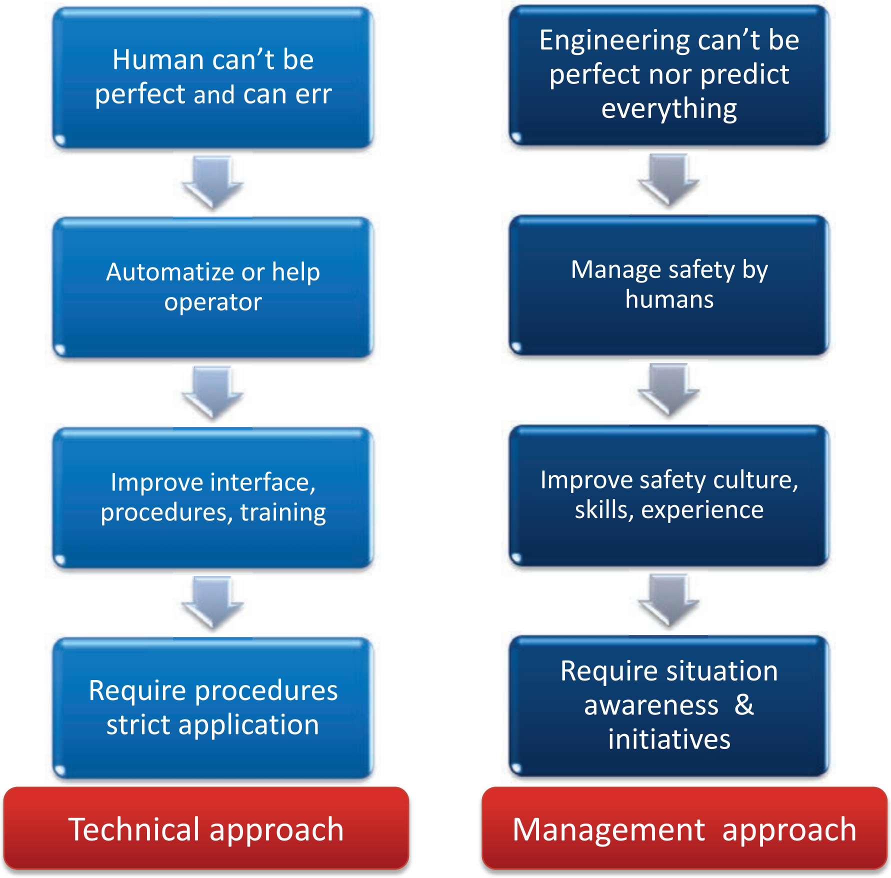
–These models are top-down : from an a priori definition of the organizational factors, these models are looking for an evaluation of their impact on safety.

–Measuring the impact of organizational factors on the safety of a Nuclear Power Plant, is feasible starting from PSA and following a bottom-up approach.

General frame: adapted SAM approach (E. Pate-Cornell)



Ultra safe systems: Humans role in safety and failure?
Two opposite rationalities



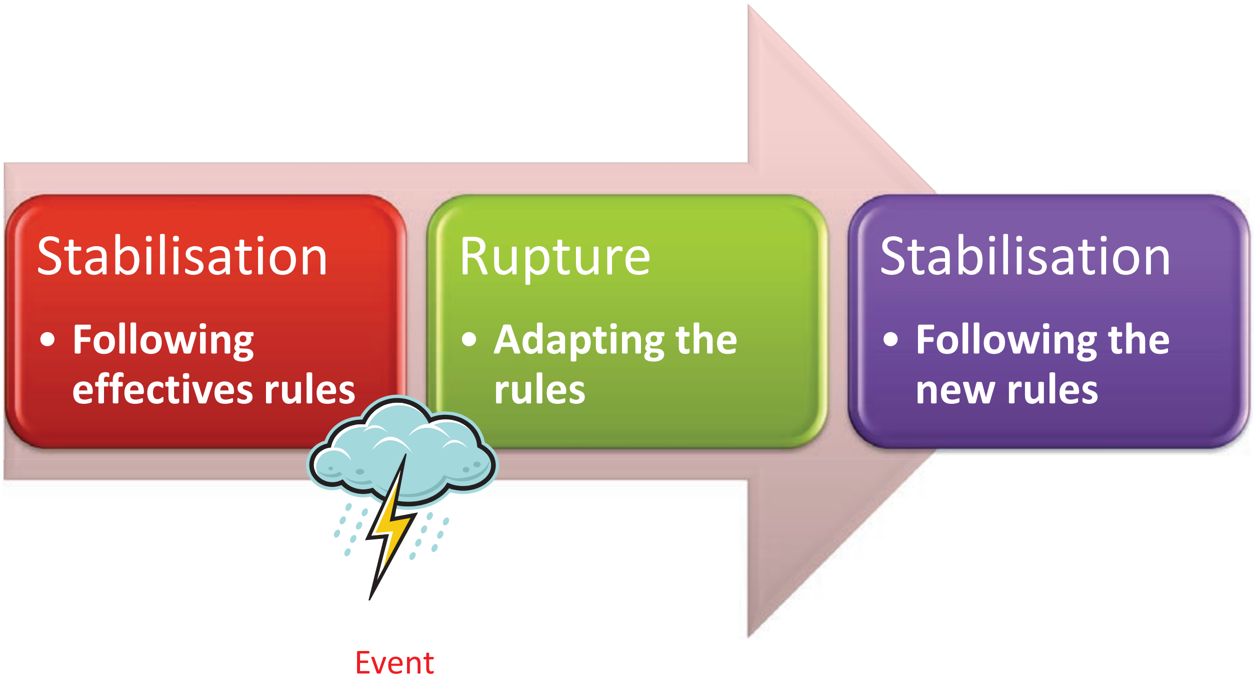
Two rationalities are necessary

(from J.D. Reynaud, Theory of Social Regulation)

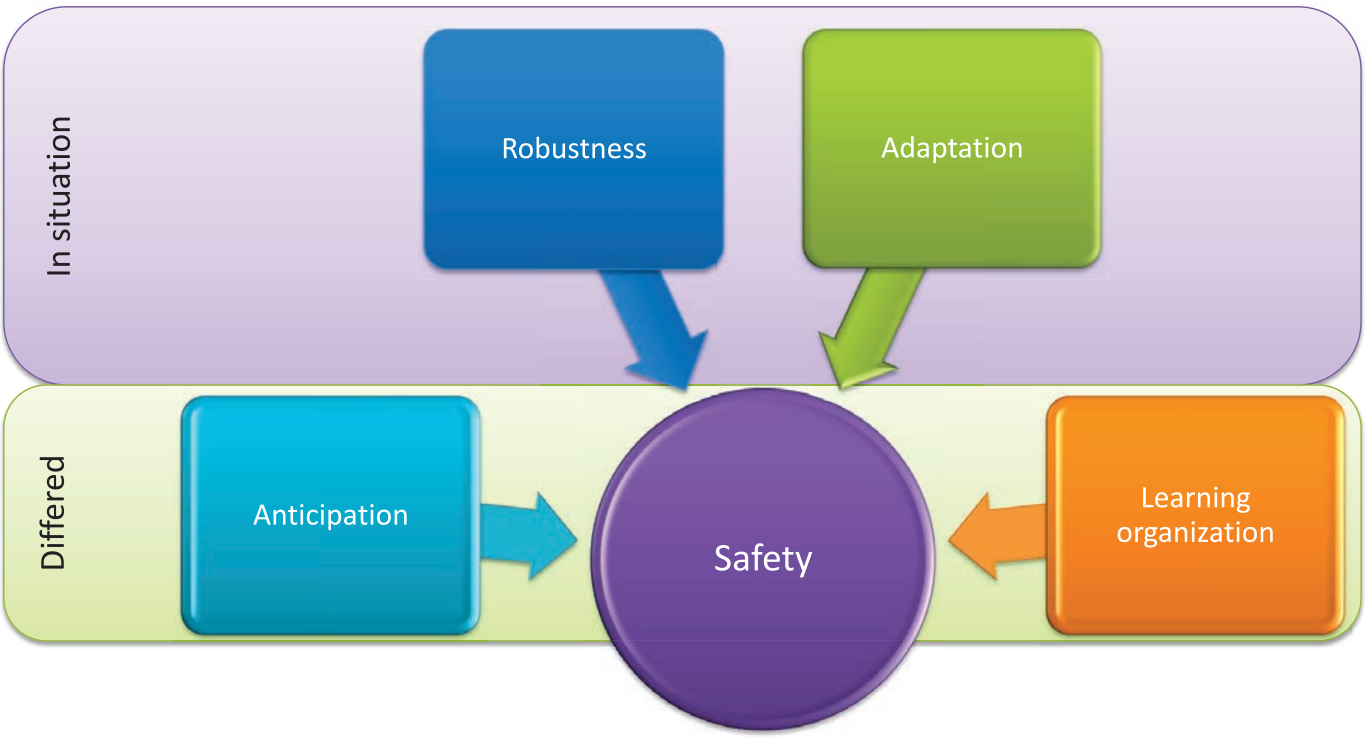
Effective rules:
-Collective
-Sensemaking
-Formal or unformal
-Contextual and temporary

To alternate Stability and Adaptability

Dynamic combination by regulation in situation and following operation rules



Safety by resilience



The MRS

Model of Resilience In Situation

Organisation and EOS required performance is described functionally

Anticipation

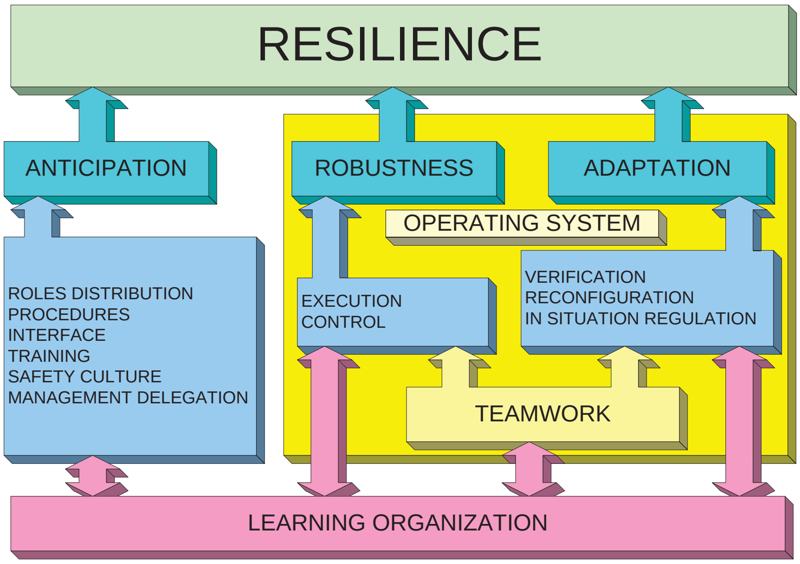
To provide the EOS with the necessary means and resources to operate the anticipated situations

Robustness

To act on the process as required in the situation

Aadaptation

To detect that operation is not adequate with the situation, to define in the situation new adequate operation and to switch to that operation



Link with HRA

- Centered on safety

- The MRS is a model upstream MERMOS, our reference HRA method
- With MERMOS a failing operation is an inadequate operation that is not interrupted in time:
  - **A failure depending on human decision and action is resulting from the failure of the adaptation of the system in the situation.**
  - **The adaptation failed to stop in time an inadequate operation leading to unacceptable consequences.**
- Adaptation is needed:
  - either by a new situation because of external causes (aggravating event)
  - either by a new situation caused by a non robust operation
    - Human error: **failure of robustness**
  - Either by a choice of an inadequate operation
    - Wrong decision: former **failure of adaptation**

2nd generation HRA methodology: MERMOS, based on MRS, extension from type C HFE

MERMOS/PSA	Simplified approach	Statistical approach	Detailed approach
Pre initiator	**(FH7)** MERMOS pre initiator simplified	MERMOS pre initiator statistique	MERMOS pre initiator détailed (under development)
Initiator		**(FH7)** Future development	
Post initiator	MERMOS post initiator forfaitaire	**Observation guide for MERMOS** **Time Related Curves**	**MERMOS post initiator detailed** Analyses Catalog
Crisis organization	MERMOS crisis team simplified (PSA level 1) (under development)	-	**MERMOS detailed (PSA level 2)**
Fire	**MERMOS Fire screening**	**MERMOS Fire fighting statistical**	MERMOS Fire fighting detailed **MERMOS Fire operation detailed**
Seism, Flood …		Future developments	

+ Application frame (choice of methods to take into account project constrains & specific objectives, HRA team organization …)

Emergency operation and normal operation/maintenance: correspondances and differences

MERMOS C	MERMOS A
Failure of a unique set of actions	Wrong configuration of a Equipment that can result from different actions
Failing actions	Failing activity (with 3 different phases: preparation/intervention/verification)
Short time window	Discontinuous time windows for each activity and each phase
One team in the same place	Several teams in different places for each activity
Recovery action	Recovery activity
Operation	Activity management
Context of actions	Context of activity

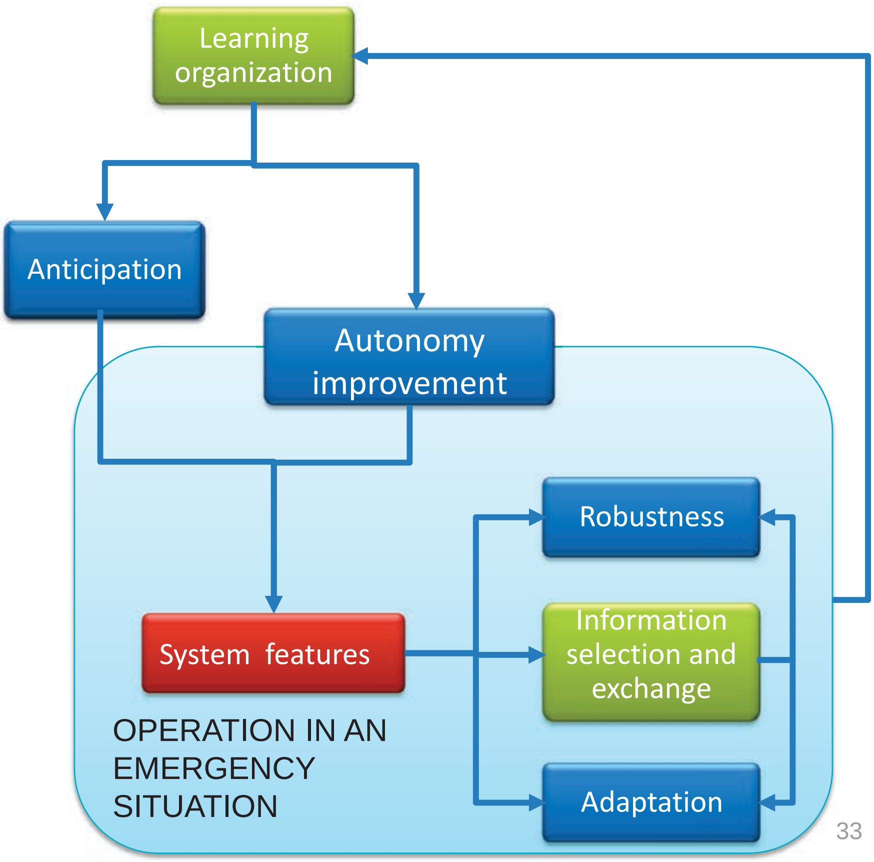
The Emergency Operating System

- Emergency operation of a NPP is **emerging from interaction between operators, procedures and interface** that constitute a system (EOS)
- The EOS is **cognitive and distributed**
  – It uses prior knowledge and produces new knowledge in real time
  – Knowledge is deposited in and elaborated by different system components.
- Its behaviour is coherent

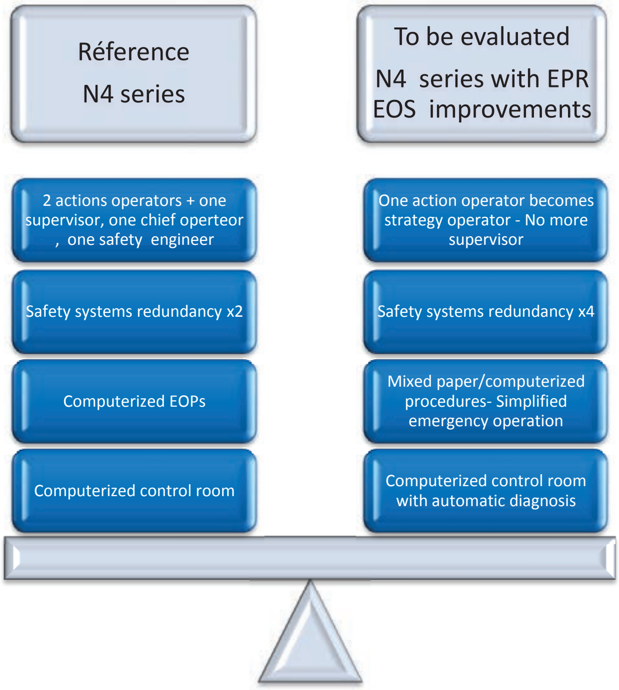
Human Reliability is the reliability of the EOS

Functional description (EOS profiling)

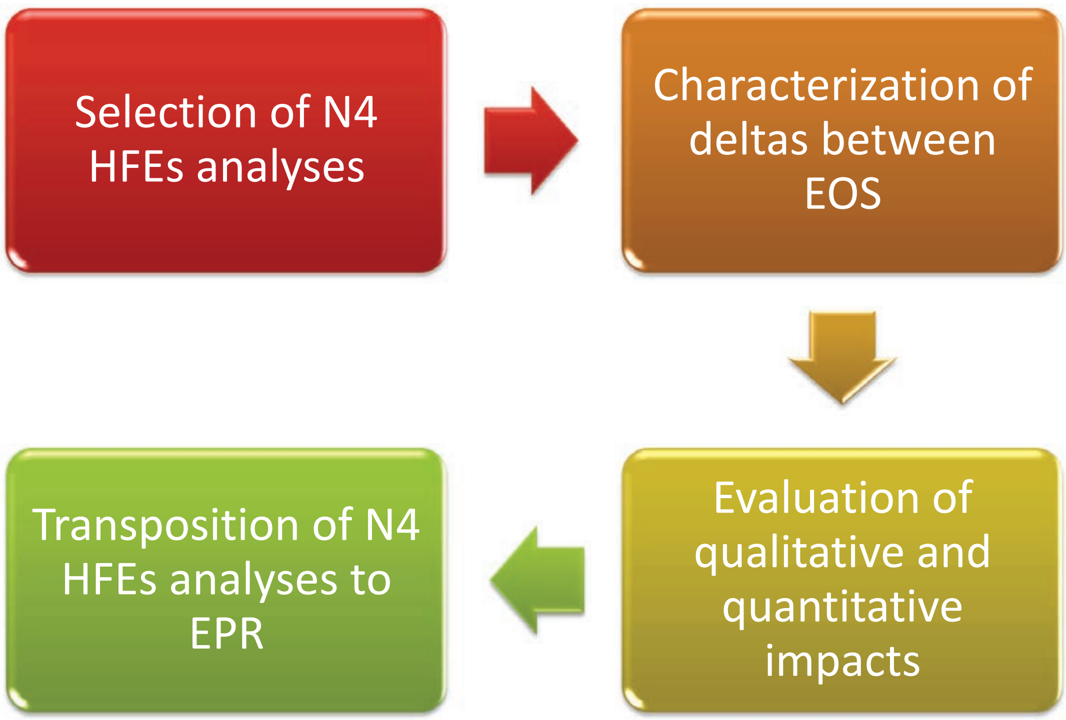
- Learning organizational process feeds the Anticipation and the Operators Autonomy Improvement , that shape EOS features.
- We focalize on resilience Function performed by the EOS in the situation **Robustness and Adaptation, that are supported by selection and exchnage of Information.**
- **EOS features influences the efficiency of theses functions, given the situation to operate.**
- (A function defines a goal of the system. A process is not necessary by itself, but it is allowing the completion of the functions)



Exploratory study - Principle



Steps

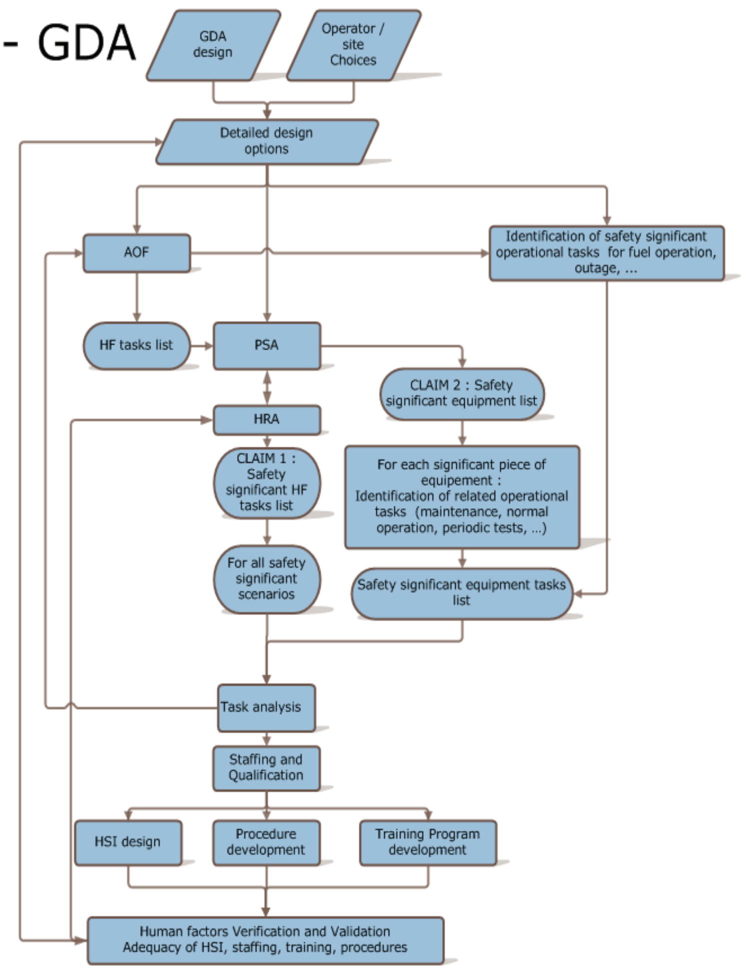


Insights

- Some EPR EOS improvements are assessed not only with positive effects but could have negative effects in specific situations
- HRA quantification with MERMOS allows to balance the +/- impacts
- First observations on simulator validate the prediction
- Some impacts could be underestimated: observations will allow to recalibrate
- The « EOS profiling » has to be refined

HFE: a process to build

POST - GDA

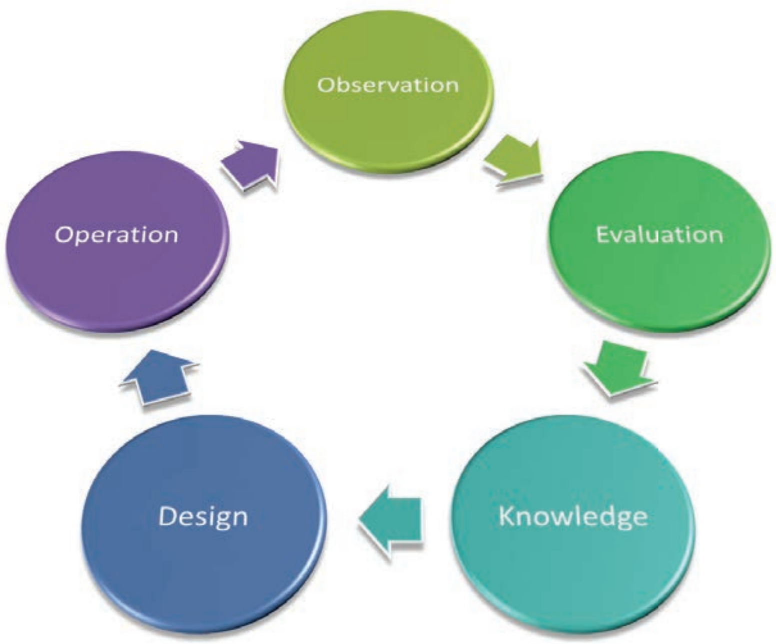


EPR UK - HFE

- Importance of HRA
- Difficulties to implement the NUREG 711
  - Iterations
  - Empirical knowledge
- Two HRAs
  - Tasks based (Task analysis)
  - Functional-requirements based (PSA)
- Importance of PSA/HRA criteria of significance

Conclusion

- **HRA will be more and more used** in the engineering process (risk informed regulation, new reactions, control room renovation …)
- **Different level of methods are necessary** (simplified, statistical, comprehensive)
- **Empirical understanding of the functioning of the EOS and other operating groups is crucial** (by simulations, on the field observations and actual events analyses)
- **The HFE process has to be better defined and controlled** in order to prevent an uncontrolled increasing of studies
- **HRA is at the center of Safety System HFE** since it is focused on the assessment of effects of HFE



HRA and Risk Management

HFC

Introduction to Human Factors, methods and theory

A. Balfour, HFS

Mer informasjon:
videre.ntnu.no/link/nv13119

Wickens, J. E., Lee. J., Lui & Gorden-Becker, S. (2003). Introduction to human factors engineering. Prentice Hall.

