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

RAPPORT

TITTEL

Human Factors fokus ved design av arbeidsplasser og arbeidsprosesser.
Resultater HFC Forum, 22. til 23.april 2009, møte #9.

FORFATTER/REDAKTØR

Johnsen S. O.

OPPDRAGSGIVER(E)

HFC forum

RAPPORTNR.	GRADERING	OPPDRAGSGIVERS REF.	
SINTEF A11793	Åpen	Throndsen, T.I. /Statoil	
GRADER. DENNE SIDE	ISBN	PROSJEKTNR.	ANTALL SIDER OG BILAG
Åpen	9788214048186	504144	168
ELEKTRONISK ARKIVKODE		PROSJEKTLEDER (NAVN, SIGN.)	VERIFISERT AV (NAVN, SIGN.)
https://project.sintef.no/eRoom/civil/504017CRIOPUserGroup/0_c45a		Johnsen, Stig O.	Bodsberg, L.
ARKIVKODE	DATO	GODKJENT AV (NAVN, STILLING, SIGN.)	
	8.6.2009	Throndsen, T.I. /Statoil	

SAMMENDRAG

Denne rapporten dokumenterer presentasjoner/artikler, agenda og deltakerliste fra HFC forum møtet den 22.-23.april 2009 i Stavanger, HFC forum møte nr 9.

De vedlagte presentasjonene og artiklene er:

Resilience in distributed teams-	S. Dekker/Lunds Universitet
Human Factors analyser – Toolbox Talk	M. Green/HCD
Dependable requirements engineering	A. Tunem/IFE
Moderne Human Factors – teorier i praksis	B. Røed, K. Gould/Scandpower
Orientering og besøk - National Oilwell	H. Andersen/NOV
Interaksjonsdesign med vekt på Human Factors	G. Andresen/IFE
Driftsättning av ny teknik och CRM	C. Weikert/HFN
Boresimulator - bidrag til varsling	R. Rommetveit/eDrilling- solutions
Human Factor in Subsea Controls	R. L. Hansen/StatoilHydro
Resultater - kartlegging av bruk av CRIOP	A. Aas/NTNU
HFC – Budsjetter og planer	S.O.Johnsen/SINTEF
Etablere standard for samhandling, oppdatere CRIOP	Workshop

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

1.1 Innledning

Vi vil med dette sende ut evaluering av HFC møtet, deltakerliste og presentasjonene fra HFC forum møtet den 22.-23.april i Stavanger. Vi minner om neste HFC møter den 21. til 22. oktober under studenteruka i Trondheim.

Dessuten minner vi om mulighetene for å ta kurset "Introduksjon til Human Factors og integrerte operasjoner" våren 2010. Planlagte datoer er: Uke 6 - den 8. ,9.og 10. februar; uke 11 - den 15., 16., 17. og 18. mars; uke 17 – den 26., 27. og 28. april. Påmelding http://videre.ntnu.no.

I det nedenstående har vi sakset inn korte punkter fra de evalueringene som deltakerne leverte inn.

1.2 Evalueringer

Generelt synes det som om de fleste er meget godt fornøyd med HFC møtene og formen som benyttes. Kommentarene vi får er positive, med gode tilbakemeldinger på det faglige og sosiale utbytte. Forumet er bredt med mange forskjellige deltakere, og utfordringen er å gi alle noe, både forskere, konsulenter og industrideltakere. Vi får derfor et bredt sett av innspill. I forbindelse med evalueringen ble følgende innlegg trukket frem som gode av de fleste som fylte ut evalueringene:

- **Boresimulator** R.Rommeltveit
- **Resilience in distributed teams** S.Dekker
- **Modern Human Factors (HF) teorier** B.Røed, K. Gould
- **Robusthet og Human Factors ved SubSea** - R.L.Hansen
- **Toolbox talk: Human Factors analyser** M.Green
- **Interaksjonsdesign med vekt på HF** G.Andresen

Det var generelt små marginer mellom de forskjellige innleggene.

1.3 Formen på HFC møtene

Tilbakemeldingene er generelt positive til formen på møtene. Det bør velges møterom som passer til deltakerne og en bør passe på å sette av nok tid til diskusjoner og refleksjoner mellom hvert innlegg..

1.4 Tema og forelesere til de neste HFC møtene

Innspill fra deltakerne og som oppsummert ble oppfattet som relevante, dvs. forslagene i nedenstående tabell:

Periode	Forslag til tema og forelesere
Høst 2009	Situational awareness (Team Cognition- E.Salas, Organisational Cognition - . K.Weick.) Samarbeid med HFN i Sverige.
Vår 2010	HF i ulykkesgranskinger, hvordan forstår vi Human Factors i ulykkesgranskninger
Høst 2010	HF i endringsprosesser, "Design for resilience", Perspektiver som Actor-network theory (ANT) i HF granskninger.
Vår 2011	Inntog i det globale: Språk, kultur, tidsforskjell, HF i global setting.
Høst 2011	Fokus på HF i andre land, somUSA og SørøstAsia – erfaringer, muligheter og trusler

Av andre tema som ble trukket frem som spesielt interessante kan nevnes:

- Operational safety og sikkerhetskultur. Human Factors i management systemer eksempelvis ledelse og Human Factors.
- Samhandling i distribuerte team - team cognition presentart fra E.Salas hadde vært veldig bra.
- Ikke bare resilience engineering, men dependability engineering, hvor ulike dependability faktorer blir diskutert både ut fra et forskningsperspektiv og ut fra praktiske erfaringer med å anvende tilgjengelige metoder og tilnærminger
- Det burde være interessant å diskutere/tematisere IO og HMS oppsider og nedsider og koplinger til ulike IO design.
- Fokus på resultatene fra god Human Factors dvs – "HF makses sense. HF/Efficiency".
- Komme med eksempler på interaksjonsdesign og kontrollsystemer. Blande teorier praktiske anvendelser, vise eksempler fra dårlige og vellykkede prosjekter, erfaring.
- Synes det er bra at vi ser på andre typer kontrollrom enn CCR og andre relevante metoder/teorier.

Av forelesere ble følgende nevnt:

- E.Salas eller noen fra gruppa hans. Andre som ble nevnt var M.Endsley (Situational awareness), G.R. Hockey fra Univ of Leeds, Mark Young, Neville Stanton.
- C. Weick eller J.Reason.
- Interessant å utvide HF mot community of practice og praksisfellesskap J.S.Brown, P.Duguide – eks hvordan mobiliserer man et praksisfellesskap?
- Ingrid Danielsson – ønskes mht interaksjonsdesign.
- K. Haukelied

1.5 Kontakt opp mot Human Factors fagnettverket i Europa og USA

I perioden 14-16 oktober vil HFES Europe Chapter møtes i Lindkøping – Sverige. For innmelding i den europeeiske Human Factors and Ergonomics Society se: hfes-europe.org.

HFES - The Human Factors and Ergonomics Society, Europe Chapter, is organised to serve the needs of the human factors profession in Europe. Its purpose is to promote and advance through the interchange of knowledge and methodology in the behavioural, biological, and physical sciences, the understanding of the human factors involved in, and the application of that understanding to the design, acquisition, and use of hardware, software, and personnel aspects of tools, devices, machines, equipment, computers, vehicles, systems, and artificial environments of all kinds.

The Chapter is an affiliate of the Human Factors and Ergonomics Society, Inc. www.hfes.org , a nonprofit corporation chartered by the State of California, USA.

HFC Møte

AGENDA

22. til 23.April
2 0 0 9

Human Factors fokus ved design av arbeidsplasser og arbeidsprosesser

Stavanger, StatoilHydro, Forus – Dag 1: Rom C1011; Dag 2: Aud L1.

Dag 1	Foredrag med spørsmål etter foredragene; Møter i Forus hagen v/IKEA rom C1011.	Ansvar/Beskrivelse
11:30-12:30	Registrering og lunsj i rom C1011	StatoilHydro
12:30-13:00	Velkommen til møtet – rundgang rundt bordet	HFC
13:00-14:30	Resilience in distributed teams, particularly their ability to manage and control escalating situations. (30 min disk.)	S. Dekker/Lunds Universitet
14:30-15:00	Human Factors analyser – Toolbox Talk	M.Green/HCD
15:00-15:30	Kaffe/Pause	StatoilHydro
15:30-16:10	Dependable requirements engineering (10 min diskusjon)	A.Tunem/IFE
16:10-16:40	Moderne Human Factors – teorier i praksis (10 min disk.)	B.Røed, K.Gould/Scandpower
16:40-17:10	Orientering fra National Oilwell	
17:10-17:30	Buss til National Oilwell - Lagerveien 20	
17:30-18:00	Besøk National Oilwell, Omvisning	National Oilwell
18:00-18:20	Busstransport tilbake til hotellet	
19:30	Middag på City Bistro (Madlaveien 18)	HFC
Dag 2	**Møter hovedinngangen/inngang 1, Forusbeen 50; møtet er i Auditorium L1.**	
08:30	Buss henter på Hotellet, drar 08:30	
08:45-09:00	Kaffe	StatoilHydro
09:00-09:30	Interaksjonsdesign med vekt på Human Factors - ”Representation aiding for multidisciplinary teams” (10 min til diskusjon)	G. Andresen/IFE
09:30-10:15	Driftsättning av ny teknik och CRM (10 min til disk.)	C. Weikert/HFN
10:15-10:45	Boresimulator - hvordan kan den bidra til varsling før kritiske hendelser (10 min til diskusjon)	R.Rommetveit/eDrilling-solutions
10:45-11:00	Kaffe/Frukt	StatoilHydro
11:00-11:30	Krav til robusthet og Human Factors forhold ved utforming av Sub-Sea installasjoner og fjernstyring av ubemannede sub-sea anlegg. (10 Min diskusjon)	R. L. Hansen/StatoilHydro
11:30-12:00	Resultater fra systematisk spørreundersøkelse - kartlegging av bruk av CRIOP og andre HF metoder	A.Aas/NTNU
12:00-12:15	HFC – Budsjetter, planer og rekruttering	HFC
12:15-13:00	Lunsj	StatoilHydro
13:00-14:30	Diskusjon og avgrensning – etablere standard for samhandlingsrom - søknad til forskningsrådet	Deltakere som vil engasjere seg

Deltakerliste HFC-forum 22. og 23. april 2009
Sted: StatoilHydro, Stavanger

	Etternavn	Fornavn	Bedrift	E-mail
1	Almklov	Petter	NTNU Samfunnsforskning AS	Petter.Almklov@apertura.ntnu.no
2	Andersen	Heidi	National Oilwell Varco	heidi.andersen@nov.com
3	Andersen	Siri	Det Norske Veritas	siri.andersen@dnv.com
4	Andresen	Gisle	IFE/NTNU	gislea@hrp.no_
5	Balfour	Adam	Human Factors Solutions	adam@hfs.no
6	Berglund	Martina	HFN, Linköpings universitet	martina.berglund@liu.se
7	Bisio	Rossella	IFE	rossella.bisio@hrp.no
8	Bjerkebæk	Eirik	Ptil	Eirik.Bjerkebak@ptil.no
9	Bunn	James	StatoilHydro	JBUN@StatoilHydro.com
10	Bäckström	Claes	Saab Security	claes.backstrom@saabgroup.com
11	Christiansen	Vidar	HMS Design & Utvikling AS	vidar.christiansen@hms-du.no
12	Dekker	Sidney	Lunds Universitet	Sidney.Dekker@tfhs.lu.se
13	Eskedal	Trond Sigurd	Petroleumstilsynet	trond.eskedal@ptil.no
14	Falmyr	Odd	IFE	odd.falmyr@hrp.no
15	Fossum	Knut	NTNU Samfunnsforskning AS	Knut.Fossum@bio.ntnu.no
16	Gould	Kristian	Scandpower AS	kgo@scandpower.com
17	Graven	Tone G.	ABB AS	tone-grete.graven@no.abb.com
18	Green	Marie	HCD	marie.green@hcd.no
19	Green	Mark	HCD	mark.green@hcd.no
20	Hansen	Roald loug	StatoilHydro	roloha@StatoilHydro.com
21	Haug	Joakim Børsheim Enne	Det Norske Veritas	joakim.haug@dnv.com
22	Heber	Hilde	Petroleumstilsynet	hilde.heber@ptil.no
23	Johnsen	Stig Ole	SINTEF Teknologi og samfunn	stig.o.johnsen@sintef.no
24	Keane	Live	ENI Norge	live.keane@eninorge.com
25	Larsen	Reidun	Eni Norge	re-g@online.no
26	Ludvigsen	Jan Tore	HMS Design & Utvikling AS	jtl@hms-du.no
27	Løland	Grete	Petroleumstilsynet	Grete-Irene.Loland@ptil.no
28	Moltu	Berit	StatoilHydro	Bmol@statoilhydro.com
29	Norheim	Vigleik	Human Factors Solutions	VIGLEIK@HFS.NO
30	Omland	Ingrid	Kongsberg Intellifield	ingrid.omland@kongsberg.com
31	Pont	Arno	StatoilHydro	apon@statoilhydro.com
32	Revheim	Bente	Aker Solutions	Bente.Revheim@akersolutions.com
33	Ringstad	Arne Jarl	StatoilHydro	ajri@statoilhydro.com
34	Robstad	Jan Arvid	Kokstad BHT	jar@kokstad-bht.no
35	Rommetveit	Rolv	eDrillingsolutions	rr@edrillingsolutions.com
36	Røed	Bjarte	Scandpower AS	bkr@scandpower.com
37	Sandnes	Charles Holst	National Oilwell Varco	CharlesHolst.Sandnes@nov.com
38	Tangeland	Kristian	ABB Holding	kristian.tangeland@no.abb.com
39	Throndsen	Thor Inge	StatoilHydro	TIT@StatoilHydro.com
40	Thunem	Atoosa P-J	IFE Halden	atoosa.p-j.thunem@hrp.no
41	Vinningland	Øystein	National Oilwell Varco	oystein.vinningland@nov.com
42	Weikert	Clemens	HFN	Clemens.Weikert@psychology.lu.se
43	Wærø	Irene	SINTEF Teknologi og samfunn	Irene.Waro@sintef.no
44	Øie	Sondre Fagerli	Det Norske Veritas	sondre.oie@dnv.com
45	Aas	Andreas	NTNU	Andreas.Aas@idi.ntnu.no

S. Dekker/Lunds Universitet

"Resilience in distributed teams, particularly their ability to manage and control escalating situations"

Go to www.lusa.lu.se/research to see presentations on "Resilience" and "Just Culture".

In addition - S.Dekker suggested to read the following articles:

- "*Resilience Engineering: Redefining the Culture of Safety and Risk Management*" By David D. Woods - HFES Bulletin - December 2006

- "*Doctors Are More Dangerous Than Gun Owners: A Rejoinder to Error Counting*" - Sidney W. A. Dekker, Lund University, Ljungbyhed, Sweden

- "*Just culture: who gets to draw the line*?" - Sidney W. A. Dekker

Resilience Engineering: Redefining the Culture of Safety and Risk Management

By David D. Woods
HFES Bulletin
December 2006

The first impulse after tragic accidents in aviation, transportation, health care, or power generation is to label human error as the cause. Headlines continue to announce human error as if that explained how the accident occurred and how similar events could be prevented in the future. But research has consistently pointed to different result: Rather than focus on an individual or specific human decision or action, the data are found to point to organizational factors that set up the conditions for failure to occur—organizational accidents.

The question then becomes, what is the difference between organizations that can manage high hazard processes well and others that inadvertently create complexity and miss signals that risks are increasing. This research often focuses on the question of what is safety culture, what are indicators of poor safety culture, and what are the ways leadership signals a commitment to safety.

Line managers push back when they hear about these results: "Changing culture is difficult and slow"; "I am under increasing schedule and financial pressure"; "I can demonstrate continual improvements in many areas of my operation"; "I have decisions to make about how to invest limited resources in risky projects."

Managing risk proactively is difficult. When organizations are struggling to meet daily pressures, how can they tell the difference between inefficiencies and buffers against the unexpected? Resilience engineering is one new approach to provide tools for proactive safety management.

To provide some structure for this article, *HFES Bulletin* Features Editor Pam Savage-Knepshield posed a series of questions, which I answer below.

How do you define "resilience engineering," and why do you consider it an emerging discipline?

Around 2000, I noticed a shift in the language and concepts that safety researchers were using to discus how organizations succeed and fail. Many of the papers began to use words like *resilience* or *robustness* to describe organizations that were able to achieve ultra-high levels of safety despite high risks, difficult tasks, and constantly increasing pressures. Resilient organizations were proactive and adaptive, and this led to organizations that not only had high safety but also were able to respond effectively to many types of changes in today's highly pressured business and operational settings.

NASA in particular realized the need for proactive safety management processes in the aftermath of, first, the series of Mars exploration failures in 1999 and, then, the *Columbia* space shuttle accident in 2003. NASA experienced how pressure to be "faster, better, cheaper" led to management decisions that pushed the organization closer to the edge of the performance envelope without anyone's realizing how risk had increased.

The common thread in the work on proactive safety was the idea that *resilience* is a critical systems property when organizations are under pressure both to be highly productive and to achieve ultra-high levels of safety. Resilience refers to the art of managing the unexpected or how a team or organization becomes prepared to cope with surprises. Resilience comes from the Latin *resilire* –" to leap back," and denotes a system property characterized by the ability to recover from challenges or disrupting events. Resilience engineering assesses changes in the adaptive capacity of an organization as it confronts disruptions, change, and pressures.

Previously, organizations focused on improving their efficiency, productivity, and effectiveness—being "faster, better, cheaper," to use the slogans of NASA senior management. The data on organizational accidents revealed how this strategy was incomplete. As NASA had discovered, a fourth parameter was needed that focused on anticipating changes in risk without waiting for accident or near miss data to accumulate. I proposed at NASA's Design for Safety meeting in 2000 that a system's resilience in the face of disruptions could serve as that fourth parameter of high-performance organizations and that proactive safety management should help organizations achieve a dynamic balance across all four of these parameters.

Many tools already exist to model, measure, and improve the parameters of efficiency, productivity, and effectiveness. I went to my colleagues in safety engineering, organizational factors, and cognitive systems engineering and suggested that the time had come when we could develop tools for organizations to model, measure, and improve their resilience. With measures of resilience included, organizations would know how and when to rebalance safety against the continuing pressure to be faster, cheaper, and better. It turned out to be easy for people to recognize that most of the work on safety was pointing toward such a concept. The key event was an international symposium held in Sweden in late 2004. The result was consensus that this was a highly promising direction, and a book was soon published that capture some of the initial ideas about the importance of resilience.

What related fields of study does resilience engineering build upon, and what new concepts or principles does it introduce?

Resilience engineering builds on advances in modeling and measuring complex adaptive systems, the insights gathered from observations of high-reliability organizations, and the results from studies of how people adapt to make systems work despite complexity in cognitive systems engineering.

The first basic concept is the adaptive capacity of an organization as it confronts disruptions, change, and pressures. Measures of adaptive capacity can be used to assess how the system is both resilient in some ways and to some challenges and brittle in the face of other challenges.

Second, focusing on resilience changes how one analyzes incident data and how one interprets indicators of organizational culture. The issue is what are the diagnostic signals that reveal when the organization is edging closer to safety limits as it copes with faster, better, cheaper pressure *without the organization realizing it is operating more precariously*.

One of the key diagnostic signals is how people or groups in the organization make sacrifice judgments. Sacrifice judgments occur in particular situations when someone faces a trade-off in trying to decide if acute production-or efficiency-related goals should be temporarily relaxed—the sacrifice—in order to reduce risks of approaching too near safety boundaries.

Examples of sacrifice judgments include the decision about when to convert from laparoscopic surgery to an open procedure in surgery and in the decision about when to break off an approach to an airport during weather that increases the risks of wind shear in aviation. If people and managers in these situations are very reluctant to sacrifice production (e.g., arrival delays) to invest extra resources in reducing possible future risks, then the organization is acting much riskier than it really wants and knows. If peers and managers react negatively when someone makes a sacrifice decision, then the organization is more brittle than management realizes.

Another key diagnostic signal about an organization's resilience can be seen in how cross-checks work. How well can people in one role—especially if that role has less status or authority in the organization—cross-check people in other roles to detect early signs of a possible misassessment or erroneous plan? If cross-checks are weak or ineffective (e.g., because they are seen as unnecessary distractions), the organization is brittle.

What do you see as the relationship between *resilience* and *brittleness,* and why is it significant?

The opposite of resilience is *brittleness*, referring to systems that break down rapidly when boundary conditions or underlying assumptions are challenged by new events. In other words, examining a system's resilience means one studies how the system in question performs when it is pushed near boundaries of how it has been designed to operate. "Surprising" events are those that challenge the boundary conditions or a combination of events that push systems close to operational boundaries. Analyses of dramatic failures of complex systems, such as the *Columbia* space shuttle accident, have shown how these organizations missed signals that operations had become more brittle as production pressure eroded various buffers and resources that had provided resilience.

Resilience is a parameter of a system that captures how well that system can adapt to handle events that challenge the boundary conditions for its operation. Such challenge events do occur (a) because plans and procedures have fundamental limits, (b) because the environment changes, and (c) because the system itself adapts given changing pressures and expectations for performance. The capacity to respond to challenge events resides partly in the expertise, strategies, and tools that people use to prepare for and respond to specific classes of challenge.

But management also monitors for signs that indicate whether the organization has the adaptive capacity to handle challenge events and how to target investments to increase adaptive capacity despite omnipresent pressures for productivity. Can the organization recharge resilience when buffers are depleted, margins are precarious, processes become stiff, and squeezes become tighter?

Which types of systems and organizations can benefit from the application of resilience engineering principles?

We are seeing the concept of resilience being picked up by organizations in the transportation and oil industries, in health care, and in business. For example, the Institute of Medicine just released a report that concluded that hospital emergency departments are the brittle point in the national health care system.

What advice do you have for researchers interested in pursuing studies in resilience engineering?

The field is at that early stage of excitement when one can feel the possibility that new insights are just around the corner. I have been so pleased with how many younger researchers have resonated with the idea of resilience and how it has inspired them to look at organizations and processes with a new kind of conceptual lens. When they do this, interesting findings result and promising new directions emerge. I am looking forward to very fast developments in this field, and I expect to be surprised by the results that emerge.

What advice do you have for organizations interested in implementing resilience engineering in their system design efforts?

Middle managers feel squeezed in today's organizations under faster, better, cheaper pressure. Resilience engineering can help identify when those pressures are squeezing out the buffers and other sources of resilience that are needed for ultra-high-quality performance in a changing and surprising environment. Resilience engineering can help make safety organizations more effective partners with line managers as they pursue ultra-high levels of safety.

But resilience engineering is young, so we are looking for organizations that recognize they are becoming more brittle to join with us as early adopters and codevelopers of the pragmatic tools for engineering resilience into organizational performance.

Where should people go to find out more about resilience engineering?

The following references are helpful.

Carthey J., de Leval, M. R., & Reason, J. T.. (2001). Institutional resilience in healthcare systems. *Quality & Safety in Health Care*, *10*, 29–32.

Committee on the Future of Emergency Care in the US. (2006). *Hospital-based emergency care: At the breaking point.* Washington, DC: National Academy Press.

Cook, R. I., & Rasmussen, J. (2005). Going solid: A model of system dynamics and consequences for patient safety. *Quality & Safety in Health Care, 14,*130–134.

Hollnagel, E., Woods, D. D., & Leveson, N. (Eds.). (2006). *Resilience engineering: Concepts and precepts*. Aldershot, England: Ashgate.

Sutcliffe, K., & Vogus, T. (2003). Organizing for resilience. In K. S. Cameron, I. E. Dutton, & R. E. Quinn (Eds.), *Positive organizational scholarship* (pp. 94–110). San Francisco: Berrett-Koehler.

Woods, D. D. (2005). Creating foresight: Lessons for resilience from Columbia. In W. H. Starbuck & M. Farjoun (Eds.), *Organization at the limit: NASA and the Columbia disaster*. Blackwell.

SPECIAL SECTION

Doctors Are More Dangerous Than Gun Owners: A Rejoinder to Error Counting

Sidney W. A. Dekker, Lund University, Ljungbyhed, Sweden

Objective: This paper analyzes some of the problems with error counting as well as the difficulty of proposing viable alternatives. **Background:** Counting and tabulating negatives (e.g., errors) are currently popular ways to measure and help improve safety in a variety of domains. They uphold an illusion of rationality and control but may offer neither real insight nor productive routes for improving safety. **Method:** The paper conducts a critical analysis of assumptions underlying error counting in human factors. **Results:** Error counting is a form of structural analysis that focuses on (supposed) causes and consequences; it defines risk and safety instrumentally in terms of minimizing negatives and their measurable effects. In this way, physicians can be proven to be 7500 times less safe than gun owners, as they are responsible for many more accidental deaths. **Conclusion:** The appeal of error counting may lie in a naive realism that can enchant researchers and practitioners alike. Supporting facts will continue to be found by those looking for errors through increasingly refined methods. **Application:** The paper outlines a different approach to understanding safety in complex systems that is more socially and politically oriented and that places emphasis on interpretation and social construction rather than on putatively objective structural features.

INTRODUCTION

There are about 700,000 physicians in the United States. The U.S. Institute of Medicine estimates that each year between 44,000 and 98,000 people die as a result of medical errors (Kohn, Corrigan, & Donaldson, 1999). This makes for a yearly accidental death rate per doctor of between 0.063 and 0.14. In other words, up to one in seven doctors will kill a patient each year by mistake. In contrast, there are 80 million gun owners in the United States. They are responsible for 1,500 accidental gun deaths in a typical year (e.g., National Safety Council, 2004). This means that the accidental death rate, caused by gun owner error, is 0.000019 per gun owner per year. Only about 1 in 53,000 gun owners will kill somebody by mistake. Doctors, then, are 7,500 times more likely than gun owners to kill somebody as a result of human error (Dekker, 2005).

Although the comparison between doctors and gun owners is ridiculous for many reasons, and is meant facetiously, organizations and other stakeholders (e.g., consumers, trade and industry groups, regulators, researchers) actually do use error counts in trying to assess the "safety health" of an organization or professional group. This would seem to carry many advantages. Not only does error counting provide an immediate, numeric estimate of the probability of accidental death, injury, or other undesirable event, it also allows comparison (this hospital vs. that hospital, this airline vs. that one). Keeping track of adverse events is thought to provide relatively easy, quick, and accurate access to the internal safety workings of a system. Adverse events can be seen as the start of, or reason for, deeper probing to search for environmental threats or unfavorable conditions that could be changed to prevent recurrence.

Over the past three decades, human factors researchers have spawned a number of error classification systems. Some classify decision errors together with the conditions that helped produce them (Kowalsky, Masters, Stone, Babcock, & Rypka,

Address correspondence to Sidney W. A. Dekker, Lund University, School of Aviation, 260 70 Ljungbyhed, Sweden; sidney.dekker@tfhs.lu.se. *HUMAN FACTORS,* Vol. 49, No. 2, April 2007, pp. 177–184.

1974). Some have a specific goal. For example, they aim to categorize information transfer problems that may happen during instructions, watch changeover briefings, or other coordination (Billings & Cheaney, 1981). Others try to divide error causes into cognitive, social, and situational (physical/environmental/ergonomic) factors (Fegetter, 1982). Yet others attempt to classify error causes along the lines of a linear information-processing/decision-making model (Rouse & Rouse, 1983). Various counting methods are founded on their own models (e.g., threat and error model; Helmreich, Klinect, & Wilhelm, 1999), whereas others apply, for example, the Swiss-cheese metaphor in the search for errors and vulnerabilities up the causal chain (Shappell & Wiegmann, 2001). This metaphor suggests that systems have multiple layers of defense but all of them have holes, which need to line up to allow an accident (see Reason, 1990).

In the categorization and tabulation of errors, researchers make a number of assumptions and take certain philosophical positions. Few of these are made explicit in the description of these methods, yet they carry consequences for the utility and quality of the error count as a measure of safety health and as a tool for directing resources for improvement. In this paper, I will examine some of those assumptions, including the naively realist idea that social phenomena (including errors) exist as facts outside of individual minds, open for objective scrutiny by anybody with an appropriate method. I will show some fairly obvious counterinstances of this assumption but then acknowledge that moving human factors away from this idea is extremely difficult because observed facts always privilege the ruling paradigm. I nonetheless conclude by making a proposal for a new standard in which the assumption is no longer that safety, once established, can be maintained by requiring human performance to stay within the prespecified boundaries of an error categorization tool. Instead, I argue for the development of better ways to understand how people and organizations themselves create safety through practice. I also argue for greater self-consciousness on the part of researchers and other stakeholders: How well calibrated are the models of safety and risk that are expressed through existing methods and proposed countermeasures? After all, the models are but instances, all negotiable and refutable, of an inherently and permanently imperfect knowledge base of what makes systems brittle or resilient.

Errors Exist "Out There" and Can Be Discovered With a Good Method

Error counting generally assumes that there is a reality "out there" that researchers should try to approach as closely as possible. For this, they need a good method. This is a firmly modernist stance, one that has dominated science for centuries. Errors, in this sense, are a kind of Durkheimian fact (Durkheim, 1895/1950). Reality exists; the truth can be found. A scientifically based method helps people do just that, as it supposedly eliminates subjective preconceptions and enables people to know reality just as it is.

But when it comes to errors, this turns out to be complicated. What, for example, causes errors? Having an idea about their cause is often crucial for the ability to categorize errors using one of the methods mentioned previously. According to Helmreich (2000), "errors result from physiological and psychological limitations of humans. Causes of error include fatigue, workload, and fear, as well as cognitive overload, poor interpersonal communications, imperfect information processing, and flawed decision making" (p. 746). But this is circular: Do errors cause flawed decision making, or does flawed decision making lead to errors? The objective observation of errors is suddenly no longer so simple. Mixing up cause and consequence is typical for error categorization methods (Dougherty, 1990; Hollnagel, 1998), but to their adherents, such causal confounds are neither really surprising nor really problematic. Truth, after all, can be elusive. What matters is getting the method right. More method will presumably solve problems of method.

Other problems supposedly related to method also occur. In a classification scheme currently popular in aviation, Line-Oriented Safety Audits (see Helmreich et al., 1999), the observer is asked to distinguish, among other things, between "procedure errors" and "proficiency errors." Proficiency errors are related to a lack of skills, experience, or (recent) practice, whereas procedure errors are those that occur while carrying out prescribed or normative sequences of action (e.g., checklists). This seems straightforward. But, as Croft (2001) reported, the following problem confronts the observer. One type of error (a pilot entering a wrong altitude in a flight computer) can legitimately end up in either of the two categories: "For example, entering the wrong flight altitude in the flight

management system is considered a procedural error.... Not knowing how to use certain automated features in an aircraft's flight computer is considered a proficiency error" (Croft, 2001, p. 77).