Stanton, N. A., Salmon P. M., Walker G.H., Baber C. & Jenkins D.P. (2005). Human factors methods: A practical guide for engineering and design. Asgate publishing.

Kirwan, B. (1992). A Guide to task analysis. Taylor and Francis

Bower, C., Salas, E., Jentsch, F. & Bowers C. A. (2006). Creating high-tech teams: Practical guidance on work performance and technology. American psychology association.

Salas, E. & Fiore, S. M.(2002). Team cognition: Understanding the factors that drive process and performance. American Psychology Association.

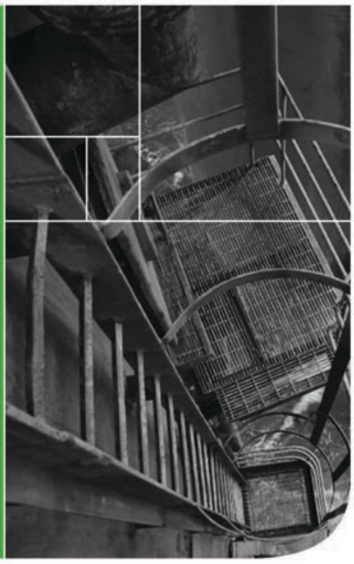
Johnsen S.O., Bjørkli C., Steiro T., Fartum H., Haukenes H., Ramberg J., Skriver J.. (2011): "CRIOP – A scenario method for Crisis Intervention and Operability analysis". See www.criop.sintef.no

ISO 11064: Principles for the design of control centres, International Organization for Standardization.

Tomorrow's human factors standards today

HFC Course
"An Introduction to Human Factors in the Oil and Gas Industry"

Adam Balfour, October 2012



Agenda

- Goals / Scope
- Syllabus
- Theory and practice
- Course assignment
- Challenges
- Reading material
- Practical

Course Goal: What we want to avoid…

Course Goals and Learning Outcomes

Course Goal

- The aim of the course is to provide ***an introduction and overview*** of human factors approaches, methods and techniques that can be applied in the Norwegian oil and gas industry for the control room/systems design. Greenfield and Brownfield. The framework for the course is the ISO 11064 standard.

Scope

- Norwegian oil and gas industry for ***control room/systems*** design. Includes cabins, systems and Integrated Operations.
- Norwegian ***PSA regulations*** and ***NORSOK*** standards apply.
- The framework for the course is the ***ISO 11064*** standard.

Goals/learning outcome

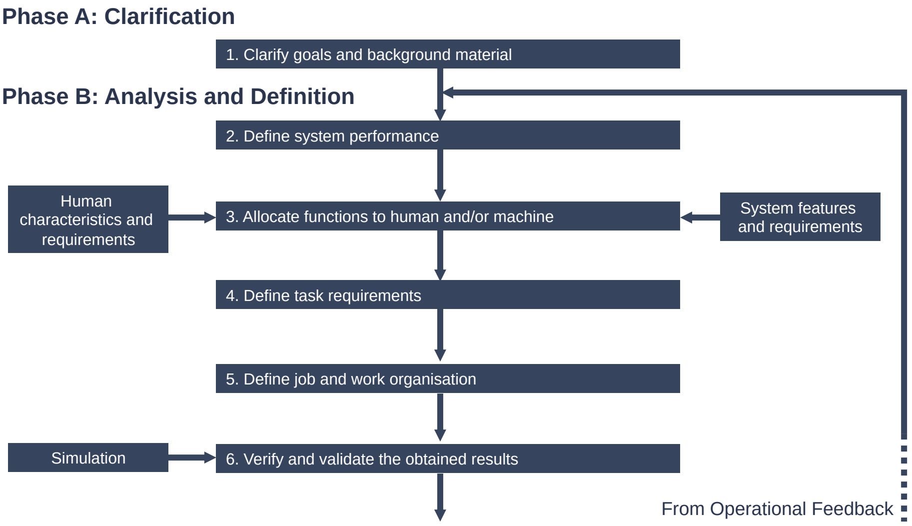
Target group

- Professionals in the oil and gas industry in Norway - engineers, equipment/systems designers, interface designers, psychologists, social scientists, ergonomists.
- "***Open minded***" to new disciplines, approaches, methods and techniques.
- Attend all lectures (50/60 lectures) + complete assignment (ca 10 days)

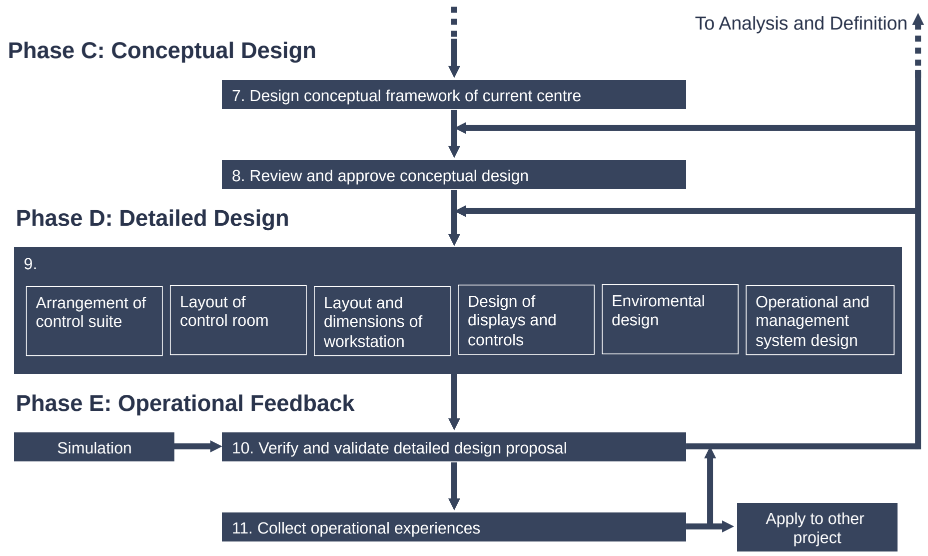
Learning Outcomes

- Working knowledge of what human factors is and the challenges when applying HF to control room/system design in the Norwegian oil and gas industry.
- An overview of the different human factors approaches, methods and techniques and where these can be applied in the ISO 11064 design process (CCR).

Framework: Design Process: ISO 11064 (1 of 2)



Framework: Design process: ISO 11064 (2 of 2)



HF Approach – Typical Syllabus

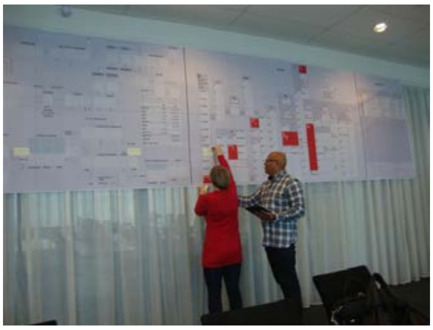
- **Day One** Introduction to Human Factors, PSA Regs, ISO 11064
- **Day Two** Clarify Goals and Overview of Analyses
- **Day Three** Overview of Analyses, Preparation and Assignment

- **Day Four** Perception and Information Processing
- **Day Five** Workstation and Control Room Design
- **Day Six** Interaction Design and Display Design
- **Day Seven** Organisation, Training and Procedures

- **Day Eight** Team work / Visit to site
- **Day Nine** Verification and Validation incl CRIOP
- **Day Ten** Human Error and Summary

Theory and Practice

- Classroom exercises
- Practical exercises
- Visit to Control Room / IO



Course Assignment

- Demonstrate ability to *apply* HF approach to Norwegian offshore oil and gas industry challenges. Use of methods, literature and knowledge
- Can relate to own work
- Wide range of assignments
- Support from lecturer
- 10 days work
- Formalities described

Challenges

- Different background / interests
- ”I want more info on IO”
- ”I want less info on IO”
- More theory vs. less theory
- I know all about HMI, do I need to attend the HMI module?
- Written course assignment – first time in 25 years…
- I just wanted to know the character size on the screen
- No time is a good time for everyone

Course Advantages

- Networking
- Understanding of human factors impact on individuals, companies and the industry
- Less than 5% drop out
- Positive written feedback

How can you contribute?

- Spread infomation about course
- Propose project assignments
- Provide facilities for demonstration

HF Approach – Reading Material

Reading list: Obligatory

- Wickens, Lee, Lui and Gorden-Becker, 2003. Introduction to Human Factors Engineering, Prentice Hall
- Kirwan : A Guide to task analysis
- Ivergård, 1989. Handbook of Control Room Design and Ergonomics, Taylor and Francis.
- Johnsen, S.O., Lundteigen, M.A., Fartum, H., Monsen, J., 2005. Identification and reduction of risks in remote operations of offshore oil and gas installations, SINTEF.
- ISO 11064: Principles for the design of control centres, International Organization for Standardization.

HF Approach – Reading Material

Reading list: Optional

- Dix, Finlay, Abowd and Beale, 2004. *Human Computer Interaction, Prentice Hall.*
- Endsley, 2003, Designing for Situation Awareness, Taylor & Francis.
- Henderson J., Wright K., Brazier A, 2002. *Human factors aspects of remote operations in process plants, Health and Safety Executive (HSE).*
- Reason, 1990. *Human Error, Cambridge University Press.*
- Redmill and Rajan, 1997. *Human Factors in Safety-Critical Systems, Butterworth Heinemann.*
- Sandom C. and Harvey R., 2004. *Human Factors for Engineers, Institution of Engineering and Technology*
- Wilson and Corlett, 1990. *Evaluation of Human Work, Taylor & Francis.*
- Weick, C. *"Sensemaking"*
- Luff.. *London Underground*

Practical

- Location: NTNU Videre Trondheim & HFS, Ski or other
- 2013 course – Feb to April
- Book by 10 January
- 10 days lecturing
- 10 days assignment
- Course material English
- Assignment English/Nordic
- Fee NOK 25.000
- 15 Study points, NTNU
- Feedback throughout course

http://videre.ntnu.no/shop/courses/displayitem.do?dn=uid=nv13119,ou=ntnuvproducts,dc=ntnu,dc=org

HFC

Human reliability analysis in major accident risk analyses in the Norwegian petroleum industry: applying SPAR-H

K. Gould; K. van de Merwe.

Mer informasjon:
Van de Merwe, G.K., Øie, S.F. & Gould, K. (2012). The application of the SPAR-H method in managed-pressure drilling operations. Proceedings of the Human Factors and Ergonomics Society 56th annual meeting. San Antonio.

Gould, K., Van de Merwe, K. & Ringstad, A.J. (2012). Human Reliability Analysis in Major Accident Risk Analyses in the Norwegian Petroleum Industry. Proceedings of the human factors and ergonomics society 56rd annual meeting, San Antonio.

Statoil

Human Reliability Assessment in Major Accident Risk Analyses

Kristian Gould, PhD

kgou@statoil.com

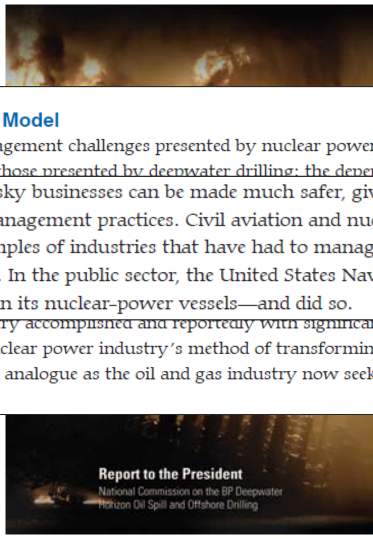
HFC, Halden 17.10.12

2012-03-01

Human Factors are critical to the onset and outcome of most major accidents in the petroleum industry

Deepwater Horizon accident (2010)
Well blowout and fire

2 2012-03-01 Statoil



The Nuclear Model

The risk-management challenges presented by nuclear power are in some respects analogous to those presented by deepwater drilling: the dependence on highly sophisticated

Even inherently risky businesses can be made much safer, given the right motivations and systems-safety management practices. Civil aviation and nuclear-fueled electric power are two good examples of industries that have had to manage the risk of catastrophic failures and losses. In the public sector, the United States Navy also faced the challenge of improving safety in its nuclear-power vessels—and did so.

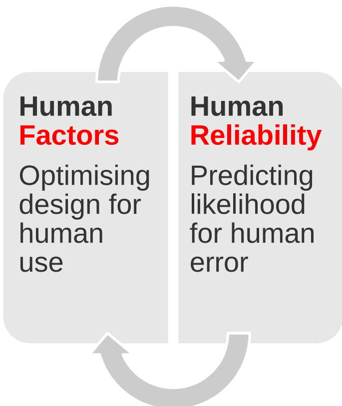
is what industry accomplished and reportedly with significant, positive results. For that reason, the nuclear power industry's method of transforming business-as-usual practices offers a useful analogue as the oil and gas industry now seeks to do the same more than 30 years later.

3 2012-03-01 Statoil

4 2012-03-01 Statoil

Human Reliability Assessment

- The use of **systems engineering** and **human factors** methods in order to render a description of the human contribution to risk and to identify ways to reduce risk
- The driving force behind the development of HRA has been the use of probabilistic risk analysis

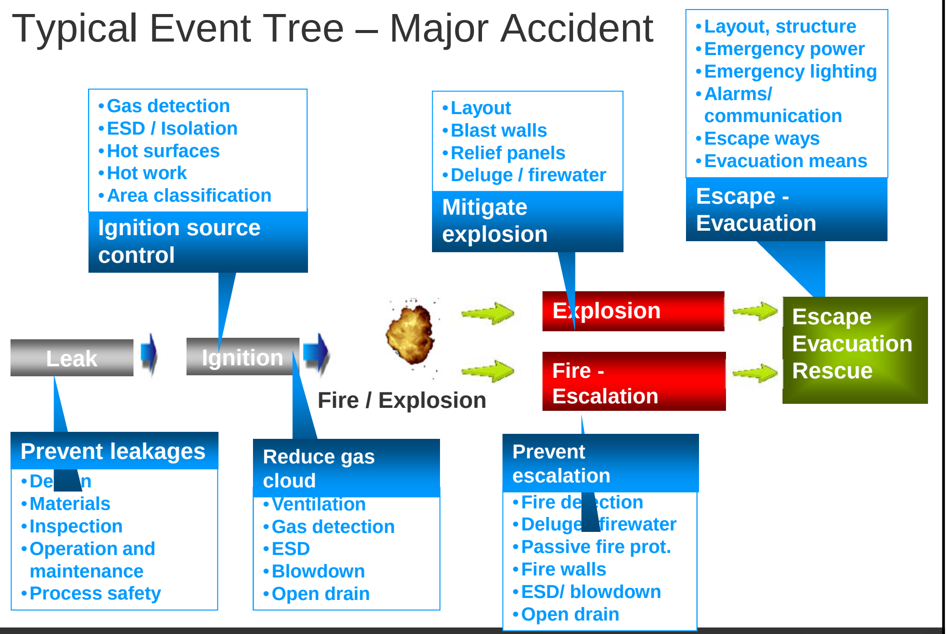


Defined major accident situations offshore

- Blowouts, including shallow gas and reservoir zones, unignited and ignited
- Process leaks, unignited and ignited
- Utility areas and systems fires and explosions
- Fire in accommodation areas
- Falling/swinging objects
- Transportation accidents
- Accidents during transport of personnel from shore to the installation
- Helicopter accidents (crashes)
- Collisions, including field related traffic and external traffic, drifting and under power
- Riser and pipeline accidents
- Accidents from subsea production systems.
- Escape, evacuation and rescue accidents, i.e. until a ‘safe place’ has been reached
- Structural collapse, including collapse of bridges between fixed and/or floating installations
- Foundation failure
- Loss of stability/position, e.g. through ballasting failures

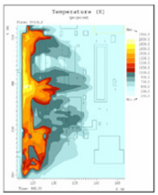
NORSOK Z-013

Typical Event Tree – Major Accident



Risk management tools used by Statoil

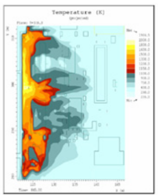
- **Methods**:
  - Risk analyses as basis for design and operation
  - Reliability and accident data (Oreda, WOAD)
  - Fire studies (Kamelon)
  - Explosion studies (FLACS)
  - Gas dispersion (Kamelon / FLACS)
- **Applications**:
  - Establishment of design accidental loads
  - Optimized layout with distances and access
  - Dimensioning of fire and explosion barriers
  - Evaluation of safety barriers, design and in operation

Statoil

Risk management tools used by Safety Technology (ST)

- **Methods**:
  - Risk analyses as basis for design and operation
  - Reliability and accident data (Oreda, WOAD)
  - Fire studies (Kamelon)
  - Explosion studies (FLACS)
  - Gas dispersion (Kamelon / FLACS)
- **Applications**:
  - Establishment of design accidental loads
  - Optimized layout with distances and access
  - Dimensioning of fire and explosion barriers
  - Evaluation of safety barriers, design and in operation

Statoil

Engineered systems do not work in isolation

Engineered systems' performance is determined by a variety of factors:

– Design, including margins of safety

– Quality of materials and construction

– Operability, including process and procedures

– People

- All in the context of an organization
- **All factors must be considered in the prevention of failure**

Statoil

Standards for risk analysis in the Norwegian oil and gas industry

NORSOK Z-013 Chapter 6.6 (QRA)	Statoil GL0282 E.4.7 Consequence modelling in TRA:
• Cause analysis and frequency data for initiating events shall contain an evaluation of the need to include evaluations of human and organisational factors. This is particularly important where accidents may be caused directly by human or organisational errors. • For the analysis of causes/frequency of initiating events in a QRA, **an explicit human reliability analysis should as far as possible be carried out.**	The consequence modelling should elaborate possible outcomes of the initiating events. All hazards that may contribute significantly to the overall risk picture should be included. The consequence modelling should reflect the specific design of the facility subjected for analysis. **The effect of human and organizational factors should be explicitly analysed to the degree possible. The probability and related severity of possible outcomes should be quantified.**

Statoil

Reliability Engineering and System Safety 96 (2011) 468–479

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Table 3
Level and number of installations.

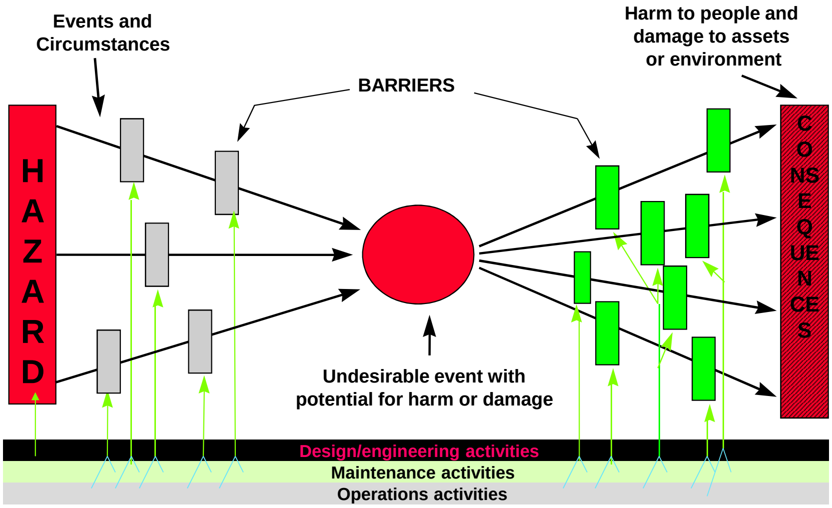
Level	Number of installations
1—None existing	5
2—Explained but not adjusted	8
3—Explained and the models are adjusted	2
4—Explained, models adjusted and included in the overall risk management	0

Available online 4 January 2011

Keywords:
Quantitative Risk Analysis
Human factors
Organizational factors

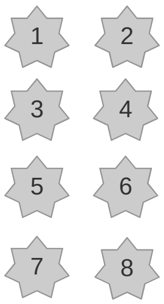
QRAs. The QRAs are categorized into four levels according to the findings. Level 1 QRAs do not describe or comment on the HOF-factors at all. Relevant research projects have been conducted to fulfill the requirements of Level 3 analyses. At this level, there is a systematic collection of data related to HOF. The methods are systematic and documented, and the QRAs are adjusted. None of the QRAs fulfill the Level 4 requirements. Level 4 QRAs include the model and describe the HOF-factors as well as explain how the results should be followed up in the overall risk management. Safety audits by regulatory authorities are probably necessary to point out the direction for QRA and speed up the development.

Bow-tie model



Analysis strategy

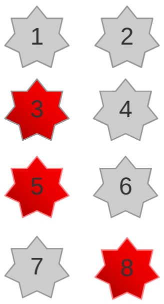
Screening



Statoil

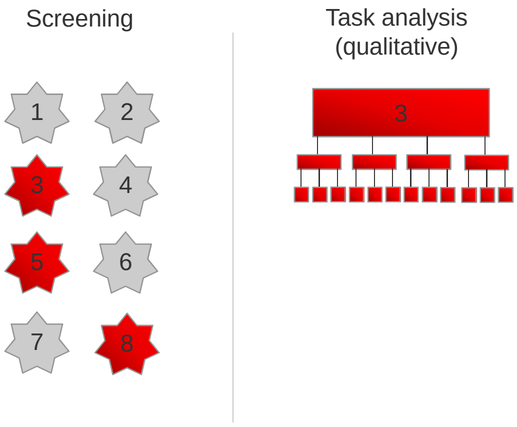
Analysis strategy used in pilot assessments

Screening

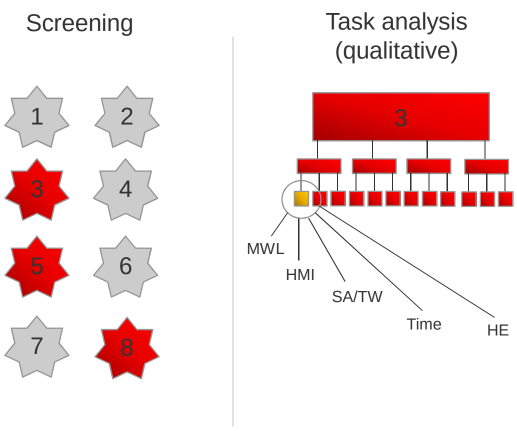


Statoil

Analysis strategy used in pilot assessments

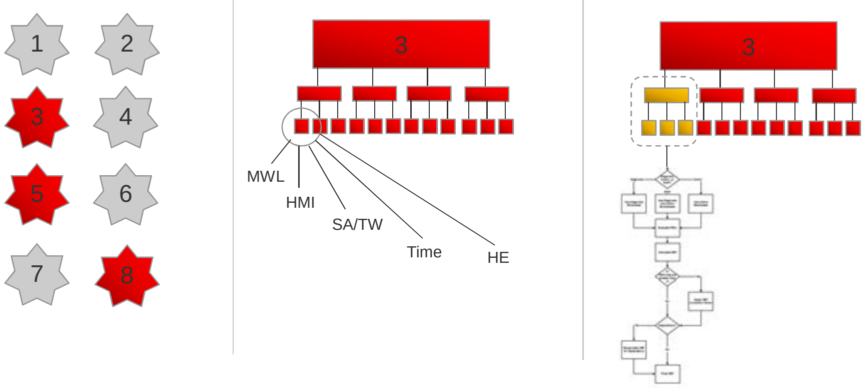


Analysis strategy used in pilot assessments



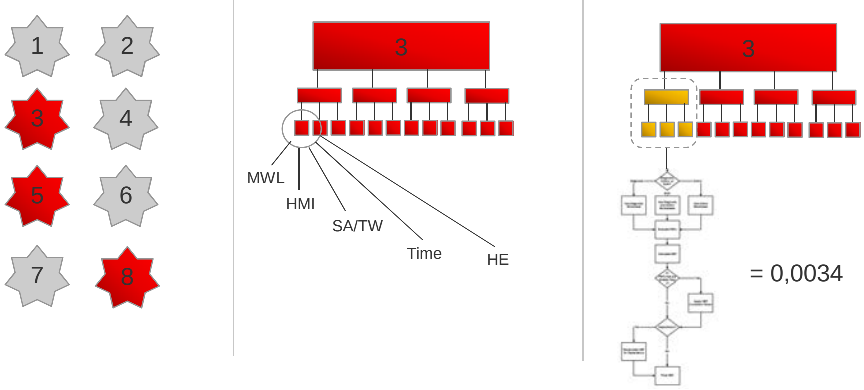
Analysis strategy used in pilot assessments

Screening | Task analysis (qualitative) | Quantitative analysis

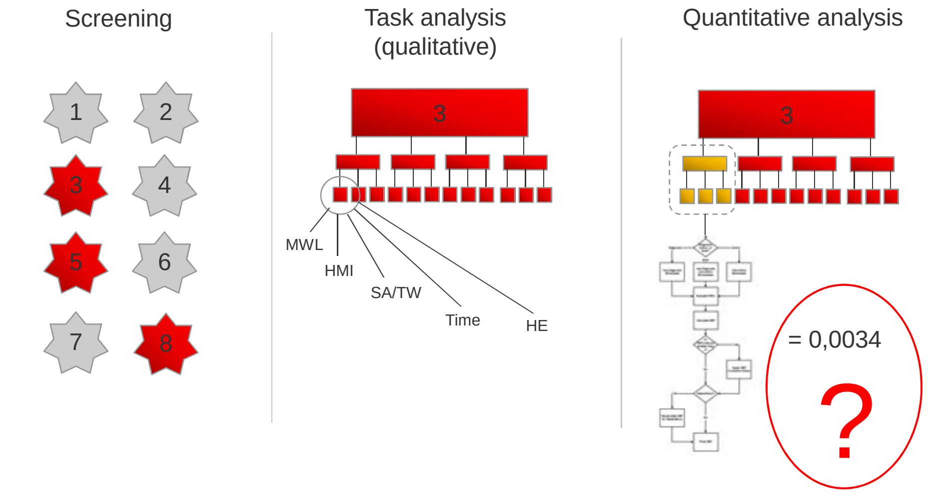


Analysis strategy used in pilot assessments

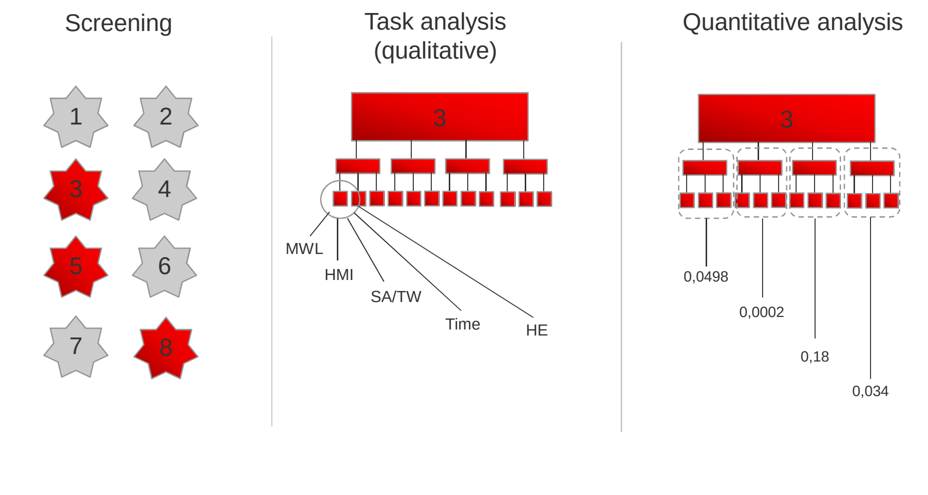
Screening | Task analysis (qualitative) | Quantitative analysis



Analysis strategy used in pilot assessments



Analysis strategy used in pilot assessments



Risk identification of human and organizational barriers in DFUs for greenfield projects

#	Hazard group	Description for AHa	Special /additional mitigating measures implemented	Human and organisational barriers relevant	Residual major accident risk	Classification
1.	Oil and gas leakage	Use of chemicals: • The design shall seek to ensure no need for environmentally black, red or Y2 (nearly red) chemicals under operation and seek to minimize the use of chemicals in general. • No major accidental potential is identified related to chemical release.	Basis: Norsok S-001/TR 1055 requirements implemented. • Focus put on access to equipment to improve maintenance and reduce human errors in operation of equipment • Strategy is to apply compact flanges for equipment > = 3" for preesure class >= 600 lbs per square inch (41 bar). Expected to cause reduced leak frequency • Reduced use corrosion inhibitor on pipelines due to liner applied inside riser/pipeline. • No obvious leak sources on HC piping between topside and substructure	Installation procedure for compact flanges sensitive to human errors.	- Major accidents covered by "Oil pollution", "Fire and explosion" or "loss of well control". - Unsolved matter: Clarify how fire and explosion escalation to in deck tanks are avoided.	
2.	Oil pollution	• Liquid production is condensate (no heavy oil) • Low production rate of HC liquids (approx 30 m^3 per hour)				
a.	• Top side		• Basis:Norsok S001/TR1055 • Very low blowout frequency topside due to wells located at subsea templates.			

- All main accident scenarios (DFUs) are been assessed for human and organisational barrier dependency
- Identified major accident scenarios form the basis for human reliability analyses to be performed during detail engineering

Statoil

HRA pilot analyses in Statoil 2010-2013


Troll C

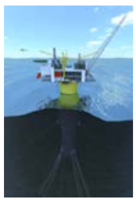

Melkøya LNG


Åsgard B


Draupner


Gullfaks C


Visund


Aasta Hansteen

Statoil

Preliminary experiences with HRA

Positive:
- Systematic approach to HF in major accident risk
- Improved decision basis
- Strengthens interdisciplinary approach to safety
- Supports prioritization

Negative:
- Lack of TRA ownership
- Can tend to be control room-centric
- Absolute values cannot be used in QRA
- Human errors do not affect overall facility risk
- Methods are based on nuclear industry

Nuclear power plants and petroleum installations - similarities and differences

- Operator tasks
- System design
- Accident scenarios
- Regulatory requirements
- Analysis methodology (PRA/QRA)

Performance-shaping factors

- Any factor that influences performance

SPAR-H (NUREG/CR-6883)			
PSFs	PSF Levels	HEP for Diagnosis[1]	HEP for Action[1]
Available Time	Inadequate time	1.0 (no multiplier)	1.0 (no multiplier)
	Barely adequate time	0.1 (10)	0.01 (10)
	Nominal time	0.01 (1)	0.001 (1)
	Extra time	0.001 (0.1)	0.0001 (0.1)
	Expansive time	0.0001 (0.1-0.01)	0.00001 (0.01)
Stress/ Stressors	Extreme	0.05 (5)	0.005 (5)
	High	0.02 (2)	0.002 (2)
	Nominal	0.01 (1)	0.001 (1)
Complexity	Highly complex	0.05 (5)	0.005 (5)
	Moderately complex	0.02 (2)	0.002 (2)
	Nominal	0.01 (1)	0.001 (1)
	Obvious diagnosis	0.001 (0.1)	N/A
Experience/ Training	Low	0.1 (10)	0.003 (3)
	Nominal	0.01 (1)	0.001 (1)
	High	0.05 (0.5)	0.0005 (0.5)
Procedures	Not available	0.5 (50)	0.05 (50)
	Incomplete	0.2 (20)	0.02 (20)
	Available, but poor	0.05 (5)	0.005 (5)
	Nominal	0.01 (1)	0.001 (1)
	Diagnostic/symptom oriented	0.005 (0.5)	N/A
Ergonomics/ HMI	Missing/Misleading	0.5 (50)	0.05 (50)
	Poor	0.1 (10)	0.01 (10)
	Nominal	0.01 (1)	0.001 (1)
	Good	0.005 (0.5)	0.0005 (0.5)
Fitness for Duty	Unfit	1.0 (no multiplier)	1.0 (no multiplier)
	Degraded Fitness	0.05 (5)	0.005 (5)
	Nominal	0.01 (1)	0.001 (1)
Work Processes	Poor	0.02 (2)	0.005 (5)
	Nominal	0.01 (1)	0.001 (1)
	Good	0.008 (0.8)	0.0005 (0.5)

PSF	PSF Level	Multiplier for Diagnosis	Multiplier for Action
Available Time	Inadequate time	P(failure) = 1.0	P(failure) = 1.0
	Barely adequate time	10	10
	Nominal time	1	1
	Extra time	0.1	0.1
	Expansive time	0.01	0.01
	Insufficient Information	1	1

Statoil

Performance-shaping factors

- Any factor that influences performance

SPAR-H (NUREG/CR-6883)			
PSFs	PSF Levels	HEP for Diagnosis[1]	HEP for Action[1]
Available Time	Inadequate time	1.0 (no multiplier)	1.0 (no multiplier)
	Barely adequate time	0.1 (10)	0.01 (10)
	Nominal time	0.01 (1)	0.001 (1)
	Extra time	0.001 (0.1)	0.0001 (0.1)
	Expansive time	0.0001 (0.1-0.01)	0.00001 (0.01)
Stress/ Stressors	Extreme	0.05 (5)	0.005 (5)
	High	0.02 (2)	0.002 (2)
	Nominal	0.01 (1)	0.001 (1)
Complexity	Highly complex	0.05 (5)	0.005 (5)
	Moderately complex	0.02 (2)	0.002 (2)
	Nominal	0.01 (1)	0.001 (1)
	Obvious diagnosis	0.001 (0.1)	N/A
Experience/ Training	Low	0.1 (10)	0.003 (3)
	Nominal	0.01 (1)	0.001 (1)
	High	0.05 (0.5)	0.0005 (0.5)
Procedures	Not available	0.5 (50)	0.05 (50)
	Incomplete	0.2 (20)	0.02 (20)
	Available, but poor	0.05 (5)	0.005 (5)
	Nominal	0.01 (1)	0.001 (1)
	Diagnostic/symptom oriented	0.005 (0.5)	N/A
Ergonomics/ HMI	Missing/Misleading	0.5 (50)	0.05 (50)
	Poor	0.1 (10)	0.01 (10)
	Nominal	0.01 (1)	0.001 (1)
	Good	0.005 (0.5)	0.0005 (0.5)
Fitness for Duty	Unfit	1.0 (no multiplier)	1.0 (no multiplier)
	Degraded Fitness	0.05 (5)	0.005 (5)
	Nominal	0.01 (1)	0.001 (1)
Work Processes	Poor	0.02 (2)	0.005 (5)
	Nominal	0.01 (1)	0.001 (1)
	Good	0.008 (0.8)	0.0005 (0.5)

PSF	PSF Level	Multiplier for Diagnosis	Multiplier for Action
Available Time	Inadequate time	P(failure) = 1.0	P(failure) = 1.0
	Barely adequate time	10	10
	Nominal time	1	1
	Extra time	0.1	0.1
	Expansive time	0.01	0.01
	Insufficient Information	1	1

→ Focus on factors that are identifiable and possible to assess in a design phase

Statoil

Performance-shaping factors

- Any factor that influences performance

SPAR-H (NUREG/CR-6883)			
PSFs	PSF Levels	HEP for Diagnosis[1]	HEP for Action[1]
Available Time	Inadequate time	1.0 (no multiplier)	1.0 (no multiplier)
	Barely adequate time	0.1 (10)	0.01 (10)
	Nominal time	0.01 (1)	0.001 (1)
	Extra time	0.001 (0.1)	0.0001 (0.1)
	Expansive time	0.0001 (0.1-0.01)	0.00001 (0.01)
Stress/ Stressors	Extreme	0.05 (5)	0.005 (5)
	High	0.02 (2)	0.002 (2)
	Nominal	0.01 (1)	0.001 (1)
Complexity	Highly complex	0.05 (5)	0.005 (5)
	Moderately complex	0.02 (2)	0.002 (2)
	Nominal	0.01 (1)	0.001 (1)
	Obvious diagnosis	0.001 (0.1)	N/A
Experience/ Training	Low	0.1 (10)	0.003 (3)
	Nominal	0.01 (1)	0.001 (1)
	High	0.05 (0.5)	0.0005 (0.5)
Procedures	Not available	0.5 (50)	0.05 (50)
	Incomplete	0.2 (20)	0.02 (20)
	Available, but poor	0.05 (5)	0.005 (5)
	Nominal	0.01 (1)	0.001 (1)
	Diagnostic/symptom oriented	0.005 (0.5)	N/A
Ergonomics/ HMI	Missing/Misleading	0.5 (50)	0.05 (50)
	Poor	0.1 (10)	0.01 (10)
	Nominal	0.01 (1)	0.001 (1)
	Good	0.005 (0.5)	0.0005 (0.5)
Fitness for Duty	Unfit	1.0 (no multiplier)	1.0 (no multiplier)
	Degraded Fitness	0.05 (5)	0.005 (5)
	Nominal	0.01 (1)	0.001 (1)
Work Processes	Poor	0.02 (2)	0.005 (5)
	Nominal	0.01 (1)	0.001 (1)
	Good	0.008 (0.8)	0.0005 (0.5)

PSF	PSF Level	Definition
Available Time	Inadequate time	If the operator cannot perform the task in the amount of time available, no matter what s/he does, then failure is certain
	Barely adequate time	Two-thirds of the average time required to complete the task is available.
	Nominal time	On average, there is sufficient time to diagnose the problem.
	Extra time	The time available is between one to two times greater than the nominal time required.
	Expansive time	The time available is greater than two times the nominal time required.
	Insufficient Information	If you do not have sufficient information to choose among the other alternatives, assign this PSF level.

Statoil

Snorre A

Fukushima Daichi

Statoil

Do we need another risk analysis process in the oil and gas industry?

Human reliability assessment

- Quantification supports qualitative analysis
- Provides a better decision basis for well-defined risks
- Allows better ranking of risks and prioritization of mitigating actions
- Is cost-effective, since it relies heavily on existing documentation

Limitiations

- The human error probabilities have no value on their own
- The analyses cannot be performed in isolation from the overall TRA
- Requires high level of skill in execution
- Requires detail in qualitative analysis

Future efforts

- Improve and test methodology
- Provide better guidelines for practical use
- Stronger cooperation with other safety disciplines
- More practical experience
- Database building
- Learning from others

Eagle or turkey?

There's never been a better time for good ideas

Human Reliability Assessment in Major Accident Risk Analyses

Kristian Gould
Principal Consultant
E-mail kgou@statoil.com
Tel: +47 911 89 657

www.statoil.com

Statoil

The application of the SPAR-H method in managed-pressure drilling operations

Koen van de Merwe (DNV), Sondre Øie (DNV) & Kristian Gould (Statoil)
17.10.2012

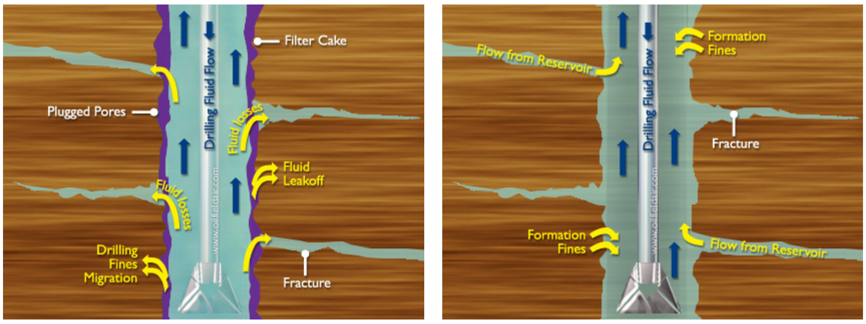
MANAGING RISK DNV

Overview

- Managed-Pressure Drilling
- SPAR-H
- Method
  - Task Analysis
  - SPAR-H
  - SHERPA
- Results
  - HEP in relation to safety
  - SPAR-H as prioritization tool
  - SPAR-H for drill floor operations
- Discussion

MANAGING RISK DNV

Managed-Pressure Drilling



Conventional drilling

Managed Pressure drilling

Source: Air Drilling Associates, Inc.

Normal drilling

Case study: Continuous Circulation concept

- Supplier proposed a novel method of managed pressure drilling
  - Continuous circulation of mud
  - Fewer disturbances because of well-control issues
  - Increased penetration rates (potentially 2-3 times faster)

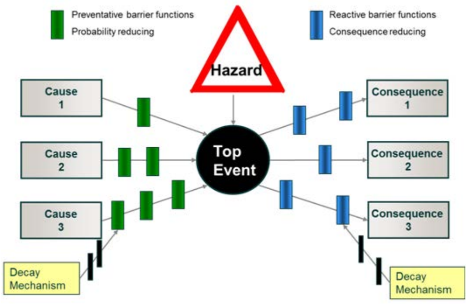
- Changes introduced on the drill floor
  - New procedures
  - New equipment (side-entry valve)
  - Additional personnel
  - Equipment under constant pressure

- What are the risks of operating the proposed concept?