If a pilot enters the wrong flight altitude in the flight management system, is that a procedural or a proficiency issue? If there are problems in matching observed facts with theory (e.g., one factual observation can comfortably fit two categories), then researchers typically see these as problems of method, calling for further refinement. For example, the measuring instruments can be made more sensitive, so that they discriminate better between different observations. Observers can also be trained better, so that they recognize subtle differences between errors and learn to code them correctly. These are typical responses of a research community to the challenges raised by mismatches between theory and observed fact.

But are these problems of method? This is the crucial question. Kuhn (1962) encouraged science to turn to creative philosophy when confronted with the inklings of problems in relating theory to observations. It can be an effective way to elucidate and, if necessary, weaken the grip of a tradition upon the collective mind. It may even suggest the basis for a new direction. For any scientific endeavor, such reconsideration is appropriate when epistemological questions arise – questions about how people know what they (think they) know.

Is It an Error? That Depends on Who You Ask

Consider a study reported by Hollnagel and Amalberti (2001), whose purpose was to test an error measurement instrument. The method asked observers to count errors and categorize errors using a taxonomy proposed by the developers. It was tested in a field setting by pairs of psychologists and air traffic controllers who studied air traffic control work in real time. Despite common indoctrination, there were substantial differences between the numbers and kinds of errors each of the two groups of observers noted, and only a very small number of errors were observed by both. Air traffic controllers relied on external working conditions (e.g., interfaces, personnel, and time resources) to refer to and categorize errors, whereas psychologists preferred to locate the error somewhere in presumed quarters of the mind (e.g., working memory) or in some mental state (e.g., attentional lapses).

Moreover, air traffic controllers who actually did the work could tell the error coders that they both had it wrong. Observed "errors" were not errors to those "committing" them but, rather, deliberate strategies intended to manage problems or foreseen situations that the error counters had neither seen nor understood as such if they had. Such normalization of actions, which at first appear deviant from the outside, is a critical aspect of understanding human work and its strengths and weaknesses (see Vaughan, 1999). Croft (2001) reported the same result in cockpits: More than half the "errors" revealed by error counters were never discovered by the flight crews themselves. Some realists may argue that the ability to discover errors not seen by people themselves confirms the superiority of the method. But such claims of epistemological privilege are hubris. As Jones (1986) pointed out, trying to study a social phenomenon, such as error, independent of meanings attached to it runs the risk of abstracting some essentialist definition of error that bears no relation to the practices and interpretations in question. In addition, it runs the risk of unconsciously imposing one's own subjective interpretation under the guise of detached, scientific observation.

Error Counting and Naive Realism

At first sight, Hollnagel's and Amalberti's air traffic control study raises the question of whose standard is right. If there is disagreement about what an observation means (i.e., whether it is an error or not), the question becomes one of arbitrage. Who can make the strongest epistemological claim? Many people would probably put their bet on the practitioner. But this misses the point. If particular observers describe reality in a particular way (e.g., this was a "procedure error"), then that does not imply any type of mapping onto an objectively attainable external reality – close or remote, good or bad. Postmodernists argue that a single, stable reality that can be most closely approximated by the best method or the most qualified observer does not exist (Capra, 1982). Although people seem to need the idea of a fixed, stable reality surrounding them, independent of who looks at it, the foregoing example denies them this.

The reality of an observation is socially constructed. The error becomes true (or appears to people as a close correspondence to some objective reality) only because a community of specialists has developed tools that would seem to make

it appear and have agreed on the language that makes it visible. There is nothing inherently "true" about the error at all. Its meaning is merely enforced and handed down through systems of observer training, labeling and communication of the results, and industry acceptance and promotion.

Observed Facts Are Created by the Method Itself

Even though an observed error may appear as entirely real and "factual" to the observer, that does not mean that it is. Facts privilege the ruling paradigm. Facts actually exist by virtue of the current paradigm. They can be neither discovered nor given meaning without it. The autonomy principle is false: Facts that are available as objective content of one theory are not equally available to another, as the theory itself helps construct them: "On closer analysis, we even find that science knows no 'bare facts' at all, but that the 'facts' that enter our knowledge are already viewed in a certain way and are, therefore, essentially ideational" (Feyerabend, 1993, p. 11).

Researchers who apply a theory of naturalistic decision making, for example, will not see a "procedure error." They may instead see a continuous control task, a flow of actions and assessments, coupled and mutually cued – a flow with nonlinear feedback loops and interactions, inextricably embedded in a multilayered evolving context. Such a characterization is hostile to the digitization necessary to fish out individual "human errors." Observers are themselves participants, participating in the very creation of the observed fact. (Even in a crude sense this would be true: Observing performance probably distorts people's normal practice, perhaps turning situated performance into window-dressed posture.)

STANDING FIRM: THE THEORY IS RIGHT

Kuhn (1962) resisted the idea that science progresses through the accumulation of observed facts that disagree with, and ultimately manage to topple, a theory. Counterinstances are seen only as further puzzles in the match between observation and theory, to be addressed by more method. It is extremely difficult for communities to renounce the paradigm that has led them into a crisis. Instead, epistemological difficulties suffered by error-counting methods (was this a cause or consequence, a procedural or proficiency error?) are entertained as reasons to engage in yet more methodological refinement consonant with the current paradigm. It can adopt a kind of self-sustaining energy, or "consensus authority" (see Angell & Straub, 1999), in which nobody questions error counting because everybody is doing it. In accepting the utility of error counting, it is likely that industry accepts its theory (and thereby the reality and validity of the observations it generates) on the authority of authors, teachers, and their texts, not because of evidence. Croft's 2001 headline in Aviation Week & Space Technology announced, "Researchers perfect new ways to monitor pilot performance." If researchers have perfected a method, there is little an industry can do other than accept such authority. What alternatives have they, Kuhn (1962) would ask, or what competence?

Nobody is willing to forgo a paradigm until and unless a viable alternative is ready to take its place. This is a sustained argument for the continuation of error counting: Researchers are willing to acknowledge that what they do is not perfect but vow to keep going until shown something better, and industry concurs. As Kuhn (1962) would say, the decision to reject one paradigm necessarily coincides with the embrace of another.

The Difficulty of Proposing an Alternative Theory

Proposing a viable alternative theory that can assimilate its own facts, however, is exceedingly difficult. Facts, after all, privilege the status quo. Galileo's telescopic observations of the sky motivated an alternative explanation about the place of the earth in the universe, which favored the Copernican heliocentric interpretation (in which Earth goes around the Sun) over the Ptolomeic geocentric one. The Copernican interpretation, however, was a worldview away from the ruling interpretation, and many doubted Galileo's data as a valid empirical window on a heliocentric universe. People were suspicious of the new instrument. Some asked Galileo to open up his telescope to prove that there was no little moon hiding inside of it (Feyerabend, 1993).

One problem was that Galileo did not offer a theory for why the telescope was supposed to offer a better picture of the sky than the naked eye. He could not, because relevant concepts (optica) were not yet well developed. Generating better data (as Galileo did) and developing new methods for better access to these data (e.g., a telescope) does in

itself little to dislodge an established theory that allows people to see a phenomenon with their naked eye and explain it with their common sense. The Sun goes around Earth. Earth is fixed. The Church was right, and Galileo was wrong. None of the observed facts could prove him right because there was no coherent set of theories ready to accommodate his facts and give them meaning. The Church was right, as *it* had all the facts – and it had the theory to assimilate them.

Interestingly, the Church kept closer to reason as it was defined at the time. It considered the social, political, and ethical implications of Galileo's alternatives and deemed them too risky to accept. Disavowing the geocentric idea would be disavowing creation itself, removing *the* common ontological denominator of the past millennium and severely undermining the authority and political power the Church derived from it. Error classification methods, too, guard a rationality that many would hate to see disintegrate. Without errors, without such a "factual" basis, how could one hold people accountable for mistakes or report safety occurrences and maintain expensive incident reporting schemes? What could people fix if there are no "causes"? They should, rather, hold onto the realist status quo and cause minimal disruption to the existing theory. And they can, for most observed facts still seem to privilege it. Errors exist. They must.

If You Cannot See Errors, You Are Not a Good Psychologist

To the naive realist, the argument that errors exist is not only natural and necessary – it is also quite impeccable. The idea that errors do not exist, in contrast, is unnatural. It is absurd. Those within the established paradigm will challenge the legitimacy of questions raised about the existence of errors and the legitimacy of those who raise the questions: "Indeed, there are some psychologists who would deny the existence of errors altogether. We will not pursue that doubtful line of argument here" (Reason & Hobbs, 2003, p. 39).

If some scientists do not succeed in bringing statement and fact into closer agreement (they do not see a "procedure error" where others would), then this discredits the scientist rather than the theory. Galileo suffered from this, too. It was the scientist who was discredited (for a while, at least), not the prevailing paradigm. So what did he do? Galileo engaged in propaganda and psychological trickery (Feyerabend, 1993). Through imaginary conversations among Sagredo, Salviati, and Simplicio, written in his native Italian rather than Latin, he put the ontological uncertainty and epistemological difficulty of the geocentric interpretation on full display. Where the appeal to empirical facts fails, an appeal to logic may still succeed. The same is true for error counting and classification. Just imagine this dialogue (see Dekker, 2005, p. 58–59):

> Simplicio: "Errors result from physiological and psychological limitations of humans. Causes of error include fatigue, workload, and fear, as well as cognitive overload, poor interpersonal communications, imperfect information processing, and flawed decision making."
> Sagredo: "But are errors in this case not simply the result of other errors? Flawed decision making would be an error. But in your logic, it causes an error. What is the 'error' then? And how can we categorize it?"
> Simplicio: "Well, but errors are caused by poor decisions, failures to adhere to instructions, failures to prioritize attention, improper procedure, and so forth."
> Sagredo: "This appears to be not causal explanation, but simply relabeling. Whether you say 'error,' or 'poor decision,' or 'failure to prioritize attention,' it all still sounds like 'error,' at least when interpreted in your worldview. And how can one be the cause of the other to the exclusion of the other way around? Can 'errors' cause 'poor decisions' just like 'poor decisions' cause 'errors'? There is nothing in your logic that rules this out, but then we end up with a tautology, not an explanation."

And yet, such arguments may not help, either. The appeal to logic may fail in the face of overwhelming support for a ruling paradigm – support that derives from consensus authority. Even Einstein expressed amazement at the common reflex to rely on measurements (e.g., error counts) rather than logic and argument: "Is it not really strange," Albert Einstein asked in a letter to Max Born (quoted in Feyerabend, 1993, p. 239), "that human beings are normally deaf to the strongest of argument while they are always inclined to overestimate measuring accuracies?"

Numbers are strong. Arguments are weak. Error counting is good because it generates numbers. It relies on putatively accurate measurements (recall Croft, 2001: "Researchers" have "perfected" ways to monitor pilot performance). People will reject no theory on the basis of argument or logic alone. They need another to take its place.

ABANDON THE IDEA OF ERRATIC PEOPLE IN SAFE SYSTEMS

The dominant safety paradigm in human factors has long been based on searching for ways to limit human variability in otherwise safe systems (Hollnagel, Woods, & Leveson, 2006; Woods, Johannesen, Cook, & Sarter, 1994). The assumption is that safety, once established, can be maintained by requiring human performance to stay within prescribed boundaries. Error counting and categorizing operationalizes this assumption by trying to observe how performance deviates from, or strays outside, established norms (e.g., violations of procedure, inadequate proficiency). Indeed, error counting assumes that the quantity measured (errors) has a meaningful relationship with the quality investigated (safety). It goes without saying that more of the quantity gives less of the quality. Such a connection is a folk model, at best, and is actually unsupported by evidence. Instead, studies of how complex systems succeed, and sometimes fail, demonstrate a much more complex, and much less instrumental, relationship among external worlds of cause and effect, social worlds of human relationships, and inner worlds of values and meaning.

The formal descriptions of work embodied in policies, procedures, and regulations – and implicitly imposed through error counting – are incomplete as models of expertise and success (e.g., Hollnagel et al., 2006). In a world of finite resources, uncertainty, and multiple conflicting goals, the knowledge base for generating safety in complex, risky operations is inherently and permanently imperfect (Rochlin, 1999), and no externally dictated logics of an error categorization system can arbitrate in any lasting way between what is safe and what is unsafe. The issue is not, therefore, whether potentially erratic human performance stays within or strays outside the perimeters of artificially imposed error categories, for those categories themselves represent only a particular slice of the knowledge base, or a particular model of risk, about what makes operations resilient or brittle. This representation is probably an obsolete, coarse approximation at best. There are two interesting issues: The first is how practitioners themselves continually contribute to the creation of safety through their practice at all levels of an organization and how self-conscious these practitioners are with respect to those constructions of safety and risk. The second is how researchers and other stakeholders develop and sustain the models of risk that find their expression in the methods and countermeasures they deploy, and whether these stakeholders are sufficiently self-conscious to acknowledge that those models may be ill calibrated, or a bad fit, and ready for reconsideration and renewal. In other words, do researchers and stakeholders themselves monitor, and critically question, how they monitor safety? In conclusion, I turn to these two issues now.

People Create Safety Through Practice

Where the creation of safety appears to have everything to do with people learning about, and adapting around, multiple goals, hazards, and trade-offs, deeper investigation of most stories of "error" show that failures represent breakdowns in adaptations directed at coping with such complexity (e.g., Cook, 1998; Hollnagel et al., 2006; Rochlin, 1999). Among other things, they indicate the following:

- Practitioners and organizations continually assess and revise their approaches to work in an attempt to remain sensitive to the possibility of failure. Efforts to create safety, in other words, are ongoing. Not being successful is related to limits of the current model of competence and, in a learning organization, reflects a discovery of those boundaries.
- Strategies that practitioners and organizations maintain for coping with potential pathways to failure can either be strong or resilient (i.e., well calibrated) or weak and mistaken (i.e., ill calibrated).
- Organizations and people can also become overconfident in how well calibrated their strategies are. Effective organizations remain alert for signs that circumstances exist, or are developing, in which that confidence is erroneous or misplaced (Gras, Moricot, Poirot-Delpech, & Scardigli, 1990/1994; Rochlin, 1993). This, after all, can avoid narrow interpretations of risk and stale countermeasures.

Safe operation, accordingly, has little to do with the structural descriptors sought by error counts ("violations," "proficiency errors"), nor is safety the instrumental outcome of a minimization of errors and their presumably measurable effects. Safety does not exist "out there," independent of people's minds or culture, ready to be measured by looking at behavior alone (Slovic, 1992). Instead, insight has been growing that research into safe operations should consider safety as a dynamic, interactive, communicative act that is created as people conduct work, construct discourse and rationality around it, and gather experiences from

it (e.g., Orasanu, 2001). Cultures of safety are not cultures without errors or violations – on the contrary. Practitioners are not merely in the business of managing risk or avoiding error, if they are that at all. Rather, they actively engage operational and organizational conditions to intersubjectively construct their beliefs in the possibility of continued operational safety. This includes anticipation of events that could have led to serious outcomes, complemented by the continuing expectation of future surprise. "Safety is in some sense a story a group or organization tells about itself and its relation to its task environment" (Rochlin, 1999, p. 1555).

Particular aspects of how organization members tell or evaluate safety stories can serve as markers (see Columbia Accident Investigation Board, 2003). In *Creating Foresight* (2003), Woods (p. 5), for example, called one of these "distancing through differencing." In this process, organizational members look at other failures and other organizations as not relevant to them and their situation. They discard other events because they appear to be dissimilar or distant. Discovering this through qualitative inquiry can help specify how people and organizations reflexively create their idea, their story of safety. Just because the organization or section has different technical problems, different managers, different histories, or can claim to already have addressed a particular safety concern revealed by the event does not mean that they are immune to the problem. Seemingly divergent events can represent similar underlying patterns in the drift toward hazard. High-reliability organizations characterize themselves through their preoccupation with failure: They continually ask themselves how things can go wrong or could have gone wrong, rather than congratulating themselves that things went right. Distancing through differencing means underplaying this preoccupation. It is one way to prevent learning from events elsewhere, one way to throw up obstacles in the flow of safety-related information.

Additional processes that can be discovered include the extent to which an organization resists oversimplifying interpretations of operational data – whether it defers to expertise and expert judgment rather than managerial imperatives, and whether it sees continued operational success as a guarantee of future safety, as an indication that hazards are not present or that countermeasures in place suffice. Also, it could be interesting to probe to what extent problem-solving processes are disjointed across organizational departments, sections, or subcontractors, as discontinuities and internal handovers of tasks increase risk (Vaughan, 1999). With information incomplete, disjointed, and patchy, nobody may be able to recognize the gradual erosion of safety constraints on the design and operation of the original system.

Monitoring How Safety Is Monitored

It is, of course, a matter of debate whether the higher order organizational processes that could be part of new safety probes (e.g., distancing through differencing, deference to expertise, fragmentation of problem solving, incremental judgments into disaster) are any more real than the errors from the counting methods they seek to replace or augment. But then, the reality of these phenomena is in the eye of the beholder. The processes and phenomena are real enough to those who look for them and who wield the theories to accommodate the results. Criteria for success may lie elsewhere – for example, in how well the measure maps onto past evidence of precursors to failure. Yet even such mappings are subject to paradigmatic interpretations of the evidence base. Indeed, consonant with the ontological relativity of the age human factors has now entered, the debate can probably never be closed. Are doctors more dangerous than gun owners? Do errors exist? It depends on whom you ask.

The real issue, therefore, lies a step away from the fray. A level up, if you will. Whether errors are counted as Durkheimian fact or safety is seen as a reflexive project, competing premises and practices reflect particular models of risk. These models of risk are interesting not because of their differential abilities to access empirical truth (because that may all be relative) but because of what they say about the creators or proponents of the models. It is not merely the monitoring of safety that should be pursued but the monitoring of that monitoring (*Creating Foresight,* 2003). To make progress in safety, one important step is to engage in such meta-monitoring. Researchers should become better aware of the models of risk embodied in their approaches to safety. Whether doctors are more dangerous than gun owners, in other words, is irrelevant. What matters is what the respective communities see as their dominant sources of risk and how that, in turn, informs the measures and countermeasures they apply.

REFERENCES

Angell, I. O., & Straub, B. (1999). Rain-dancing with pseudo-science. *Cognition, Technology and Work, 1,* 179–196.

Billings, C. E., & Cheaney, E. S. (1981). *Information transfer problems in the aviation system* (NASA Tech. Paper 1875). Moffett Field, CA: NASA Ames Research Center.

Capra, F. (1982). *The turning point.* New York: Simon and Schuster.

Columbia Accident Investigation Board. (2003). *Report Volume 1, August 2003*. Washington, DC: U.S. Government Printing Office.

Cook, R. I. (1998). Two years before the mast: Learning how to learn about patient safety. In *Proceedings of Enhancing Patient Safety and Reducing Errors in Health Care: A Multidisciplinary Leadership Conference* (pp. 61–65). Rancho Mirage, CA: Annenberg Center for Health Sciences at Eisenhower.

Creating foresight: How resilience engineering can transform NASA's approach to risky decision making: U.S. Senate testimony for the Committee on Commerce, Science and Transportation, 108th Cong., Future of NASA SR-253 (2003) (testimony of David Woods, Professor, Institute for Ergonomics, The Ohio State University).

Croft, J. (2001). Researchers perfect new ways to monitor pilot performance. *Aviation Week and Space Technology, 155(3),* pp. 76–77.

Dekker, S. W. A. (2005). *Ten questions about human error: A new view of human factors and system safety.* Mahwah, NJ: Erlbaum.

Dougherty, E. M., Jr. (1990). Human reliability analysis: Where shouldst thou turn? *Reliability Engineering and System Safety, 29,* 283–299.

Durkheim, E. (1950). *The rules of the sociological method*. New York: Free Press. (Original work published 1895)

Fegetter, A. J. (1982). A method for investigating human factors aspects of aircraft accidents and incidents. *Ergonomics, 25,* 1065–1075.

Feyerabend, P. (1993). *Against method* (3rd ed.). London: Verso.

Gras, A., Moricot, C., Poirot-Delpech, S. L., & Scardigli, V. (1994). *Faced with automation: The pilot, the controller, and the engineer* (J. Lundsten, Trans.). Paris: Publications de la Sorbonne. (Original work published 1990)

Helmreich, R. L. (2000). On error management: Lessons from aviation. *British Medical Journal, 320,* 745–753.

Helmreich, R. L., Klinect, J. R., & Wilhelm, J. A. (1999). Models of threat, error and CRM in flight operations. In R. S. Jensen (Ed.), *Proceedings of the 10th International Symposium on Aviation Psychology* (pp. 677–682). Columbus: Ohio State University.

Hollnagel, E. (1998). *Cognitive reliability and error analysis method (CREAM).* Oxford, UK: Elsevier Science.

Hollnagel, E., & Amalberti, R. (2001). The emperor's new clothes: Or whatever happened to "human error"? In S. W. A. Dekker (Ed.), *Proceedings of the 4th International Workshop on Human Error, Safety and Systems Development* (pp. 1–18). Linköping Sweden: Linköping University.

Hollnagel, E., Woods, D. D., & Leveson, N. G. (2006). *Resilience engineering: Concepts and precepts.* Aldershot, UK: Ashgate.

Jones, R. A. (1986). *Emile Durkheim: An introduction to four major works*. Beverly Hills, CA: Sage.

Kohn, L. T., Corrigan, J. M., & Donaldson, M. (Eds.). (1999). *To err is human: Building a safer health system.* Washington, DC: Institute of Medicine.

Kowalsky, N. B., Masters, R. L., Stone, R. B., Babcock, G. L., & Rypka, E. W. (1974). *An analysis of pilot error related to aircraft accidents* (NASA CR-2444). Washington, DC: NASA.

Kuhn, T. (1962). *The structure of scientific revolutions.* Chicago, IL: University of Chicago Press.

National Safety Council. (2004). *Injury facts 2004 edition.* Itasca, IL: Author.

Orasanu, J. M. (2001). The role of risk assessment in flight safety: Strategies for enhancing pilot decision making. In *Proceedings of the 4th International Workshop on Human Error, Safety and Systems Development* (pp. 83–94). Linköping Sweden: Linköping University.

Reason, J. T. (1990). *Human error*. Cambridge, UK: Cambridge University Press.

Reason, J. T., & Hobbs, A. (2003). *Managing maintenance error: A practical guide*. Aldershot, UK: Ashgate.

Rochlin, G. I. (1993). Defining high-reliability organizations in practice: A taxonomic prolegomenon. In K. H. Roberts (Ed.), *New challenges to understanding organizations* (pp. 11–32). New York: Macmillan.

Rochlin, G. I. (1999). Safe operation as a social construct. *Ergonomics, 42,* 1549–1560.

Rouse, W. B., & Rouse, S. H. (1983). Analysis and classification of human error. *IEEE Transactions on Systems, Man, and Cybernetics, SMC-13,* 539–549.

Shappell, S. A., & Wiegmann, D. A. (2001). Applying Reason: The human factors analysis and classification system (HFACS). *Human Factors and Aerospace Safety, 1,* 59–86.

Slovic, P. (1992). Perception of risk: Reflections on the psychometric paradigm. In S. Krimsky & D. Golding (Eds.), *Social theories of risk* (pp. 117–152). Westport, CT: Praeger.

Vaughan, D. (1999). The dark side of organizations: Mistake, misconduct, and disaster. *Annual Review of Sociology, 25,* 271–305.

Woods, D. D., Johannesen, L. J., Cook, R. I., & Sarter, N. B. (1994). *Behind human error: Cognitive systems, computers and hindsight.* Dayton, OH: CSERIAC.

Sidney W. A. Dekker is a professor of human factors and system safety and director of research at the School of Aviation, Lund University, Sweden. He gained his Ph.D. in cognitive systems engineering from the Ohio State University in 1996.

Date received: May 8, 2005
Date accepted: January 17, 2006

Cogn Tech Work
DOI 10.1007/s10111-008-0110-7

ORIGINAL ARTICLE

Just culture: who gets to draw the line?

Sidney W. A. Dekker

Received: 15 October 2007 / Accepted: 14 January 2008

Abstract A just culture is meant to balance learning from incidents with accountability for their consequences. All the current proposals for just cultures argue for a clear line between acceptable and unacceptable behavior. This alone, however, cannot promote just culture as it falsely assumes that culpability inheres in the act, bearing immutable features independent of context, language or interpretation. The critical question is not where to draw the line, but who gets to draw it. Culpability is socially constructed: the result of deploying one language to describe an incident, and of enacting particular post-conditions. Different accounts of the same incident are always possible (e.g. educational, organizational, political). They generate different repertoires of countermeasures and can be more constructive for safety. The issue is not to exonerate individual practitioners but rather what kind of accountability promotes justice and safety: backward-looking and retributive, or forward-looking and change-oriented.

Keywords Incident reporting · Just culture · Human error · Accountability · Criminalization · Culpability

1 Drawing a line between legitimate and illegitimate behavior

The desire to balance learning from failure with appropriate accountability has motivated safety–critical industries and organizations to develop guidance on a so-called "just culture". In this paper I question whether such guidance can merely focus on a clear line between acceptable and unacceptable behavior—which all such guidance today does. This is based on the essentialist assumption that inherently culpable acts exist and should be dealt with as such. The counterproposition I advance in this paper is that culpable acts have no essentialist properties or immutable features, but that designations of acceptability or culpability are the result of processes of social construction steeped in context, language, history. After setting out the constructionist argument, I assess various alternatives of who gets the power to draw the line, and review the negative consequences for safety of leaving it in the hands of a judiciary alone. Then I try to clear up confusion between blame-free and accountability-free, suggesting that some forms of accountability, and accountability relationships between stakeholders, can be more constructive for safety than others. I conclude with a list of suggestions for organizations on building the basis for a just culture.

1.1 Balancing accountability and learning

Concern about just cultures has grown out of our changing interpretation of accidents since the 1970s (such as the nuclear incident at Three Mile Island, and the twin Boeing 747 disaster at Tenerife). We no longer see such accidents as meaningless, uncontrollable events, but rather as failures of risk management, and behind these failures are people and organizations (Green 2003). Today, almost every accident is followed by questions centering on "whose fault?" and "what damages, compensation?" It seems as if every death must be charged to somebody's account (Douglas 1992). We have increasingly begun to see

S. W. A. Dekker (✉)
Lund University School of Aviation, 260 70 Ljungbyhed, Sweden
e-mail: sidney.dekker@tfhs.lu.se

accidents as the result of people not doing their jobs properly, and the possibility of punishing them for that is no longer is remote. In 2006, for example, a nurse from Wisconsin was charged with criminal "neglect of a patient causing great bodily harm" in the medication death of a 16-year-old girl during labor. Instead of giving the intended penicillin intravenously, the nurse accidentally administered a bag of epidural analgesia. She lost her job, faced action on her nursing license and the threat of 6 years in jail as well as a 25,000$ fine. Her predicament likened that of three nurses in Denver in 1998, who administered benzathine penicillin intravenously, causing the death of a neonate. The nurses were charged with criminally negligent homicide and faced 5 years in jail (Cook et al. 2000). This in turn was similar to a nurse in Sweden convicted of manslaughter in an order-of-magnitude medication error that led to an infant's death (Dekker 2007).

Criminalization of any act is not just about retribution and explanation of misfortune, but also about putative deterrence, and so it is with the criminalization of human error. Responding to the 1996 ValuJet accident, where mechanics loaded oxygen generators into the cargo hold of a DC-9 airliner which subsequently caught fire, the editor of *Aviation Week and Space Technology* "strongly believed the failure of SabreTech employees to put caps on oxygen generators constituted willful negligence that led to the killing of 110 passengers and crew. Prosecutors were right to bring charges. There has to be some fear that not doing one's job correctly could lead to prosecution" (North 2000, p. 66). The deterrence argument is problematic, however, as threats of prosecution do not deter people from making errors, but rather from reporting them (e.g. Merry et al. 2001; Cohen-Charash and Spector 2001; Sharpe 2003). Instead, anxiety created by such accountability leads for example to defensive medicine, not high-quality care, and even to a greater likelihood of subsequent incidents (e.g. Dauer 2004). The anxiety and stress generated by such accountability adds attentional burdens and distracts from conscientious discharge of the main safety–critical task (Lerner and Tetlock 1999).

A just culture, then, is particularly concerned with the sustainability of learning from failure through the reporting of errors, adverse events, incidents. If operators and others perceive that their reports are treated unfairly or lead to negative consequences, the willingness to report will decline (e.g. Ruitenberg 2002 cited a 50% drop in incident reports after the prosecution of air traffic controllers involved a near-miss). Writings about just culture over the past decade (e.g. Reason 1997; Marx 2001; Dekker 2008) acknowledge this central paradox of accountability and learning: various stakeholders (e.g. employers, regulators) want to know everything that happened, but cannot accept everything that happened and will want to advertise their position as such. Thus, rating certain behavior as culpable is not just about that behavior or its antecedent intentions, it performs a wider function of regulating a distinction between normal and abnormal, between order and disorder. "A 'no-blame' culture is neither feasible nor desirable. Most people desire some level of accountability when a mishap occurs" (GAIN 2004 p. viii). These are neo-Durkheimian ideas (see Durkheim 1950, 1895) about the boundary-maintaining function of the organizational rituals and languages that keep such a distinction in place:

"Confrontations in the form of criminal trials, excommunication hearings, courts-martial … act as boundary-maintaining devices in the sense that they demonstrate … where the line is drawn between behavior that belongs in the special universe of the group and behavior that does not" (Erikson 1966 p. 11).

Demonstrating a border between acceptable and unacceptable is deemed critical. After all, an environment of impunity, the argument holds, would neither move people to act prudently nor compel them to report errors or deviations. If there is no line, "anything goes". So why report anything?

1.2 The line is a judgment, not a location

The essentialist assumption that animates current guidance on just culture is that some behavior is inherently culpable, and should be treated as such. The public must be protected against intentional misbehavior or criminal acts, and the application of justice is a prime vehicle for this (e.g. Reason 1997). As Marx (2001 p. 3) puts it, "It is the balancing of the need to learn from our mistakes and the need to take disciplinary action that (needs to be addressed). Ultimately, it will help you answer the question: 'Where do you draw the disciplinary line?" As another example (Eurocontrol 2006), a just culture is one in which "front-line operators or others are not punished for actions, omissions or decisions taken by them that are commensurate with their experience and training, but where gross negligence, willful violations and destructive acts are not tolerated". Such proposals emphasize the establishment of, and consensus around, some kind of separation between legitimate and illegitimate behavior: "in a just culture, staff can differentiate between acceptable and unacceptable acts" (Ferguson and Fakelmann 2005 p. 34). Similarly, "in a Just Culture environment the culpability line is more clearly drawn" (GAIN 2004 p. viii).