SPAR-H

- Standardized Plant Analysis Risk – Human Reliability Analysis
  - Developed for the nuclear power industry
  - Fairly simple method
  - Validity
  - Inter-rater reliability

- Applied to normal operations

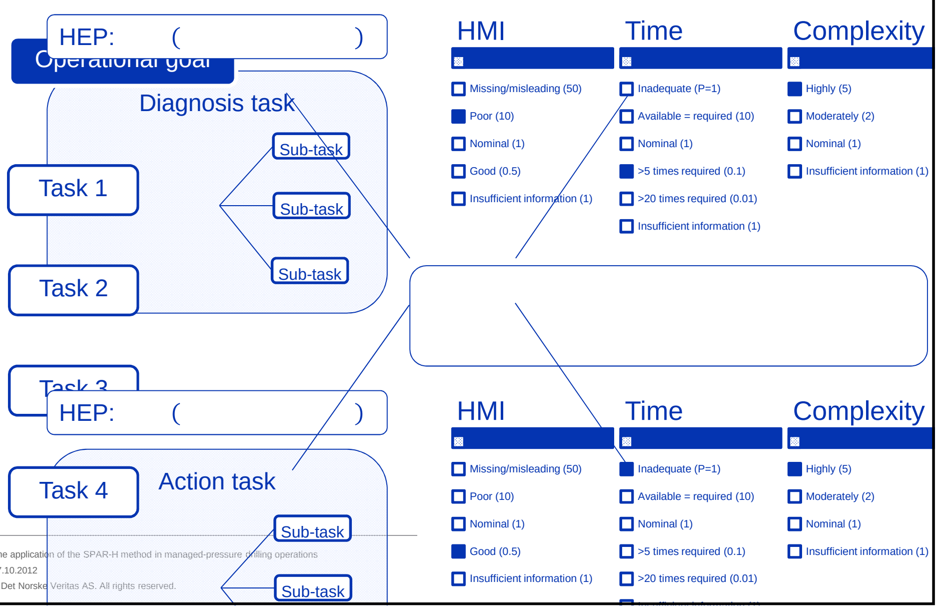


Method - Workshop

- Preparation
  - Choosing a scenario: normal operations
  - Data gathering
    - Documentation
    - Video
    - Procedures
- Workshop (2 days)
  - Perform task analysis
    - Identification of tasks
    - Breaking down into concrete operations
  - Define task characteristics (input to PSFs)
    - Checklists
    - Interviews
  - Apply Human Error Identification technique (SHERPA)

MANAGING RISK DNV

SPAR-H analysis method (simplified)



Prioritization based on HEP

Original

Task	HEP
2. Remove cap	HEP = 0.504
3. Prepare connector	HEP = 0.200
5. Divert flow SEV to TDS	HEP = 0.501
7. Divert flow TDS to SEV	HEP = 0.501

Prioritized

Human Error Identification

- Systematic Human Error Reduction and Prediction Approach (SHERPA)

Task step	Error mode	Error description	Consequence	Recovery	Criticality
5.1	A1	Opening the valve too quickly.	Potential damage to the NSD system due to hammer effect.	None	!
	A6	Opening of the wrong valve.	Opening X6: Diverting mud to the bleed system instead of the NSD system. No circulation.	Via the driller (trip tank level continues to rise).	!
	A8	Failure to open the valves to the NSD hose (X1).	No flow to the side entry valve.	None	!
5.2	A4	Failure to completely closing the ball valve	Maintain pressure and mud in the TDS.	Task 5.4: via the driller (trip tank level continues to rise).	!
	A8	Failure to close the ball	Maintain pressure and	Task 5.4:	!

Prioritization based on HEP

Original

2. Remove cap	HEP = 0.504
3. Prepare connector	HEP = 0.200
5. Divert flow SEV to TDS	HEP = 0.501
7. Divert flow TDS to SEV	HEP = 0.501

Prioritized

★

★

★

Prioritized mitigations based on PSF & SHERPA

SPAR-H

2. Remove cap ★
- Complexity A
- Experience B
- Procedures C

5. Divert flow SEV to TDS ★
- Procedures A
- HMI B

SPAR-H & SHERPA

2. Remove cap ★
- Design A
- Training B
- Procedures C

5. Divert flow SEV to TDS ★
- Procedures C
- Layout B
- Logic A

Lessons learned and recommendations

1. Scenario choice, HEP and their relation to safety
   - Normal operations and the SPAR-H requires additional safety analyses
   - Avoids tasks with high HEP that are not safety critical (risk-based)

2. SPAR-H purely as a prioritisation tool
   - Ordinal ranking between tasks based on HEP
   - Further ordinal ranking within tasks based on SHERPA

3. Using the SPAR-H for drill-floor operations
   - PSF descriptions have nuclear focus (training time, wording)
   - PSF multiplication factors

   - Nuclear control room to oil & gas control room
   - Nuclear control room to drill floor operations?

Conclusion

(Combined) methods provide structured approach to assessing human error, but…

…a relative approach to HEPs may be the best way forward at the moment.

Safeguarding life, property and the environment

www.dnv.com

15

MANAGING RISK

HFC

Barrier Management - Technical, operational and organizational barrier elements, is it possible to define performance requirements to operational and organizational barrier elements? A regulators perspective

Ø. Lauridsen

Mer informasjon:
www.ptil.no/nyheter/prinsipper-for-barrierestyring-article8268-24.html

Barrier management

Technical, operational and organizational barrier elements.
Is it possible to define performance requirements to operational and organizational barrier elements?
A regulators perspective

Øyvind Lauridsen
Principal engineer, Ph.D.
Petroleum Safety Authority Norway
(PSA)

PTIL/PSA

List of contents

- The PSA's central requirements related to barriers and barrier management
- The barrier management process
- Barrier strategy
- The barrier concept and definition
- Examples of performance requirements to barrier elements and the distinction to performance shaping factors
- Conclusion

PTIL/PSA

2

The PSA's requirements related to barriers and barrier management

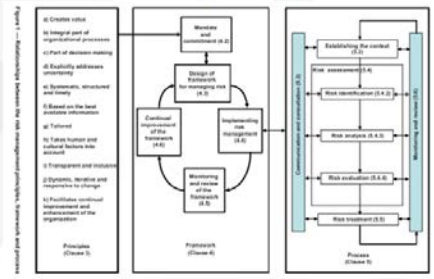
- Barriers shall be established that:
  - reduce the probability of failures and hazard and accident situations developing,
  - limit possible harm and disadvantages.
- The operator shall
  - stipulate the strategies and principles that form the basis for design, use and maintenance of barriers, so that the barriers' function is safeguarded throughout the facility's life.
- Establish barriers – and it shall be known:
  - Which function the barriers shall maintain
  - Which requirements for performance have been placed on the technical, operational or organisational elements that are necessary to ensure that the individual barrier is effective
  - Which barriers are non-functioning or weakened
  - Implement necessary compensating measures to restore or compensate for missing or weakened barriers

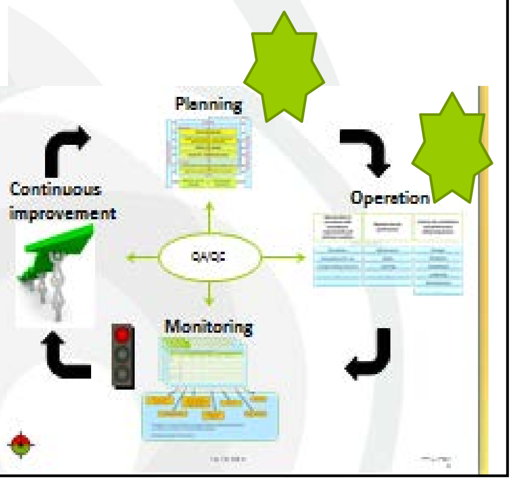
Management regulation section 5 (summary)

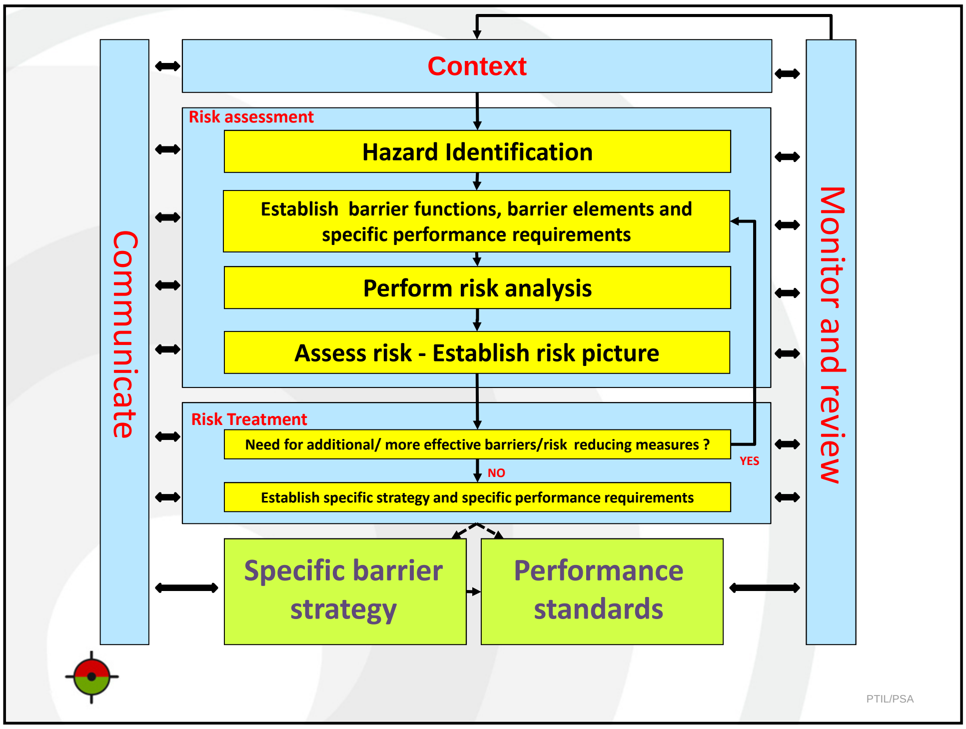
2012-10-19
PTIL/PSA
3

The barrier management process

ISO 31000 Risk Management



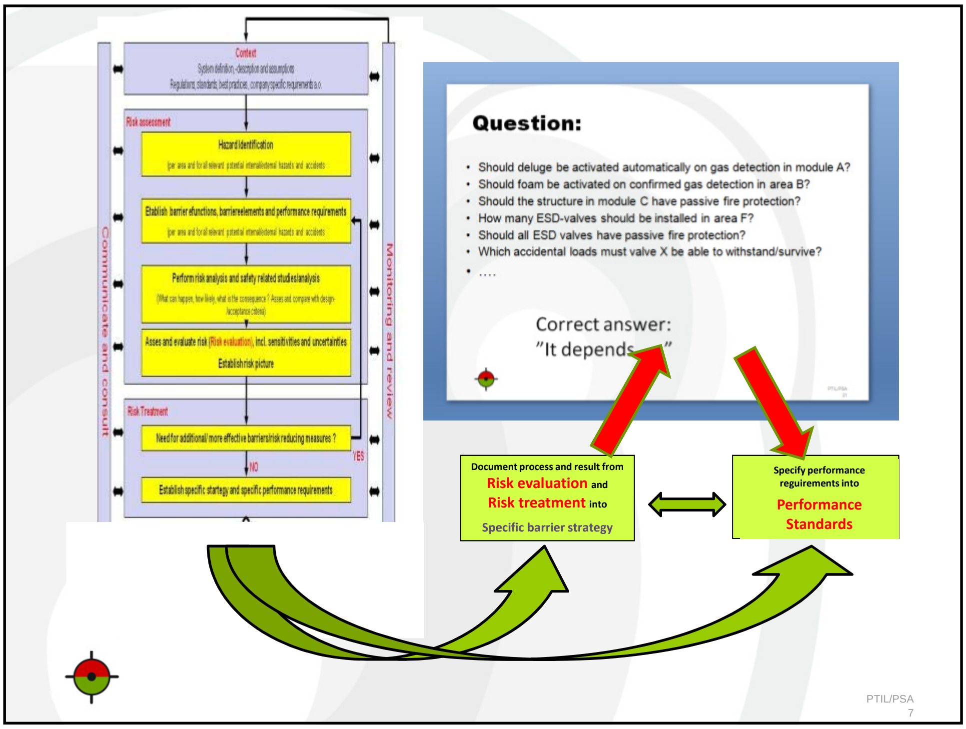




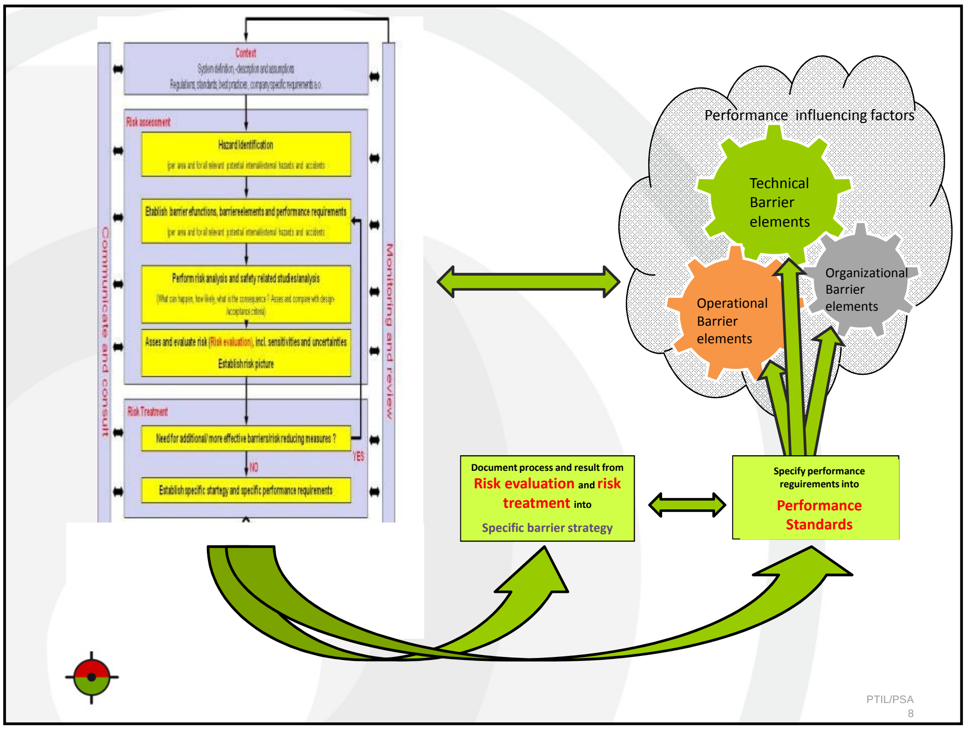
Operational phase

Operate plant in accordance with assumptions, requirements and technical condition	Maintain barrier performance	Control risk contributors and performance influencing factors
Procedures	Maintenance	Changes
Assumptions for use	Audits	Deviations
Compensating measures	Learning	Competency
...	...	Leadership
...	...	Risk awareness
		...

PTIL/PSA
6



Context
Risk assessment
Hazard identification
Establish barrier functions, barrierelements and performance requirements
Perform risk analysis and safety related studies/analysis
Asses and evaluate risk (Risk evaluation), incl. sensitivities and uncertainties
Establish risk picture
Risk Treatment
Need for additional/ more effective barriers/risk reducing measures ?
YES
NO
Establish specific startegy and specific performance requirements
Communicate and consult
Monitoring and review
Question:
Should deluge be activated automatically on gas detection in module A?
Should foam be activated on confirmed gas detection in area B?
Should the structure in module C have passive fire protection?
How many ESD-valves should be installed in area F?
Should all ESD valves have passive fire protection?
Which accidental loads must valve X be able to withstand/survive?
....
Correct answer:
"It depends....."
Document process and result from Risk evaluation and Risk treatment into
Specific barrier strategy
Specify performance reguirements into
Performance Standards
PTIL/PSA
7



Context
Risk assessment
Hazard identification
Establish barrier functions, barrierelements and performance requirements
Perform risk analysis and safety related studies/analysis
Asses and evaluate risk (Risk evaluation), incl. sensitivities and uncertainties
Establish risk picture
Risk Treatment
Need for additional/ more effective barriers/risk reducing measures ?
YES
NO
Establish specific startegy and specific performance requirements
Communicate and consult
Monitoring and review
Performance influencing factors
Technical Barrier elements
Operational Barrier elements
Organizational Barrier elements
Document process and result from Risk evaluation and risk treatment into
Specific barrier strategy
Specify performance reguirements into
Performance Standards
PTIL/PSA
8

What Characterises a Good Strategy?

- It shows the connection between the risk and hazard assessments, the role/task of barrier functions (**Role of risk reducing measures**) and corresponding need for barrier elements (**Need for risk reducing measures**).
  - The strategy is broken down into appropriate ”area levels” on the installation and is kept updated at all times.
- The strategy process (which, among other things, includes risk analyses and results evaluation) leads to robust design accidental loads as well as specified performance standards for safety systems, safety functions and scenarios.
  - The performance standards shall contain detailed performance requirements of the barrier elements (i.o.w. operation, personnel, equipment and systems) that are necessary in order to realise the barrier function.
- The strategy and the performance standards give all involved parties the necessary understanding as to why barrier functions have been established and which performance requirements are placed on different barrier elements.
  - Important to ensure that the use of the facility complies with the technical condition of the facility and the assumptions regarding safe use of it.

2012-10-19
PTIL/PSA
9

Barrier Concept

- The word ”barrier” is often used in daily speech, and many different environments have an ownership of the concept, which therefore has acquired many and partially differing interpretations. ”.

PTIL/PSA

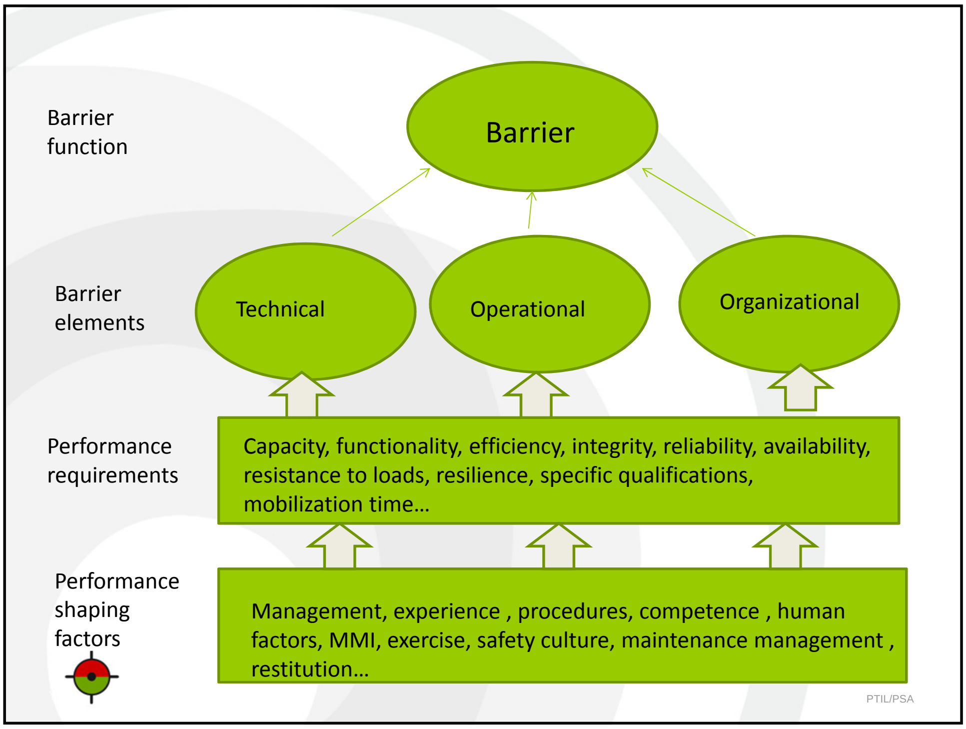
The Barrier definition used in the management regulation and detailed in the memorandum "Principles for barrier management in the petroleum industry"

- Barrier : Technical, operational and organizational elements which individually or together shall:
  a) reduce the possibility of occurrence of specific errors or hazards, or
  b) reduce or prevent damage if they occur.
- Barrier elements : Technical, operational or organizational measure or solution necessary for realizing a barrier function
- Barrier function: The task or role of the barrier

PTIL/PSA

http://www.ptil.no/nyheter/prinsipper-for-barrierestyring-article8268-24.html

PTIL/PSA



Hydrocarbon leak
Examples of barrier elements

- Gas detection
- Logic (preprogrammed)
- Emergency shutdown
  - ESD valves close
  - ignition source inhibit
  - deluge release (if appropriate)
  - blow down to flare
- General alarm
- Emergency team muster
- Further actions taken at the field, in CCR and by emergency management

Kick
Examples of barrier elements

- The mud logger detect influx of formation fluids
  - Evaluate the situation
  - Warn the driller
- The driller collect information from mud logger and own instruments
  - Evaluate the situation
  - Decide to shut in the well
- Push the button to shut the BOP
- The BOP seal the well
  - eventually emergency shutdown of production process
  - ignition source inhibit
- General alarm
- Normalizing the well
  - Choice of methods

Black: Technical barrier elements
Red: Operational and organizational barrier elements

PTIL/PSA

Hydrocarbon leak

- Gas detection
- Logic (preprogrammed)
- Emergency shutdown
  - ESD valves close
  - ignition source inhibit
  - deluge release (if appropriate)
  - blow down to flare
- General alarm
- Emergency response team muster
- Further actions taken at the field, in the CCR and by the emergency management

Performance requirements
examples

- Positions, category and number of gas detectors
- Criteria for initiating the emergency shutdown
- Functional requirement to ESD valves (shut down time, flow rate criteria)
- Number of members and competence for the emergency team, CCR and emergency mngt.
- Response time
- Duties and responsibility

Performance shaping factors
examples

- Management of engineering, risk assessment and commissioning processes
- HF, MMI
- Inspection procedures
- Test interval, handling of test results related to accept criteria
- Maintenance management
- General capacity and competence in the organization
- Work load and number of duties for important positions
- Restitution
- Adequate procedures and their quality and availability
- Team experience and exercise
- Safety culture
- Management follow up and prioritization of safety

Kick

- The mud logger detect influx of formation fluids
  - Evaluate the situation
  - Warn the driller
- The driller collect information from mud logger and own instruments
  - Evaluate the situation
  - Decide to shut in the well
- Push the button to shut the BOP
- The BOP seal the well
  - eventually emergency shutdown of production process
  - ignition source inhibit
- General alarm
- Normalising the well
  - Choice of methods

Performance requirements
examples

Qualification requirements for dedicated positions
Pit discipline
Heel criteria (rig stability)
Criteria for action
Response time
Sensor availability and functionality
Operability for critical pit valves
Communication lines and means
Functional requirements of BOP (shut in time, flow rate criteria)
Duties and responsibility

Performance shaping factors
examples

- Management of engineering, risk assessment and commissioning processes
- HF, MMI
- Communication and familization between involved parties
- Inspection procedures and maintenance management
- Test interval, handling of test results related to accept criteria
- Capacity and competence
- Work load and number of duties for important positions
- Restitution
- Adequate procedures, their quality and availability
- Team experience and exercise
- Safety culture
- Management follow up and prioritization of safety

Performance requirements - emergency preparedness

- The organization's specific requirements for emergency ("VSKTB'er")– an old example of typical organizational and operational performance requirements:
  - for instance mustering time of emergency response teams, requirements for pickup person in the sea, time for POB control…
- Performance shaping factors
  - Content in the training of rescue teams, communications in an emergency situation, training in a deputy role…

PTIL/PSA

Some remarks about the distinction between barrier elements and performance shaping factors

- Procedures are not organizational or operational barrier elements – but can be guiding on establishing, testing and maintaining barrier elements
- Safe Job Analysis (SJA) are not organizational or operational barrier elements – but can identify operational risk that has to be handled by operational or organizational barrier elements
- Work permits are not operational or organizational barrier elements – but can stipulate barrier elements that shall be established before the work starts
- Management is not an operational or organizational barrier element – but can ensure that barriers are established and maintained

PTIL/PSA

Conclusion

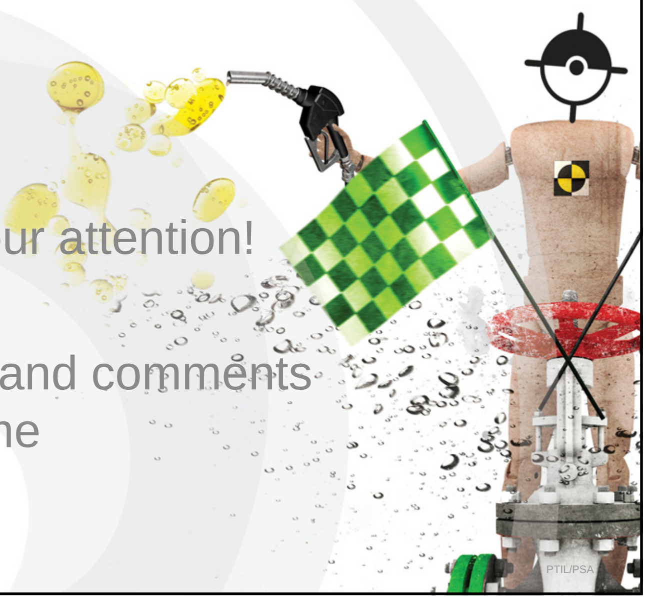
- The question was:
  - Is it possible to define performance requirements to operational and organizational barrier elements?
- The answer is:
  - If you follow the intention in the management regulation section 5 about barrier management

  and use
  - the principle and definitions in the memorandum “Principles for barrier management in the petroleum industry”
- it is fully possible to define performance requirements to operational and organizational barrier elements in the same manner as for technical barrier elements.