But drawing an a priori line between the acts an organization will accept and those it will not is difficult. Culpability does not inhere in the act. Whether something is judged culpable is the outcome of processes of interpretation and attribution that follow the act, in which

assumptions of other people's volitional behavior and outcome control, as well as causal control, play a dominant role (Alicke 2000). Thus, to gauge whether behavior should fall on one side of the line or the other, variations on a basic decision tree are in circulation (e.g. Reason 1997). Yet its questions confirm the negotiability of the line rather than resolving its location:

- *Were the actions and consequences as intended*? This invokes the judicial idea of a mens rea ("guilty mind"), and seems a simple enough question. Few people in safety–critical industries intend to inflict harm, though that does not prevent them from being prosecuted for their "errors" (under charges of manslaughter, for example, or general risk statutes that hail from road traffic laws on "endangering other people," see e.g. Wilkinson 1994). Also, what exactly is intent and how do you prove it? And who gets to prove this, using what kind of expertise?
- *Did the person knowingly violate safe operating procedures*? People in operational worlds knowingly adapt written guidance, and have to do so to bridge the gap between prescriptive routines and actual work in worlds of imperfect knowledge, time constraints and infinite variation (Suchman 1987; Rochlin 1999; Vaughan 1999; Woods and Shattuck 2000; Smith 2001; Dekker 2003). Calling such adaptations "violations" (Reason 1997) already implies a moral judgment about who is wrong (the worker) and who is right (the rule). It is easy to show in hindsight which procedures would have been applicable, available, workable and correct for a particular task (says who, though?), but such overestimations of the role of procedural non-compliance in the wake of incidents conceals the real operational dilemmas faced by people (McDonald et al. 2002).
- *Were there deficiencies in training or selection*? "Deficiencies" seems unproblematic but what is a deficiency from one angle can be perfectly normal or even above industry standard from another.

Questions such as the ones above may form a good start, but they themselves cannot arbitrate between culpable or blameless behavior. Rather, they invoke new judgments and negotiations. This is also true for the very definition of negligence (a legal term, not a human performance concept):

"Negligence is a conduct that falls below the standard required as normal in the community. It applies to a person who fails to use the reasonable level of skill expected of a person engaged in that particular activity, whether by omitting to do something that a prudent and reasonable person would do in the circumstances or by doing something that no prudent or reasonable person would have done in the circumstances. To raise a question of negligence, there needs to be a duty of care on the person, and harm must be caused by the negligent action. In other words, where there is a duty to exercise care, reasonable care must be taken to avoid acts or omissions which can reasonably be foreseen to be likely to cause harm to persons or property. If, as a result of a failure to act in this reasonably skillful way, harm/injury/damage is caused to a person or property, the person whose action caused the harm is negligent" (GAIN 2004 p. 6).

There is no definition that captures the essential properties of "negligence". Instead, definitions such as the one above open a new array of questions and judgments. What is "normal standard?" How far is "below?" What is "reasonably skillful?" What is "reasonable care?" What is "prudent?" Was harm indeed "caused by the negligent action?" Of course, making such judgments is not impossible. In fact, they remain judgments—made by somebody or some group in some time and place in the aftermath of an act—not objective features that stably inhabit the act itself. That judgments are required to figure out whether we deem an act culpable is not the problem. The problem is guidance that suggests that a just culture only needs to "clearly draw" a line between culpable and blameless behavior. Its problem lies in the false assumption that acceptable or unacceptable behavior form stable categories with immutable features that are independent of context, language or interpretation.

2 Different accounts and meanings of failure

2.1 The social construction of culpability

Just as the properties of "human error" are not objective and independently existing, so does culpability arise out of our ways of seeing and describing acts. What ends up being labeled as culpable does not inhere in the act or the person. It is constructed, or "constituted" as Christie (2004 p. 10) put it:

"The world comes to us as we constitute it. Crime is thus a product of cultural, social and mental processes. For all acts, including those seen as unwanted, there are dozens of possible alternatives to their understanding: bad, mad, evil, misplaced honour, youth bravado, political heroism—or crime. The same acts can thus be met within several parallel systems as judicial, psychiatric, pedagogical, theological".

It is tempting to think that culpability, of all things, must make up some essence behind a number of possible descriptions of an act, especially if that act has a bad outcome. We hope that the various descriptions can be sorted out by the rational process of an investigation, a hearing or a trial, and that it will expose Christie's "psychiatric, pedagogical, theological" explanations (I had failure anxiety! I was not trained enough! It was the Lord's will!) as false.

The application of reason will strip away the noise, the decoys, and the excuses to arrive at the essential story: whether culpability lay behind the incident or not. And if culpable behavior turns out not make up the essence, then there will be no retribution. But Christie argued that culpability is not an essence that we can discover behind the inconsistency and shifting nature of the world as it meets us. Culpability itself is that flux, that inconstancy, a negotiated arrangement, a tenuous, temporary stability achieved among shifting cultural, social, mental and political forces. Concluding that an unwanted act is culpable, is an accomplished project, a purely human achievement:

> … deviance is created by society … social groups create deviance by making the rules whose infraction constitutes deviance and by applying those rules to particular persons and labeling them as outsiders. From this point of view, deviance is not a quality of the act the person commits, but rather a consequence of the application by others of rules and sanctions to an "offender". The deviant is the one to whom the label has successfully been applied; deviant behavior is behavior that people so label (Becker 1963 p. 9).

Becker argues that what counts as deviant or culpable is the result of processes of social construction. According to this, if an organization decides that a certain act constituted "negligence" or otherwise falls on the wrong side of the line, then this is the result of using a particular language and enacting a particular repertoire of post-conditions that turn the act into culpable behavior and the involved practitioner into an offender (e.g. Burr 2003).

2.2 Alternative readings of the same act

The social constructionist argument about culpability is that by seeing human error as a crime, we have evoked just one language for describing and explaining an event, relative to a multitude of other possibilities. If we subscribe to this one reading as true, it will blind us to alternative readings or framings that can frequently be more constructive. Take as an example a British cardiothoracic surgeon who moved to New Zealand (Skegg 1998). There, three patients died during or immediately after his operations, and he was charged with manslaughter. Not long before, a professional college had pointed to serious deficiencies in the surgeon's work and found that seven of his cases had been managed incompetently. The report found its way to the police, which subsequently investigated the cases. This in turn led to the criminal prosecution against the surgeon. But the same unwanted act can be construed to be a lot of things at the same time, depending on what questions you asked to begin with. Ask Christie's theological question and you may see in an error the manifestation of evil, or the weakness of the flesh. Ask pedagogical questions and you may see in it the expression of underdeveloped skills. Ask judicial questions and you may begin to see a crime. Calling the surgical failures a crime is one possible interpretation of what went wrong and what should be done about it. Other ways are possible too, and not necessarily less valid:

- For example, we could see the three patients dying as an issue of cross-national transition: are procedures for doctors moving to Australia or New Zealand and integrating them in local practice adequate?
- And how are any cultural implications of practicing there systematically managed or monitored, if at all?
- We could see these deaths as a problem of access control to the profession: do different countries have different standards for who they would want as a surgeon, and who controls access, and how?
- It could also be seen as a problem of training or proficiency-checking: do surgeons submit to regular and systematic follow-up of critical skills, such as professional pilots do in a proficiency check every 6 months?
- We could also see it as an organizational problem: there was a lack of quality control procedures at the hospital, and the surgeon testified having no regular junior staff to help with operations, but was made to work with only medical students instead.
- Finally, we could interpret the problem as socio-political: what forces are behind the assignment of resources and oversight in care facilities outside the capital?

It may well be possible to write a compelling argument for each of these explanations of failure—each with a different repertoire of interpretations and countermeasures following from it. A crime gets punished away. Access and proficiency issues get controlled away. Training problems get educated away. Organizational issues get managed away. Political problems get elected or lobbied away. This also has different implications for what we mean by accountability. If we see an act as a crime, then accountability means blaming and punishing somebody for it. Accountability in that case is backward-looking, retributive. If, instead, we see the act as an indication of an organizational, operational, technical, educational or political issue, then accountability can become forward-looking. The question becomes: what should we do about the problem and who should bear liability for implementing those changes?

2.3 Overlapping and contradictory versions of history

The point is not that one interpretation of an incident is right and all the others are wrong. All the accounts are

inherently limited. Telling the story from one angle necessarily excludes the aspects from other angles. And all the interpretations have different ramifications for what people and organizations think they should do to prevent recurrence. Finding an act culpable, then, is settling onto one particular version or description of history. This version is not just produced for its own sake. It may serve a range of social functions, from emphasizing moral boundaries and enhancing solidarity (Erikson 1966), to sustaining subjugation or asymmetric power distribution within hierarchies (Foucault 1981), to protecting elite interests after an incident has exposed possibly expensive vulnerabilities in the whole industry (Perrow 1984; Byrne 2002), to mitigating public or internal apprehension about the system's ability to protect its safety–critical technologies against failure (Vaughan 1996; Galison 2000). This also denies the modernist objectification of history (captured, for example, in "probable cause" statements in incident reports) that considers the past to be an object; bygone, coagulated. Instead, the past is a dimension of our present experience. The past offers all kinds of opportunities to express and handle current issues, address current concerns, accommodate current agendas. This makes it critical to consider who owns the right to write history. Who has the power to tell a story of performance in such a way—to use a particular rhetoric to describe it, ensuring that certain subsequent actions are legitimate or even possible (e.g. pursuing a single culprit), and others not—so as to, in effect, own the right to draw the line?

3 Whom do we give the power to draw the line?

3.1 Judicial drawing of the line

People increasingly turn to the legal system to furnish them with an answer about the culpability of a practitioner's performance (Laudan 2006). For example, a directive from the European Union (2003/42/EC) says that a state must not institute legal proceedings against those who send in incident reports, apart from cases of gross negligence. But who gets to decide whether an act amounts to gross negligence? The same state, through its judiciary. Even so, we expect a court to apply reason, and objectivity. A disinterested party takes an evenhanded look at the case, the appropriate person gets to be held accountable and consequences are meted out. We tend to believe that an "objective" account (one produced by the rational processes of a court, or an independent investigation of the incident) delivers superior accuracy because it is well-researched and not as tainted by interests or a particular, partisan perspective. Many aspects of the justice system (and of formal accident investigation) are indeed designed to impart an image of rationality, of consideration, objectivity and impartiality (e.g. Lady Justitia's blindfold, or the party system in certain investigations). But truths (or accounts that are taken as valid) are always brought into being by historically and culturally located groups of people, and as such open to the myriad influences that impact any social process.

Judicial involvement can consist of:

- The participation of law enforcement officials in investigations. There are countries in the developed world where the police is witness or participant in accident investigations (in for example road traffic or aviation). This can impede investigatory access to information sources, as pressures to protect oneself against criminal or civil liability can override a practitioner's willingness to cooperate in the accident probe.
- Judicial authorities stopping an investigation or taking it over when evidence of criminal wrong-doing emerges. This often restricts further access to evidence for safety investigators.
- Launching a criminal probe independent of a safety investigation or its status. Accident investigation boards typically say this retards their efforts to find out what went wrong and what to do to prevent recurrence (North 2002). For example, while the US National Transportation Safety Board was investigating a 1999 pipeline explosion near Bellingham, Washington, that killed three people, federal prosecutors launched their own criminal probe. They reportedly pressured employees of the pipeline operator to talk. Several invoked the US Constitution's Fifth Amendment, which protects against self-incrimination. They refused to answer questions from Safety Board investigators as well as from the police (McKenna 1999).
- Using a formal accident report in a court case. Even though using such reports as evidence in court is proscribed through various statutory arrangements (Eurocontrol 2006), these can get overridden or circumvented. And nobody can prevent a prosecutor or judge from simply reading a publicly-available accident report.
- Getting access to safety-related data (e.g. internal incident reports) because of freedom-of-information legislation in that country, under which any citizen (including the judicial system) has quite unfettered access to many kinds of organizational data. This access is particularly acute in organizations that are government-owned (such as many air traffic control providers, or hospitals).
- Taking the results of a safety inspection if these expose possibly criminal or otherwise liable acts. This does not have to take much: an inspection report listing

"violations" (of regulations, which in turn are based in law) can be enough for a prosecutor to start converting those violations (which were discovered and discussed for the purpose of regulatory compliance and safety improvement) into prosecutable crimes.

In all these ways, judicial involvement (or the threat of it) can engender a climate of fear and silence (Ter Kulle 2004). So even as a court of law cannot bring the "truth" about human performance into necessarily sharper focus than any other social process (Nagel 1992), it has measurably negative consequences for practitioners' (and sometimes even regulators') inclination to share safety information (Ruitenberg 2002; Dekker 2008). A recent European-wide Air Traffic Control survey confirms how the threat of judicial involvement after incidents (and certainly accidents) dampens people's willingness to come forward with safety information (Eurocontrol 2006), and other examples are not hard to come by (e.g. Wilkinson 1994). In the wake of a June 1995 crash of an Ansett de Havilland Dash 8 near Palmerston North in New Zealand, accident investigators turned the aircraft's cockpit voice recorder (CVR) over to criminal prosecutors. The crash killed four persons on the aircraft, but not the pilots, who faced charges of manslaughter. Pilots in New Zealand sued to block the police use of the CVR, arguing recorders should only be used for safety and educational purposes. But prosecutors prevailed and regained access to the CVR. Pilots soon began disabling CVR's on their flights, prompting legislative changes that involved the country's High Court and proscribing the public us of CVR information (McKenna 1999).

3.2 Alternatives to judicial drawing of the line

To mitigate the negative side-effects of judicial interference, some countries have moved ahead with installing a so-called judge of instruction, who functions as a go-between before a prosecutor can actually go ahead with a case. A judge of instruction gets to determine whether a case proposed by a prosecutor should be investigated (and later go to trial). The judge of instruction, in other words, can check the prosecutor's homework and ambitions, do some investigation him- or herself, and weigh other stakeholders' interests in making the decision to go ahead with a further investigation and possible prosecution or not. It is still the judge of instruction who gets to draw the line between acceptable and unacceptable (or: between worthy of further investigation and possible prosecution or not), but broader considerations can make it into the drawing of the line too (e.g. the interests of other industry stakeholders, as long as those are fairly represented).

Another adaptation is to make the prosecutor part of the regulator, as has been done in some countries (particularly in aviation). The prosecutor him- or her-self has a history in or affiliation with the domain, guaranteeing an understanding of and concern for its sources of safety. It is thus likely that the prosecutor is better able to balance the various interests in deciding whether to draw a line, and better able to consider subtle features of the professional's performance that non-domain experts would overlook or misjudge. The risk in this solution, of course, is that the regulator itself can have played a role (e.g. insufficient oversight, or given dispensation) in the creation of an incident and can have a vested interest in the prosecution of an individual practitioner so as to downplay its own contribution. There is no immediate protection against this in this local solution, except for regulatory self-restraint and perhaps the possibility of appeals higher up in the judiciary.

Disciplinary rules within the profession are another alternative. Many professional groups (from accountants to physicians to hunters to professional sports players) have elaborate systems of disciplinary rules. These are meant foremost to protect the integrity of a profession. Usually, a judiciary delegates large amounts of legal authority to the boards that credibly administer these professional disciplinary rules. Professional sanctions can range from warning letters (which are not necessarily effective) to the revocation of licenses to practice. The judiciary will not normally interfere with the internal administration of justice according to these disciplinary rules. There is, however, great variation in the administration of internal professional justice and thus a variation in how much confidence a country can have in delegating it to an internal disciplinary board. And of course, it does not remove the problem of where the line goes: the judiciary will still have to judge whether a line has been crossed that prompts them to step in. This even raises a possible paradox in the justness of professional disciplinary rules. Because disciplinary rules aim to maintain the integrity of a profession, individual practitioners may still get "sacrificed" for that larger aim (especially to keep the system free from outside interference or unwelcome judicial scrutiny).

4 Blame-free or accountability-free?

4.1 A discretionary space for accountability

Moves to redirect the power to draw the line away from the judiciary can be met with suspicions that operators want to blame "the system" when things go wrong, and that they do not want to be held liable in the same way as other citizens (Merry et al. 2001; Pellegrino 2004). Yet perhaps

the choice is not between blaming people or systems. Instead, we may reconsider the accountability relationships of people in systems (Berlinger 2005). All safety–critical work is ultimately channeled through relationships between human beings (such as in medicine), or through direct contact of some people with the risky technology. At this sharp end, there is almost always a discretionary space into which no system improvement can completely reach. This is in part a space in the almost literal sense of "room for maneuvering" that operators enjoy while executing their work relatively unsupervised (in the examination room, the operating theatre, cockpit). It is also a space in a metaphorical sense, of course, as its outlines are not stipulated by decree or regulation, but drawn by actions of individual operators and the responses to them. It is, however, a final kind of space filled with ambiguity, uncertainty and moral choices. And a space that is typically devoid of relevant or applicable guidance from the surrounding organization, leaving the difficult calls up to the individual operator or crews. Systems cannot substitute the responsibility borne by individuals within that space. Individuals who work in those systems would not even want that. The freedom (and concomitant responsibility) that is left for them is what makes them and their work human, meaningful, a source of pride.

But organizations can do a number of things. One is to be clear about where that discretionary space begins and ends. Not giving practitioners sufficient authority to decide on courses of action, but demanding that they be held accountable for the consequences anyway, creates impossible and unfair goal conflicts (for which managers may sometimes be held accountable, but they too could have been the recipients of similar goal conflicts). It effectively shrinks the discretionary space before action, but opens it wide after any bad consequences of action become apparent. Second, an organization must deliberate how it will motivate people to conscientiously carry out their duties inside the discretionary space. Is the source for that motivation fear or empowerment? There is evidence that empowering people to affect their work conditions, to involve them in the outlines and content of that discretionary space, most actively promotes their willingness to shoulder their responsibilities inside of it (Kohn 1999; Wiegmann et al. 2002; Dekker and Laursen 2007). For example, during surgery, an anesthetist reached into a drawer that contained two vials that were side by side, both with yellow labels and yellow caps. One, however, had a paralytic agent, the other a reversal agent for when paralysis was no longer needed. At the beginning of the procedure, the anesthetist administered the paralyzing agent. But toward the end, he grabbed the wrong vial, administering additional paralytic instead of its reversal agent. There was no bad outcome in this case. But when he discussed the event with his colleagues, he found that this had happened to them too, and that they were all quite aware of the potential risks. Yet none had spoken out about it, which could raise questions about the empowerment anesthetists may have felt to influence their work conditions, their discretionary space (Morreim 2004).

4.2 Blame-free is not accountability-free

Equating blame-free systems with an absence of personal accountability, as some do (e.g. Pellegrino 2004) is wrong. The kind of accountability wrung out of practitioners in a trial is not likely to contribute to future safety in their field, and in fact may hamper it. We can create such accountability not by blaming people, but by getting people actively involved in the creation of a better system to work in. Holding people accountable and blaming people are two quite different things. Blaming people may in fact make them less accountable: they will tell fewer accounts, they may feel less compelled to have their voice heard, to participate in improvement efforts. Blame-free or no-fault systems are not accountability-free systems. On the contrary: such systems want to open up the ability for people to hold their account, so that everybody can respond and take responsibility for doing something about the problem. This also has different implications for what we mean by accountability. If we see an act as a crime, then accountability means blaming and punishing somebody for it. Accountability in that case is backward-looking, retributive. If, instead, we see the act as an indication of an organizational, operational, technical, educational or political issue, then accountability can become forward-looking (Sharpe 2003). The question becomes what should we do about the problem and who should bear responsibility for implementing those changes.

5 Creating the basis for a just culture

Whereas the judicial climate in a country can discourage open reporting and honest disclosure (e.g. Berlinger 2005), this does not mean that an organization charged with running a safety-critical operation (in e.g. healthcare, aviation, nuclear power generation) cannot try to build a basis for a just culture. The first steps involve a normalization of incidents, so that they become a legitimate, acceptable part of organizational development. Then, the organization must consider what to do about the question "who gets to draw the line?" both inside its own operation and in influencing the judicial climate surrounding it. Here are some suggestions:

First, normalize and try to legitimize incidents:

- An incident must not be seen as a failure or a crisis, neither by management, nor by colleagues. An incident is a free lesson, a great opportunity to focus attention and to learn collectively.
- Abolish financial and professional penalties (e.g. suspension) in the wake of an occurrence. These measures render incidents as something shameful, to be kept concealed, leading to the loss of much potential safety information and lack of trust.
- Monitor and try to prevent stigmatization of practitioners involved in an incident. They should not be seen as a failure, or as a liability to work with by their colleagues.
- Implement, or review the effectiveness of, any debriefing programs or critical incident/stress management programs the organization may have in place to help practitioners after incidents. Such debriefings and support form a crucial ingredient in helping practitioners see that incidents are "normal", that they can help the organization get better, and that they can happen to everybody.
- Build a staff safety department, not part of the line organization that deals with incidents. The direct manager (supervisor) of the practitioner should not necessarily be the one who is the first to handle the practitioner in the wake of an incident. Aim to decouple an incident from what may look like a performance review or punitive retraining of the practitioner involved.
- Start with building a just culture at the very beginning: during basic education and training of the profession. Make trainees aware of the importance of reporting incidents for a learning culture, and get them to see that incidents are not something individual or shameful but a good piece of systemic information for the entire organization. Convince new practitioners that the difference between a safe and an unsafe organization lies not how many incidents it has, but in how it deals with the incidents that it has its people report.
- Ensure that practitioners know their rights and duties in relation to incidents. Make very clear what can (and typically does) happen in the wake of an incident (e.g. to whom practitioners were obliged to speak, and to whom not). A reduction in such uncertainty can prevent practitioners from withholding valuable incident information because of misguided fears or anxieties.

Second, the important discussion for an organization is who draws the line between acceptable and unacceptable inside the organization? This means not only who gets to handle the immediate aftermath of an incident (the line organization: supervisor/manager, or a staff organization such as safety department), but how to integrate practitioner peer expertise in the decision on how to handle this aftermath, particularly decisions that relate to the individual practitioner's stature. Empowering and involving the practitioner him- or her-self in the aftermath of an incident is the best way to maintain morale, maximize learning, and reinforce the basis for a just culture.

Third, think about how to protect the organization's data from undue outside probing (e.g. by a prosecutor). The consequences of this step must be thought through. One problem is that better protection for incident reporters can lock information up even for those who rightfully want access to it, and who have no vindictive intentions (e.g. patients or their families). The protection of reporting can make disclosure to such parties more difficult.

Fourth, it could be profitable to start a discussion with the prosecuting authority in the country on how to help them integrate domain expertise (to support them in making better judgments about whether something is worthy of further investigation and prosecution). This may require that previous mistrust is overcome and may seem difficult in the beginning. In the end, however, it may tremendously benefit all parties, as it may also create a better understanding of each other's point of view and interests.

Uncertainty about, and perceived unfairness of, who gets to draw the line is likely to overrule any guidance in use today on where that line goes. The socially constructed judgment of that line means that its location will forever be more unpredictable than relatively stable arrangements among stakeholders about who gets to draw the line, with or without help from others.

Acknowledgment Part of the work for this paper was conducted on a grant from The European Organisation for the Safety of Air Navigation (Eurocontrol) to study the interface between the judiciary and air navigation service providers. With thanks to Tony Licu and his people in Brussels.

References

Alicke MD (2000) Culpable control and the psychology of blame. Psychol Bull 126:556–74

Becker HS (1963) Outsiders: studies in the sociology of deviance. Free Press, New York

Berlinger N (2005) After harm: medical error and the ethics of forgiveness. The Johns Hopkins University Press, Baltimore

Burr V (2003) Social constructionism. Routledge, London

Byrne G (2002) Flight 427: anatomy of an air disaster. Copernicus books, New York

Christie N (2004) A suitable amount of crime. Routledge, London

Cohen-Charash Y, Spector PE (2001) The role of justice in organizations: a meta-analysis. Organ Behav Hum Decis Processes 86:278–321

Cook RI, Render M, Woods DD (2000) Gaps in the continuity of care and progress on patient safety. BMJ 320:791–794

Dauer EA (2004) Ethical misfits: mediation and medical malpractice litigation. In: Sharpe VA (ed) Accountability: patient safety and policy reform. Georgetown University Press, Washington, pp 185–202

Dekker SWA (2003) Failing to adapt or adaptations that fail: contrasting models on procedures and safety. Appl Ergon 34:233–238

Dekker SWA (2007) Discontinuity and disaster: gaps and the negotiation of culpability in medication delivery. J Law Med Ethics 35:463–470

Dekker SWA (2008) Just culture: balancing safety and accountability. Ashgate Publishing Co, Aldershot

Dekker SWA, Laursen T (2007) From punitive action to confidential reporting. Patient Saf Qual Healthc 5:50–56

Douglas M (1992) Risk and blame: essays in cultural theory. Routledge, London

Durkheim E (1950/1895) The rules of the sociological method. Free Press, New York

Erikson K (1966) Wayward puritans. Wiley, New York

Eurocontrol Performance Review Commission (2006) Report on legal and cultural issues in relation to ATM safety occurrence reporting in Europe: outcome of a survey conducted by the Performance Review Unit in 2005–2006. Eurocontrol, Brussels

Ferguson J, Fakelmann R (2005) The culture factor. Front Health Serv Manage 22:33–40

Foucault M (1981) The order of discourse. In: Young R (ed) Untying the text: a post-structuralist reader. Routledge, London, pp 48–79

GAIN (2004) Roadmap to a just culture: Enhancing the safety environment. Global Aviation Information Network (Group E: Flight Ops/ATC Ops Safety Information Sharing Working Group)

Galison P (2000) An accident of history. In: Galison P, Roland A (eds) Atmospheric flight in the twentieth century. Kluwer, Dordrecht, NL, pp 3–44

Green J (2003) The ultimate challenge for risk technologies: controlling the accidental. In: Summerton J, Berner B (eds) Constructing risk and safety in technological practice. Routledge, London

Kohn LT, Corrigan JMK, Donaldson M (eds) (1999) To err is human. Institute of Medicine, Washington DC

Laudan L (2006) Truth, error and criminal law: an essay in legal epistemology. Cambridge University Press, Cambridge

Lerner JS, Tetlock PE (1999) Accounting for the effects of accountability. Psychol Bull 125:255–75

Marx D (2001) Patient safety and the "just culture": a primer for health care executives. Columbia University, New York

McDonald N, Corrigan S, Ward M (2002 June). Well-intentioned people in dysfunctional systems. Keynote paper presented at the 5th Workshop on human error, safety and systems development, Newcastle

McKenna JT (1999) Criminal and safety probes at odds. Aviat Week Space Technol 47–48 (13 December)

Merry AF, McCall Smith A (2001) Errors, medicine and the law. Cambridge University Press, Cambridge

Morreim EH (2004) Medical errors: pinning the blame versus blaming the system. In: Sharpe VA (ed) Accountability: patient safety and policy reform. Georgetown University Press, Washington, pp 213–232

Nagel T (1992) The view from nowhere. Oxford University Press, Oxford

North DM (2000 May 15) Let judicial system run its course in crash cases. Aviation Week Space Technol, p 66

North DM (2002, February 4) Oil and water, cats and dogs. Aviation Week Space Technol, p 70

Pellegrino ED (2004) Prevention of medical error: where professional and organizational ethics meet. In: Sharpe VA (ed) Accountability: patient safety and policy reform. Georgetown University Press, Washington, pp 83–98

Perrow C (1984) Normal accidents: living with high-risk technologies. Basic Books, New York

Reason JT (1997) Managing the risks of organizational accidents. Ashgate Publishing Co, Aldershot

Rochlin GI (1999) Safe operation as a social construct. Ergonomics 42:1549–1560

Ruitenberg B (2002) Court case against Dutch controllers. The Controller 41:22–5

Sharpe VA (2003) Promoting patient safety: an ethical basis for policy deliberation. Hastings Center Report Special Suppl 33(5):S1–S20

Skegg PDG (1998) Criminal prosecutions of negligent health professionals: the New Zealand experience. Med Law Rev 6:220–46

Smith K (2001) Incompatible goals, uncertain information and conflicting incentives: the dispatch dilemma. Human Factors Aerospace Safety 1:361–380

Suchman LA (1987) Plans and situated actions: the problem of human-machine communication. Cambridge University Press, Cambridge

Ter Kulle A (2004) Safety versus justice. Canso News 18:1–2

Vaughan D (1996) The challenger lauch decision: risky technology, culture and deviance at NASA. University of Chicago Press, Chicago

Vaughan D (1999) The dark side of organizations: mistake, misconduct, and disaster. Annu Rev Sociol 25:271–305

Wiegman D, Zhang H, von Thaden T, Sharma G, Mitchell A (2002) A synthesis of safety culture and safety climate research (Technical report ARL-02-3/FAA-02-2). Aviation Research Lab, University of Illinois, Urbana-Champaign

Wilkinson, S. (1994) The Oscar November incident. Air Space, pp 80–87 (February–March)

Woods DD, Shattuck LG (2000) Distant supervision: local action given the potential for surprise. Cogn Technol Work 2:242–245

Toolbox Talk : Human Error

…part 2

Common views…

Human errors are due to carelessness…

…they are random and cannot be predicted…

…all errors are bad.