- But if you define performance shaping factors as barrier elements it will probably be hard to define performance requirements relevant for them

Thanks for your attention!

Questions and comments are welcome



PTIL/PSA

HFC

Lessons learned from human reliability applications in the US space program.

R. Boring

Mer informasjon:
http://www.hq.nasa.gov/office/codeq/rm/docs/HRA_Report.pdf

Lessons Learned from Human Reliability Applications in the US Space Program

Human Factors in Control Workshop
Institute for Energy Technology
October 17, 2012

Ronald Laurids Boring, PhD
Human Factors Principal Scientist
Idaho National Laboratory

Overview of Today's Talk

- Brief History of Human Reliability Analysis (HRA)
- NASA HRA Selection Guide
- NASA PRA Guide
- NASA HRA Database
- NASA Shuttle HRA Review
- Summary

But First, My Rocky Road with Norsk

- Living in Halden in 2007, I'd go to grocery store, get to checkout counter, and someone would ask me something I didn't understand

`Vil du ha en p/?/se?`

`Vil du ha en` **`pause`**`?`

`Vil du ha en` **`pose`**`?`

`Vil du ha en` **`pølse`**`?`

Preventing a Rocky Road with HRA

HRA was developed for the nuclear industry

The bits and pieces are all there for other industries, but there may be some translation involved

Look at NASA to see if they can be the universal translator

Lesson Learned 1

As other industries start using HRA, study the example of those who have successfully adapted it from nuclear.

October 17, 2012

5

Brief History of HRA

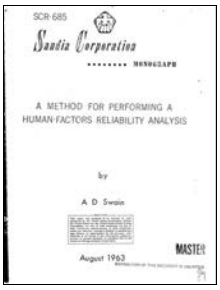
October 17, 2012

6

HRA Timeline

US Air Force weapons safety projects at Los Alamos and Sandia — 1962 Human Factors Conference: Symposium of Human Error Quantification — Technique for Human Error Rate Prediction (THERP) — 1976: WASH-1400 Application to Nuclear Power — 1983: NUREG/CR-1278 THERP —

- Simplified 1G Methods (ASEP, SPAR-H, HEART)
- 2G Methods (CREAM, ATHEANA, MERMOS)
- 3G Methods (MicroSaint, IDAC, MIDAS)


SCR-685

Sandia Corporation

MONOGRAPH

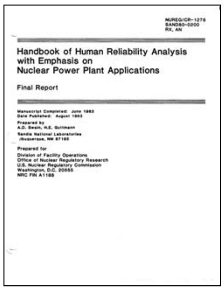
A METHOD FOR PERFORMING A HUMAN FACTORS RELIABILITY ANALYSIS

by

A. D. Swain

MASTER

August 1963


NUREG/CR-1278

Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications

Final Report

Swain's Observations on THERP History

- 1960s, main emphasis was on collecting data
  - Sandia Human Error Rate Bank (SHERB, with Rigby) database
  - Equally interested in predicting human success and human error
- c. 1970, Jens Rasmussen invited Alan Swain to Risø National Laboratory to discuss use of HRA for nuclear power
  - Rasmussen very impressed with Swain's insights into nuclear power operations
  - Two years later, Swain finally was able to take a course on nuclear engineering
- 1975: WASH-1400 articulated THERP approach for nuclear power
- 1983: NUREG/CR-1278 formalized approach for nuclear power

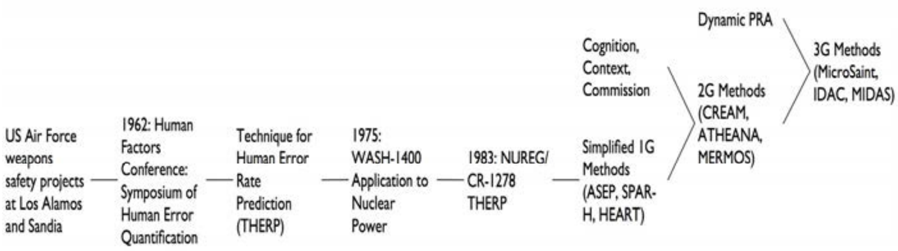

Ron Boring and Alan Swain, December 2009

Regrets

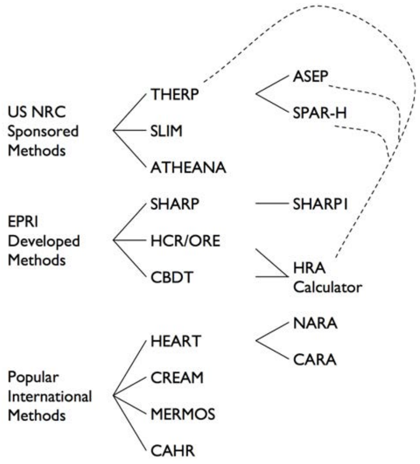
Alan Swain, 1972

"There should have been many more changes had the research been done to develop more hard data on HEPs for human tasks. That failure has been a disappointment to me....I always said that the data tables in [THERP] were not written in stone, and I was not Moses coming down from a mountain with these tables so inscribed."

History of HRA (Sample of Methods)



Evolution of Selected HRA Methods



- Methods developed for different purposes by different teams with different philosophies

Lesson Learned 2

THERP was only the beginning!

NASA HRA Selection Guide

October 17, 2012

13

Context

- By mid 2000s, NASA had some experience using HRA to support the probabilistic risk assessments (PRAs) for the Space Shuttle and the International Space Station
- Analyses conducted at Johnson Space Center
- Some confusion over which of the methods to use
  - THERP was most common method, but it was a bit of a stretch in some cases
  - Too many other methods to choose from
- In 2005, NASA Headquarters Office of Safety and Mission Assurance wanted to formally review methods and select most applicable for NASA missions

October 17, 2012

14

Approach

- Formal review of HRA methods by criteria
- Formal workshop with HRA experts

Results from NASA Selection

- Use HRA throughout the life cycle of the system, beginning early in the system design process
- Human factors design efforts should pay special attention to the accident scenarios identified by the HRA
- HRA must be an integral part of the PRA development

Lesson Learned 3

Align HRA with human factors and risk analysis (PRA/QRA) in your domain.

Results from NASA Selection

- HRA should include errors of omission and commission and pre-initiating, initiating, and post-initiating actions
- HRA should include evaluation of errors for both cognitive responses and physical actions
- A screening analysis allows analyst to establish risk significant events

Results from NASA Selection

- Risk significant human errors should be included in the PRA
- The HRA should specifically consider those performance shaping factors (PSFs) unique to space and explicitly document the relationship to those PSFs included in HRA methods
  - Microgravity and isolation

Lesson Learned 4

Figure out how your domain is different from nuclear and document how that is mapped in the HRA.

Results from NASA Selection

- HRA methods selected
  - THERP
    - Comprehensive
  - CREAM
    - Cognitive factors
  - SPAR-H
    - Simplified
  - NARA
    - Empirically validated

- Selection criteria
  - Applicability to existing designs
  - Ability to quantify
  - Screening capability
  - Task decomposition guidance
  - Flexible PSF list
  - Broad coverage of error sources
  - Errors of omission/commission
  - Error recovery
  - Dependence
  - Validation
  - Usability
  - Wide use and acceptance

Lesson Learned 5

Don't leave it to chance which HRA methods are used. Do a rigorous selection of the best methods for your domain.

Lesson Learned 6

HRA can be very political, both within your organization and across methods. Use rigorous criteria to find the best methods for your use.

NASA PRA Guide

PRA at NASA

- While risks considered since 1969, PRA not formally undertaken until post Challenger
  - 1986 *Investigation of the Challenger Accident* showed NASA could not determine probability of failure of Shuttle events
  - 1988 *Post-Challenger Evaluation of Space Shuttle Risk Assessment and Management* recommended PRA
  - 2002 *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners*
    - Included instructions on using THERP
    - 2012 revision greatly expanded discussion of HRA and included full instructions for using THERP, SPAR-H, CREAM, and NARA

Lesson Learned 7

Ensure the proper tools, guidance, and training are available to use HRA once it is implemented.

The NASA HRA Database

Integrating HRA into Human Factors

New Requirements

- NASA Procedural Requirement 8705.2A: *Human-Rating Requirements for Space Systems* (2005)
  - Specifies a design review process for all new systems that are used by humans or that come in contact with human systems
  - Purpose: Ensure that no single-point and no two inadvertent actions cause death or permanent disability to crew, public, passengers, or ground personnel
  - A system may be human-certified when it demonstrates that it has fully considered safety aspects in the design of the system

HRA for Human Rating Certification

How Can NASA Achieve Human-Certification?

- The problem is twofold
  - Traditional human factors engineering/ergonomics involved in design and testing of new technologies to be used by humans
    - Much emphasis on usability (e.g., Nielsen), enjoyment (e.g., Norman), and safety (e.g., Palanque)
    - There is no concise process to ensure that the design and testing have covered all bases and have met safety goals
  - Traditional HRA involved in assessment and modeling of designs in the context of a larger system safety
    - HRA often used in diagnostic analysis ex post facto, including a safety review of a designed system
    - HRA rarely used in an iterative way as part of the system design process

The Human Rating Framework

One Solution

- Merge human factors engineering/ergonomics with HRA
  - Emphasis on human factors for reliability
    - Integrate human factors design and evaluation within the probabilistic risk framework found in HRA
  - Emphasis on human reliability for design
    - Integrate HRA into the design phase such that it becomes a prescriptive tool for generating design ideas that can be tested and verified
- Use of HRA to establish safety levels to meet Human Rating Requirements for new system designs

Lesson Learned 8

HRA is not used just because it's attractive. It's used because it supports safety and is required. Ensure that the regulatory framework supports HRA.

A New Human Reliability Database for NASA

Collect Data to Inform HRAs in Space Domain

Redresses Three Shortcomings in Existing HRA

- Domain-Specificity
  - Targets data outside the traditional realm of nuclear power plant operations
- Data Sources
  - Includes specific fields for incorporating completed HRAs, incident reports, psychological research using human subjects or simulation, and operations logs
- Utility of Information
  - Applicable to both HRA and system design
  - Incorporates quantitative information appropriate to HRA such as Human Error Probabilities (HEPs) and PSFs
  - Incorporates qualitative information appropriate to system design such as overall "lessons learned"

HR Database Overview

Data Structures Recorded in Taxonomy

Data Overview (All Data Sources)						
Unique Record ID	Year	Short Title	Citation of Data Source	Industry	Keywords	Relevant Space Activity Type

Data Overview (All Data Sources) (cont)						
Summary/ Abstract	Link to Source	HRA Identification Level	HRA Modeling Level	HRA Quantification Level	HRA Design Level	Related Records

Research Data Sources				
What Was Manipulated (Independent Variable)	What Was Measured (Dependent Variable)	What Was Found/ Qualitative Finding	What Was Found/ Quantitative Finding	Design of Study

Incident, Event, or Accident Report Data Sources			
Lessons Learned	Problem/Root Cause	Corrective Action/Fix	PSFs

HRA and HRA Method Data Sources						
Activity/ Scenario Modeled	PSFs	Error Type	Analysis Method Used	Hardware Systems Affected	HEP/Failure Rate	Recovery Modeled

Operations and Training Log Data Sources	
Lessons Learned	Other Observations

- Fields represent a high-level classification, not a minutely detailed categorization of the data
- Fields are open-ended

Lesson Learned 9

To support future use and reuse, provide examples of HRA applied in the new domain.

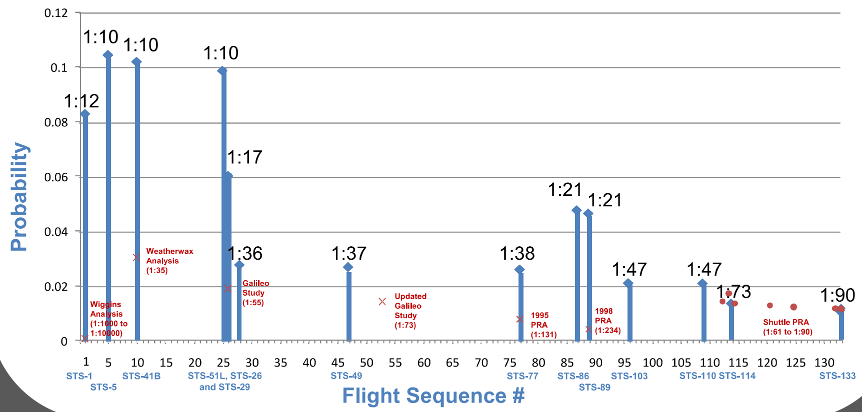
NASA Shuttle HRA Review

October 17, 2012 35

Ongoing NASA Review of PRA

Review in 2011 by Teri Hamlin and Colleagues at Johnson Space Center

- Consistent historic underestimation of the risk of Loss of Crew Vehicle (LOCV)
- Red indicates previous overall failure probability; blue is updated value



October 17, 2012 36

Revisiting Previous PRA and HRA

Increased Fidelity in Modeling

- Additional hardware and software systems modeled, introducing new types of failure
- Estimates of crew error did not change significantly
- However, some design changes and process improvements were difficult to account for in the HRA
  - Independent oversight
  - Management structure
  - Safety Organization
  - Communication
  - Maintenance safeguards
- The lack of these human factors improvements might have meant even larger failure rates for earlier shuttle missions
- These factors could also mean lowered failure rates for later missons

Lesson Learned 10

Learn and improve! Review HRA after it's been used for a while, and don't be afraid to revise guidance or methods where there are inadequacies.

Summary

October 17, 2012 39

Ten Lessons Learned Applying HRA at NASA

1. As other industries start using HRA, study the example of those who have successfully adapted it from nuclear.
2. THERP was only the beginning!
3. Align HRA with human factors and risk analysis (PRA/QRA) in your domain.
4. Figure out how your domain is different from nuclear and document how that is mapped in the HRA.
5. Don't leave it to chance which HRA methods are used. Do a rigorous selection of the best methods for your domain.
6. HRA can be very political, both within your organization and across methods. Use rigorous criteria to find the best methods for your use.
7. Ensure the proper tools, guidance, and training are available to use HRA once it is implemented.
8. HRA is not used just because it's attractive. It's used because it supports safety and is required. Ensure that the regulatory framework supports HRA.
9. To support future use and reuse, provide examples of HRA applied in the new domain.
10. Learn and improve! Review HRA after it's been used for a while, and don't be afraid to revise guidance or methods where there are inadequacies.

October 17, 2012 40

Ten Lessons Learned Applying HRA at NASA

Adapting HRA from nuclear energy requires

- A risk framework
- Understanding of the HRA methods as they are used in nuclear
- Thorough knowledge of the new domain and human factors issues in the new domain
- Patience to apply the methods
- Resources to create new guidance for the methods or refinements of the methods

NASA's example has been successful

- HRA now fully integrated into the safety requirements and system design process
- HRA **will** be successful in reducing the risk of the Shuttle replacement vehicles

October 17, 2012

41

Questions?

ronald.boring@inl.gov

October 17, 2012

42

HFC

The Petroleum Safety Authority has accused Statoil for lacking the ability to learn - are they right?

K. Hansen

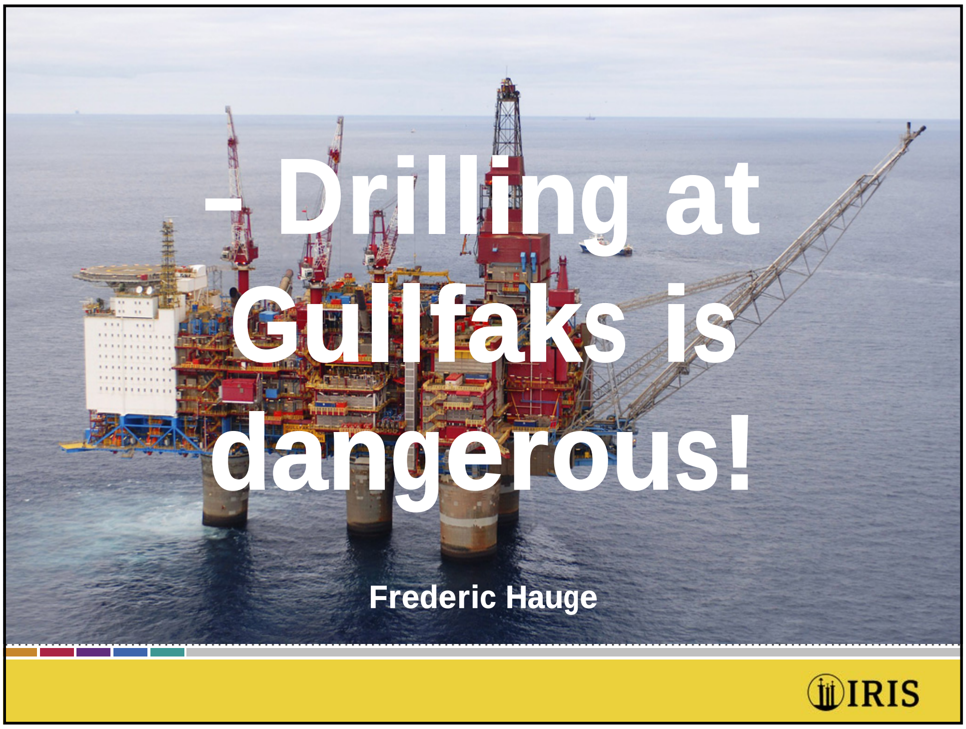
Mer informasjon:
IRIS: "Læring av hendelser i Statoil" Rapport IRIS-2011/156

The PSA has accused Statoil for lacking the ability to learn - are they right?

Kåre Hansen

IRIS

IRIS


– Drilling at Gullfaks is dangerous!
Frederic Hauge
IRIS


– The police will investigate Statoil
Dagbladet.no
IRIS

About the assignment

IRIS

About the assignment (I)

- Based on an order from the Petroleum Safety Authority Norway (Petroleumstilsynet)
- **Four main parts:**

1. Reveal underlying causes of the incident at Gullfaks C
2. Discuss the relevance between Snorre A and Gullfaks C
3. Discuss Statoil's abilities to learn from failures – reveal potential learning barriers.
4. Develop improvement measures

IRIS

About the assignment (II)

- Duration of 3,5 months
- A ”mission impossible”

7

IRIS

What did we do to find the answers?

IRIS

Method (I)

51 interviews

3746 responses

11 scientists

IRIS

51 in-depth interviews

- Statoil employees (36)
- Three subcontractors/suppliers (15)
- Seven different interview guides
- Duration of 45 minutes to 2(+) hours
- App. 72 hours of sound recording

IRIS

3746 answers - survey

- Statoil employees (730) response: 62,7 %
- 9 subcontractors/suppliers (2513)
  response: 45,8 %

Document analysis

- Supervisory investigation reports
- Internal reports and media coverage

11 scientists

- Interdisciplinary group
- 3 technologists (drilling and well)
- 8 social scientists / economists
- Experience from the trial research programme on the Statoil & Hydro merger
- Core group of 6 scientists
- Stavanger and Bergen

IRIS

Underlying causes of the incident at Gullfaks C

IRIS

Method

- We have asked employees and managers in Statoil and three subcontractor companies that directly or indirectly were involved in the incident:
- *What happened before, during, and after the incident?*
- *Why did it happen?*
- *Why, why, why...*

IRIS

4 causes

IRIS

1 Governing documentation and compliance

2 Management and decision making

3 Competence and training

4 Communication and documentation

IRIS

Learing from incidents – what are the main barriers?

IRIS

NRK > Nyheter > Distrikt > Møre og Romsdal

Møre og Romsdal | Siste fjernsynssendinga

- Statoil har ikke lært av alvorlige episoder

En flere tonn tung gjenstand falt ned fra heisekrana på Heidrun-plattforma i april.
Foto: Statoil

Petroleumstilsynet mener Statoil ikke har lært av alvorlige hendelser med heisekraner på plattformene.