Resulting in common solutions:

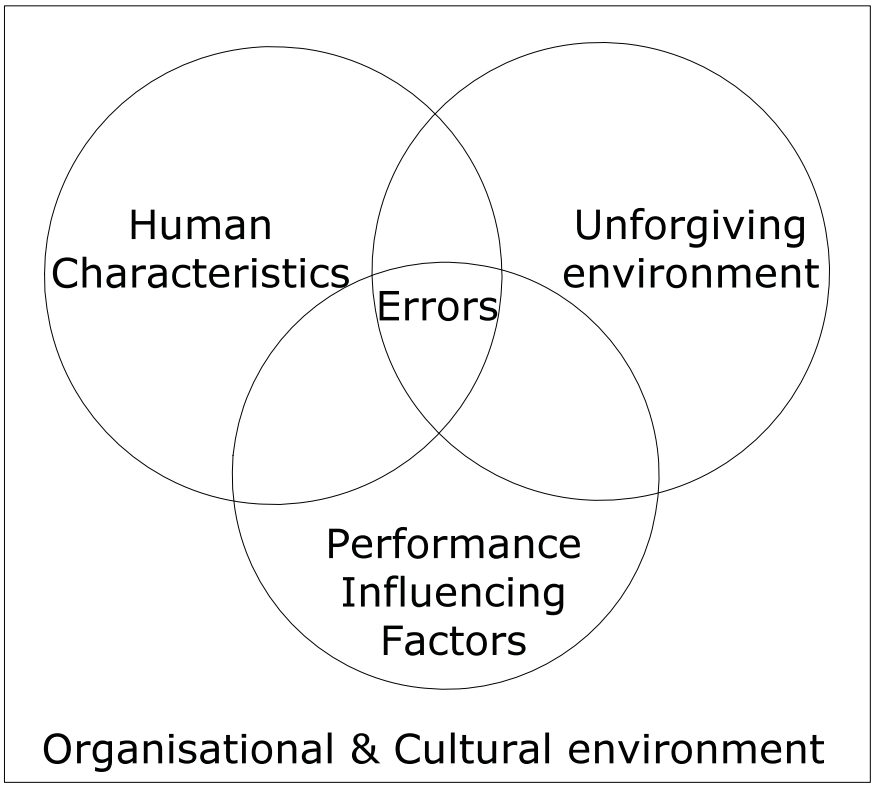
- Design the human out of the system
- Automate safety systems
- Create technical barriers
- Train and motive staff to do the right thing
- Warn staff if they do things wrong

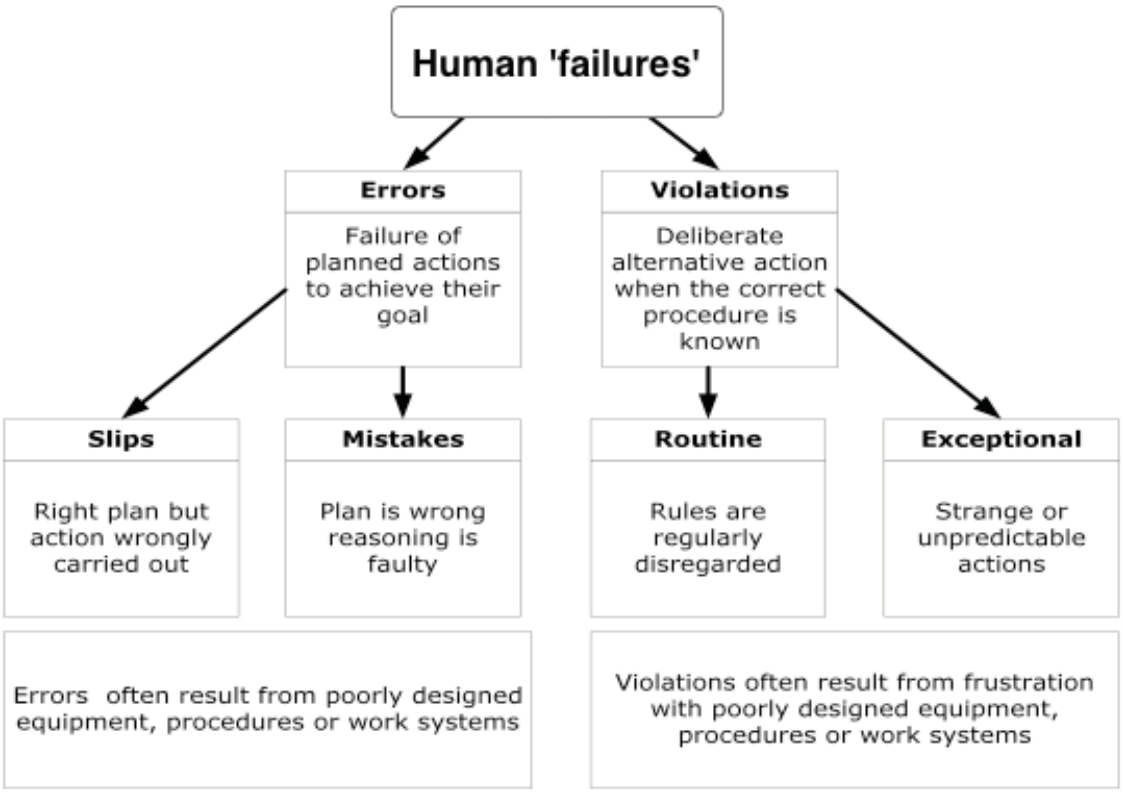
Points from video

- Autopilot
- Skilled errors
- Causes are the same
- Sequences
- Conscious – automatic
- Biases are the same

Video

A Human Factors view of Error





Types of errors (handouts)

Process control

- Planning errors
- Action Errors
- Operation too long/too short
- Checking errors
- Retrieval errors
- Communication errors
- Selection errors

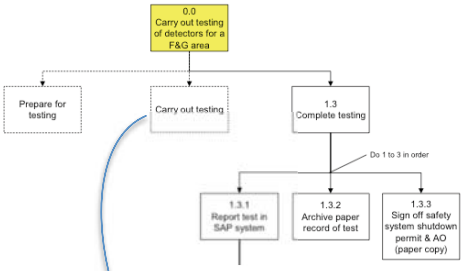
Aviation

- Timing of action
- Selection of action
- Information transfer

Use in…

- Critical tasks
- Task Analysis (e.g. F&G testing)
- Identifying training needs
- Procedures
- Incident investigation

Note: NOT just CCR operations - maintenance, crane operations, IO



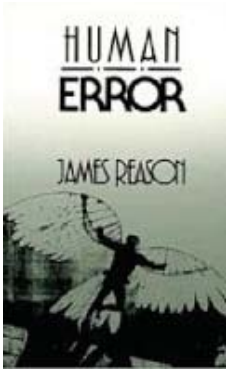
Critical tasks

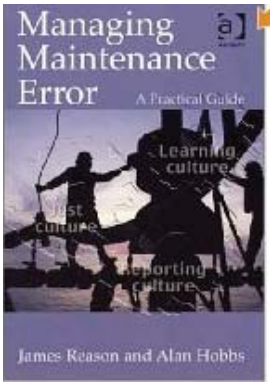
Task element	Performed by	Operator decisions	Info req. & source	Feed back	Communication	Possible errors/ consequences.	Recommendations
Direct FO to detector (using tag number)		which detector to test?	e plan list & on-line C&E diagram Search on tag number in SAS? –Yes this can done Location of detector, height, direction- shown on SAS display		to/from FO	wrong detector Information on placement of detector is wrong	accurate description of detector, height & placement. In both alarm text & SAS display. Ensure Commissioning team carry out check between alarm text description & detector location

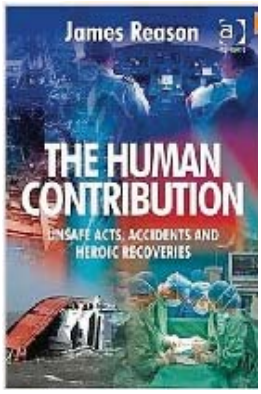
References

Long:

- Reason's books







Short:

- Parliamentary note
- HRA error paper

will send out pdf's of these 2

mark.green@hcd.no

Parliamentary Office of Science and Technology

postnote

June 2001 Number 156

MANAGING HUMAN ERROR

The recent (June 2001) publication of the Cullen Report into the Paddington rail crash has once more focused media and public attention on large-scale accidents. Such incidents are often followed by calls for blame to be allocated to individuals at the 'sharp end' of the industry in question. In addition, small-scale workplace accidents account for over 200 deaths per year and over 180,000 injuries. This briefing looks at human factors which are liable to cause such errors, examines how their effects can be minimised and analyses the implications for health and safety policy.

Background

It has been estimated that up to 90% of all workplace accidents have human error as a cause[1]. Human error was a factor in almost all the highly publicised accidents in recent memory, including the Bhopal pesticide plant explosion, Hillsborough football stadium disaster, Paddington and Southall rail crashes, capsizing of the Herald of Free Enterprise, Chernobyl and Three-Mile Island incidents and the Challenger Shuttle disaster. In addition to these acute disasters some industries, notably health-care, experience long-term, continuous exposure to human error. The costs in terms of human life and money are high[2]. Placing emphasis on reducing human error may help reduce these costs.

Limitations of human behaviour

In order to address human factors in workplace safety settings, peoples' capabilities and limitations must first be understood. The modern working environment is very different to the settings that humans have evolved to deal with. This section examines human characteristics that can lead to difficulties interacting with the working environment. The box on page 2 provide details on the main factors involved, including:

- Attention - the modern workplace can 'overload' human attention with enormous amounts of information, far in excess of that encountered in the natural world. The way in which we learn information can help reduce demands on our attention, but can sometimes create further problems (e.g. the Automatic Warning System on UK trains, see box on page 2).
- Perception - in order to interact safely with the world, we must correctly perceive it and the dangers it holds. Work environments often challenge human perception systems and information can be misinterpreted.
- Memory - our capacity for remembering things and the methods we impose upon ourselves to access information often put undue pressure on us. Increasing knowledge about a subject or process allows us to retain more information relating to it.
- Logical reasoning - failures in reasoning and decision making can have severe implications for complex systems such as chemical plants, and for tasks like maintenance and planning.

Addressing human error

The types of problems caused by these factors are often unavoidable. In certain situations, human beings will always make mistakes, and there is a limit to what can be done to modify behaviour itself. However, there are other methods of dealing with human error, and these are discussed in more detail in this section.

As it is inevitable that errors will be made, the focus of error management is placed on reducing the chance of these errors occurring and on minimising the impact of any errors that do occur. In large-scale disasters, the oft-cited cause of 'human error' is usually taken to be synonymous with 'operator error' but a

Human characteristics and the working environment

Attention

Attention on a task can only be sustained for a fairly short period of time, depending on the specifications of the task. The usual figure cited is around 20 minutes, after which, fatigue sets in and errors are more likely to occur. This is why air traffic controllers are obliged to take breaks from their attention-intensive work at regular intervals. However, there are a number of other reasons why the attentional system is responsible for errors. These include:

- Information bottleneck – it is only possible to pay attention to a small number of tasks at once. For example, if an air traffic controller is focussed on handling a particular plane, then it is likely that they will be less attentive to other aspects of safety, or other warning signals (although this depends on the nature of the signal).
- Habit forming - if a task is repeated often enough, we become able to do it without conscious supervision, although this 'automatisation' of regular and repetitive behaviour can force us into mistakes. In 1979, an operator at Oyster Creek Nuclear Power Plant intended to close off two pump discharge valves. Through an attentional slip, he accidentally closed off two other valves as well, and in doing so, closed off all circulation to the reactor core.

The **Automatic Warning System** installed on all passenger trains in the UK is an example of a system that was not designed with limitations of human attention in mind. It is a device fitted in the train cab, based on the now obsolete mechanical system of signalling that used to signal either STOP or PROCEED. It sounds a bell when a clear (green) signal is passed and a buzzer when caution or danger is signalled. If the buzzer is not acknowledged by the press of a button, then the train begins to stop automatically. In commuter traffic, most signals will be at the 'caution' aspect, and given the frequency of signals (spaced 1km apart), most drivers will face two signals per minute. Given the tendency for the attentional system to automate highly repetitive behaviour, many drivers lose focus on the reasons for carrying out this repetitive task, and act in reflex whenever the buzzer sounds. The end result is that drivers often hear the buzzer and press the button reflexively without actively thinking about train speed and location.
Source: Davies, D. (2000): Automatic Train Protection for the Railway Network in Britain – A study. RA Eng., London.

Perception

Interpreting the senses - one of the biggest obstacles we face in perceiving the world is that we are forced to *interpret* information we sense, rather than access it directly. The more visual information available to the perceiver, the less likely it is that errors will be made. Bearing this in mind, systems that include redundant information in their design may cause fewer accidents. An example of this was the change in electrical earth wire colour coding in the 1970's to include not only colour, but also a striped pattern.

Signal detection - the more intense a stimulus (such as a light or a noise), the more powerful the response elicited (such as brain activity or a physical movement). This has implications for the way danger signals are perceived at work. For instance, the order in which the severity of danger is signalled on UK rail tracks is single red (most dangerous), followed by single yellow, then double yellow and finally green (no danger). Research suggests there may be some merit in swapping the order of the yellow signals, as the double yellow is more intense and thus more noticeable than the single yellow signal. However, this point must be offset against the fact that the current system provides automatic mechanical failsafe if a yellow bulb blows, and the psychological notion that double yellow serves a useful role as a countdown to the single.

Memory

Capacity - short-term memory has an extremely limited capacity. In general, people can remember no more than around seven individual items at a time. This has safety implications in areas such as giving new workers a set of instructions to follow from memory or attempting to remember the correct sequence of procedures within a new task. However, trained individuals are able to retain larger chunks of information in memory. For example, chess grandmasters can remember the location of more pieces on a chessboard than can a novice because they see the pieces not as single units, but as parts of larger conceptual units which form coherent wholes.

Accessibility - even when items are stored in memory, it is sometimes difficult to access them. There has been much research into the ways in which recall of information can be improved. For example, research has shown that people are much more likely to remember information if they are in similar conditions to when they encoded the information. This was illustrated in a study involving divers who were given lists of words to learn on dry land and underwater. Words learned on the surface were best recalled on the surface, and those learned underwater best recalled underwater. This has implications for training programmes, where albeit under less extremely contrasting situations, staff trained in an office environment may not be able to remember relevant details on the shop floor.

Levels of processing - another way in which information can be more reliably remembered is to learn it at greater depth. For instance, if it is necessary to remember lists of medical symptoms, then it helps to understand more about the conceptual framework behind the list. If only the 'surface' features (such as the words on the list) are remembered, then there is a higher chance of information being forgotten.

Sources: Chase, W.G. & Simon, H.A. (1973): Perception in chess. Cognitive Psychology, ***4:*** *55-81.*
Tulving, E. (1979): Relation between encoding specificity and levels of processing. In, L.S. Cernak & F.I.M. Craik (Eds.), Levels of processing in human memory. Hillsdale, N.J.:Lawrence Erlbaum.

Logical reasoning

Humans are not very good at thinking logically, but in technological situations, logical procedures are often necessary (for example, troubleshooting a complex system which has broken down). Illogical behaviour is a common source of error in industry. During the Three Mile Island incident in 1979, two valves which should have been open were blocked shut. The operators incorrectly deduced that they were in fact open, by making an illogical assumption about the instrument display panel. The display for the valves in question merely showed that they had been instructed to be opened, whereas the operators took this feedback as an indication that they were actually open. Following this, all other signs of impending disaster were misinterpreted with reference to the incorrect assumption, and many of the attempts to reduce the danger were counterproductive, resulting in further core damage.

measure of responsibility often lies with system designers. For instance, during the Second World War, designers attempted to introduce a new cockpit design for Spitfire planes. During training, the new scheme worked well, but under the stressful conditions of a dogfight, the pilots had a tendency to accidentally bail out. The problem was that the designers had switched the positions of the trigger and ejector controls; in the heat of battle, the stronger, older responses resurfaced.

Recent research[3,4] has addressed the problem of how to design systems for improved safety. In most safety-critical industries, a number of checks and controls are in place to minimise the chance of errors occurring. For a disaster to occur, there must be a conjunction of oversights and errors across all the different levels within an organisation. This is shown in the figure below from which it is clear that the chances of an accident occurring can be made smaller by narrowing the windows of accident opportunity at each stage of the process. Factors such as training and competence assurance, management of fatigue-induced errors and control of workload can eliminate some errors. But errors caused by human limitations and/or environmental unpredictability are best reduced through improving system interface design and safety culture.

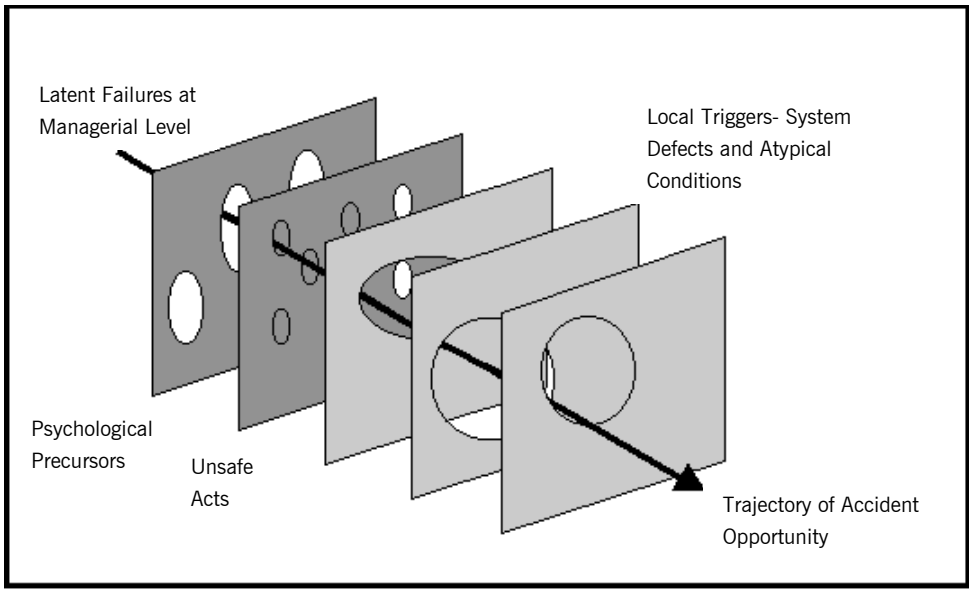
System design

A good system should not allow people to make mistakes easily. This may sound obvious, but all too commonly system design is carried out in the absence of feedback from its potential users which increases the chance that the users will not be able to interact correctly with the system. A set of design principles has been proposed[4] which can minimise the potential for error. These are discussed below.

Accurate mental models

There is often a discrepancy between the state of a system and the user's mental model of it. This common cause of erroneous behaviour arises because the user's model of the system and the system itself will differ to some extent, since the user is rarely the designer of the system. Problems that can arise as a result of this discrepancy are illustrated by the Three Mile Island incident cited in the box on page 2. In this incident, the system had been designed so that the display showed whether the valves had been *instructed* to be open or closed. The most obvious interpretation to the user was that the display reflected the *actual status* of the system. Designers need to exploit the natural mappings between the system and the expectations and intentions of the user.

The Swiss cheese model of accident causation



The figure shows a trajectory of accident opportunity and its penetration through several types of defensive system. The combined chances of an accident occurring are very small, as the holes in the various defence systems must all line up. Some are active failures of human or mechanical performance, and others are latent conditions, such as management factors or poor system design. However, it is clear that if steps are taken in each case to reduce the defensive gaps, the overall chance of accident will be greatly reduced. Organisational planning can reduce the latent failures at the managerial level, psychological failings can be reduced by paying attention to the types of task that are required of workers and unsafe acts can be reduced by good interface design.

Source: Reason, J. (2000): Human error: Models and management. British Medical Journal, ***320:*** *768-770.*

Another example of the importance of user familiarity with the working system is demonstrated by a laboratory study which examined how useful it was to give staff an overview of a fictitious petrochemical plant's structure and day-to-day functioning. One group was given rules about which buttons to press if a dangerous situation arose; another was given the rules and an overview of the workings of the plant. Both groups were equal in their ability to deal with the expected problems, but when new problems arose, only the group which understood the plant's functioning were able to deal with the situation[5].

Managing information
As our brains are easily distracted and can overlook necessary tasks, it makes sense to put information in the environment which will help us carry out complex tasks. For example, omission of steps in maintenance tasks is cited as a substantial cause of nuclear power plant incidents[6]. When under time pressure, technicians are likely to forget to perform tasks such as replacing nuts and bolts. A very simple solution to this problem would be to require technicians to carry a hand-held computer with an interactive maintenance checklist which specifically required the technician to acknowledge that certain stages of the job had been completed. It could also provide information on task specifications if necessary. This would also allow a reduction in paperwork and hence in time pressure.

Reducing complexity
Making the structure of tasks as simple as possible can avoid overloading the psychological processes outlined previously. The more complex the task specifications, the more chances for human error. Health-care systems in the US are currently addressing this issue. With the realisation that a leading cause of medical error in the United States was related to errors in prescribing drugs, a programme was undertaken to analyse and address the root causes of the problem. A computerised system of drug selection and bar-coding reduced the load on memory and knowledge on the part of the prescriber, and errors of interpretation on the part of the dispenser, resulting in an overall reduction in prescription errors. Examples such as this emphasise the fact that reducing task complexity reduces the chance of accidents.

Visibility
The user must be able to perceive what actions are possible in a system and furthermore, what actions are desirable. This reduces demands on mental resources in choosing between a range of possible actions. Perhaps even more important is good quality feedback which allows users to judge how effective their actions have been and what new state the system is in as a result of those actions. An example of poor feedback occurred during the Three Mile Island incident; a poorly-designed temperature gauge was consistently misread by experienced operators (they read 285 degrees Fahrenheit as 235 degrees), which led them to underestimate the severity of the situation.

Constraining behaviour
If a system could prevent a user from performing any action which could be dangerous, then no accidents would occur. However, the real world offers too complex an environment for such a simplistic solution: in an industrial operation, a procedure which could be beneficial at one stage in the process may be disastrous at another. Nevertheless, it is possible to reduce human error by careful application of 'forcing functions'. A good example of a forcing function is found in the design of early cash machines. People used to insert their card, request cash, take it and walk away, leaving their cash card behind. It was a natural enough response, as the main objective of the action had been achieved: obtaining money. The task was thus mentally marked as being complete before all necessary stages of the transaction had been carried out. After a great deal of thought, the systems designers came up with a very simple solution which has been effective ever since: as the target objective of the task was to obtain money, placing this stage at the very end of the transaction would avoid the problem. Hence, the card is now given back before the money is. Functions such as this relieve the user of the responsibility of deciding what actions are appropriate whilst interacting with the system, and are very effective in preventing dangerous incidents.

Design for errors
In safety-critical systems, such as nuclear power plants, numerous safety systems are in place which can mitigate accidents. One approach is 'defence in depth' (implementing many independent systems simultaneously); another is 'fail-to safe state' system design. However, designers must assume that mistakes will occur, and so any useful system must make provision for recovery from these errors. Another consideration is that the design should make it difficult to enact non-reversible actions. Although this is an underlying principle of design, it needs to be applied carefully. For instance, most home computers have a 'recycle bin' or 'trash' folder, in which all deleted files are stored. They are recoverable from here, but when this folder is emptied, files cannot be recovered at all. Attempts to empty this folder result in a message asking the user to confirm deletion. The problem is that the user is often asked to confirm such requests, and, just like the train drivers with the AWS system (see box on page 2), learns to associate the appearance of the warning message with the pressing of the 'OK' button. The result is that the pop-up messages may not be read, and on occasion, files are accidentally destroyed. A safer option would be to use this type of pop-up box less regularly, and to require different user input each time.

Standardisation
When systems are necessarily complex but have been made as accessible and easy to use as possible and errors are still being made, then standardisation is sometimes used as an attempt to make the situation predictable. It has been suggested that medicine is one of the areas most amenable to standardisation. For instance, resuscitation units in accident and emergency

hospitals vary considerably in their design and operation. This diversity, coupled with the movement of staff between hospitals, mean that errors can be made and delays occur. Another example where standardisation might be of use in medicine is across different brands of equipment, since staff often do not have training in all the available designs. If all hospital equipment had standard placement and design, then all staff would be able to locate and operate equipment with ease.

One problem with standardisation is that if any advances in design or usage are made, then it is a very costly process to re-implement standardisation across all departments of an industry. Also, a standardised system may be ideal for one set of tasks, but very inefficient for another set. Such practical considerations have tended to limit the application of standardisation as an approach for reducing human errors.

User-centred design
Another basic principal of design is that it should be centred around the user at all stages from initial conception, through evolution and testing, to implementation. In practice however, systems designers are often given a brief, create the system and impose it upon the users without appropriate feedback. This can result in unexpected system behaviour and over-reliance on manuals which themselves have been written by the system designers from their own perspective. Systems designed in this way will be opaque to the end user, and this can hinder effective interaction. Designers of computer interfaces often fall into this trap.

Safety Culture
Attribution of accidents to human failures at the 'sharp end' of an industry may not provide a full picture of all the factors involved. The management of the organisation must also take responsibility for decisions which affect the safe functioning of the organisation as a whole[7]. Unwise decisions at this level are more difficult to link directly to an accident, as they are often implemented well before an accident occurs, and they do not make their presence urgently felt. Good decisions at this level can create a culture of safety which can remove the precursor conditions for accidents (see figure on page 3) or ameliorate their consequences.

Safety Culture is a term that was first introduced after the Chernobyl disaster in 1986. The safety culture of an organisation is the product of the individual and group values, attitudes, competencies and patterns of behaviour that determine the style and proficiency of an organisation's health and safety programmes. A positive safety culture is one in which shared perceptions of the importance of safety and confidence in preventative measures are experienced by all levels of an organisation. According to the Health and Safety Executive (HSE, the statutory body that ensures that risks to health and safety from work activities are properly controlled), factors that create this positive culture include:

- leadership and the commitment of the chief executive;
- a good line management system for managing safety;
- the involvement of all employees;
- effective communication and understood/agreed goals;
- good organisational learning/responsiveness to change;
- manifest attention to workplace safety and health;
- a questioning attitude and rigorous and prudent approach by all individuals.

If one or more of these factors is lacking, an organisation may be prone to corner-cutting, poor safety monitoring, and poor awareness of safety issues. In these settings, errors are common and disasters more probable. Impoverished safety culture contributed to major incidents such as the pesticide plant explosion at Bhopal in 1985, the Herald of Free Enterprise disaster (box, below) and a number of recent rail crashes (box, page 6). It has also been found that workers in poor safety cultures have a 'macho' attitude to breaking safety rules, and tend to ascribe the responsibility of safety to others.[8]

Assessing safety culture
Assessment of safety culture relies upon a safety auditing system. However, such approaches are 'top-down'

The 'Herald of Free Enterprise' disaster
The Herald of Free Enterprise capsized on the 6th March, 1987, killing ~200 people. It sank because its inner and outer bow doors had been left open on sailing, as a result of a combination of factors and decisions. The subsequent investigation found that all of these could have been avoided or ameliorated. Management failures set up a culture which compromised safety and allowed individual human errors to occur. Disaster could have been avoided if management had addressed safety in a more informed and committed way.

Management Failures. Management put pressure on crews to sail early by sending memos to staff demanding that ships leave 15 minutes early. To speed up sailing times, the chief officer, who was responsible for ensuring the bow doors were closed, was required to be on the bridge before sailing, rather than on the car loading deck. He was thus on the bridge before the cars had finished being loaded. It was the management's responsibility to ensure that a safe procedure was in place to prevent this type of omission. Another failure included orders that only 'negative reporting' should be employed; officers on board the ship were to assume that all was well unless they heard otherwise.

Supervisory and Organisational Failure. The assistant boson, whose job it was to actually close the doors was asleep in his cabin after a maintenance and cleaning shift. If more attention had been paid to rostering and monitoring staff, this would not have occurred. The boson left the deck without checking either that his assistant was on duty, or that the doors had been closed.

System Design Failure. Ship masters had repeatedly requested that bow door warning indicators be installed on the bridge, but management did not act on these requests. For an estimated £400, the equipment could have been installed and the ship's master would have known about the state of the doors before he left port. Other design failures included the top-heavy design of the ferry and inadequate equipment to remove water from the flooded deck.

Sources: Reason, J (1989): Human error. Cambridge, CUP.
Sheen, B. (1987): Herald of Free Enterprise, Report of Court no. 8074 formal investigation. London.

methods, and may enumerate systems already in place, without necessarily assessing how effective they are. Performance indicators can also be used, with management experts setting target levels (often linked to bonus payments), which can have a negative effect on error reporting[9]. Such measures are not always an informative indication of safety performance: the shutting down of a reactor may be the result of human error or the result of human cautiousness. Research suggests that this kind of top-down approach be supplemented by assessments of the attitudes of staff toward safety, as it is their attitudes which determine behaviour.

For some industries there is evidence that achieving a positive safety culture through documenting accidents and investigating errors improves both efficiency and profitability. For instance, the US healthcare system, estimates that when litigation and take-up of hospital resources is taken into account, an effective error-reporting and handling system could save money[10]. Error reporting depends upon trust between hierarchical levels of the organisation, and it is suggested that incident reporting is itself an indicator of staff perceptions of managerial commitment to safety[11].

Finally there is the question of ensuring that lessons are learned - and remembered - from accidents. Such experience may be lost to an organisation when members of staff leave or retire. One way of preserving it and making it more widely accessible is for industry sectors to pool information into computerised databases which can be searched by keywords as part of a risk assessment. One example of such an initiative is the Institution of Chemical Engineer's Accidents Database.

Implementation

Previous sections have examined individual human limitations that make errors in the workplace inevitable. Research has shown ways in which good system design and organisational safety culture can help prevent errors from occurring and minimise the impact of those that do occur. This section outlines issues arising from the application of this knowledge to improving health and safety in the workplace. It examines specific legislative proposals as well as more general approaches building on the existing regulatory framework (outlined in the box on page 7) under the Government's 'Revitalising Health and Safety Strategy'. Launched in June 2000 by the HSC and the Government, this sets a number of targets to be achieved by 2010. These include reducing:

- working days lost from work-related injury and ill-health by 30% (from the current 97,000 days lost per 100,000 workers to 68,000 days per 100,000);
- work related ill health by 20% (from the current 1,400 to 1,120 new cases per 100,000 workers);
- fatalities and major injuries by 10% (from the current 260 to 230 cases per 100,000 workers).

Corporate killing

Disasters such as the sinking of the Herald of Free Enterprise, the King's Cross fire, and the Southall and Clapham Junction rail disasters have all prompted calls for new legislation. In each case, subsequent inquiries found the corporate bodies at fault and criticised them severely. But in none of these cases was it possible to successfully prosecute the corporate bodies for man-slaughter. This is because current UK law requires that before such a body can be convicted of manslaughter, an individual who can be "*identified as the embodiment of the company itself*" must first be shown to have been guilty of manslaughter.

In practice this is very difficult to achieve, particularly in large organisations with diffuse management structures and areas of responsibility. Indeed, there have only ever been three successful prosecutions of corporations for manslaughter in the UK; in each case, the corporations involved were small. This has led to a widespread perception that a new law dealing with corporate killing is required.

Safety culture in the rail industry

The safety culture of an organisation depends on the degree of control it has over working practises and their consequences within the industry. Fragmentation of any such industry – whether through privatisation or other means – raises concerns over compromising safety. Privatisation of British Rail gave rise to over fifty franchises, with numerous sub-contractors having responsibility for sections of the railway. When plans for privatisation were first mooted, the Health and Safety Commission (1993) expressed concerns that safety might suffer as a result. Worries of increasing numbers of accidents were initially not borne out. However, following the recent spate of serious accidents, the debate has resurfaced and the safety culture of the rail industry is once again being scrutinised. Recent inquiries into the Hatfield, Southall and Paddington rail incidents implicate management failings as a factor, via under-investment in track maintenance, a lack of equipment and inadequate staffing levels. These, and other concerns are expected to be outlined in a report into the Hatfield rail crash, due to be published in July 2001.

Another concern is that while the *Railways (Safety Case) Regulations 1994* call for the active sharing of information between franchises, there is no specific requirement that errors be analysed at an industry-wide level. There was also concern from HSE that Railtrack, the company responsible for monitoring safety in the industry, did not focus on 'soft' measures, such as safety culture and human factors (although it now has human factor specialists in post).

Following recommendations by the Heath and Safety Executive (HSE), Railtrack is adopting a new safety policy which includes the introduction of trials of a confidential incident reporting programme and the proposed creation of a safety intelligence centre within the Railtrack Safety and Standards Directorate (now Railway Safety Ltd). Initiatives such as this have been able to identify key danger areas, and suggest strategies for reducing the chances of an accident.

Sources: Clarke, S. (1998): Safety culture on the UK railway network. *Work and Stress* **12:** 285-292.
HSC (1993): *Ensuring Safety on Britain's Railways*.HMSO.
Railway Group Safety Plan 2001/2002.
(www.railwaysafety.org.uk/railplan0102.asp)
The Ladbroke Grove Rail Enquiry Report, HSC (www.pixun limited.co.uk/pdf/news/transport/ladbrokegrove.pdf)

Current regulatory framework

The **Health and Safety Commission/Executive** are the regulatory bodies responsible for ensuring that risks encountered in the workplace are properly controlled. The Commission is responsible for securing the health, safety and welfare of persons at work and protecting the public generally against risks arising out of work activities. It sponsors research, promotes training and advises Ministers on all aspects of health and safety legislation. It also has general oversight of the work of the Health and Safety Executive (HSE). The Executive inspects workplaces, investigates accidents and ill health, enforces good standards, publishes guidance, advice and other information, and conducts research. Laws and regulations administered by the HSE include:

The Health and Safety at Work Act 1974 is the foundation stone of British health and safety law. It sets out general duties which employers have towards employees and members of the public, and employees have to themselves and to each other. Such duties are qualified in the Act by the principle of "*so far as is reasonably practicable*" – i.e. the idea that the degree of risk needs to be balanced against the time, trouble, cost and physical difficulty of taking measures to avoid or reduce it. The law requires that the risks are evaluated and that sensible measures are taken to tackle them.

Management of Health and Safety at Work Regulations 1992 (MHSWR) - make more explicit what employers are required to do to manage health and safety under the Act. They require employers to conduct a risk assessment and adapt company safety policy accordingly.

Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) - require employers to report some work-related accidents, diseases and dangerous occurrences. These include all deaths or major injuries, any other injury that leaves the employee off work for three days or more, any work-related disease and any dangerous occurrence (i.e. an incident that does not result in a reportable injury, but which clearly could have done).

Corporate Killing

The Law Commission has recommended that:

- A special offence of corporate killing should be introduced.
- The test for the corporate offence should be whether the corporation's conduct in causing death fell far below what could reasonably be expected.
- The corporate offence should not require that the risk be obvious or that the defendant be capable of appreciating the risk.
- A death should be regarded as having been caused by the conduct of the corporation if it is caused by a 'management failure', and the way in which its activities are managed or organised fails to ensure the health and safety of persons employed in or affected by its activities.
- Such a failure will be regarded as a cause of a person's death even if the immediate cause is the act or omission of an individual.
- Individuals within a company could still be liable for the offences of reckless killing and killing by gross carelessness as well as the company being liable for the offence of corporate killing.

Source: The Home Office.

The Law Commission recently recommended that a special offence of corporate killing be introduced (see box opposite for details). Its proposals are broadly supported by the Home Office; indeed, it is likely that the proposed new legislation will be the subject of a White Paper in the near future. However, not all agree with the proposal. For instance, the Confederation of British Industry (CBI) have labelled the new suggestions as being unfair to businesses. It sees the way forward as building on current health and safety legislation, resourcing enforcers, encouraging best practice, and through consultation on new penalties.

Accident investigation

Current UK (RIDDOR) regulations (see box) require employers to *report* work-related accidents. Although there are duties under some health and safety law that may lead employers to *investigate* accidents, and to take account of the lessons learned, there is no explicit duty to do so. According to the HSC many employers do undertake accident investigation in order to ensure lessons are learned, but this is not universal and investigation practices vary across industry sectors and types of business. It thus recently outlined a number of proposed changes to the law to make investigation of workplace incidents compulsory. These proposals are under consultation[12] until September 2001 and cover issues including:

- the legislative route to be taken (e.g. whether the proposals become part of RIDDOR or the MHSWR);
- what sort of accidents should be investigated (e.g. just those currently reported under RIDDOR);
- who should be responsible for the investigation;
- arrangements for keeping a record of investigation;
- who should have access to the investigation findings (e.g. should those affected by the accident have a right to view the findings).

Directors' responsibilities

HSC are also developing a code of practice on directors' responsibilities for health and safety, in conjunction with stakeholders, and has published a draft code. Under the proposed code, boards of directors need to:

- accept formally and publicly their collective and individual role in providing health and safety leadership in their organisation;
- ensure all Board decisions reflect their health and safety intentions as laid down in their health and safety policy statement;
- recognise their role in engaging the active participation of their staff in health and safety;
- ensure they are kept informed of and alert to relevant health and safety risk management issues (HSC recommends each Board to appoint a health and safety director).

This has been welcomed by RoSPA (Royal Society for the Prevention of Accidents) which had been running a campaign to promote a more active role for Directors in improving health and safety in the workplace. However, the CBI is seeking clarification over the legislative status of the code of practice, and would oppose its introduction as a formal approved code of practice.

Improving consultation
The HSC recently proposed a new package to improve employers' consultation with workers on health and safety issues. Among the proposals were new regulations to harmonise general consultation arrangements, and to empower employees to decide whether they wish to be consulted on health and safety directly or through elected representatives. The regulations specify the functions of elected representatives and are backed up by a new Approved Code of Practice. HSC will launch a formal consultation in the Summer 2001. The CBI opposed several of the legislative options suggested (including roving safety representatives) stating that any regulatory system should retain flexibility to allow employers to consult in a way which is appropriate for their workplace and workforce. It is currently considering the issues and whether changes would be appropriate to the current regulations.

Annual reporting of health and safety
Companies are not currently required by law to include health and safety information in their annual reports. However HSC guidance makes it clear that it regards this as good practice and encourages companies to include:

- general health and safety information (e.g. goals, risks, progress towards achieving stated health and safety aims, consultation arrangements);
- the number of deaths and injuries reported under RIDDOR, including brief details of any fatalities and the steps taken to prevent any recurrence;
- details of employee days lost to the company through health and safety problems, details of any convictions or enforcement notes and an assessment of the cost to the company of the occupational injuries and illnesses suffered by the company's staff.

Organisations such as the CBI point out that many companies already report their health and safety performance in various ways. While it supports a requirement that allows companies the flexibility to report relevant data in a format most suited to the audience with which they wish to communicate, it would oppose any prescriptive legal requirement for annual reporting.

Health and safety performance monitoring
HSE guidance recommends that systems measuring a company's health and safety performance should include both active and reactive monitoring. Active monitoring gives feedback on performance before risks result in injury, ill health, etc. (e.g. by systematic inspection, environmental monitoring and health surveillance). Reactive monitoring involves looking at incidents causing injuries or ill health as well as 'near misses'. One such system has recently been introduced to the rail industry throughout the UK. CIRAS (Confidential Incident Reporting and Analysis System)[13] is a system for anonymous reporting of errors, near-misses and breaches of procedure on the rail network. Data obtained under a trial period have provided evidence of 'sharp end' errors and difficulties such as perception of signals and maintaining attention, as well as latent factors, such as attitudes of management toward safety issues. The benefit of this broad-based analysis is twofold. First, specific reports can be acted upon to improve safety (e.g. changes to braking procedures and signalling). Second, a database of human factors issues can be built up, serving as a valuable resource for the whole rail industry, allowing generalisations as to the likelihood of accidents in particular contexts. Confidential error-reporting schemes are increasingly seen as essential features of all industries where safety is an issue.

Overview

Human error is inevitable. Reducing accidents and minimising the consequences of accidents that do occur is best achieved by learning from errors, rather than by attributing blame. Feeding information from accidents, errors and near misses into design solutions and management systems can drastically reduce the chances of future accidents. Hence, studying human error can be a very powerful tool for preventing disaster.

Endnotes

1 Feyer, A.M. & Williamson, A.M. (1998): Human factors in accident modelling. In: Stellman, J.M. (Ed.), *Encyclopaedia of Occupational Health and Safety, Fourth Edition.* Geneva: International Labour Organisation.
2 Institute of Medicine (2000): *To err is human: Building a safer health system.* Washington: National Academy Press.
3 Reason, J. (1989): *Human Error*. Cambridge: CUP.
4 Norman, D. (1988): *the Psychology of Everyday Things.* New York: Basic Books.
5 Duncan, K. D. (1987). Fault diagnosis training for advanced continuous process installations. In: Rasmussen, J., Duncan, K., and Leplat, J. (Eds), *New Technology and Human Error*. Chichester: Wiley.
6 Rasmussen, J. (1980). The human as a systems component. In: Smith, H.T. and Green, T.R.G. (Eds), *Human Interaction with Computers*. London: Academic Press.
7 Health and Safety Executive (1999): *Reducing error and influencing behaviour*. London: HMSO.
8 Guest, D.E., Peccei, R. & Thomas, A. (1994): Safety culture and safety performance: British Rail in the aftermath of the Clapham Junction disaster. Paper presented at the Bolton business school conference on changing perceptions of risk, Bolton, February 1994.
9 Lee, T. & Harrison, K. (2000): Assessing safety culture in nuclear power stations. *Safety Science,* **34:** 61-97.
10 Leape, L. (1994): Error in medicine. *Journal of the American Medical Association* **272:** 1851-1857.
11 Clarke, S. (1998): Organisational factors affecting the incident reporting of train drivers. *Work & Stress* **12:** 6-16.
12 HSE/C (2001): Proposals for a new duty to investigate accidents, dangerous occurrences and disasters. http://www.hse.gov.uk/condres visited on 11/05/01.
13 Davies, J.B., Wright, L., Courtney, E. & Reid, H. (2000): Confidential incident reporting on the UK railways: The CIRAS system. *Cognition, Technology & Work* **2:** 117-125.

POST is an office of both Houses of Parliament, charged with providing independent and balanced analysis of public policy issues that have a basis in science and technology.

The Parliamentary Office of Science and Technology, 7 Millbank, London SW1P 3JA Tel 020 7219 2840

POST is grateful to the British Psychological Society for funding Andrew Turvey's secondment to Parliament to research this briefing note.

www.parliament.uk/post/home.htm

Understanding Human Behaviour and Error

David Embrey

Human Reliability Associates
1, School House, Higher Lane,
Dalton, Wigan,
Lancashire. WN8 7RP

1. The Skill, Rule and Knowledge Based Classification

An influential classification of the different types of information processing involved in industrial tasks was developed by J. Rasmussen of the Risø Laboratory in Denmark. This scheme provides a useful framework for identifying the types of error likely to occur in different operational situations, or within different aspects of the same task where different types of information processing demands on the individual may occur. The classification system, known as the Skill, Rule, Knowledge based (SRK) approach is described in a number of publications, e.g. Rasmussen (1979, 1982, 1987), Reason (1990). An extensive discussion of Rasmussen's influential work in this area is contained in Goodstein et al (1988) which also contains a comprehensive bibliography.

The terms skill, rule and knowledge based information processing refer to the degree of conscious control exercised by the individual over his or her activities. Figure 1 contrasts two extreme cases. In the knowledge based mode, the human carries out a task in an almost completely conscious manner. This would occur in a situation where a beginner was performing the task (e.g. a trainee process worker) or where an experienced individual was faced with a completely novel situation. In either of these cases, the worker would have to exert considerable mental effort to assess the situation, and his or her responses are likely to be slow. Also, after each control action, the worker would need to review its effect before taking further action, which would probably further slow down the responses to the situation.

The skill based mode refers to the smooth execution of highly practiced, largely physical actions in which there is virtually no conscious monitoring. Skill based responses are generally initiated by some specific event, e.g. the requirement to operate a valve, which may arise from an alarm, a procedure, or another individual. The highly practiced operation of opening the valve will then be executed largely without conscious thought.

In Figure 2, another category of information processing is identified which involves the use of rules. These rules may have been learned as a result of interacting with the plant, through formal training, or by working with experienced process workers. The level of conscious control is intermediate between that of the knowledge and skill based modes.

Knowledge-Based Mode **Conscious**	**Skill-Based Mode** **Automatic**
Unskilled or occasional user	Skilled, regular user
Novel environment	Familiar environment
Slow	Fast
Effortful	Effortless
Requires considerable feedback	Requires little feedback
Causes of error: • Overload • Manual Variability • Lack of knowledge of modes of use • Lack of awareness of consequences	Causes of error: • Strong habit intrusions • Frequently invoked rule used inappropriately • Situational changes that do not trigger the need to change habits

Figure 1: Modes of Interacting with the World (based on Reason, 1990)

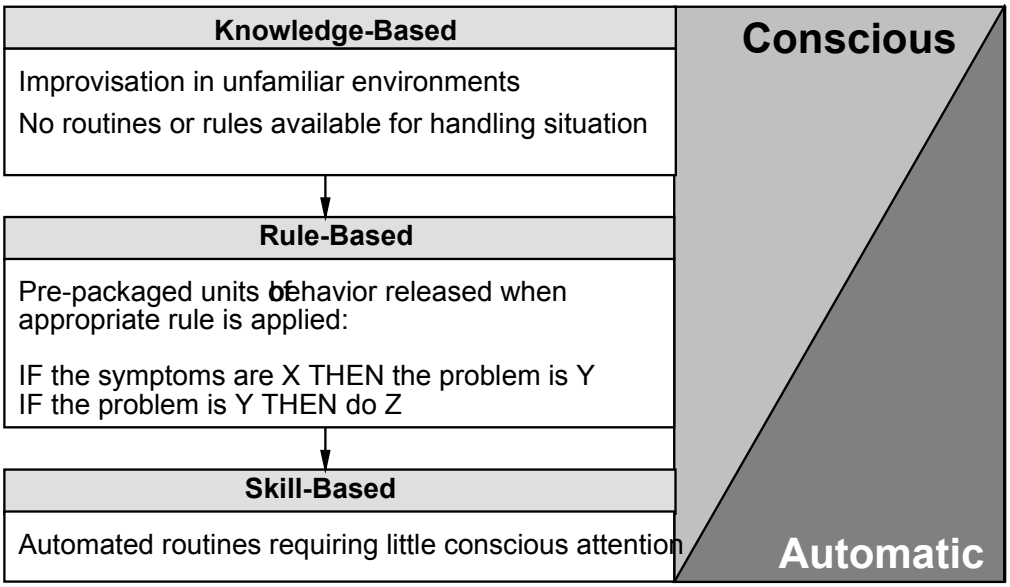


Figure 2: The Continuum Between Conscious and Automatic Behavior (based on Reason, 1990)

2. The Generic Error Modeling System (GEMS)

GEMS is an extension of the SRK Approach and is described in detail in Reason (1990). GEMS is intended to describe how switching occurs between the different types of information processing (skill, rule, knowledge) in tasks. GEMS as shown in Figure 3. The way in which GEMS is applied is illustrated most effectively by means of a specific example.

Consider a process worker monitoring a control panel in a batch processing plant. The worker is executing a series of routine operations such as opening and closing valves and turning on agitators and heaters. Since the worker is highly practiced, he or she will probably be carrying out the valve operations in an automatic skill-based manner only occasionally monitoring the situation at the points indicated by the 'OK?' boxes at the skill based level in Figure 3.

If one of these checks indicates that a problem has occurred, perhaps indicated by an alarm, the worker will then enter the rule based level to determine the nature of the problem. This may involve gathering information from various sources such as dials, chart recorders and VDU screens, which is then used as input to a diagnostic rule of the following form:

<IF> symptoms are X <THEN> cause of the problem is Y

Having established a plausible cause of the problem on the basis of the pattern of indications, an action rule may then be invoked of the following form:

<IF> the cause of the problem is Y <THEN> do Z

If, as a result of applying the action rule, the problem is solved, the worker will then return to the original skill based sequence. If the problem is not resolved, then further information may be gathered, in order to try to identify a pattern of symptoms corresponding to a known cause.

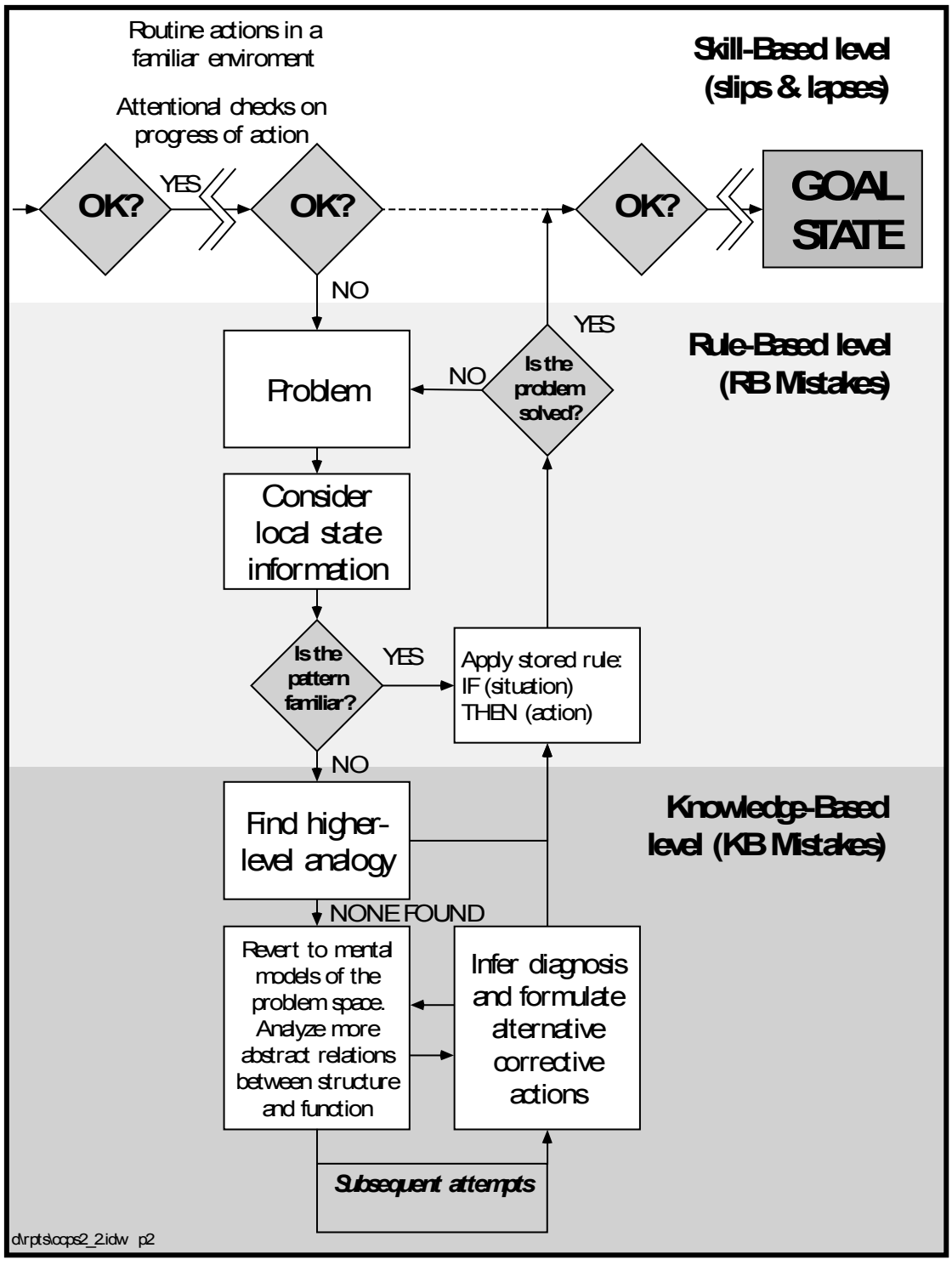


Figure 3: Dynamics of Generic Error Modeling System (GEMS) (adapted form Reason, 1990)

In the event that the cause of the problem cannot be established by applying any available rule, the worker may then have to revert to the knowledge based level. The first strategy likely to be applied is to attempt to find an analogy between the unfamiliar situation and some of the patterns of events for which rules are available at the rule based level. If such a diagnostic rule can be found which validly applies, the worker will revert back to the rule based level and use the appropriate action rule. However, if a suitable analogy cannot be found, it may be necessary to utilize chemical or engineering knowledge to handle the situation. This process is illustrated in the following example:

Example A: Moving between the Skill, Rule and Knowledge Based Levels in the GEMS Model

While scanning a control panel, a process worker notices that a pressure build-up is occurring during a routine transfer of reactant between the reactors (a skill based check). He first checks if the appropriate valves have been opened (rule based check: if pressure build-up, then transfer line may not have been opened.) Since the valve line-ups appear to be correct, he then moves to the knowledge based level to draw upon other sources of information. The use of a data sheet of the chemical properties of the reactant and a piping diagram at the knowledge based level identify the problem as solidification of the chemical in the line due to low ambient temperature. The formulation of corrective actions involves moving back up to the rule based level to find an appropriate corrective action, for example turning on electric heat tracing at the point in the line where the blockage had occurred. If this action is successful, then the situation reverts to the skill-based level where the problem originally occurred.

This example illustrates the fact that several levels of processing may occur within the same task.

3. Classification of Errors

3.1 Slips and mistakes

The categorization set out in Figure 4 is a broad classification of the causes of human failures which can be related to the SRK concepts discussed in the last section. The issue of violations will not be addressed here. The distinction between slips and mistakes was first made by Norman (1981).

> *Slips are defined as errors in which the intention is correct, but a failure occurring when carrying out the activities required. For*

example, a worker may know that a reactor needs to be filled but instead fills a similar reactor nearby. this may occur if the reactors are poorly labeled, or if the worker is confused with regard to the location of the correct reactor. Mistakes, by contrast, arise from an incorrect intention, which leads to an incorrect action sequence, although this may be quite consistent with the wrong intention. An example here would be if a worker wrongly assumed that a reaction was endothermic and applied heat to a reactor, thereby causing overheating. Incorrect intentions may arise from lack of knowledge or inappropriate diagnosis.

In Figure 4, the slips/mistakes distinction is further elaborated by relating it to the Rasmussen SRK classification of performance discussed earlier. Slips can be described as being due to misapplied competence because they are examples of the highly skilled, well practiced activities that are characteristic of the skill-based mode. Mistakes, on the other hand, are largely confined to the rule and knowledge based domains.

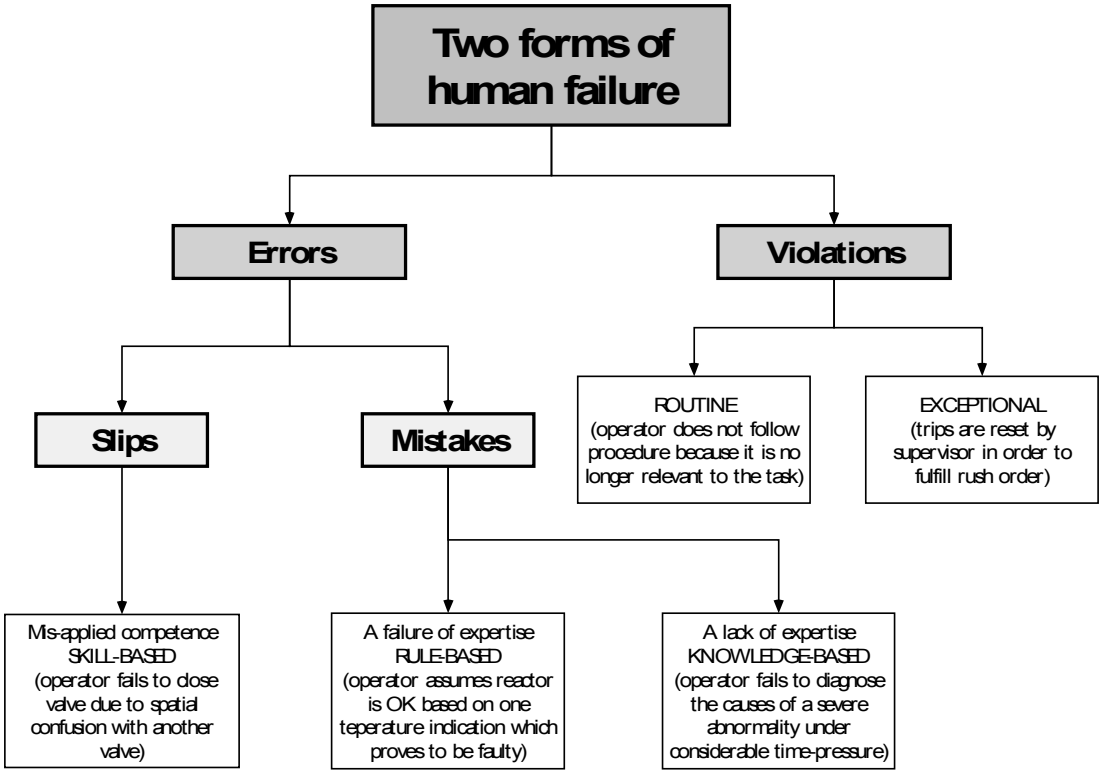


Figure 4: Classification of Human Errors (adapted from Reason, 1990)

In the skill-based mode, the individual is able to function very effectively by using 'pre-programmed' sequences of behavior which do not require much conscious control. It is only occasionally necessary to check on progress at particular points when operating in this mode. The price to be paid for this economy of effort is that strong habits can take over when attention to checks is diverted by distractions, and when unfamiliar activities are embedded in a familiar context. This type of slip is called a 'strong but wrong' error.

3.2 Rule based mistakes

With regard to mistakes, two separate mechanisms operate. In the rule-based mode, an error of intention can arise if an incorrect diagnostic rule is used. For example, a worker who has considerable experience in operating a batch reactor may have learned diagnostic rules which are inappropriate for continuous process operations. If he or she attempts to apply these rules to evaluate the cause of a continuous process disturbance, a misdiagnosis could result, which could then lead to an inappropriate action. In other situations, there is a tendency to overuse diagnostic rules that have been successful in the past. Such 'strong' rules are usually applied first, even if they are not necessarily appropriate.

There is a tendency to force the situation into the mold of previous events. Following some modifications to a pump, it was used to transfer liquid. When movement was complete, the worker pressed the stop button on the control panel and saw that the 'pump running' light went out. He also closed a remotely operated valve in the pump delivery line. Several hours later the high-temperature alarm on the pump sounded. Because the worker had stopped the pump and seen the running light go out, he assumed the alarm was faulty and ignored it. Soon afterward there was an explosion in the pump. When the pump was modified, an error was introduced into the circuit. As a result, pressing the stop button did not stop the pump but merely switched off the running light. The pump continued running, overheated, and the material in it decomposed explosively.

In this example, a major contributor to the accident was the worker's assumption that the pump running light being extinguished meant that the pump had stopped even though a high temperature alarm occurred which would usually be associated with an operating pump. The rule 'IF Pump light is extinguished THEN pump is stopped' was so strong that it overcame the evidence from the temperature alarm that the pump was still running. By analogy with the 'strong but wrong' action sequences that can precipitate skill based slips, the inappropriate use of usually successful rules can be described as 'strong but wrong' rule failures. Other types of failure can occur at the rule based level and these are described extensively by Reason (1990).

3.3 Knowledge based mistakes

In the case of knowledge based mistakes, other factors are important. Most of these factors arise from the considerable demands on the information processing capabilities of the individual that are necessary when a situation has to be evaluated from first principles. Given these demands it is not surprising that humans do not perform very well in high stress, unfamiliar situations where they are required to 'think on their feet' in the absence of rules, routines and procedures to handle the situation. Kontogiannis and Embrey (1990) and Reason (1990) describe a wide range of failure modes under these conditions. For example, the 'out of sight, out of mind' syndrome means that only information which is readily available will be used to evaluate the situation. The 'I know I'm right' effect occurs because problem solvers become over-confident in the correctness of their knowledge. A characteristic behavior that occurs during knowledge-based problem solving is 'encystment' where the individual or the operating team become enmeshed in one aspect of the problem to the exclusion of all other considerations (the Three Mile Island accident is a notable example). The opposite form of behavior, 'vagabonding' is also observed, where the overloaded worker gives his attention superficially to one problem after another, without solving any of them. Janis (1972) provide detailed examples of the effects of stress on performance.

3.4 Error recovery

In the skill-based mode, recovery is usually rapid and efficient, because the individual will be aware of the expected outcome of his or her actions and will therefore get early feedback with regard to any slips that have occurred which may have prevented this outcome being achieved. This emphasizes the role of feedback as a critical aspect of error recovery. In the case of mistakes, the mistaken intention tends to be very resistant to disconfirming evidence. People tend to ignore feedback information that does not support their expectations of the situation. This is the basis of the commonly observed 'mindset' syndrome.

4. The Step Ladder Model

The GEMS model is based on a more detailed model of human performance known as the Step Ladder Model developed by Rasmussen, (see Rasmussen 1986) and illustrated in Figure 5. In this model, Rasmussen depicted the various stages that a worker could go through when handling a process disturbance.

Only if the worker has to utilize the knowledge based mode will he or she traverse every information processing stage represented by the boxes connected by the heavy arrows. As in the GEMS model, if the situation is immediately recognized, then a pre-programmed physical response will be executed in the skill based mode (e.g. by moving the process on to the next stage by pressing a button).

If the nature of the problem is not readily apparent, then it might be necessary to go to the rule based level. In this case a diagnostic rule will be applied to identify the state

of the plant and an action rule used to select an appropriate response. Control will revert to the skill based level to actually execute the required actions. More abstract functions such as situation evaluation and planning will only be required at the knowledge based level if the problem cannot not be resolved at the rule based level.

The lighter arrows represent typical short cuts which omit particular stages in the information processing chain. These short cuts may be 'legitimate', and would only lead to errors in certain cases. For example, the worker may erroneously believe that he or she recognizes a pattern of indicators and may immediately execute a skill based response, instead of moving to the rule based level to apply an explicit diagnostic rule. The dotted lines in the diagram indicate the various feedback paths that exist to enable the individual to identify if a particular stage of the processing chain was executed correctly. Thus, if the operating team had planned a strategy to handle a complex plant problem, they would eventually obtain feedback with regard to whether or not the plan was successful. Similar feedback loops exist at the rule and skill based levels, and indicate opportunities for error correction.