IRIS

FAKTA

Statoils tabbeliste

Petroleumstilsynet kritiserer Statoil for ikkje å ha lært av desse hendingane

28. november 2005
Ukontrollert gassutblåsing på havbotnen på Snorre A. Ei av dei mest alvorlege hendingane på norsk sokkel, meinte Petroleumstilsynet. Berre flaks hindra storulykke med tap av menneskeliv.

16. oktober 2008
Oljelekkasje under vedlikehaldsarbeid på eit av skafta på Stafjord A-plattforma. Eksplosjonfare på grunn av oljedamp. Nær ved å kunne bli ei ulukke med omkomne og omfattande ureining.

19. mai 2010
Den siste av ei rekkje hendingar på Gullfaks C. Barrieren som skulle hindre gassutblåsing heldt ikkje, og gass strøymde ut. Berre tilfeldig at det ikkje blei storulykke.

4. desember 2010
Gasslekkasje på Gullfaks B. Tilsynet konkluderer med alvorlege manglar ved planlegging, godkjenning og gjennomføring av arbeidet. Eksplosjonsfare. Kunne utvikla seg til ei storulukke.

24. mars 2011
Petroleumstilsynet skuldar Statoil for å ikkje ha tatt lærdom av alle nære-på-ulykkene sidan 2005, og krev at konserndirektør for Undersøkjing og produksjon Noreg, Øystein Michelsen, svarar på kva selskapet vil gjere for å forbetre seg.

9. april. 2011
63 av 123 tilsette på Visundplattforma vart ekvakuerte etter gasslekkasje. Lekkasjen kom frå eit stigerør som fraktar olje og gass opp til plattforma. Petroleumstilsynet skal granske hendinga.

Kilde: BT

IRIS

Method

In the interviews and survey we have asked:

- *What are the main barriers for learning from incidents in Statoil and why do they excist*
- *Knowledge, use and judgement of the major tools for learning*
- *What should Statoil do to improve its ability to learn?*

IRIS

Learning in Statoil versus the suppliers

35 % of the employees in Statoil agrees that their company has a good capability to learn, compared to 68 % among the suppliers

IRIS

Investigation, measures and learning

- Scarce and rigid timelimits for investigations.
- Lacking routines for spreading of knowledge from investigations
- Overproduction of measures. ("Tiltakstretthet")
- "Incident-investigation-order-measures-incident..» creates stress and noice in the organisation. The relation between PSA and Statoil is one side of the problem.

IRIS

Power and learning (I)

- Learning requires openness, sincerity and honesty.
- The ability to learn is weakened by struggles between management and unions, and between the unions
- Incidents are used to gain power and influence. Creates noise and a resulting lack in the capasity to handle HSE.

IRIS

Power and learning (II)

- Informal networks («små kongedømmer») within D&W. Executes power, mainly outside the formal organisation
- Internal fight about ”what happened at Gullfaks”
- **Management lack the ability to bind power to the formal organisation. This is a major barrier for learning.**

IRIS

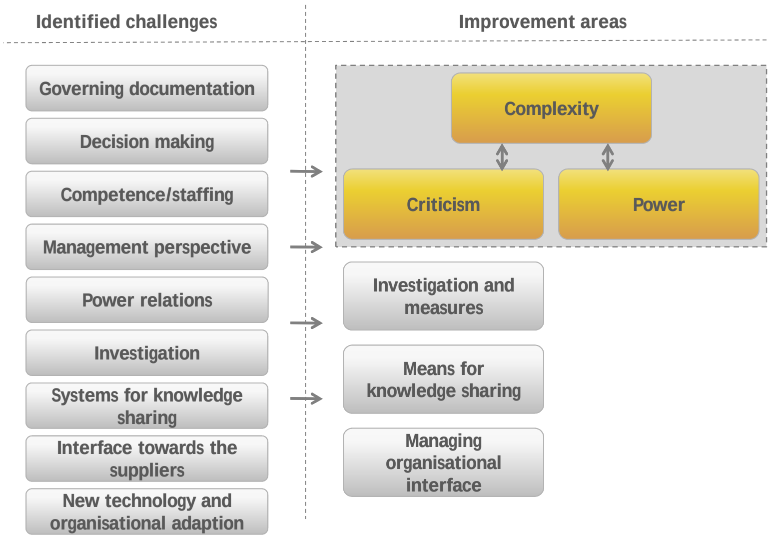
Management perspective

- Strong belief in systems and regulations among upper management
- Excessive belief in systems may produse overspesialisation and increased organisational complexity
- Result: increased gap between procedures and practice
- We find signs of this type of developments in Statoil

IRIS

?

Our suggestions to Statoil



3

Three major challenges

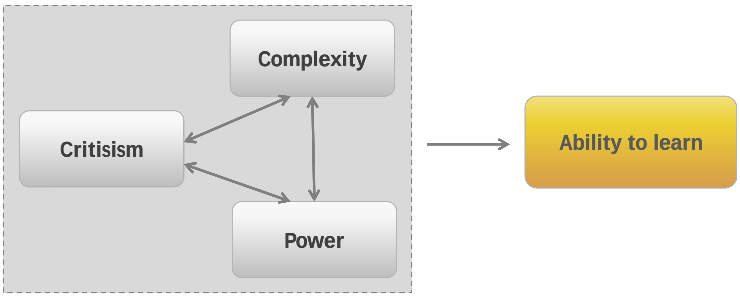
1 **Complexity in governing documentation and organisation**

2 **Power is not sufficiently tied up to the formal positions and arenas in the organisation**

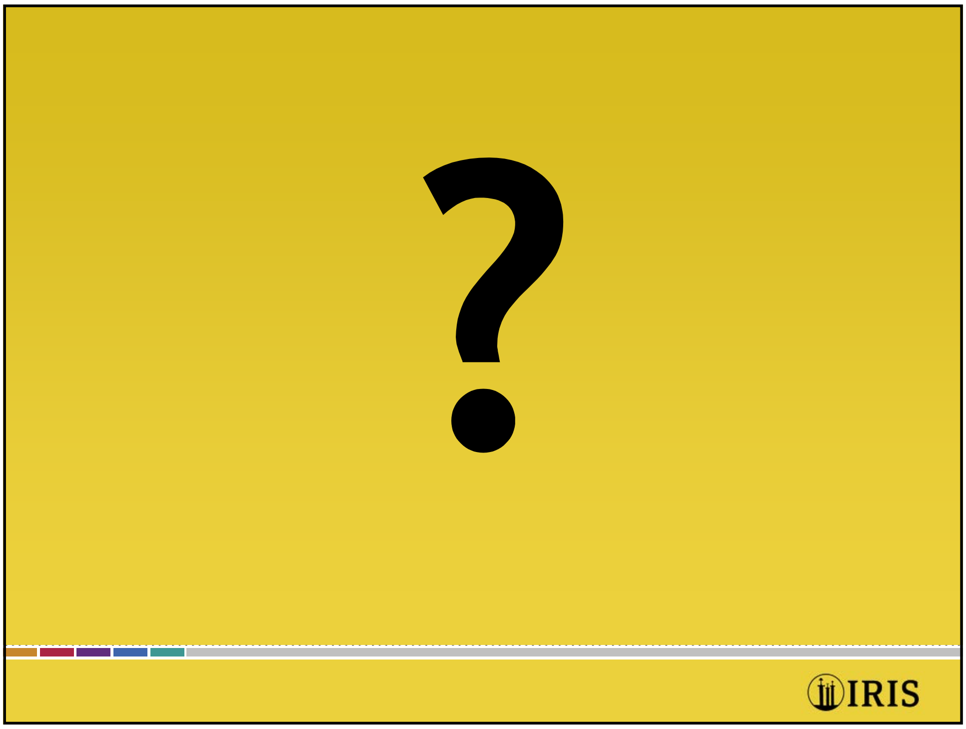
3 **Poor handling of criticism**

IRIS

The basic challenges



IRIS



Summary

The Petroleum Safety Authority Norway (PSA) has ordered Statoil to conduct follow-up investigations after the incident with well C06A at Gullfaks 19.05.2010. This report is a part of Statoil's follow-up, and describes the results of an independent study carried out by IRIS. The assignment has been to:

1) Conduct an analysis of underlying causes of the incident at Gullfaks C, related to governance, management and other organizational factors.
2) Analyze why measures for improvement initiated after previous incidents, among them the blowout at Snorre A in 2004, have not had the desired effects at Gullfaks.
3) Identify the most significant barriers preventing Statoil from learning from failures.
4) Present a recommendation of initiatives for improvement (in prioritized order) related to governance, management and other organizational factors, both for Gullfaks and for the company as a whole.

The study is based on interviews with employees at different organizational levels, both in Statoil and central contractors. In addition, data from a survey carried out in Statoil D&W and nine contractors are also reported on.

Underlying causes of the incident at Gullfaks C

Our study identifies several underlying causes of the incident at Gullfaks C, and some of these are related to the *organizational context* of the incident. In 2007, Statoil and Hydro Oil & Gas were merged, and a full integration of activities, resources and governing documents was initiated. All employees were given new job positions, and new functions, tasks, and responsibilities were assigned. As part of the integration process, large parts of Statoil's system for governing documents (DocMap) were included in Hydro's system (APOS). This resulted in an increase in complexity. In this respect, the results show that the procedures consist of too many documents, and that it is challenging to distinguish between processes, requirements, and methods. This is related to a lack of compliance. More specifically, the procedures are perceived as cumbersome and hard to relate to, and can further be difficult to comply with as there may be contradicting requirements related to a single operation. Factors related to *governing documents and compliance* may therefore represent underlying causes of the incident at Gullfaks C.

There are also several factors indicating that the change of manning effectuated in 2009 and 2010, had consequences for *management and decision making* at Gullfaks C. A large part of the management team at Gullfaks C was replaced, and our data indicate that this process was characterized by a low degree of transfer of experience. This resulted in a lack of *field- specific competence*. In addition, our analyses show that there was a low involvement of Statoil's central professional resources (MPD-experts) during the operation. Several aspects related to *planning* of the drilling operation are also emphasized. For example, it is a common perception that critical comments and remarks were dealt with in unfortunate ways. There were also important weaknesses of

the *risk evaluation* related to use of MPD. The perception of haste in carrying out the operation is highlighted in several interviews, and both economic aspects and internal pressure are in this respect pointed out as important explanatory factors.

However, our data also indicate that several risk evaluations were carried out without being documented. This indicates that there is a lack of (or insufficient) routines when it comes to documentation of discussions (e.g. in minutes), which means that decisions may be based on selective and limited action data. This will further strengthen the challenges related to transfer of experience. The analyses also show that there is a lack of systems that ensure appropriate handling of expressions of concern. Several aspects related to *communication and documentation* are thus highlighted as underlying causes of the incident at Gullfaks C.

From Snorre A to Gullfaks C

A central part of the assignment has been to analyze why measures initiated after previous incidents have not had the desired effects at Gullfaks C. The blowout at Snorre A in 2004 represents the basis for this analysis. A fundamental premise is in this respect that the incident at Snorre A (and the subsequent improvement measures) is relevant for Gullfaks C. Our analysis is strongly supportive of this, and we find several important similarities between the underlying causes of these two incidents. Factors related to "organizational context", "management and decision making", and "compliance" are central in both cases. The merger between Statoil and Hydro Oil & Gas has thus contributed to the occurrence of the same type of challenges revealed in the Snorre A investigation. In particular, aspects related to rotation, knowledge transfer, and governing documents are emphasized in this respect.

There are several factors that contribute to missing learning effects. Taken individually, several of the initiatives of improvement are appropriate; they are wide-reaching, concern important areas of improvement, and refer to the deficiencies that PSA pointed out. However, one of the main challenges is that the measures undertaken in order to implement individual initiatives, represent a hindrance for reaching the goals of one or several other initiatives. For example, the focus on planning and risk evaluation has resulted in more specific and detailed work processes and more bureaucracy, while other measures were directed at reducing the governing documentation and reduction of bureaucracy. Another central factor concerns the lack of acknowledging that improvement measures generally take a long time to implement (and reveal significant effects), and thus that initiatives have to be followed up over a longer time-span. It further seems that the focus on implementation and documentation of corrective actions related to the deficiencies pointed out by PSA, come at the expense of an organizational learning perspective on the incident.

Does Statoil learn from failures?

Statoil is a distributed organization, meaning that different units at multiple locations carry out similar operations. Accordingly, there is a great potential for knowledge exploitation across units, projects, and geographical locations, both within the organization and between Statoil and contractors. Learning does in this way to a large extent concern sharing and transfer of knowledge across organizational boundaries. Even though such processes occur on a daily basis in Statoil, our analyses show that there are challenges and potential for improvement within this topic area. Several means/tools (e.g. ICT-systems) for knowledge sharing do for example not function in adequate ways, and information relevant for work conduct is generally not perceived as easily accessible. There are further challenges related to organization and standardized coordination of the learning centers/academies in Statoil. Our study also shows that the *interface between Statoil and contractors* represents an area with significant potential for improvement. Key challenges within this topic area concern management of different governing documents, and that Statoil's follow-up processes of contractors today to a limited extent support/facilitate knowledge sharing and learning across organizational boundaries.

Another important factor that is highlighted is related to the existing power structures in the company. Our analyses show that the management in Statoil is not capable of *linking the authority and command to the formal positions* in the company in a satisfactory way. This renders possible the occurrence and development of informal power structures. In a learning perspective, the consequence of this is that the company may miss important learning opportunities. This happens when informal networks oppose the attempts of creating constructive loops of learning initiated by the formal organization.

Investigation and measures development is another important topic area when it comes to learning abilities in organizations. This is an area where Statoil has a great potential for improvement. Our study shows that the processes and procedures initiated after incidents are not adequate in a learning perspective. The time-frames for investigations are often too limited, and it seems like the company is more interested in closing the corrective actions rather than ensuring satisfactory organizational learning processes. Related to this, we also find that Statoil generates an excessive amount of measures, which has resulted in a condition of "initiative fatigue" in the organization. This further indicates a lack of abilities to prioritize, which to a certain extent is a consequence of the relationship between Statoil and PSA. Data from the interviews point to an occurring growth of nervousness in the organization regarding the possibilities for new incidents and ensuing orders from PSA. The consequence of this is a production of numerous measures that often are implemented too hasty, and that often lack internal consistency and a well thought-out basis. In addition, the reviews and follow-ups of corrective actions are also often inadequate.

A final aspect that influences Statoil's learning approach concerns *management perspective*. Interviews with senior leaders in the company indicate that there is a strong system confidence among central leaders in Statoil. More specifically, this means that there exists a belief that failures and incidents that occur are caused by employees' misuse of existing systems (e.g. APOS). A consequence of this is that the systems and potential underlying causes that may relate to failures that occur, to a lesser extent are subject for investigations and evaluations.

The analyses of learning barriers and underlying causes of the incident at Gullfaks C have implications for Statoil's organization and management system. More specifically, we find that there is a discrepancy between Statoil's organizational principles and work conduct in the organization. We also consider the findings to be incompatible with the value of "openness" in Statoil. There is further a mismatch between the findings and the organization and management system when it comes to the complexity of the governing documents, and also the roles of the process owners in Statoil.

Measures

On basis of the underlying causes of the incident at Gullfaks C, and the identified learning barriers in Statoil (D&W), we propose four areas of improvement. The first three areas are *investigation and measures development*, *adaptation and use of tools for knowledge sharing*, and *follow-up of contractors*. Several measures related to these areas are defined and discussed. However, we find that Statoil has more fundamental challenges related to a *complicated governance system*, *linking the authority and command to the formal positions*, and *handling criticism in the organization*. These issues are interrelated, and affect Statoil's learning abilities. These issues constitute our fourth area of improvement, and we perceive this area to be more fundamental than the other three areas. Succeeding with measures related to the first three areas of improvement is thus contingent upon a systematic and constructive handling of complexity, power relations, and criticism in the organization.

In order to succeed with this, we believe that the issue of linking authority and command to the formal positions in the organization has to be dealt with at all levels of management in Statoil. A holistic and collective focus aiming at strengthening the formal positions is necessary. Statoil should further develop a clear and overall policy for encouraging employees and leaders to express nonconforming points of view in constructive ways, with the objective of securing a more formal handling of nonstandard opinions and understandings, and by this avoid a situation where criticism is being expressed through informal networks and power structures. Finally, Statoil's governance system should be simplified. Measures in order to clarify the distribution of responsibility and authority in the matrix organization should be effectuated, along with initiatives that increase the comprehensibility and ease of use of governing documents. This will require a long-term perspective, but we believe that a priority programme emphasizing these issues is necessary in order to improve Statoil's learning abilities.

HFC

Lessons and experiences from applying human reliability analysis in the Swedish nuclear industry.

U. Kahlbom

Mer informasjon:

Risk Pilot
Your Risk Navigator

HRA - Experiences and lesson learned from the Swedish NPPs

i.e. a smorgasbord, or rather a starter, of relevant HRA-related questions

Ulf.Kahlbom@riskpilot.se

Risk Pilot
Your Risk Navigator

Risk Pilot – largest supplier for PRA/HRA in Sweden

- HFE-coordinators and HFE-specialists for the Oskarshamn 2 modernization project;
  - reactor safety and availability upgrades
  - the worlds highest nuclear power uprate.
- Safety evaluation of organizational change; PhD-thesis to download (in Swedish)
- PRA/HRA support in the procurement process for new builds in Finland.

Risk Pilot
Your Risk Navigator

Nine HRA related questions

1. Extent of plant visits and “analyst competence profiles”?
2. Process safety (i.e. core meltdown), or occupational safety?
3. How advanced are the methods used? Generation 1, 2 or ….. ½?
4. How do we deal with the large amounts of manual actions relevant on a NPP?
5. Which operational phases are we considering – and where are the major challenges?

Risk Pilot
Your Risk Navigator

Nine HRA related questions

6. Only PRA-driven HRA, or also “stand alone” HRA?
7. How to deal with manual action in the context of residual risk?
8. Is there a link between having conservative rules for inclusion of manual actions in the operational PRA/HRA and later modernization changes?
9. Organizational factors in PRA/HRA – Crucial to consider…. Or a dead end…..?

Risk Pilot
Your Risk Navigator

Plant visits and “analyst competence profiles”?

- Plants visits important; interviews, plant walk downs, ”dry runs”/talk through of scenarios.
- Analysts often familiar with nuclear power plant technology and organizations, and also experienced in incident analysis, safety culture etc. Mostly engineering background.
- Example of challenge on site
  - Getting harder to get hold of key personnel , subject matter experts.
- Possible solution
  - If suitable, get access to personnel in their day-to-day work

www.riskpilot.se 5

Risk Pilot
Your Risk Navigator

Process or occupational safety?

- Only process safety – (i.e. core meltdown)?

www.riskpilot.se 6

Risk Pilot
Your Risk Navigator

Process or occupational safety?

- Or, only occupational safety?
- Perspectives on safety given by the assignment:
  - *"WorkSafe has been on site, and determined that everything is under control"*

Risk Pilot
Your Risk Navigator

Process or occupational safety?

- Only focus on process safety, i.e.:
  - identifying sequences that lead to core meltdown
  - estimating the probabilities for sequences leading to core meltdown
- However, the approaches for detailed HRA is of course also applicable for occupational safety – and for general reliability analysis

Risk Pilot
Your Risk Navigator

How advanced are the methods used? Generation 1, 2 or ….. ½?

- For screening; simplified THERP/ASEP
  - Cat A&B ➔ Tables
  - Cat C ➔ Conservative Time-Diagnosis Curve

- For detailed analysis, Hierarchical and Tabular Task Analysis (HTA&TTA) + possibilities for expert judgment

Risk Pilot
Your Risk Navigator

Category A & B

Risk Pilot
Your Risk Navigator

How advanced are the methods used? Generation 1, 2 or ….. ½?

- Tables for Cat A&B; Screening HEP)

Difficulty	HEP	Description
Very easy	0,002	Mishaps/misunderstanding almost impossible AND very simple actions ………..
----	----	----
----	----	----
Rather difficult	0,1	Obvious risk for mishaps/misunderstanding /coordination problem, OR, action difficult due to local conditions …..
----	----	----

- Other tables used for ”immediate recovery”

www.riskpilot.se 11

Risk Pilot
Your Risk Navigator

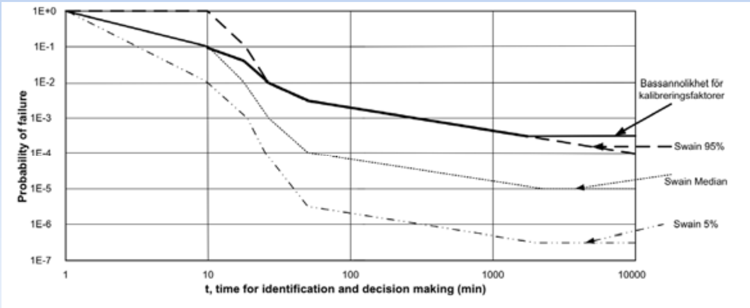
Category C

www.riskpilot.se 12

Risk Pilot
Your Risk Navigator

Category C

- For Cat C ➔ Conservative Time - Diagnosis Curve
- Calibration factors (”PSFs”)
  - Procedures, Training, Feedback
  - Stress, Coordination



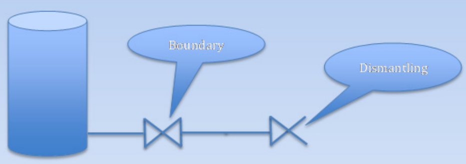
- *However - long time might worsen the situation*
- *Shorter time windows might be credited – but not in screening*

www.riskpilot.se 13

Risk Pilot
Your Risk Navigator

Handling of large amounts of manual actions-

Screening strategies; Cat B actions – leakage; hypoth. example



Work started on ”non-bounded off” component	**Leakage while dismantling component**							**Leakage; dismantled component**					
Plant specific screening value	Cond. for leakage – Dismantl. **Dis**				Leakage **Lea**			Opening ”Boundary” **Bo**			Time window **Ti**		
Ex: 1E-2	Dis1	Dis2	Dis3	etc	Lea1	Lea2	Etc.	Bo1	Bo2	Etc.	Ti1	Ti2	Etc.
	Res.risk	2E-3	1,0	---	1E-2	1,0	---	2E-5	1E-2	---	1E-2	1,0	---
Sign X for characteristics													

- $P_{leakage}$ (component X)=(1E-2*Dis*Lea)+(Bo*T)

www.riskpilot.se 14

Risk Pilot
Your Risk Navigator

Handling of large amounts of manual actions

1. Integration of PRA/HRA
2. Running of codes
3. Result; which are the most important actions with regards to core damage?
4. Most important: detailed analysis
   - Mostly Cat B actions that (if done wrong) lead almost directly to core damage
   - Some Cat C actions very important,
     e.g. recovering reserve electrical power supply after station black out (loss of external grid, diesels and gas turbines).