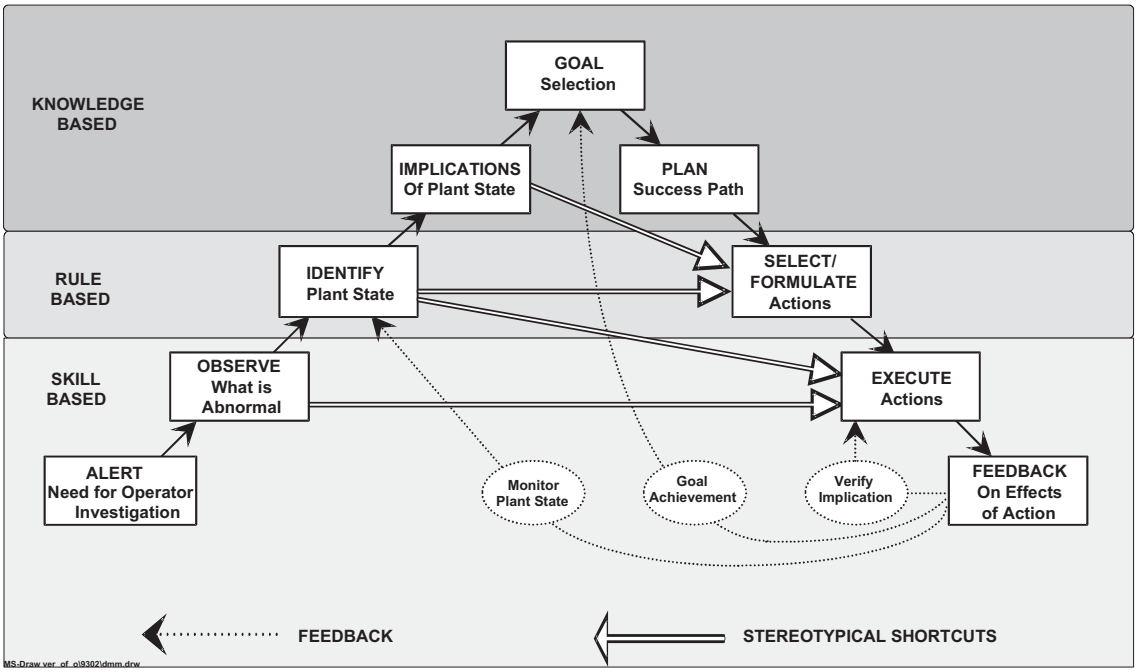


Figure 5: Decision-Making Model (adapted from Rasmussen) including Feedback

Process control: Error Classification (Based on Reason)

Planning Errors	**Checking errors**
Planning preconditions ignored	Checking omitted
Incorrect plan carried out	Checking incomplete
Correct but inappropriate plan executed	Right check wrong object
Correct plan executed too soon/late	Wrong check right object
Correct plan executed in wrong order	Checking mistimed
Action errors	**Retrieval errors**
Operation too long/ too short	Information not obtained
Operation mistimed	Wrong information obtained
Operation in wrong direction	Information retrieval incomplete
Operation too little/too much	
Misalign	**Information Communication errors**
Right Operation on wrong object	Information not communicated
Wrong Operation on right object	Wrong Information obtained
Operation omitted	Information retrieval incomplete
Operation in complete	
	Selection Errors
	Selection omitted
	Wrong selection made

Table 4: Error Types (ETs) and definitions

Timing of action	*Examples*
The controller's action was too fast	*The controller took over position too quickly after a break*
The controller's action was too slow	*The OJTI spoke too slowly to the trainee*
The controller's action was too early	*The controller transferred the aircraft too early*
The controller's action was too late	*The supervisor waited too long to split the sectors*
The controller repeated the wrong	*The controller repeated a wrong data input*
The controller did the right action in the wrong order	*The controller arranged the aircraft strips in the wrong sequence*
Selection of action	
The controller forgot to	*The controller forgot to clear traffic to a higher FL*
The controller failed to	*The controller failed to separate two aircraft before transfer*
The controller gave too much / too little	*The controller instructed a greater speed control than was necessary*
The controller made the wrong action	*The controller dialled the wrong number into the communication panel*
The controller gave the wrong action to the right a/c	*The controller requested the correct aircraft to turn in the wrong direction*
The controller gave the wrong action to the wrong a/c	*The controller requested the wrong aircraft to turn in the wrong direction*
The controller gave the right action to the wrong a/c	*The controller requested the correct descent from the wrong aircraft*
The controller gave an unnecessary action	*The controller re-cleared an aircraft although there was no conflict*
Information transfer	
The controller transmitted/sent unclear, muffled or indistinct	*The controller gave a pushback clearance very unclearly*
The controller wrote/typed unclear, obscure or indistinct	*The controller wrote/typed the FPS amendment indistinctly*
The controller received unclear, muffled or indistinct	*The controller received a request from a foreign pilot which was not clear*
The controller failed to get the required	*The controller failed to get the readback from the pilot*
The controller failed to transmit/send the	*The controller did not transmit/send the airport information*
The controller failed to write/type the	*The controller failed to write/type the FPS amendment*
The controller transmitted/sent partial/incomplete	*The controller sent incomplete information regarding the latest NOTAMS*
The controller wrote/typed partial/incomplete	*The controller wrote/typed incomplete information regarding the weather*
The controller transmitted/sent incorrect	*The controller sent incorrect information regarding the taxiway closure*
The controller wrote/typed incorrect	*The controller prepared the FPS incorrectly*

Dependable Requirements Engineering

Atoosa P-J Thunem
atoosa.p-j.thunem@hrp.no
Division Industrial Psychology, Department MTO
Institute for Energy Technology, OECD Halden Reactor Project

"Human-Organization-Technology" (HOT) Systems

- Complex nature
- Multipurpose nature (fundamental characteristic)
- Living nature – purposes can change
- Vulnerable nature – different sets of purposes can be mutually contradicting
- Driven by various types of agents
- Driven by various types of assets
- Therefore: Can be described and analyzed only by a holistic, interdisciplinary and dependable approach

Examples of Complex Multipurpose HOT Systems

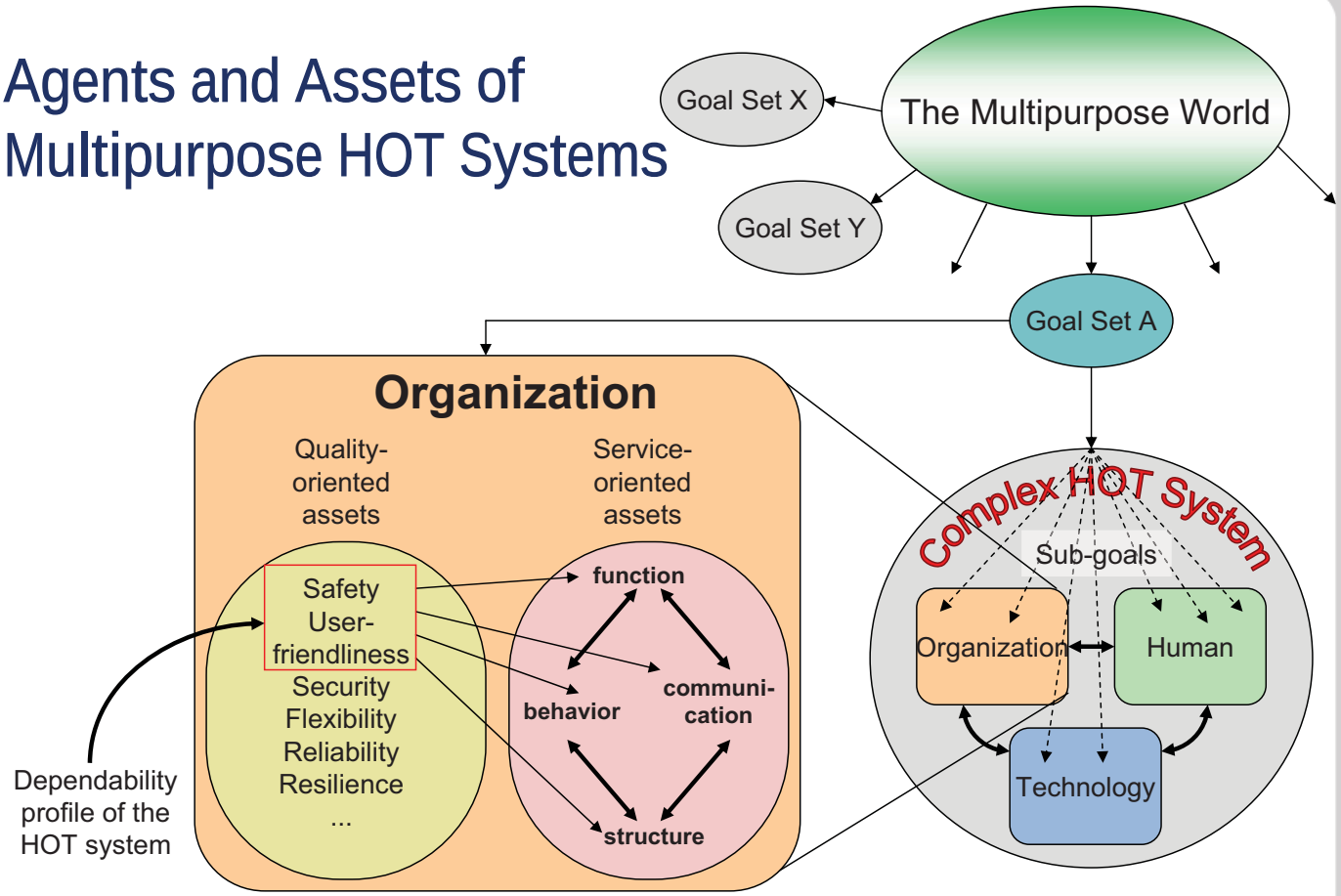
- A cell phone

- An enterprise

Agents and Assets of Multipurpose HOT Systems

- Three groups of agents: H, O and T
- Two groups of assets: Service-oriented and quality-oriented
- Service-oriented assets: structural, behavioral, communicational, functional
- Quality-oriented assets: Dependability factors such as safety, reliability, resilience, security, flexibility, efficacy (performance), efficiency (cost-effectiveness), availability, usability and user-friendliness
- Dependability profiling

Agents and Assets of Multipurpose HOT Systems



Important Observation about HOT Systems' Dependability (Trustworthiness)

- Various ***dependability profiles*** for the same system
- Some profiles can exist and be valid at the same time
- Some profiles can be mutually in conflict, and should not be valid at the same time
- Some profiles can change to new ones
- The new profiles might call for reengineering of some assets
- The new profiles can make previously valid profiles invalid

Organization Science and Theory: Three Different Schools of Thoughts

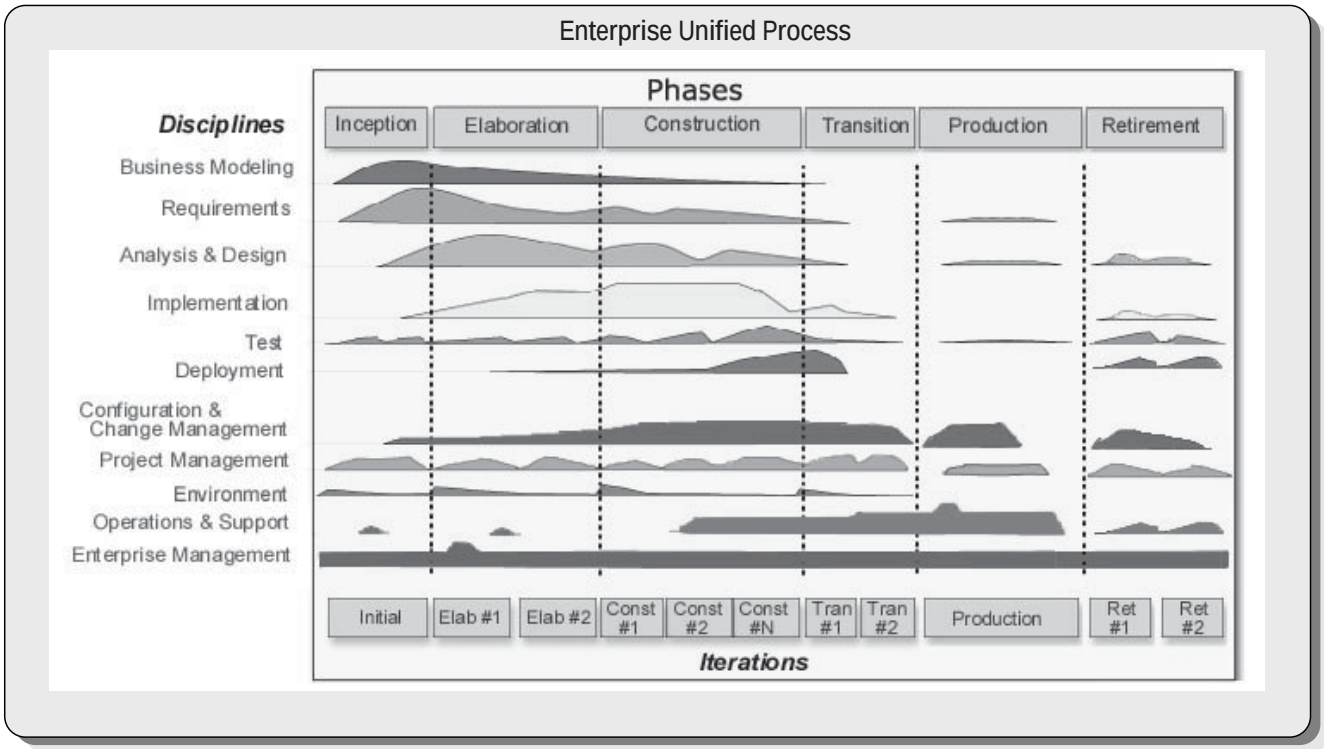
- Industrial and organizational psychology
- Industrial and organizational sociology
- Human factors (ergonomics)

But then, everything is about REQUIREMENTS!

Traditional Requirements Engineering of HOT Systems

- Narrow interpretation of “requirements”
- Dealing with requirements only during the very first stage of the overall systems development process or its associated life-cycle model
- No explicit focus on human- and organization-oriented requirements
- No explicit focus on quality-oriented (dependability) requirements

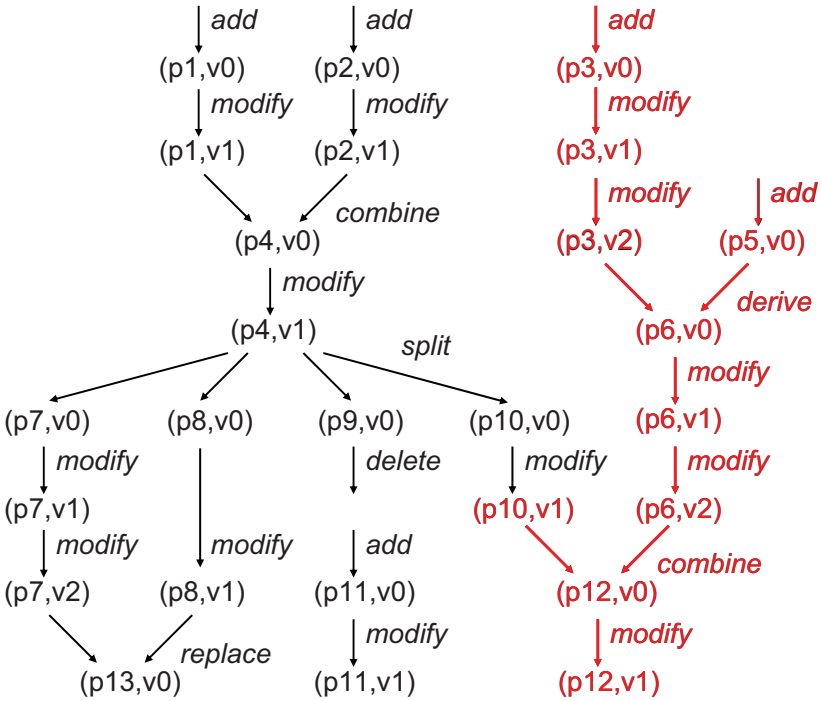
Systems Development Process (Life-Cycle Model)



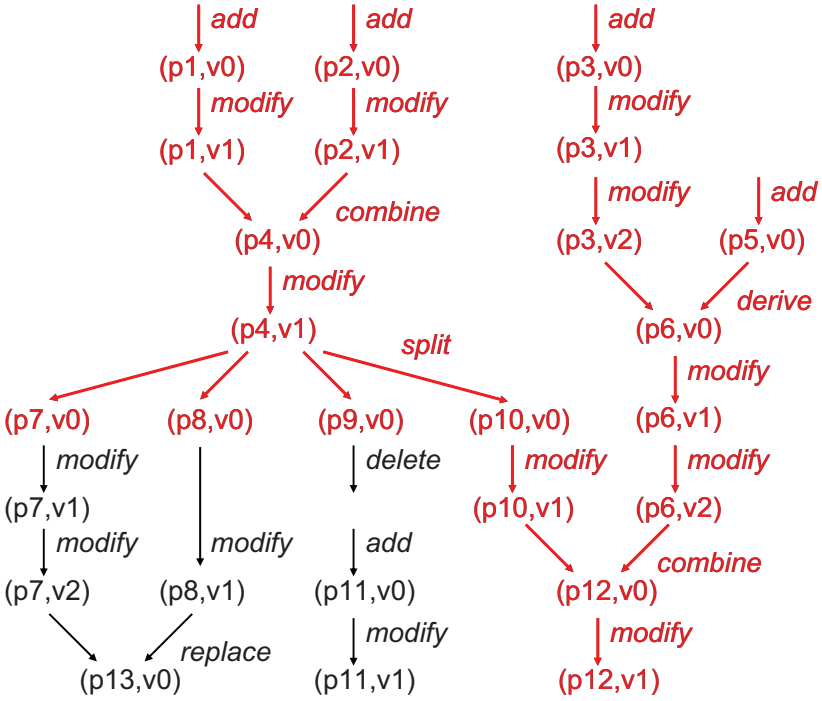
Dependable Requirements Engineering

- Advocates the idea that HOT systems' requirements are identified, specified and implemented for all stages of the system lifecycle, and not only for the highest stage.
- Advocates that explicit links between the requirements belonging to a particular stage or different stages of the lifecycle should be established, by means of well-defined traceability mechanisms.
- Advocates an analysable system and its lifecycle, through the integration of dependability profiles (profiling a set of dependability factors such as safety, security, reliability, and maintainability) into the system lifecycle.
- Recognises the relationship between how a requirement can be met and how it can be opposed to (due to unexpected or unwanted events), thus supporting traceability trees of "dysrequirements" related to vulnerabilities, errors and faults.

Example: Forwards Traceability from p3, v0

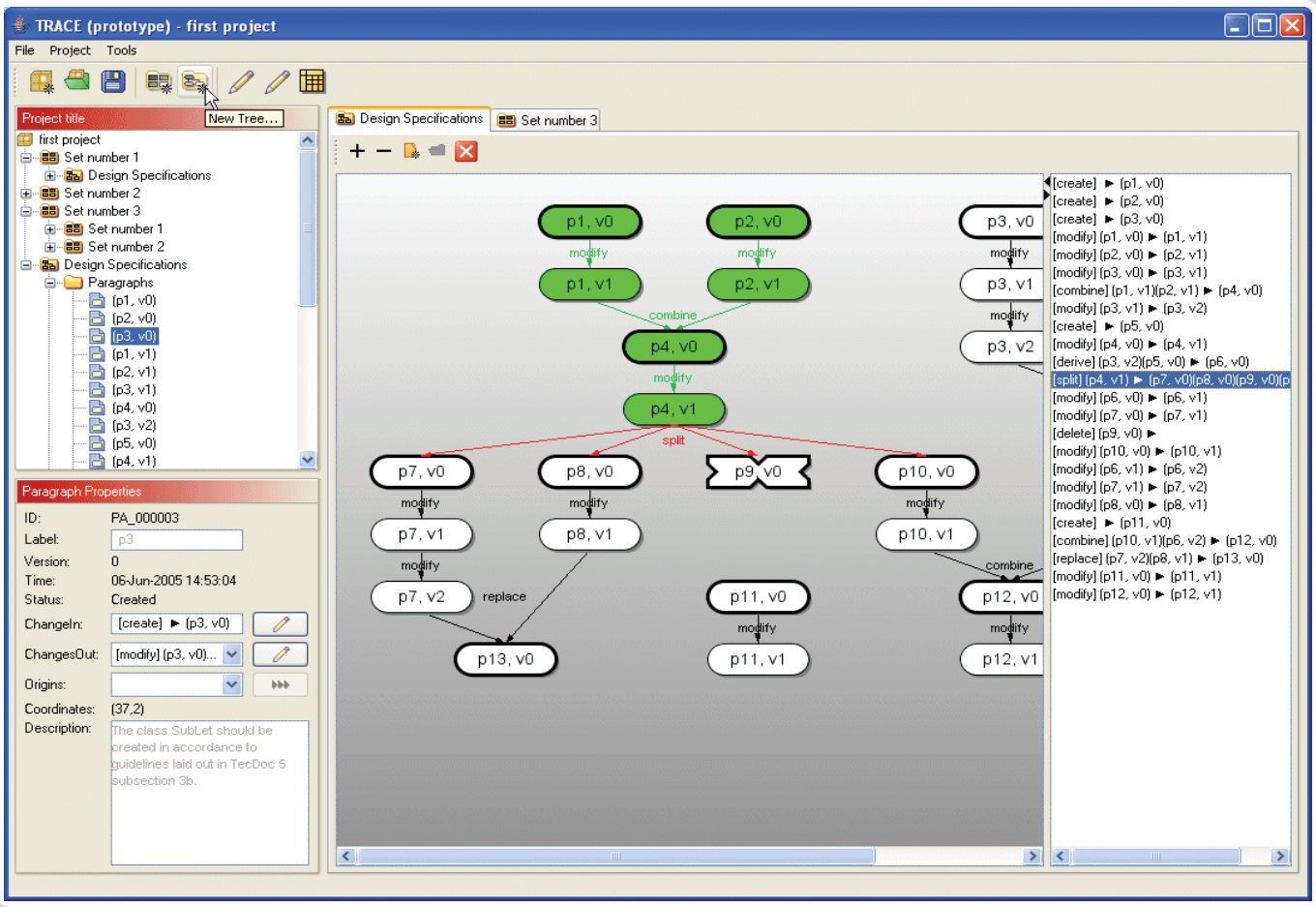


Example: Backwards Traceability from p12, v1



TRACE:
Traceability of Requirements for Analysable Computerised Environments

- Paragraph-oriented as opposed to file-oriented, thus providing a very detailed yet systematic analysis
- Adaptable for a wide range of applications at different abstraction levels, including setting up safety cases, configurable performance measuring experiments, configurable work processes, change management in upgrading, dependability and risk analysis and assessment, maintenance and licensing
- Particularly suitable for detailed and explicit visualization of human- and organization-oriented requirements



Sixth American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies
NPIC&HMIT 2009, Knoxville, Tennessee, April 5-9, 2009, on CD-ROM, American Nuclear Society, LaGrange Park, IL (2009)

TOWARDS A HOLISTIC AND DEPENDABLE FRAMEWORK FOR DEALING WITH HOT SYSTEMS' VULNERABILITIES INVOLVING HUMAN AND ORGANIZATIONAL FACTORS

Atoosa P-J Thunem
Institute for Energy Technology, OECD Halden Reactor Project
Postal Address: PB 173, NO-1751 Halden, NORWAY
atoosa.p-j.thunem@hrp.no

ABSTRACT

This paper explains in brief an initiative towards a holistic and dependable framework that can be used for identification, categorization, progress modeling and analysis of vulnerabilities in HOT systems (HOT: Human-Organization-Technology), which in particular involve human and organizational factors. In that regard, HOT systems' properties are discussed based on a certain system view. Addressing the role of systems dependability, the paper briefly describes the main elements of an approach for Dependable Requirements Engineering (DRE), and how this approach and its supporting tool can be utilized for explicit visualization of human- and organization-centered requirements as well as their progress throughout the life-cycle stages for HOT systems. The application of the approach for setting up trustworthy safety cases is highlighted as an example. Through the course of reasoning, the framework in focus is advocated.

Key Words: Organization science and theory, multipurpose HOT systems, dependability profiles, dependable requirements engineering

1 INTRODUCTION

Many years ago, when the word *system* was almost automatically associated with mechanical and technical factors, the complexity of a complex system was usually categorized as functional, operational and structural types. Some literature began defining complexity as of either logical or physical (intangible or tangible) origin. With the establishment and increasing influence of reliability engineering, the term *non-functional* was introduced to address some system aspects that decide the quality (or goodness) of functional, operational and structural elements of a system, thus offering a new dimension of system complexity. Nowadays, a system is no longer associated with purely technical factors, but acknowledged as a compound created by not only Technical, but Human and Organizational factors. This is true, no matter what the system really is – it can be a cell phone[1], a water supply system, or a multinational enterprise. The complexity associated with each of the three groups of factors can still be categorized as functional, operational, structural, non-functional, etc.

A fundamental characteristic of a complex system is its multipurpose nature. The purpose of a cell phone can be defined quite differently, e.g., depending on who is building and who is using the device. In fact, different users can have different ideas about the purpose of the device, as each individual sees it. Also, they can alter their preferred definition of the purpose, e.g., as a

[1] Although not immediately obvious, a personal cell phone indeed has a set of organizational factors the device either influences or is depending upon.

consequence of learning more about the designer-built functionalities and capabilities of the device. Similarly, different groups of employees at an enterprise, or even each individual in one group, can describe the purpose of the enterprise very differently, deducing into different sets of preferred visions and strategies, hence work conditions, work processes, business terms and portfolio. Of course, not everybody can expect her wishes to be fulfilled, and the management of the enterprise has a specific responsibility to come up with the best possible and representative purpose and set of visions and strategies for the whole enterprise, as the designer team behind a cell phone is responsible for meeting the needs of a target costumer group. Nevertheless, the overall purpose of both the cell phone and the enterprise will gradually be altered or replaced, due to new technology advances, new sources of knowledge and competence, and more efficient, motivating and value-adding ways of organization management. The driving force behind a living complex system and a prerequisite for its evolvement is exactly its response to different purposes defined for the system by its different stakeholders.

Numerous methods and techniques have been developed by scientists and practitioners to view and analyze human- and organization-centered elements of HOT[2] systems (HOT: Human-Organization-Technology). Although they are produced by combined contribution of various scientific disciplines such as sociology, anthropology, psychology, philosophy, biology, mathematics and informatics, the established trend in many communities studying HOT systems still seems to be that the focus of the studies is driven by the current prevailing school of thought or discipline that has formed the dominating origin of the environment's platform of scientific education. The disadvantage of such a focus is that the problems to be solved are derived from and defined by preferred vocational orientation and resulting solution methods and techniques, rather than a general driving goal of making HOT systems more dependable and trustworthy, in spite of their multipurpose nature and thus growing complexity. Of course, it is only natural from such a general platform to direct the attention towards specific problems defined by specific needs, often defined by or for the customers. Nevertheless, as long as the general platform is well-defined and systematically addresses the core characteristics of complex HOT systems and their major vulnerabilities, and as long as such a platform is acknowledged and applied to direct further research and study towards several specific problem domains and not only one or two, it is this author's belief that such approach will increase the likelihood of viewing and analyzing HOT systems from a more holistic and trustworthy perspective, contributing to a growing awareness about the synergy effects across human, organizational and technological factors, which, after all, *together* explain the multipurpose nature of complex HOT systems.

This paper explains in brief an initiative towards a holistic and dependable framework that can be used for identification, categorization, progress modeling and analysis of vulnerabilities in HOT systems, which in particular involve human and organizational factors. In that regard, dependability profiles of HOT systems defining the required quality and trustworthiness of the systems are discussed. Reference to some approaches that deal with particular dependability aspects and related unexpected and unwanted events involving people and organizations is also included. Then, the paper briefly describes the main elements of an approach for Dependable Requirements Engineering (DRE), and how this approach and its supporting tool can be utilized for explicit visualization of human- and organization-centered requirements as well as their

[2] The use of this acronym is deliberate, partly in order to contribute to a gradual replacement of "man" with "human", and partly in order to highlight the very central role of "organization" in more dependable exploitation of human and technology resources and their synergy effects (the "O" binding the "H" and "T" together).

progress throughout the life-cycle stages for HOT systems. The application of the approach for setting up trustworthy safety cases is highlighted as an example. The benefits of the approach are also viewed in the light of the multipurpose nature of complex systems and processes, as a major cause for dependability breach, hence, a major reason for why it is so difficult and at the same time so crucial to be able to incorporate human and organization related dependability factors into all stages of the life cycle for HOT systems and processes. Through this course of reasoning, the framework in focus is advocated.

2 A THEORY: AGENTS AND ASSETS OF MULTIPURPOSE HOT SYSTEMS

Generally, the assets (properties) of HOT systems can be categorized into two main groups, *service-oriented* and *quality-oriented* [1]. Service-oriented assets are usually unilaterally viewed and analyzed, as they are typically specified based on a set of goals (formed by an overall purpose) that are mutually complementing and not contradicting. Service-oriented assets can, roughly speaking, be grouped into structural, behavioral, communicational, and functional assets. From an agent-oriented point of view, the technology, human and organization can be regarded as three different types of agents that by means of their service-oriented assets contribute to the attainment of the overall set of goals. Quality-oriented assets deciding the level of quality (goodness, trustworthiness, dependability) for service-oriented assets are together an indication of *how well* the agents contribute to the attainment of the overall set of goals. Both types of assets are in fact the manifestation of the multipurpose nature of HOT systems. Examples of quality-oriented assets, all intangible, are safety, reliability, robustness (resilience), security, flexibility, efficacy (performance), efficiency (cost[3] effectiveness), availability, (re)usability and user-friendliness. Obviously, quality-oriented assets can be mutually in conflict, as a consequence of (or reason for, depending on how to view the matter) conflicting purposes defined for the HOT system, but by different (groups of) stakeholders[4]. Therefore, a particular set of goals for a system ought to include clear indication of desirable and feasible quality-oriented assets for the system that will not jeopardize but help attaining the goals. These will comprise a valid and desired *dependability profile* for the system, based on a certain set of goals. Thus, different dependability profiles for the same HOT system can result in quite different (and even contradicting) service-oriented assets for the system. For example, a very secure process control room with secured/cleared agents involved[5] might undergo radical changes in order to become much less secure and much more efficient or robust, as security, efficiency and robustness are mutually very often in conflict. Similarly, flexible (lean) work processes being a part of an enterprise' organizational assets are not necessarily efficient. *Agile* work processes, on the other hand, can be a result of a trade-off between flexibility and efficiency, or "flexibility in the context of efficiency".

---

[3] Many scholars do not define cost merely within the context of economy, following, among others, C.I. Barnard's then controversial definition of organizational efficiency, but also influenced by M.C.E. Weber's work on organizational sociology [5].

[4] Of course, this can also be true for service-oriented assets. In fact, the author has elaborated on another type of service-oriented asset called capability [1], a type of asset that is directly a cause of the multipurpose characteristic of the system, and that can activate unexpected or even unwanted behavioral and communicational assets, in conflict with the overall set of goals in focus.

[5] Agents can be the operating individuals (an operator viewing and responding to information), the operating organization (affecting the response of the operator by means of, e.g., an exception handling procedure), or the operating technology (a fully computerized alarm device detecting and informing in a technology-driven particular manner).

The above view on HOT systems can be called a general theory and is believed to form a solid basis for more detailed and also application-oriented observations and analyses. It is roughly illustrated in Figure 1.

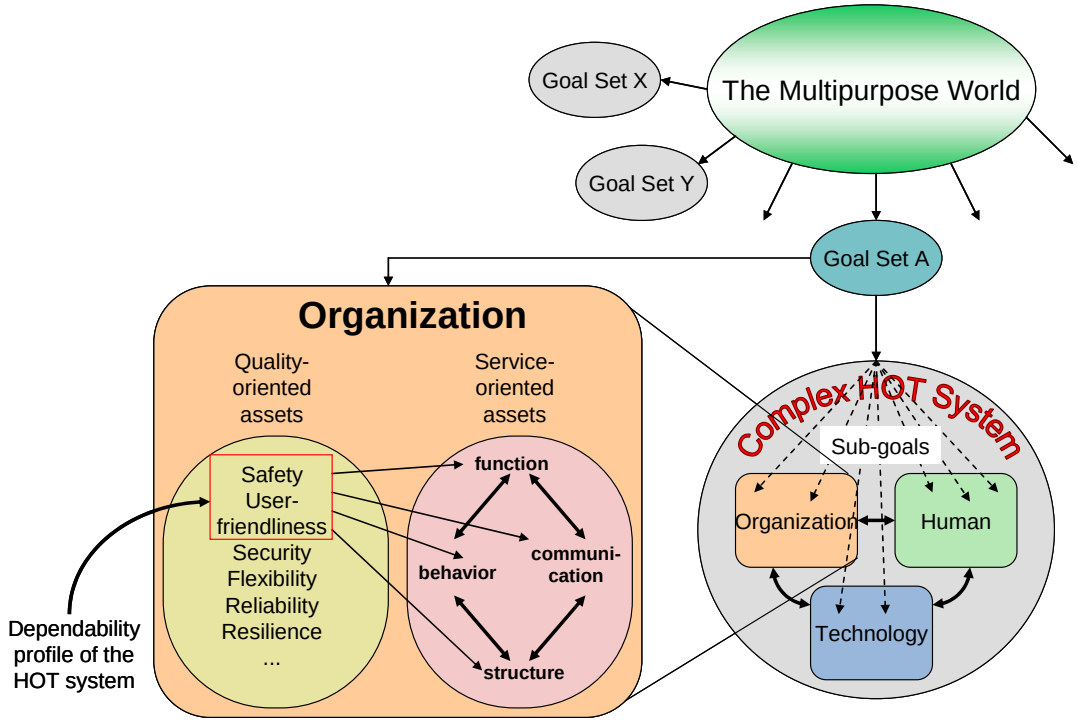


Figure 1. Multipurpose nature of complex HOT systems, their collaborating agents and the agents' assets contributing to a specific set of goals specified for the system

Main disciplines dealing with human and organizational factors and having influenced organization science and theory can be claimed to be sociology, psychology, anthropology, philosophy, and also interdisciplinary scientific fields of cognitive science and informatics (i.e., computer science/information and communication science). From these, however, branches are formed that can be regarded as most influential, especially during the 20th century. At least, scientists and practitioners viewing and analyzing human and organizational factors within the very broad scope of organization science and theory seem to be the supporters of one of the three branches of industrial and organizational psychology [2, 3, 4], industrial and organizational sociology [5, 6, 7, 8], and human factors [9, 10, 11]. Although the branches are related regarding many aspects and thus cannot be distinguished from one another completely, they are indeed different schools of thought.

The prime focus in industrial and organizational psychology is on a particular dependability factor – the human performance. This focus is usually in the context of safety within those industrial domains that have safety as the most significant dependability factor, such as the nuclear domain. Nevertheless, only those human and organization factors affecting and affected by human performance are usually studied by followers of this school of thought.

The concern of industrial and organizational sociology seems, on the other hand, to be of much more diverse character. Greatly influenced by practicing scholars at the end of 20th century, such as Peter F. Drucker and Peter M. Senge [12, 13], many new fields of study within

organization science and theory have emerged from this school of thought. Among those are organizational culture, learning organization, knowledge management and organizational change management.

Most often used as synonymous with ergonomics, the branch of human factors can be, roughly speaking, claimed to deal with both physical and cognitive properties (assets) of a human being, influencing how humans understand and relate to their surroundings. As a scientific and engineering field, the school of thought has had tremendous influence on understanding patterns of relationship and interactions between humans and machines. It yields therefore, that topics of study within human factors/ergonomics can be emerged from various types of focus on dependability (goodness, trustworthiness) factors for parts of or the whole HOT system.

3 DEPENDABLE REQUIREMENTS ENGINEERING

Systematic analysis and treatment of requirements related to various applications of HOT systems has long been subject to research. Existing literature includes more or less established terms such as requirements traceability, requirements management and requirements engineering. The literature also shows that the approaches developed have their theoretical foundation within cognitive and social sciences, and therefore fundamentally operate with a broad perception of the term requirement. Parallel with this, the term has been extensively used by different branches applying systems engineering and dealing in one way or another with design, construction, operation, analysis, maintenance and modernization of HOT systems. A significant observation in this area is that dealing with requirements is almost without exception understood as an activity carried out only during the very first stage of the overall systems development process or its associated life-cycle model. Therefore, the term requirement has a considerably narrow interpretation in all existing systems life-cycle models emerged from systems engineering. Another important observation is that this narrow interpretation of requirements within systems engineering does not address the human- and organization-centered requirements in any clear and explicit manner. Instead, they are either hidden in apparently "pure" technical/technological requirements, or discussed separately and detached from the life-cycle model, which after all is supposed to deal with all aspects of a HOT system. The consequence of these two problems with traditional systems engineering is that the stakeholders can risk not being aware of the impacts of the unexpressed or hidden requirements before they have caused problems such as contradicting requirements and requirements difficult to codify, implement or change.

Based on a belief that it is indeed possible to set up systematic means for describing and managing all requirements (all of them dependability-driven) related to design, construction, operation, analysis, maintenance and modernization of dependable HOT systems, and based on awareness about the multipurpose nature of complex systems and processes as a major cause for dependability breach and therefore a major reason for why it is so difficult and at the same time so crucial to be able to incorporate the intended dependability factors into the system or process, a generic approach for Dependable Requirements Engineering and its supporting tool TRACE were developed within the Halden Reactor Project [14, 15]. The approach advocates a perception of a requirement to be applicable for all stages of the systems life-cycle and not only the high-level stages. Furthermore, acknowledging diverse roles of the three types of agents in HOT

system, the approach supports inter-disciplinary contribution for requirements identification, engineering and analysis based on awareness about different purposes and thus different applications with different sets of systems dependability profiles [14]. This means that dependability factors in focus are forced to be an integrated part of the requirement specification. Additionally, the approach recognizes the relationship between how a requirement can be met and how it can be opposed to, due to unexpected or unwanted events defined in the context of a certain dependability profile in focus. Thus, the requirements can also be perceived as sources of vulnerabilities that can be related to possible deficiencies, errors, faults, failures and risks in a very explicit manner. Finally, the approach can specifically facilitate a systematic implementation of change management, as the approach makes visible the life of each single requirement throughout the systems life-cycle.

Assuming that safety is the main dependability measure for a given HOT system, the approach for DRE is believed to constitute a very powerful platform for a detailed yet systematic manner of developing safety cases by means of coherent course of reasoning and continuous and explicit connection between the claims and their associated evidence, through the arguments and assumptions for improved reinforcement of the arguments.

The generic nature of the DRE approach is evident also through its supporting tool that can be tailor-made for any application with any sets of overall goals driven by any kind of dependability profile [16][6]. The approach and its tool enable therefore also a more visible basis for comparison between, e.g., different versions of a subsystem (within the HOT system) affected by different levels of automation, or different versions of organization-centered requirements of the HOT system with different levels of influence from the involved stakeholders [17][7], or different functional, behavioral, communicational and structural patterns among the agents (of H, O or T type) driven by different dependability profiles defined for the same HOT system. For example, work processes within an enterprise with particular focus on resilient agents will be fundamentally different from those emerged from a desire for reliable agents, bearing in mind that the former agents are *prepared for* occurrence of errors and faults under stated conditions for a stated period of time, whereas the latter agents are engineered with the prime goal of *avoiding* those errors and faults. In fact, the field of “resilience engineering”, having received some attention during recent years, ought to be based on a fundamental recognition of multipurpose characteristics of complex HOT systems, in order to be considered as a feasible field of study, regardless of whether it is considered to be wise or unwise to make systems resilient. Recalling what resilience/robustness actually means, any attempt to make the systems or their associated processes resilient is practically impossible without continuously considering and modeling the multipurpose characteristics of those systems and processes. The DRE approach and its supporting tool provide a solid ground for visualizing such characteristics, and they do this, not through attention towards certain dependability/goodness/trust factors such as safety or resilience, but rather through awareness about *all* such factors manifesting the multipurpose nature of HOT systems, so that the effects of the factors’ mutual discrepancies and conflicts through different versions of the same system can be better described and analyzed.

[6] Access to this reference is restricted to those readers that are members of the OECD Halden Reactor Project.

[7] For an enterprise, the Stakeholder theory advocates taking into account needs, demands and interests of not only the traditional four types of stakeholders: Investors, employees, suppliers, and customers, but also those of governmental bodies, political groups, trade unions, future investors/employees/suppliers/customers, and even competitors. The theory argues that also these groups should be treated as true stakeholders.

The approach for DRE and its tool can be utilized as a means for systematic and detailed dependability engineering, where the concept of *dependability* is an integrated part of the concept of *requirement*.

4 CONCLUSION: TOWARDS A HOLISTIC AND DEPENDABLE FRAMEWORK

Considering today's complex systems to be a compound of interrelated and interacting agents of human, organizational or technological nature, and bearing in mind that a fundamental characteristic of a complex system is its multipurpose nature, this paper has placed the assets of the three types of agents into the two main groups of service-oriented and quality-oriented assets. The paper has argued that service-oriented assets are usually unilaterally viewed and analyzed, as they are typically specified based on a set of goals (formed by an overall purpose) that are mutually complementing and not contradicting. For the sake of readability, service-oriented assets have been roughly addressed as structural, behavioral, communicational, and functional assets. Quality-oriented assets deciding the level of quality (goodness, trustworthiness, dependability) for service-oriented assets are together an indication of how well the agents contribute to the attainment of the overall set of goals. Both types of assets are in fact the manifestation of the multipurpose nature of HOT systems. The paper has provided examples of quality-oriented assets, such as safety, reliability, robustness (resilience), security, flexibility, efficacy (performance) and efficiency (cost effectiveness). As quality-oriented assets can be mutually in conflict, the paper has covered the concept of dependability profiles, each emerging from a specific purpose materialized into a specific set of goals for the system, and each giving rise to inclusion of a certain group of service-oriented assets as "valid" assets for the system.

Through discussion on three scientific and vocational branches dealing with organization science and theory: Industrial and organizational psychology, industrial and organizational sociology and human factors, the paper has argued that each of these branches, although related with regard to many aspects, indeed constitutes a disparate school of thought. It is also implied that the followers of each branch either tend to prioritize certain aspects or do not offer a coherent platform for a need- and application-oriented treatment of human and organizational factors in HOT systems.

Based on a belief that it is indeed possible to set up systematic means for describing and managing all requirements (all of them dependability-driven) related to design, construction, operation, analysis, maintenance and modernization of dependable HOT systems, and based on awareness about the multipurpose nature of complex systems and processes, a generic approach for Dependable Requirements Engineering and its supporting tool TRACE has been explained as a contributor for a holistic and dependable framework that can be used for systematic identification, categorization, progress modeling and analysis of vulnerabilities in HOT systems, which in particular involve human and organizational factors.

The theory on HOT systems and the perspective on the role of dependability assets/factors offered in Chapter 2 and 3 are believed to be beneficial in setting up a generic yet systematic and trustworthy framework for more holistic treatment of all valid assets and thus sources of vulnerabilities in HOT systems, especially those involving human and organizational factors that currently are not addressed in any branches and models within systems engineering.

5 REFERENCES

1. Atoosa P-J Thunem, "Modelling of Knowledge Intensive Computerised Systems Based on Capability-Oriented Agent Theory (COAT)", *Proceedings of international IEEE Conference on Integration of Knowledge Intensive Multi-Agent Systems, IEEE-KIMAS'03*, Cambridge, MA, USA, September 30 – October 4, 2003, pp. 58-63.
2. Adam Smith, *An Inquiry into the Nature and Causes of the Wealth of Nations*, Edinburgh, 1776.
3. Frederick W. Taylor, *The Principles of Scientific Management*, Harper & Brothers Publisher, 1911.
4. Hugo Münsterberg, *Psychology, General and Applied*, Appleton and Co. Publisher, 1914.
5. Chester I. Barnard, *The Functions of the Executive*, Harvard University Press, Cambridge, MA, 1938.
6. Kurt Lewin, "Defining the Field at a Given Time", *Psychological Review*, **Vol. 50**, pp.292-310, 1943.
7. Herbert A. Simon, *Models of Bounded Rationality, Vol. 3*, The MIT Press, Cambridge, MA, 1997.
8. Karl E. Weick, *The Social Psychology of Organizing*, McGraw Hill, 1979.
9. Elias H. Porter, *Manpower Development: The System Training Concept*, Harper and Row, New York, 1964.
10. Christopher D. Wickens, John D. Lee, Yili Liu, Sallie E. Gordon-Becker, *Introduction to Human Factors Engineering (2nd Edition)*, Prentice Hall, 1997.
11. David Meister, *The History of Human Factors and Ergonomics*, Lawrence Erlbaum Associates, Mahwah, New Jersey, 1999.
12. Peter F. Drucker, *Management Challenges for the 21st Century*, HarperCollinsBusiness, 1999.
13. Peter M. Senge, *The Fifth Discipline: The Art and Practice of the Learning Organization (2nd Edition)*, Currency, 2006.
14. Atoosa P-J Thunem, "Dependable Requirements Engineering and Change Management of Security-Critical ICT-Driven Systems", *Proceedings of 8th PSAM conference*, New Orleans, LA, USA, May 14-19, 2006, ASME Press, Topic Area: Security, paper: PSAM-0101.
15. Atoosa P-J, Thunem, Harald P-J Thunem, "TRACE: Traceability of Requirements for Analysable Computerised Environments", *Proceedings of IAEA Technical Meeting on Implementing and Licensing Digital I&C Systems and Equipment in Nuclear Power Plants*, Espoo, Finland, November 22-24, 2005.
16. Atoosa P-J Thunem, Harald P-J Thunem, Halden Work Report 846: "Dependable Requirements Engineering – The Approach behind TRACE", *Proceedings of the Enlarged Halden Programme Group meeting*, Storefjell, Norway, March 12-15, 2007.
17. Robert Phillips, R Edward Freeman, *Stakeholder Theory and Organizational Ethics*, Berrett-Koehler Publishers, 2003.

Nyere teorier i human factors: ørner og kalkuner

Bjarte Knappen Røed, PhD
Kristian Gould, MSc

HFC Forum, Stavanger
22.04.09

SCANDPOWER
Risk Management

Bakgrunn

- Human factors i forskning og anvendt human factors er to ulike ting
- Erfaringer fra human factors forskning og fra konsulentarbeid
- Hvilke metoder klarer overgangen fra teorier og til praktisk anvendelse?

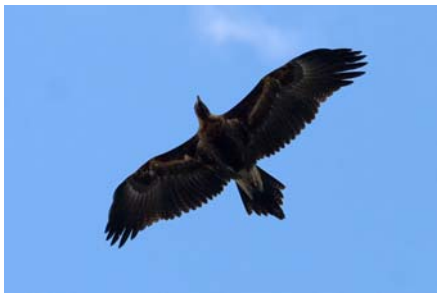
SCANDPOWER
Risk Management

Bakgrunn

- Human factors i forskning og anvendt human factors er to ulike ting
- Erfaringer fra human factors forskning og fra konsulentarbeid
- Hvilke metoder klarer overgangen fra teorier og til praktisk anvendelse?

SCANDPOWER
Risk Management

Ørn eller kalkun?



SCANDPOWER
Risk Management

Metoder og teorier

1) Konseptuelle rammeverk:

- Distribuert kognisjon
- Aktivitetsteori

2) Biopsykologiske rammeverk:

- Mental arbeidsbelastning
- Kognitive ressurser

SCANDPOWER
Risk Management

Distribuert kognisjon

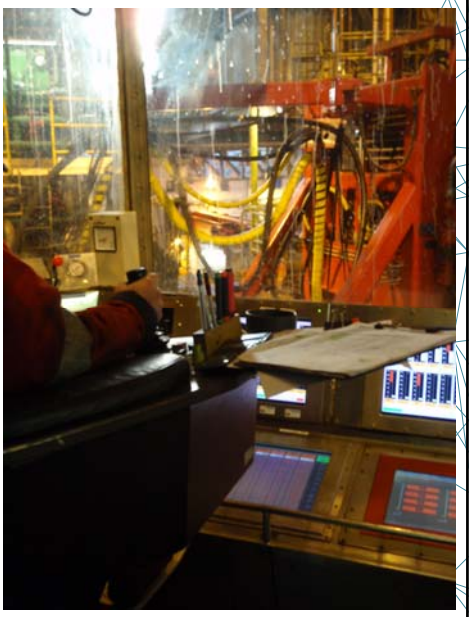
- Kognisjon er ikke begrenset til den menneskelige hjerne
- Mennesker bruker fysiske gjenstander i kognitivt arbeid
- Kognisjon er distribuert ut i et system som består av mennesker og teknologi, dvs et sosioteknologisk system
- Teknologi er ikke bare ting, men har også en kognitiv funksjon.

SCANDPOWER
Risk Management

Borekabin

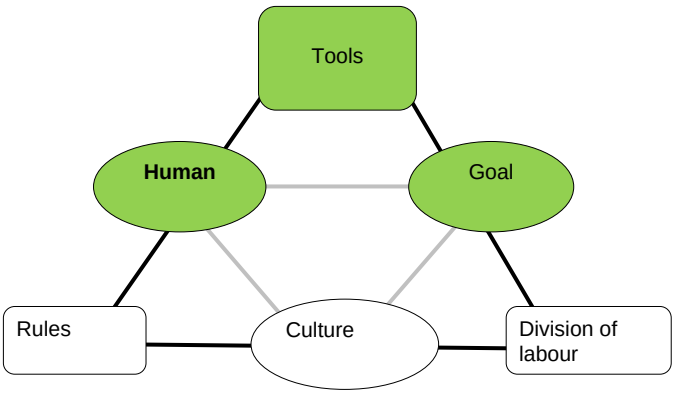
Støtte til boreren:

- Sjekklister
- Displayer
- Skrivesaker



SCANDPOWER
Risk Management

Aktivitetsteori



SCANDPOWER
Risk Management

Aktivitetsteori

- **Eksempler:**
  - Beskrivelse av menneskers mål, arbeidsfordeling, kulturelle forhold
  - Kontinuerlig endring av fysiske gjenstander

SCANDPOWER
Risk Management

Potensiell anvendelse

- **Forstå adferd hos personer som bruker tekniske systemer f.eks:**
  - Navigatører
  - Kontrollromsoperatører
  - Borere
- **Informere design av kontrollrom**

SCANDPOWER
Risk Management

Ørn eller kalkun?

SCANDPOWER
Risk Management

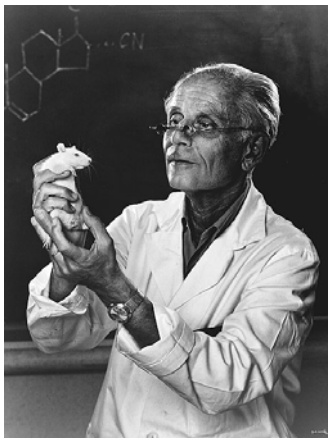
SCANDPOWER
Risk Management

Konseptuelle rammeverk

- Stor deskriptiv verdi for kognitive mekanismer
- Mangler terminologi til å formidle funn for konkret designutvikling
- Mottaker trenger kunnskap om teoriene for å ha utbytte av resultatene
- For stort gap fra teorienes beskrivelser og til kundenes behov for informasjon i en designprosess.

SCANDPOWER
Risk Management

Biopsykologiske rammeverk



SCANDPOWER
Risk Management

Biopsykologiske rammeverk

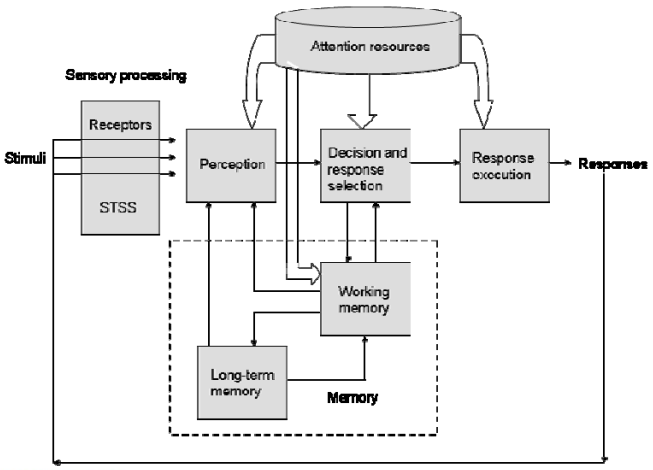
SCANDPOWER
Risk Management

Kognitiv arbeidsbelastning (”mental workload”)

- Definert som ”mengden kognitive ressurser brukt på et gitt tidpunkt”
- Beskriver menneskers evne til å utføre kognitive arbeidsoppgaver
- Mennesker har store begrensninger

SCANDPOWER
Risk Management

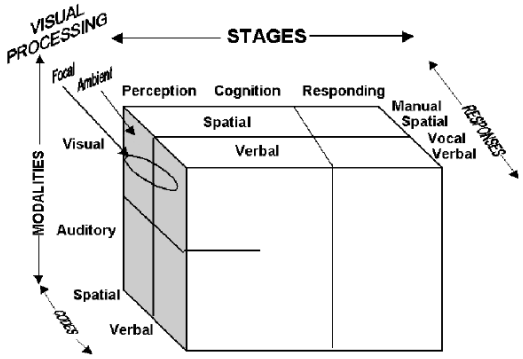
Wickens' opprinnelige modell for informasjonsprosessering (1984)



SCANDPOWER
Risk Management

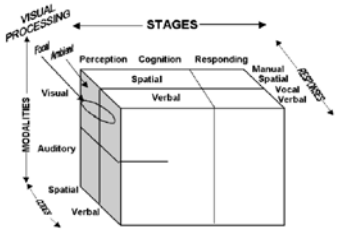
SCANDPOWER
Risk Management

Wickens' 4-dimensjonale modell for informasjonsprosessering (2006)



SCANDPOWER
Risk Management

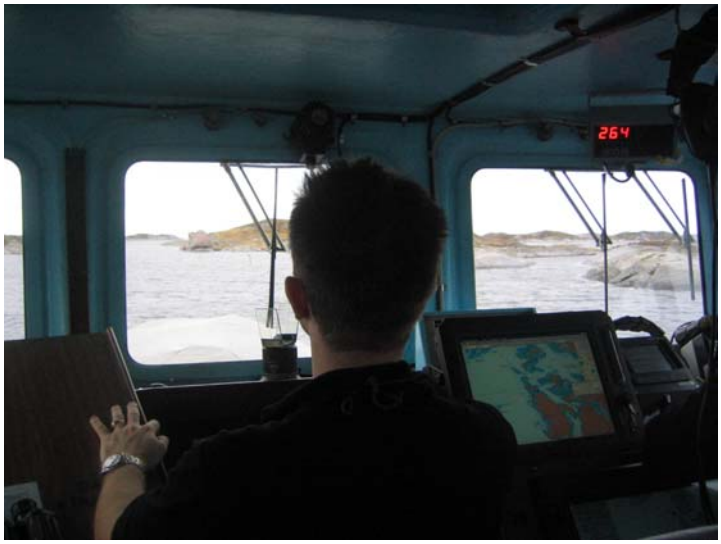
Wickens' 4-dimensjonale modell for informasjonsprosessering (2006)



Hva forteller modellen?

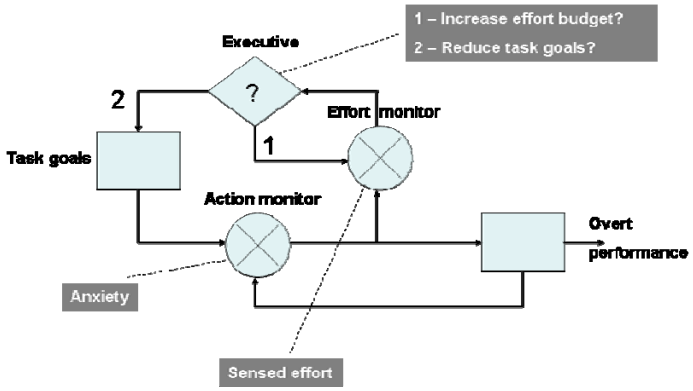
- Hvilke ressurser kreves i forskjellige steg av informasjonsprossessering
- Krav forbundet med billedlig kontra verbal informasjon
- Beskriver kapasitet til å samtidig behandle auditiv og visuell informasjon
- Beskriver effekten av fovealt kontra perifert syn

SCANDPOWER
Risk Management



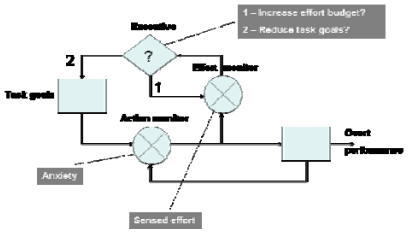
SCANDPOWER
Risk Management

Kompensatorisk kontrollteori
Hockey (1997/2003)



SCANDPOWER
Risk Management

Kompensatorisk kontrollteori
Hockey (1997/2003)

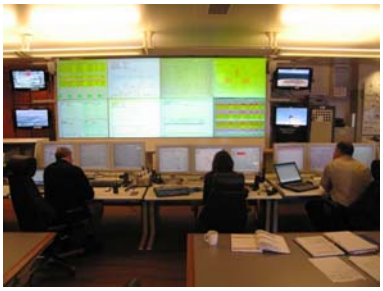


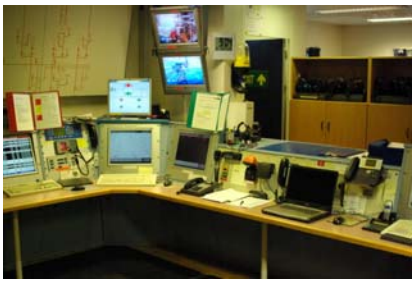
Hva forteller modellen?

- Motivasjon vil føre til opprettholdelse av prestasjon under høye kognitive krav
- Prestasjon vil opprettholdes først gjennom økt innsats, deretter endret strategi
- Prestasjonsfall vil primært sees i sekundæroppgaver

SCANDPOWER
Risk Management

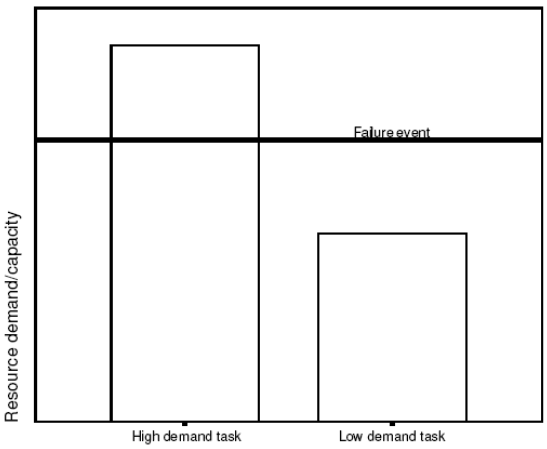
Hva er forskjellen på disse to kontrollrommene?





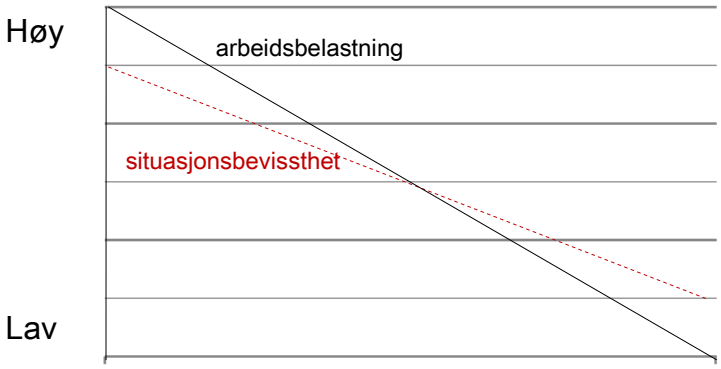
SCANDPOWER
Risk Management

Malleable attention resource theory
Young & Stanton (2002)



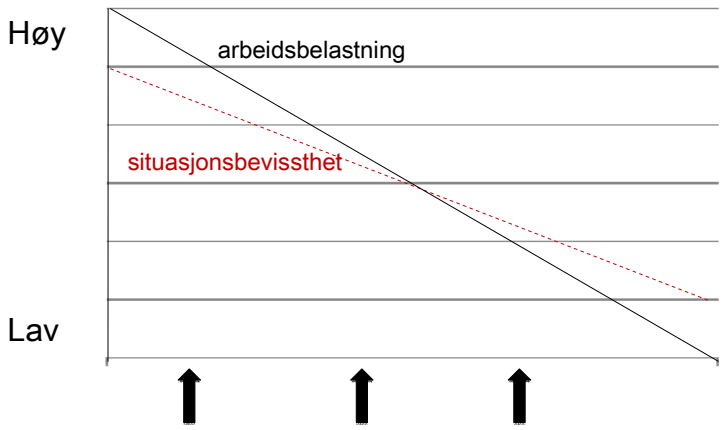
SCANDPOWER
Risk Management

Balansere arbeidsbelastning mot situasjonsbevissthet



SCANDPOWER
Risk Management

Balansere arbeidsbelastning mot situasjonsbevissthet



SCANDPOWER
Risk Management

Hva er felles for disse modellene?

- Sterk psykofysiologisk basis
- Validert i forskning
- Til en viss grad kontekstspesifikke
- Krever ikke detaljert informasjon for å kunne anvendes
- Beskriver bare en del av bildet

SCANDPOWER
Risk Management

Ørn eller kalkun?

...med noen forbehold:

- Krever tid
- Krever kunnskap
- Krever data

SCANDPOWER
Risk Management

Takk for oppmerksomheten!

SCANDPOWER
Risk Management

Diskusjon:

Hvordan kan vi minske gapet mellom HF-teori brukt i forskning og i praksis?

SCANDPOWER
Risk Management

www.scandpower.com

Kort om HMI og HF i NOV Stavanger

HFC Forum 22 april 2009
Heidi.andersen@nov.com

Agenda

- Kort om NOV
- Utvikling
- Drillers Cabin
- Cyberbase
- Displays
- Drilling Advisory
- HF Utfordringer

National Oilwell Varco

Norges hovedkontor i Kristiansand

"***Vi skal være den ledende og mest innovative leverandøren av bore-, håndteringsutstyr og tjenester til olje og gass industrien."***

NOV Stavanger

- Ca 600 personer (ansatte + innleide).
- Levert over 250 borekabiner
- I 2009: 28 kabiner.
- Levert over 350 Cyberbaser
- I 2009: Over 70 Cyberbaser

Vi skal forbedre forholdet mellom menneske, maskin og miljø

Vi skal være den foretrukne partner for integrerte løsninger og oppgraderinger

NATIONAL OILWELL VARCO
One Company . . . Unlimited Solutions

Sitat

**“We cannot change the human condition,
but we can change the conditions under which humans work”**

James Reason, professor of psychology, article Human error: Models and management)

NATIONAL OILWELL VARCO
One Company . . . Unlimited Solutions

Utvikling

- Få mennesket vekk fra boredekk
  - Drillers Cabin
    - Flere modeller
    - Større kabiner
    - Flere funksjoner
- Integrert maskin kontroll
  - Cyberbase
    - Mennesket i sentrum
    - Ett grensesnitt
    - En boremaskin

NATIONAL OILWELL VARCO
One Company . . . Unlimited Solutions

Utvikling

- Integrasjon
  - Integrerte operasjoner (rett info til rett person til rett tid, rett k
    - Falcon, eHawk
  - Integrerte systemer (hvem har ansvaret)
    - Interface mot 3.parts leverandør, MWD, ML etc
  - Integrert 3.parts kontroll (hvem har kontrollen)
    - Cyberlink
  - Integrert prosesskontroll (sikre kommunikasjon ogkontroll)
    - Drilltronics
  - Online Support (hva hvis oppgaven feiler
- Stadig økt grad av automasjon og integrasjon
  - Hvordan sikre kommunikasjon og kontroll?
  - Hvem har kontrollen, hvem har ansvaret?