Integrate PRA/screening HRA

Run Fault tree/Event tree code

Evaluate results

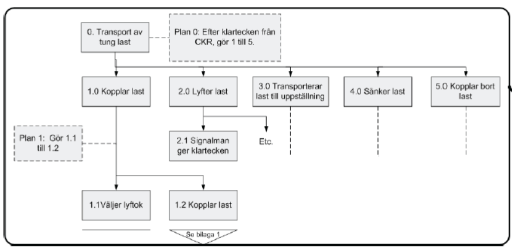
For most significant human actions ➔ perform detailed analysis

www.riskpilot.se 15

Risk Pilot
Your Risk Navigator

How advanced are the methods used? Generation 1, 2 or ….. ½?

- Detailed analysis, HTA&TTA, possibilities for expert judgment – APJ (Absolute Probability Judgment).
- PSF's important!
- If complicated sequences – use manual fault tree strategy
- So… rather a set of tools than a ”method”



Uppgift	Fel	Konse-kvens	Barriär
1.0 Koppla last			

Risk Pilot
Your Risk Navigator

Operational phases – major challenges – full power?

www.riskpilot.se 17

Risk Pilot
Your Risk Navigator

Operational phases – major challenges - outage?

www.riskpilot.se 18

Risk Pilot
Your Risk Navigator

Operational phases – major challenges?

- Historically, only full power
- Mid 90's, in Sweden also outage + start up & low power
- HRA is critical for the outage period; lots of manual actions (Category B), and reduced "defence in depth"

Risk Pilot
Your Risk Navigator

PSA-driven or stand alone HRA?

- Mainly PRA-driven
- Some risk significant human actions have been analyzed as stand alone, for example:
  - heavy loads
  - component work that could lead directly to core damage (large leakage from main circulation pumps)
- Especially stand alone HRAs have been important input for:
  - safety decision; e.g. working on main circulations pumps with nuclear fuel in the reactor vessel
  - design change
  - occupational safety aspects

Risk Pilot
Your Risk Navigator

Residual risks?

- Tricky to ”prove” that a human action (such as LOCA) is a residual risk
- Suggested solution:
  - The total sequence of HEPs should be less than 1E-7!
  - Explicit discussion regarding dependencies
    - At least three totally independent actions required for IE
    - (For example, different times and different work groups)
  - Or our previous example;
    - slowly increasing clear feedback……

www.riskpilot.se 21

Risk Pilot
Your Risk Navigator

Conservative rules and modernization changes

- In order to have conservative models we sometimes put strict demands for including Cat C actions
  - 30 minute rule
  - Req. procedures
- When modernizing, HRA-results should be taken into account (e.g. NUREG-0711)
- If important sensitive manual actions are screened out:
  - they don’t enter the experience feedback loop for reevaluating important human actions
  - …but they will probably be identified with other tools

www.riskpilot.se 22

Organizational factors in HRA/PSA?

- Some organizational factors are very hard to include; problems with cause-effect relations. Examples:
  - Routines for organizational change management, time since last reorganization, routines for handling of technical change, routines for documentation, Human Relations policies etc.

- Suggestion (PPOV):
  - Apply at least two perspectives, PRA/HRA + stand alone organizational analysis
  - Discuss both results in an integrated analysis
  - *Organizational factors are, however, implicitly included when performing expert judgment (if they are raised for discussion)…..*

Conclusions

- Analysts familiar with NPP technology and organization, try to include SMEs as much as possible.
- Screening criteria in order to take large amounts of actions into account, while limiting the amount of detailed analysis.
- The methods used range from generation 1 (screening) to 1,5 (detailed)…..
- Consider all operational phases, one very important phase from a HRA-point of view is outage, the shut down period.
- Mainly PRA-driven HRA, but also stand alone HRA

Conclusions

- Residual risk; HEP sequence for IE less than 1E-7 AND at least three different totally independent HEPs
- Conservative approaches when including manual actions, in the operational PSA, can affect input to modernization issues, i.e. risk of missing significant important human actions (Cat C)
- Add a stand alone assessment of organizational factors and integrate this with the results of the PRA/HRA discussions

www.riskpilot.se 25

Questions?

www.riskpilot.se 26

HFC

Reflections on the recent serious events in the offshore oil and gas sector from a risk assessment perspective with focus on human and organizational factors.

J.E. Vinnem

Mer informasjon:

Vinnem, J.E. (2010) Risk analysis in the planning processes of hazardous facilities – a case of an LNG plant in an urban area, Reliability Engineering and System Safety 95 (2010), pp. 662-670

Vinnem, J.E. (2010) Risk indicators for major hazards on offshore installations, Safety Science 48, pp. 770-787

Skogdalen, J.E., Utne, I.B. & Vinnem, J.E. (2011) Developing safety indicators for preventing offshore oil and gas deepwater drilling blowouts, Safety Science 49, pp. 1187–1199

Skogdalen, J.E., Vinnem, J.E., (2011). Quantitative risk analysis offshore-Human and organizational factors. Reliability Engineering & System Safety, 96, 468–479.

Skogdalen, J.E., Khorsandi, J.D. & Vinnem, J.E., (2012). Escape, Evacuation, And Rescue Experiences From Offshore Accidents Including The Deepwater Horizon. Loss Prevention in the Process Industries, 25/1, Pp 148-158

Skogdalen J.E., Vinnem J.E., (2011). Combining precursor incidents investigations and QRA in oil and gas industry. Reliability Engineering & System Safety, 101, pp. 48-58

Skogdalen, J.E., Vinnem, J.E., (2012). Quantitative risk analysis of oil and gas drilling, using Deepwater Horizon as case study. Reliability Engineering & System Safety, 100, 58–66.

Vinnem, J.E., (2012). On the Analysis of Hydrocarbon Leaks in the Norwegian Offshore Industry, Loss Prevention in the Process Industries, 25/4, pp. 709–717

Reflections on the recent serious events in the offshore oil and gas sector from a risk assessment perspective with focus on human and organizational factors

Presentation
Professor II Jan Erik Vinnem
University of Stavanger
jan.erik.vinnem@preventor.no

Universitetet i Stavanger

Overview

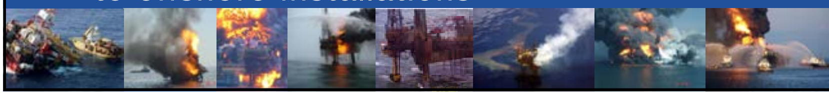
Major hazard focus

- Background and challenges
- Brief history
- Trends in accidents & incidents
- Trends in modelling of major accidents
- Goal-setting regime
- Life-cycle perspective
- Main regulatory principles
- Modelling practices
- Could risk assessment have prevented Macondo or Gullfaks C?
- Barrier management
- Conclusions

Universitetet i Stavanger

Background

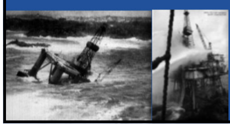
- Serious OO&G accidents since year 2000:
  - Capsize and sinking of Roncador P-36 (Brazil, 2001)
  - Burning blowout on Temsa field (Egypt, 2004)
  - Riser rupture and fire on Bombay High North (India, 2005)
  - Burning blowout on Usumacinta (Mexico, 2007)
  - Blowout on Montara field (Australia, 2009)
  - Burning blowout on Macondo field (US, 2010)
  - Pollution from well leak in Frade project, Campos Basin (Brazil, 2011)
  - Capsizing and sinking of Kolskaya jack-up during tow, (Russia, 2011)
  - Burning blowout on Endeavour jack-up platform (Nigeria, 12)
  - Uncontrolled well leak on Elgin platform in North Sea (UK, 12)
- Also several fatal helicopter accidents, during transit to offshore installations



Universitetet i Stavanger

Recent trends worldwide – offshore

- 2001–10 compared to 1991–2000:
  - Notably fewer major accidents in earlier period
  - Most severe ever, the explosions and fire on Piper Alpha in the North Sea in July 1988 in previous decennium
- Is this total failure of risk management?
- Proof that risk based regulations do not function?
- Virtually all offshore regions are represented
  - Looking to the North Sea, North Atlantic, Norwegian Sea and Barents Sea
    - Most severe accidents occurred some 20 to 30 years ago
    - No severe accidents at all during the latest period
    - Very serious near-misses recently



HFC Oct 2012 JEV rev0 4

Universitetet i Stavanger

Risk Level project (N)

- Objective
  - Establishing a realistic and jointly agreed picture of trends in HES work
    - In order to support the efforts made by the PSA and the industry to improve the HES level within petroleum operations
- History
  - April 2001
    - 1. report issued, for period 1996-2000
  - January 2004
    - Responsibility for HES for offshore & onshore petroleum facilities taken over by Petroleum Safety Authority
  - April 2007
    - 1. report with 8 onshore plants included, based on 2006 data
  - 2010
    - Extension from risk to personnel to risk for spills to sea
  - Regular schedule
    - Annual reports (risk to personnel) issued in April
    - Separate spill report in September

www.ptil.no/rnnp

Risk level project (RNNP)

- Major hazard risk one element of RNNP
  - Indicators suggest that major hazard risk has been reduced since year 2000
    - Precursor based indicators
    - Proactive (‘leading’) indicators based on barrier elements
  - On the other hand
    - Some installations are dramatically worse than average
    - Some are also exceptionally good
    - Large differences is a challenge for authorities
  - Modeling based on risk analysis R&D

Offshore risk management – success story?

- Impression
  - Norwegian & UK systems have been successful
    - Confirmed by Presidential Commission (US)
  - Large accidents have been avoided in NW Europe for long time
    - UK: after 1988
    - Norway: after 1985
- Is the situation so glorious as may be inferred from this?

Universitetet i Stavanger

Perspective: Alexander Kielland To Macondo

- Capsize and sinking of Alexander Kielland (Norway, 1980)
- Burning blowout on Macondo field (US, 2010)
- 30 years separation:
  - Capsize of the flotel Alexander L. Kielland in Norwegian North Sea
  - Burning blowout on Deep Water Horizon in US GoM
- Encompasses the development and use of risk assessments in risk management offshore

Universitetet i Stavanger

Brief history: Use of risk analysis (N)

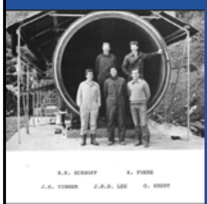
- Early start in late 1970s
- Regulatory requirement since 1981
- Approach initially based on practices in nuclear power plants
  - Usually no 3rd party personnel risk to consider offshore
- Development over time away from nuclear PSA approach
- QRA studies are not in the public domain
- Few cases where ethical controversies are known

- Offshore QRA
  - Focus on consequences (ignited HC leaks)
  - Limited focus on barrier failure probabilities
  - Causes of initiating events traditionally not covered
- NPP PSA
  - Focus on probability of defined scenarios
  - High focus on common mode & cause failures, etc
  - "Living PSA"

Universitetet i Stavanger

Brief history: Use of risk analysis

- Main application of risk assessments in the Norwegian industry in the 1980ties and 1990ties
  - Design tool, in order ensure that new installations had sufficient capabilities
    - To prevent major accidents and protect personnel in the case of such accidents
    - Significant investments in consequence modelling software tools, most well known is FLACS code



Universitetet i Stavanger

Brief history: Use of risk analysis

- Official inquiry by Lord Cullen in the UK, following Piper Alpha accident in 1988
  - Recommended that QRAs should be introduced into UK legislation
    - Corresponding to the way as in Norway nearly 10 years previously
  - Parallel focus on documentation through Safety Case documents

Universitetet i Stavanger

Brief history: Use of risk analysis

- Safety case
  - Primarily a tool for risk management in relation to existing installations
    - Main focus on consequences, layout and mitigation barriers
  - Similar approaches also adopted by several other countries (Denmark, Canada, Australia,..) & Shell on a worldwide scale ('HSE case')
- Many countries, most notably US, still have prescriptive regulations

Universitetet i Stavanger

Events that made marks on history

- NPPs
  - Three Mile Island (1979)
  - Chernobyl (1986)
  - Fukushima (2011)
- Accidents that have had similar extensive impact for the offshore operations:
  - Capsize of Flotel Alexander L. Kielland, 1980
  - Capsize of Mobile Offshore Drilling Unit Ocean Ranger, ‘82
  - Explosion & fire on fixed production platform Piper A, ‘88
  - Burning blowout on Deep Water Horizon mobile drilling unit, 2010

Impacts on Standards and Practices

- Capsize of the flotel Alexander L Kielland
  - Basic safety training for personnel
  - Use of conventional lifeboats in severe weather
  - Construction safety
  - Barriers to prevent rapid capsizing following major structural damage

Impacts on Standards and Practices

- Capsize of drilling rig Ocean Ranger
  - Improvement of ballast system flexibility for stabilizing the unit in high inclination angles
  - Training of ballast operators
  - Evacuation during severe weather conditions
  - Rescue of survivors following evacuation in severe weather

Universitetet i Stavanger

Impacts on Standards and Practices

- Explosion and fire on Piper Alpha
  - Active fire protection
  - Passive fire protection
  - Protection of Temporary Refuge (shelter area)
  - Barriers against high inventories in pipelines
  - Compliance with procedures & documentation

Universitetet i Stavanger

Trends in offshore QRAs (10–15 years)

- Very limited further development
  - Some further development of consequence tools
  - Precursor data and barrier performance data through RNNP (N)
- Development of tools and methods for incorporation of
  - Causes of initiating events within HOF envelop
    - Collisions with offshore vessels
    - HC leaks

HFC Oct 2012 JEV rev0 17

Universitetet i Stavanger

Overall purpose FPSO Operational Safety Project

- Develop models and tools for predictive human reliability analysis
- Test out methodology on selected case studies
- Illustrate results that may be obtained

Tandem loading configuration

HFC Oct 2012 JEV rev0 18

Universitetet i Stavanger

Objectives

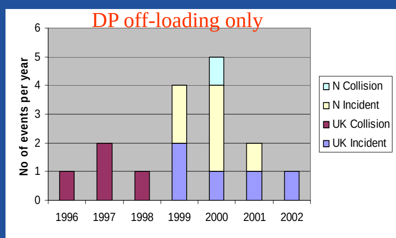
- Demonstrate importance of HOF collision risk
- Identify and evaluate the important HOF factors
- Propose potential risk reduction measures relating to HOF

Contractors:
NTNU
SINTEF

Sponsors:
ExxonMobil
HSE
Statoil
Navion

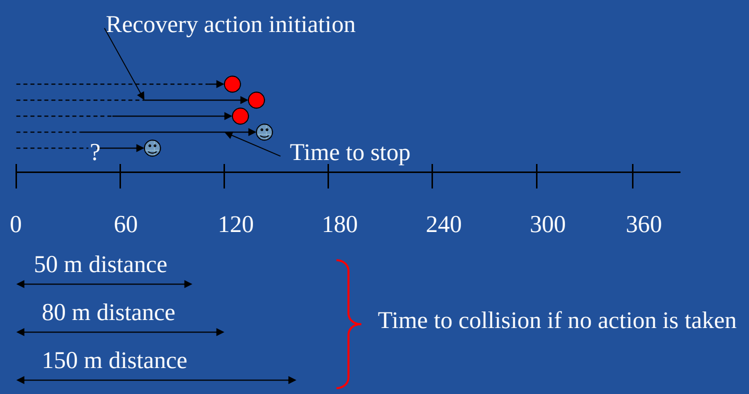
Importance

- Several incidents 1996–2001
- Low velocity impacts (high mass, up to 30 MJ)
- Cargo penetration unlikely
- Accident chain may imply very severe consequences
- After 2002, 2–3 minor accidents



Comparison

Experienced times and maximum times available



Universitetet i Stavanger

Risk Modelling, Integration of Organisational, Human and Technical factors (Risk_OMT)

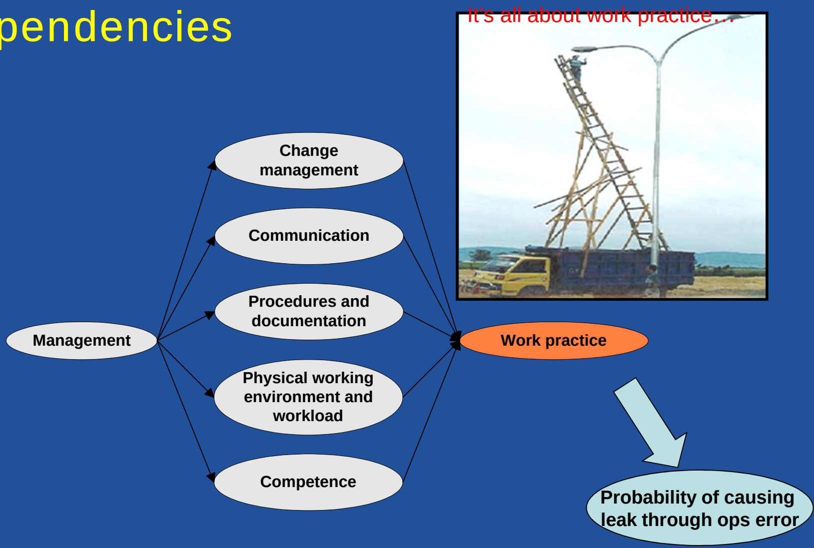
- Ambitions for the Risk_OMT programme:
  - Extension of verification of barrier performance
    - From existing technical focus into a focus where operational barriers have similar weight
  - Provide sound quantitative basis
    - for analysis of operational risk reducing measures
  - Learn how the best managed installations
    - are achieving performance of operational barriers
  - Propose key performance indicators
    - enable identification proactively when operational conditions are deviating from a high standard

R&D PARTNERS:
•UiS, NTNU, SINTEF, IFE
•Statoil

Project sponsors (2007-11):
•Norwegian Research Council
•Statoil

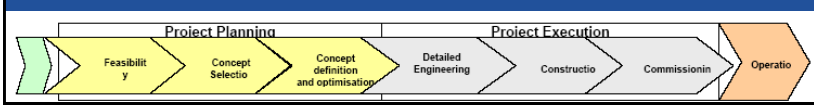
Universitetet i Stavanger

Dependencies



Life cycle perspective

- The life cycle perspective is most obvious in Norwegian legislation, which apply for all phases of petroleum activity
- UK legislation has the same perspective
- The Norwegian legislation may be described as functional, risk-based (or risk informed)
  - Based on use of risk assessments in all phases



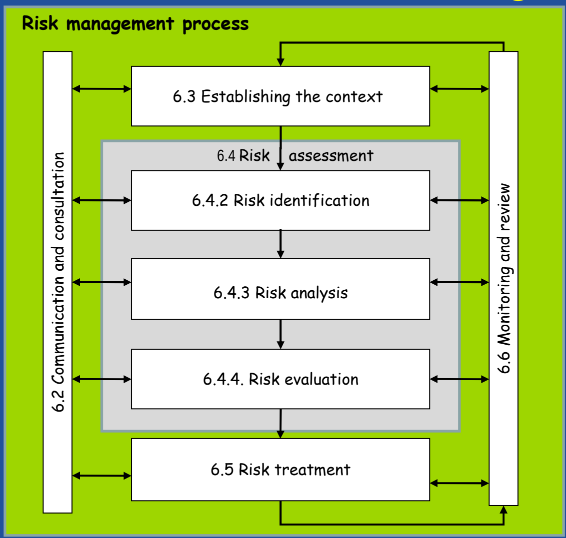
Offshore petroleum: Use of risk analysis

- QRA (quantitative risk analysis)
  - New development
    - Concept selection
    - Concept optimization
    - Engineering
    - Fabrication
    - Pre start-up ('as built')
  - Operations phase
    - When modifications are implemented
    - Otherwise regularly (say every 3-5 years)
    - Prior to start of decommissioning
- Qualitative risk analysis
  - As design tool (HAZOP, etc)
  - As operational tool (HAZID, etc)

Goal-setting regime

- Implications of goal-setting approach:
  - Industry has more flexibility vis-à-vis fulfilling regulations & finding optimum solutions
  - Preventive and protective systems and actions may be tailored to relevant hazards
  - Models need to be available to distinguish between different levels of threats, and to tailor the solutions to the circumstances

ISO 31000 – Risk Management



- Also the basis for:
  - NORSOK Standard Z-013 Risk analysis and emergency preparedness assessment

Universitetet i Stavanger

Misuse of risk analysis in petroleum sector

- PSA:
  - Risk analysis primary use to identify & assess risk reducing measures in ALARP context
  - Risk analysis shall not be used to ‘prove’ acceptability of deviation from laws, regulations, standards, common practice, etc.
- HSE [UK] has made similar remarks
- Misuse
  - Was an issue in 1980s, with limited QRA experience
  - Reiterated warning in 2007

Universitetet i Stavanger

Robust regulations?

- Combination of internal control and risk-informed regulations appear to be fragile and far from robust combination for
  - Industry
  - Authorities
- No apparent focus in research

Could risk assessment prevented Macondo?

- Presidential Commission makes reference to North Sea legislation as possible model for US
  - ≈2 years after the accident:
    - no change so far
  - Some are sceptical that anything will change

Could risk assessment prevented Macondo?

- Reflections on this question
  - PSA has confirmed that Macondo accident could have occurred in Norwegian sector
  - Several incidents/accidents during 2004–10
    - Full blown subsea gas blowout in Nov. ‘04 on Snorre A (Norwegian North Sea)
      - Lack of compliance with procedures one root cause
      - Also one of success factors of the well killing operations

Universitetet i Stavanger

Could risk assessment prevented Macondo?

- One of the common factors in recent well associated incidents & accidents:
  - Lack of proper risk assessment to
    - Identify criticality of various factors and deviations from plans & procedures that have to be made
- Common factor with the Macondo accident
  - Failure to assess risk as basis for MOC one crucial failure
- Effective management of major accident risk is strongly dependent on
  - Adequate modelling (i.e. insight) of hazard mechanisms
  - Stringent management of barriers throughout field life
    - Crucial factor in Montara accident

Universitetet i Stavanger

Could risk indicators prevented Macondo?

- Parallel with Texas City refinery explosion, where occupational injury statistics had been used to monitor major hazard risk
- Deepwater Horizon had been 7 years without significant occupational injuries
- Norwegian petroleum industry (RNNP)
  - Indicator for blowout risk based on occurrence of kicks (influx from high pressure zones into wellbore)
    - Typically 1 per 20 regular wells drilled
      - Deepwater wells (possibly up to 1 per 3 wells)
    - Insufficient to monitor performance in well drilling

Universitetet i Stavanger

Could risk indicators prevented Macondo?

- Study in recent R&D project has shown:
  - Blowout probability strongly influenced by
    - Inadequate planning of well operations
    - Inadequate management of change during drilling operations
- How should indicators be defined?
- Even if we had indicators
  - Would they be able to identify in time?
    - Failures of well planning
    - Failures during management of change during drilling operations

Universitetet i Stavanger

Could risk indicators prevented Macondo?

- Reference to Snorre A gas blowout (2004)
  - Undetected failures
    - Reentry into well planned without realizing leaks in casing
    - Risk assessment bypassed due to lack of resources
    - Failures were not detected before operations started
  - Unignited gas blowout
    - No injuries, no spill
    - Top kill within few hours, before ignition
      - Ignition could have caused total loss of installation and very extensive spills
- No indicators were able to identify well planning failures
- Is indicators the right way to go?

Universitetet i Stavanger

Could risk indicators prevented Macondo?

- Skogdalen et al.: possible use of major accident risk indicators to prevent accidents like Macondo
  - Many essential barrier elements are operational
    - Evaluation of the negative pressure test, which is one of the examples of the crucial misinterpretation of the tests
  - On every occasion that the drilling crew were supposed to make decisions balancing efficiency and risk (Pres. Com.)
    - Decided in favour of efficiency
      - thereby each time increasing the risk of a blowout
      - at the end failed to detect indications that there was a serious problem under development
- It appears very demanding to develop indicators that could have picked up this development

Universitetet i Stavanger

Could risk assessment prevented Gullfaks C?

- Lack of risk assessment identified as 1 root cause
  - PSA: why was risk assessments omitted?
- IRIS report identified significant management deficiencies
  - Limits Statoil's ability to learn from accidents & incidents
- Investigation practices are also counterproductive with respect to learning
- More important than risk assessment:
  - Significant improvements to management attitudes & supervision
- A-standard appears to have significant effect
  - Reduced frequency of HC leaks in 2012

Risk assessment of drilling and well operations

- PSA has repeatedly claimed that risk assessment tools used by the Norwegian petroleum industry are not suitable for operational decision-making
  - Survey (PSA, 2009–10) pointed to need for further development of risk analysis tools
    - Usable as input to day-to-day decisions on installations; minor modifications, maintenance and interventions
  - Same observation would be applicable also for drilling operations

- Large difference between the NPPs and offshore installations with respect to development of online risk monitoring

Risk assessment for operational decision-making

- Simplistic or detailed modeling?
- Illustration
  - – Decisions on how to install long process lines
    - Alt. A: Welding work
      - – implies increased ignition risk during installation
    - Alt. B:, 'Cold' installation methods, flanged connections
      - – may increase leak probability over remaining life cycle
- Can robust decisions be made without detailed modeling?

Universitetet i Stavanger

Risk assessment of drilling and well operations

- Online risk monitoring for management of operations, maintenance and modifications to facilitate decisions relating to:
  - – When a leaking valve needs to be repaired (example)
    - Whether it needs to done immediately in order to control the major accident risk
    - Whether it can wait for some time for the next scheduled plant shutdown
- Online risk monitoring of drilling and well operations is altogether another league
  - – Models are not available at all
  - – Extensive research effort is needed to develop suitable models
    - Mainly in the HOF field!

Universitetet i Stavanger

Barrier management

- PSA in follow-up after the Macondo blowout proposed also development of a scheme for barrier management
- Barrier failures were also obvious on the Deep Water Horizon mobile drilling rig, such as failure of blowout preventer (BOP)
- Lack of proper management of barriers is also common in the Norwegian industry
  - Poor RNNP barrier data year after year
  - HOF improvement in LOC data

Universitetet i Stavanger

Barrier management

- Management of barriers (ref. PSA) dependent on proper modelling in planning phase
  - Implies that inadequacy of risk models for drilling and well operations will also prevent the basis for barrier management to be established
- Lack of proper risk models will also limit how well risk indicators could be developed

Universitetet i Stavanger

Conclusions

- Prevention of major accidents most effectively through risk-informed decision-making
  - US & others should follow after UK & Norway

- Probably not a coincidence that severe accidents and incidents
  - Have occurred worldwide during the last ten years
  - Not in NW Europe

Universitetet i Stavanger

Conclusions

- Threat from EU to 'throw out' all the good experience in UK and Norway
  - Directive proposal apparently mainly aimed at environmental spill protection
- Step back from risk-informed to compliance basis
- Industry is probably partly to blame
  - No focus for many years to develop suitable risk based tools, especially for drilling and well operations

Universitetet i Stavanger

Conclusions

- Modelling of barrier performance is area where substantial improvement is needed
  - Grossly inadequate, especially for drilling
  - Operational barriers extra challenge
- Improvement of risk-informed management of major hazard risk in day-to-day decision-making
- Operational barrier elements the main challenge

HFC Oct 2012 JEV rev0 45

Universitetet i Stavanger

Conclusions

- Can major accidents be eliminated?
  - No, one can occur tomorrow even if the probability is very low
- Risk-informed decision-making more advanced for process plant operation
  - Even in this area we have identified significant development needs
  - Drilling and well operations less well developed
- Possibility to learn from NPPs

HFC Oct 2012 JEV rev0 46

Universitetet i Stavanger

HFC

Barrier management in the PDS project, PDS- Reliability of safety instrumented systems.

S. Hauge

Mer informasjon:
http://www.sintef.no/PDS

"Barrier management in the PDS project (PDS = "Reliability of Safety Instrumented Systems")

Stein Hauge, SINTEF Society and Technology

HFC forum – 18th October, Halden

Content

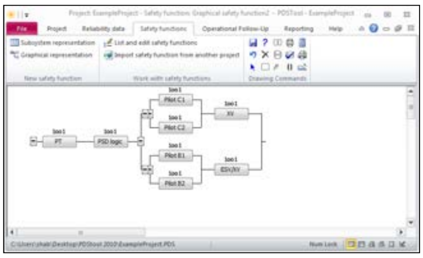
- Briefly about PDS
- The new PDS project on barrier management
- Some reflections about barrier management

The PDS forum (1986 -)

PDS projects and reports

PDS method / handbooks

The PDSTool



www.sintef.no/pds

Different perspectives on the DWH / Macondo accident

*"**One perspective**": Most of the events and missteps related to the Deepwater Horizon disaster can be traced back to an overarching failure of management and communication (ref. President Commissions' report)*

*"**Another perspective**": if the cement at the bottom of the well had been leak-tight or the BOP had closed successfully, this accident would not have happened!*

Source: Getty Images

The new PDS innovation project in Petromaks:

"Tools and guidelines for overall barrier management and reduction of major accident risk in the petroleum industry"

(Norwegian: " Verktøy og retningslinjer for helhetlig barrierestyring og reduksjon av storulykkesrisiko i petroleumsvirksomheten")

The project is financed by the Research Council of Norway ("HMS i Petromaks" program) and the PDS members (23 off)

Background for the PDS "Barrier management" project

- The Norwegian Petroleum industry and the authorities have taken a strong interest in safety barriers and barrier management for the last years
- Reports from recent incidents and accidents, PSA audits and various research activities and reports have identified that barrier management is an area of great improvement potential
- Here, the importance of focusing on the complete barriers, including the technical, operational and organisational elements are stressed
- Multiple barrier failure is a repeated feature in major accidents. Considering dependencies between barrier elements in more detail seem necessary.

Main "holes" in barrier management as per today (1)

- No clear and common understanding of notions such as "barrier", "barrier management" and "organisational and operational barrier elements" (and their relationship to "performance shaping factors")
- How do we define and limit the barrier elements, especially related to drilling and well control (but also other hazards)?
- Limited use of risk assessment to identify installation specific barriers. Poor or insufficient risk assessments often in combination with inadequate planning are often concluded in audits and investigation reports

SINTEF Technology for a better society 7

Main "holes" in barrier management as per today (2)

- Performance requirements for important safety barriers, in particular related to drilling and well intervention, are missing or inadequate
- Inadequate follow up of barrier status and existing performance requirements
- Dependencies between barriers and barrier elements is an area of too little study and concern – "how could so many barriers fail simultaneously"?

SINTEF Technology for a better society 8

Main objective of the "PDS barrier management" project:

Provide tools and guidelines to improve barrier management in the petroleum industry

Main activities of the "PDS barrier management" project

- Identify and define technical and operational barrier elements related to process events and drilling & well operations
- Consider factors /conditions that influence the performance of these barrier elements, including the effect from new technology
- Develop / suggest performance requirements for the identified barrier elements
- Develop improved models and data for modelling of dependencies between barriers and barrier elements
- Develop a practical industry guideline for overall barrier management including technical and operational barrier elements for all relevant lifecycle phases

If the barriers are well defined and functional you are OK!

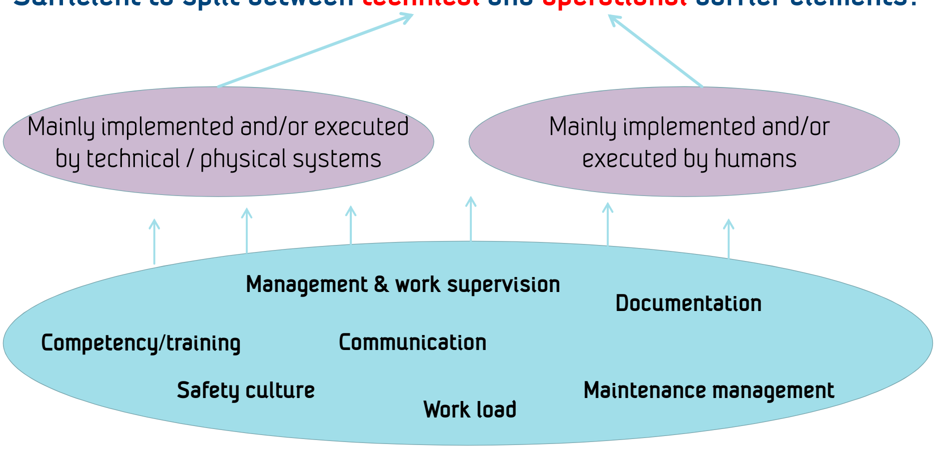
Barrier management is all co-ordinated activities required to obtain this

Getting rid of all flaws in management, communication, responsibilities, training programmes, risk analyses and various work processes (planning, modifications, etc.) appear to be a "mission impossible"……

Ensuring that the safety barriers do work appears somewhat more achievable!

But then we need to limit our definition of a barrier!

Sufficient to split between technical and operational barrier elements?



Performance shaping factors (PSF) / Risk influencing factors (RIF)

What does "inadequate risk assessments" really express?

Poor methods, poor planning processes, the wrong personnel involved, inadequate learning from previous incidents, or simply belated wisdom?

If "deficient risk assessments" are set in context with other underlying causes, we see that conditions such as "inadequate data basis", "deficient involvement of relevant technical personnel" and "deficient learning from previous incidents" are among the causes that occur the same time as deficient analyses (RNNP, 2011)

Thank you for the attention!

EXTRAS

What do we mean by "barrier management"?

Barrier management (PSA):

Coordinated activities to ensure that the barriers are established and maintain their functionality at any time.

Barrier management therefore include the processes, systems, solutions and measures that must be in place to ensure required risk reduction through implementation and follow-up of barriers

Five key elements and activities in "barrier management"

1. **Establish barrier functions** based on risk assessment and good engineering practice
2. Stipulate **performance requirements** for the technical, operational and organisational barrier elements and establish performance standards that document the requirements
3. Establish a **barrier strategy** which substantiate the relationship between the identified hazards and the established barriers, the function of the barriers and the basis for the stipulated performance requirements
4. **Implement and realize the barriers**, both the technical as well as the operational and organisational
5. **Monitor the barrier status** in operation and ensure that the required **barrier performance is maintained** during all relevant phases of the lifecycle (incl. modifications)

SINTEF Technology for a better society 17

Four main challenges to the industry – well control incidents

1. ***Stronger emphasis on technical measures to improve safety***
   67% of the triggering causes are related to technology but only 19% of the suggested measures are technical.
2. ***Stronger focus on barrier management and more adapted risk analyses***
   The industry should focus on improving the risk analysis process and broaden their understanding of "barriers" and "barrier management".
3. ***Stronger focus on major accident risk – more investigations***
   For the period 2002-2009, 130 of 158 registered HC-leaks in the process area were investigated. For the period 2003-2010, only some ten out of 146 well control incidents were investigated.
4. ***Creating conditions ("rammebetingelser") for good collaboration between operating company, contractors and subcontractors***

SINTEF Technology for a better society 18

Four main challenges identified for the industry – HC leaks

1. ***Design factors as a major cause***
   The petroleum industry should put effort into avoiding poor or defective design solutions. The industry should also have a more proactive attitude towards modifying or rebuilding poor technical solutions rather than accepting and adapting to them

2. ***Formulation of more specific measures***
   The petroleum industry has a significant improvement potential with respect to developing more specific risk reducing measures

3. ***Learning from previous events***
   The industry has a significant improvement potential with respect to ensure learning from previous events and in a systematic and effective manner apply information from event databases and other sources in their work to avoid HC leaks

4. ***Improved risk assessment and analyses***
   The industry should apply risk assessment and risk analyses more effectively in order to avoid HC leaks.

HFC

Analysis of human actions as barriers in major accidents in the petroleum industry, application of human reliability analysis methods.

K. Laumann

Mer informasjon:

Analysis of human actions as barriers in major accidents in the petroleum industry,
application of human reliability analysis methods

Petro-HRA

Petromaks project
2012-2016

Participants

- IFE
- Statoil
- DNV
- SINTEF
- NTNU
- INL

Knowledge needs

Quantitative risk analysis (QRA) is used to predict the likelihood of failures:

- mainly focused on technical barriers
- no standardized method for how HRA is performed
- no standard for how human error probability data should be integrated in QRA

Goals

Test, evaluate and adjust existing HRA methods to accident scenarios in the petroleum industry

- SPAR-H

Four Work Packages

1) Evaluation and adjustment of contextual factors (or performance shaping factors)

2) Task analyses and human error identification analyses

3) Qualitative data collection: interviews, observations and questionnaires.

4) Studies for the quantification by an expert group

1. Evaluation and adjustment of contextual factors (or PSFs) in accident scenarios

- Evaluate the suitability of SPAR-H to analyze the human error probabilities in the 15 main accident scenarios.
  - If not, other alternative methods like e.g. the ATHEANA method will be evaluated.
- Develop descriptions of performance shaping factors (PSFs) and nominal values in SPAR-H for the petroleum industry.
  - Evaluate the need for other PSFs.

2. Task analyses and human error identification analyses

- Define and describe tasks that act as human failure events in the accident scenario
- Evaluate different task analyses method and give guidelines about which one to use.
- Look at how much of the task analysis that can be reused for different installations
- Look at inter-analyst reliability
- Develop a database with reusable tasks and scenarios for petroleum HRA applications
- Include human error probabilities into the qualitative risk analysis (QRA)

3. Qualitative data collection: interviews and questionnaires

- Decisive for the quality of the final quantitative part of the analysis.
  - Develop interview guides and questionnaires.
  - Explore which information is needed to get consistent expert evaluations and values in agreement with more objective data.
  - Develop a best practice for how relevant information is collected, refined and reported.

4. Studies for the quantification by an expert group

- **Development of guidelines for structured expert judgments**
  - **Literature review including a state of the art for other industries.**
- **Define a basis for evaluation and validate of HRA parameters as needed in Work Package 1.**

Birds and methods – owl, eagle and turkey.

- Most owls share an innate ability to fly almost silently and also more slowly in comparison to other birds of prey



INVITASJON

Human Factors in Control

17.-18. oktober 2012

Safety analysis and major accidents – how to include human and organisational elements

Kjære deltaker.

Vi vil med dette invitere til møte i HFC-forum (Human Factors in Control). Møtet holdes onsdag 17. og torsdag 18.oktober 2012 i Halden, hos IFE, i auditoriet, Os Alle 5. Vi starter kl 11.00 onsdag med lunsj og avslutter etter lunsj på torsdag, med en omvisning i "Future Lab".

Tema for møtet er "*Safety analysis and major accidents – how to include human and organisational elements*" hvor vi diskuterer organisatoriske og menneskelige barrierer med eksempler på bruk av kvalitative og kvantitative analyser. Hva er god praksis når vi skal vurdere menneskelige og organisatoriske faktorer? Vi har lagt opp til en paneldiskusjon med tema "*Gir kvantifisering et vesentlig bidrag? Hva med rammebetingelser og organisatoriske faktorer?".* Vi har innlegg fra IFE, EDF - Électricité de France, Statoil, DNV, Ptil, Idaho National Laboratory, IRIS, Riskpilot, UiS, SINTEF og NTNU.

Vi har reservert rom på Thon Hotel Halden, Langbrygga 1, Halden, tlf: 69 21 33 00. Frist for beskjed om rombestilling er 1.oktober, for å sikre at dere får rom på hotellet. Vi kan også bestille rom for dere – kryss da av på siste side.

Programmet i grove trekk

Foredrag holdes bl.a. av: P. Le Bot fra EDF: "Human reliability analysis (HRA) in the human factor engineering process"; J.E. Vinnem fra UiS "Reflections on the recent serious events in the offshore oil and gas sector from a risk assessment perspective with focus on human and organizational factors "; Ø. Lauridsen fra Ptil; A. Bye fra IFE; R. Boring fra Idaho National Laboratories; K.Gould fra Statoil; K. van de Merwe fra DNV; K. Hansen fra IRIS; U.Kalhlbom fra Riskpilot; S. Hauge fra SINTEF og K. Laumann fra NTNU.

Visjon og hovedoppgave for HFC forumet

HFC visjon: "Kompetanseforum for bruk av HF innen samhandling, styring og overvåkning i olje og gass-virksomheten." HFC hovedoppgave: "Å være et forum for erfaringsoverføring som bidrar til å videreutvikle HF metoder til bruk ved design og vurdering av driftskonsepter." (Om HFC, se: www.hfc.sintef.no)

Vi vil også benytte anledningen til å minne om kurset "MTO-Human factors" ved UiS som går høsten 2013, og NTNU kurset "Introduksjon til Human Factors, metoder og teorier med eksempler fra integrerte operasjoner" som arrangeres våren 2013 - 5,6,7 februar; 11,12,13,14 mars; 9,10,11 april, se videre.ntnu.no, http://videre.ntnu.no/link/nv13119.

Vennlig hilsen

Arne Jarl Ringstad /Statoil, Andreas Bye /IFE, Mark Green /HCD, Koen van de Merwe /DNV og Stig Ole Johnsen /SINTEF.

Vær vennlig og returner registreringen innen 1.oktober 2012 til:
jannicke.neeb@hrp.no, IFE (FAX: 69 21 24 90)

HFC Møte

AGENDA

17. til 18. oktober 2012

Safety analysis and major accidents – how to include human and organisational elements

IFE, Halden, Os Alle 5 - auditoriet

Dag 1	Innlegg og diskusjon	Ansvar
11.00-12.00	Lunsj.	IFE
12.00-12.30	Velkommen til seminaret og runde rundt bordet.	
12.30-13.00	Introduction, safety analysis in complex industries.	A. Bye/ IFE
13.00-13.45	HRA in the human factor engineering process.	P. LeBot/ EDF
13.45-14.15	Diskusjon og pause.	
14.15-14.30	Kursinfo – Introduksjon til Human Factors	A. Balfour/ HFS
14.30-15.00	Human reliability analysis in major accident risk analyses in the Norwegian petroleum industry: applying SPAR-H	K. Gould/ Statoil; K. van de Merwe/ DNV
15.00-15.30	Diskusjon og pause.	
15.30-16.00	Barrier Management - Technical, operational and organizational barrier elements, is it possible to define performance requirements to operational and organizational barrier elements? A regulators perspective.	Ø. Lauridsen/ Ptil
16.00-16.15	Diskusjon og pause	
16.15-16.45	Lessons learned from human reliability applications in the US space program.	R. Boring/ Idaho National Laboratory
16.45-17.15	Diskusjon og pause.	
17.15-17.45	The Petroleum Safety Authority has accused Statoil for lacking the ability to learn - are they right?	K. Hansen/ IRIS
17.45-18.00	Diskusjon og pause.	
18.00-18.30	Lessons and experiences from applying human reliability analysis in the Swedish nuclear industry.	U.Kahlbom/ Riskpilot
18.30-18.45	Diskusjon og pause.	
19.30-	Middag - Haldens Klub.(Kart lagt ut i auditoriet)	

Dag 2	Innlegg og diskusjon	Ansvar
08.30-09.00	Kaffe og noe å bite i.	
09.00-09.45	Reflections on the recent serious events in the offshore oil and gas sector from a risk assessment perspective with focus on human and organizational factors.	J.E. Vinnem/ UiS
09.45-10.00	Diskusjon og pause.	
10.00-10.30	Barrier management in the PDS project, PDS- Reliability of safety instrumented systems.	S. Hauge/ Sintef
10.30-10.45	Diskusjon og pause.	
10.45-11.45	Paneldiskusjon: What does quantification add to other types of safety analysis? How can broader, organisational or industry-specific factors be included?	Le Bot, Gould, Vinnem, Boring, Lauridsen, ordstyrer: A. Bye
11.45-12.00	Diskusjon og pause.	
12.00-12.30	Informasjon om Petromaks, avslutning og oppsummering.	K. Laumann/NTNU,HFC
12.30-13.30	Lunsj.	IFE
13.30-14.00	Omvisning Future Lab v/IFE.	IFE