NATIONAL OILWELL VARCO
One Company . . . Unlimited Solutions

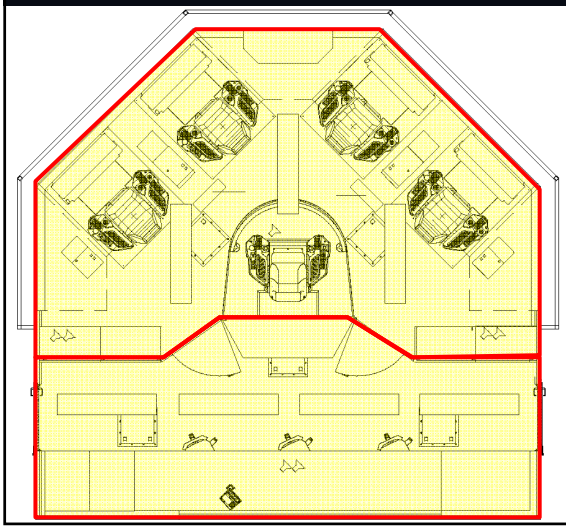
Drillers Cabin - Hovedfokus

- Sikkerhet
  - Plassering, gitter, rammer, materialer, trykk
  - Ex utgave eller som overtrykks rom
- Funksjon og oppgaver, layout
  - Optimal sikt, arbeidsro, oversikt og kontroll
- Støttefunksjoner
  - Kommunikasjon, vedlikehold, dokumentasjon
- Arbeidsmiljø
  - Ergonomi, lys, luft, lyd, temperatur, vibrasjoner
- Kravspesifikasjoner
  - Offentlig, bransje, kunde

NATIONAL OILWELL VARCO

One Company . . . Unlimited Solutions

Trender innen borekabiner – Layout #1

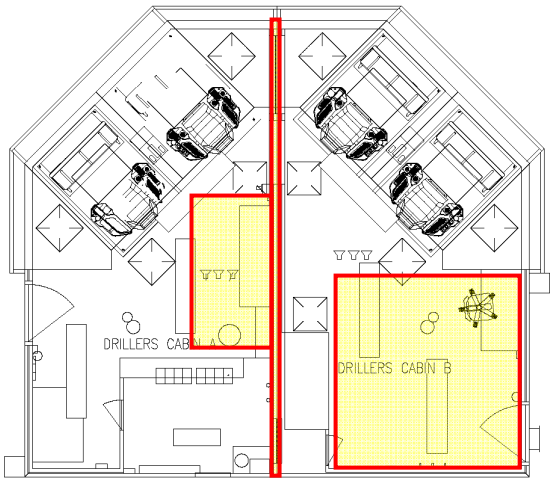


- Separat kontordel
- Glassvegg som fysisk skille
- Ingen skille i operativ del

NATIONAL OILWELL VARCO

One Company . . . Unlimited Solutions

Trender innen borekabiner – Layout #2

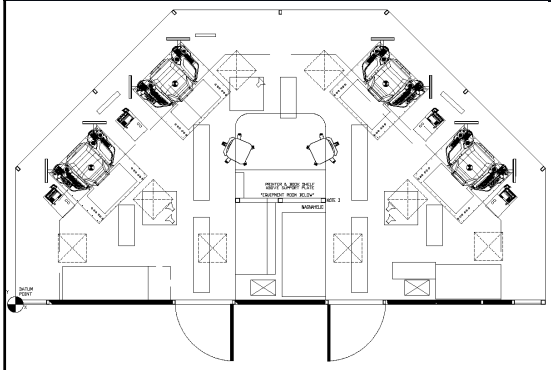


- Kontordel for hver kabin men ikke adskillt fra operatørene
- Fysisk skille mellom de to boreenhetene men med mulighet for åpne opp dør.

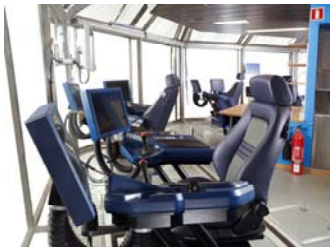
NATIONAL OILWELL VARCO

One Company . . . Unlimited Solutions

Trender innen borekabiner – Layout #3



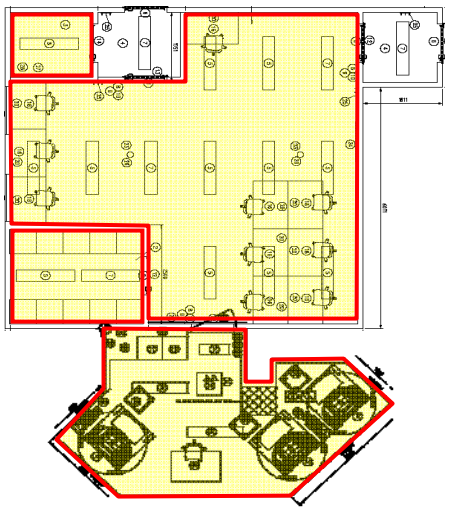
- Ett stort felles rom
- Ingen skiller mellom kontordel og operativ del



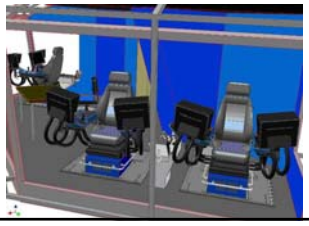
NATIONAL OILWELL VARCO

One Company . . . Unlimited Solutions

Trender innen borekabiner – Layout #4



- Egen operativ del
- Stor kontordel / operasjonssenter i tilknyttning til borekabin
- Eget toalett
- Utstyrsrom



NATIONAL OILWELL VARCO
One Company . . . Unlimited Solutions

Cyberbase: Hovedfokus

- Sikkerhet
  - Rømmingsmulighet
  - Feiltolerant system
  - Taktil tilbakemelding
- Oppgavefokus
  - Tilpasse til oppgaver
  - Ulik oppgavemodus
  - Siktlinjer
  - Maskin og prosess status
- Menneskesentert design
  - Ergonomisk utforming
  - Justerbarhet
  - Rollerball, trackerball, Joystick
  - Grafisk fremstilling

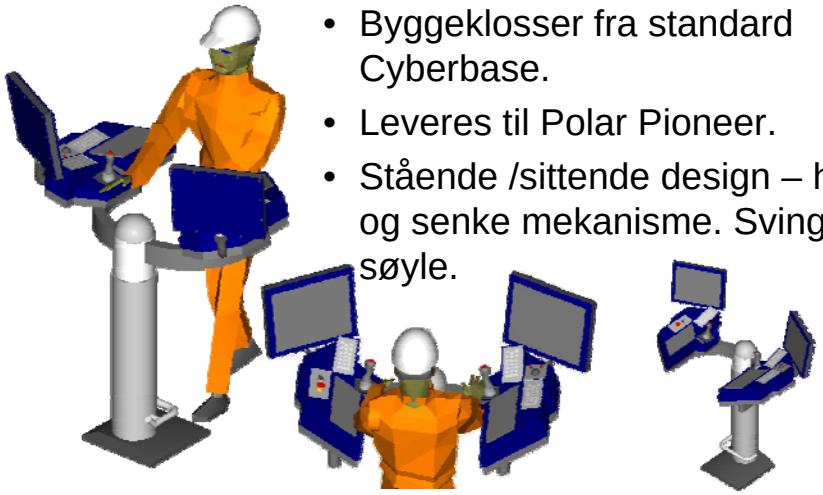
NATIONAL OILWELL VARCO
One Company . . . Unlimited Solutions

Oversikt Cyberbase

NATIONAL OILWELL VARCO

One Company . . . Unlimited Solutions

2009 Cyberbase for stående/sittende operasjon

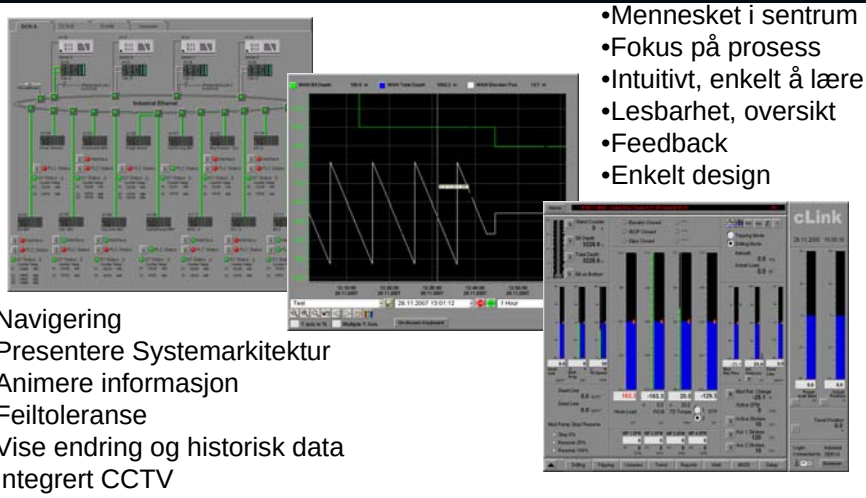


- Byggeklosser fra standard Cyberbase.
- Leveres til Polar Pioneer.
- Stående /sittende design – heve og senke mekanisme. Svingbar søyle.

NATIONAL OILWELL VARCO

One Company . . . Unlimited Solutions

HMI Displays: Hovedfokus



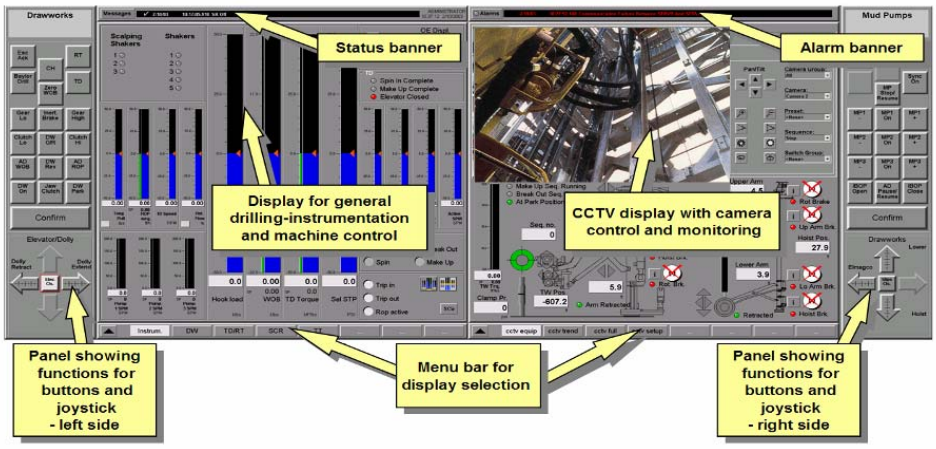
- Mennesket i sentrum
- Fokus på prosess
- Intuitivt, enkelt å lære
- Lesbarhet, oversikt
- Feedback
- Enkelt design

- Navigering
- Presentere Systemarkitektur
- Animere informasjon
- Feiltoleranse
- Vise endring og historisk data
- Integrert CCTV

NATIONAL OILWELL VARCO

One Company . . . Unlimited Solutions

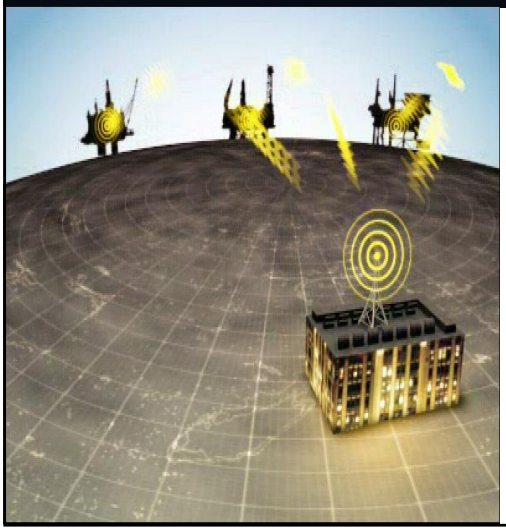
Eksempel HMI Displays



NATIONAL OILWELL VARCO

One Company . . . Unlimited Solutions

Bedre beslutningsstøtte... Integrasjon

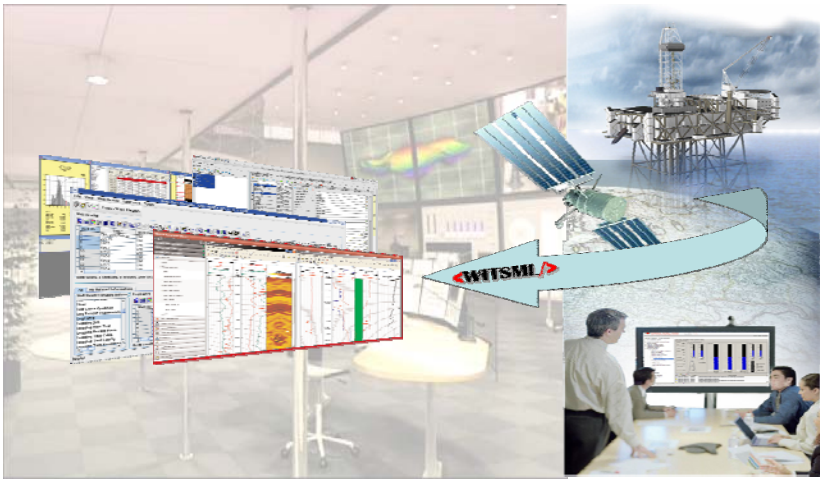


- Online support (eHawk)
- Integrerte operasjoner mot land (Falcon)
- Integrert prosesskontroll (Drilltronics)
- Integrerte 3.parts systemer (Eksterne leverandører av MWD, ML etc)
- Integrert ekstern kontroll (Cyberlink)

Online support: eHawk

- 24/7 operasjonsenter
  - Online assistanse
  - Fjerndiagnose,
  - Fintuning
  - Mindre korrigeringer
  - Software oppgraderinger
- Enkel oppkobling
- Kunden må godkjenne oppkoblingen, egne rutiner etableres

Forespørsel om informasjon: Falcon



NATIONAL OILWELL VARCO

One Company . . . Unlimited Solutions

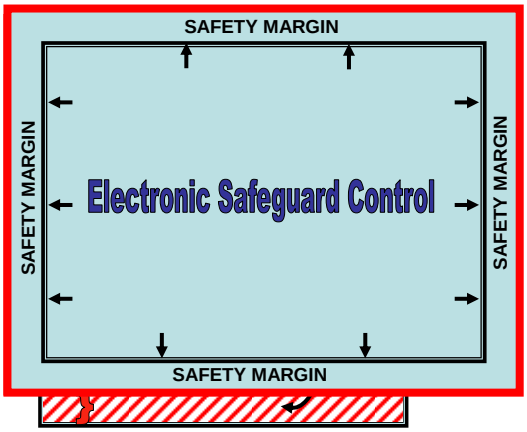
Forespørsel om aksjon: Cyberlink

NATIONAL OILWELL VARCO

One Company . . . Unlimited Solutions

Integrert prosesskontroll: Drilltronics

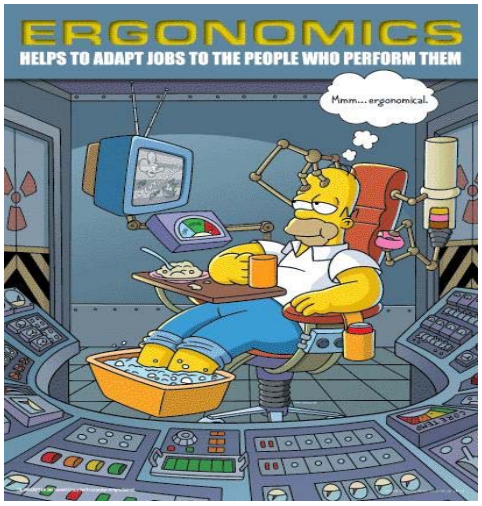
Når millisekundene teller...



NATIONAL OILWELL VARCO

One Company . . . Unlimited Solutions

HF Utfordringer



NATIONAL OILWELL VARCO

One Company . . . Unlimited Solutions

HF Utfordringer

- Mennesket – kilde til feil
- Mengde informasjon
  - Rett informasjon i rett format til rett person
  - Overbelastning
  - Aggregert og animert informasjon
- Opplæring og kompetanse
  - Krav til borer endres; raskere stigning i gradene, mer komplekse systemer
  - Rig spesifikke kurs, Bruk av simulator, Technical Training College
  - Komplekse og kritiske operasjoner
- Dokumentasjon
  - Tilgjengelighet for operatør
  - Endringer på site, korrekt ”as built”

NATIONAL OILWELL VARCO
One Company . . . Unlimited Solutions

HF Utfordringer

- Høy grad av automatisering
  - Allokering mellom menneske og maskin
  - Konsekvens for mennesket og prosess
  - Grad av automatikk
- Integrasjon
  - Hvem har kontrollen? Hvem har ansvaret?
  - Hvordan kommunisere?
  - Hvem har ansvaret for at integrasjonen er komplett?
- Alarmhåndtering
  - YA-710
- Større arealbehov i kabin
- Belastning, fysisk og kognitiv

NATIONAL OILWELL VARCO
One Company . . . Unlimited Solutions

- Ønsker dere mer informasjon om våre produkter, våre tanker om HMI og HF eller en omvisning, ta kontak så ordner vi det!
- **Tur til NOV sitt Cabin verksted:**
  - Buss frakter oss
  - Paul, Manager Cabins, tar imot oss
  - Det er lov å se, det er lov å røre, det er lov å prøve. Og ikke minst, det er lov å spørre
- Takk for meg og oppmerksomheten

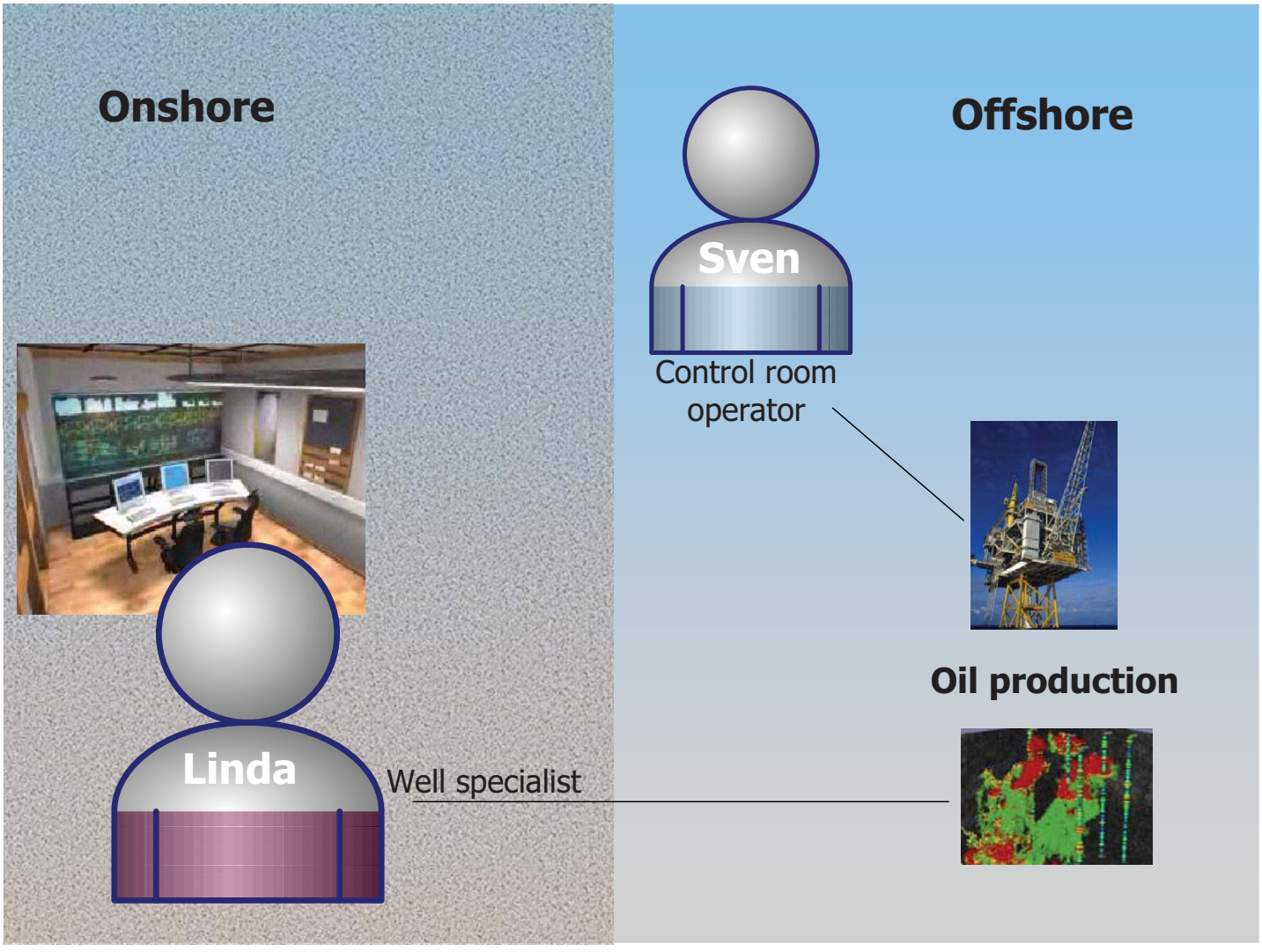
Besøk hos National Oilwell

Bilder fra middagen

Work surfaces for supporting interdisciplinary teams

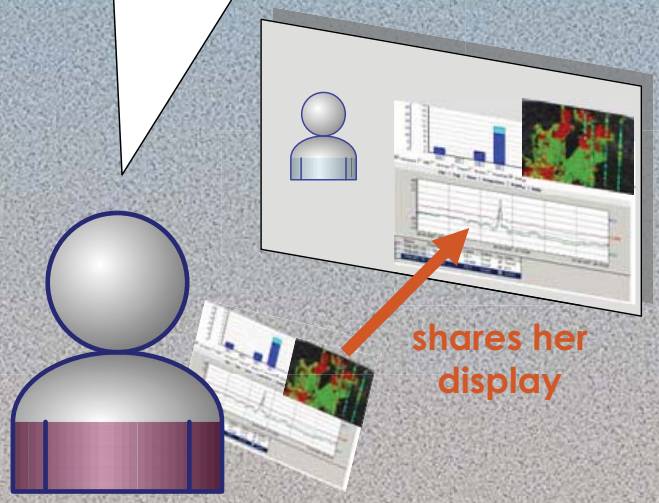
Gisle Andresen and Øystein Veland
Center for Integrated Operations

HFC forum 22-23 April, 2009



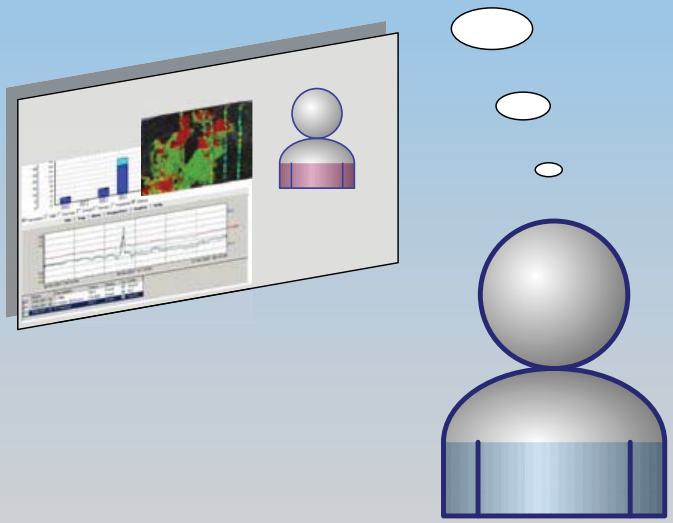
Linda:

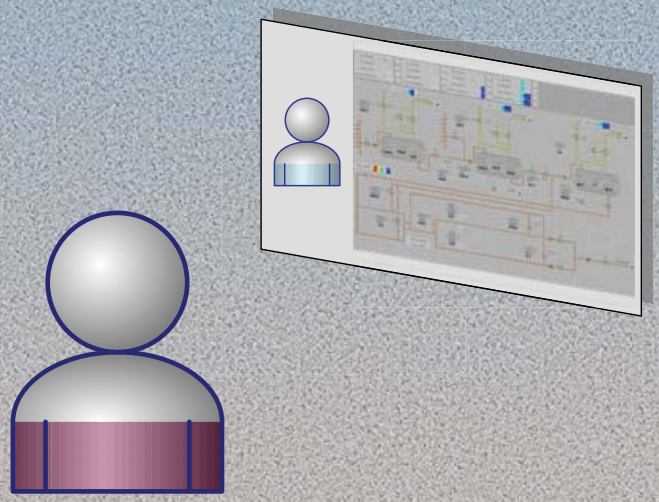
We recommend an increase of production from well 5 from 60% to 75%



shares her display

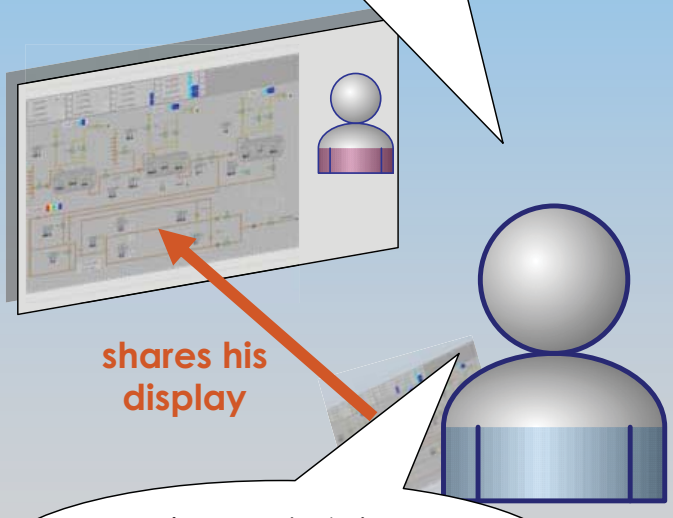
Such an increase will cause problems the way we are operating now...





Sven: Explains his concerns

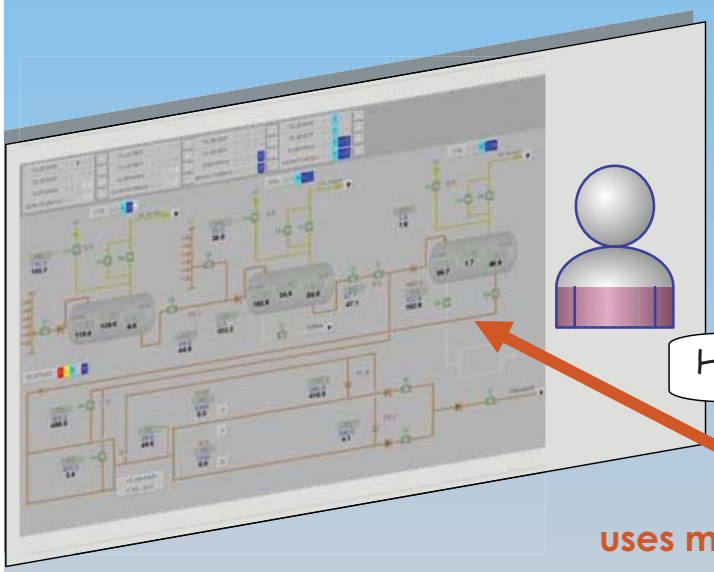
Look here -I'll tell you what the problem would be with that....



shares his display

I reality we don't have as much capacity as it may seem....

Sven works hard to get his message across



Things are more complicated than they think!

This display shows the problem

Here you can see....

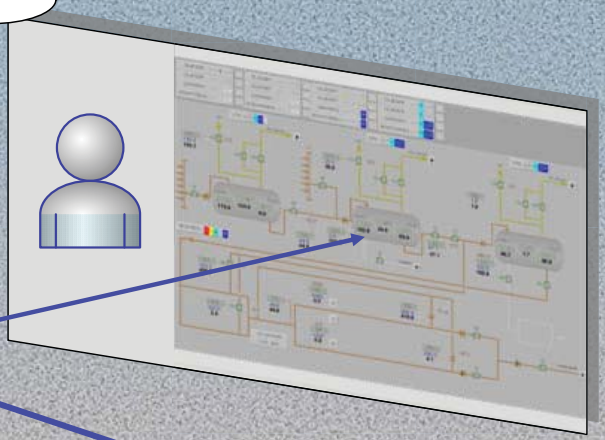
uses mouse to point and gesture

Maybe I should draw this on the Smartboard?

Linda's experience while Sven is talking...

What is he talking about now

This is far too detailed!



I still don't see the relevance

It's not so easy to ask ....

Disengagement

The result ....

I still don't see why this is such a big problem – we will go ahead

Well, just don't say I didn't warn you!

He's just worried there'll be a little more work for them...

disturbance

Shutdown

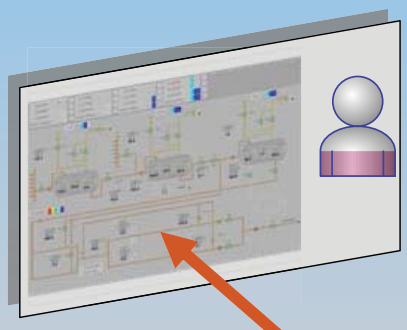
10 000 000

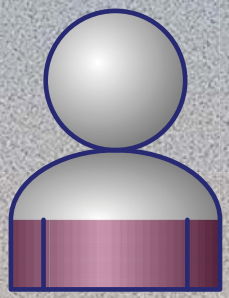
08.12

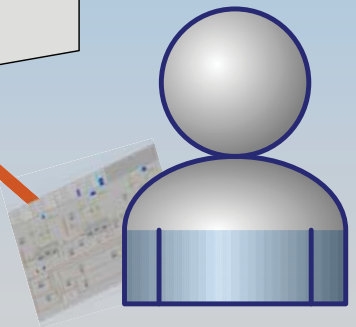
21.42

How does the design shape this collaboration?

Turn-taking







"My" displays and "your" displays
(from different "visual cultures"?)

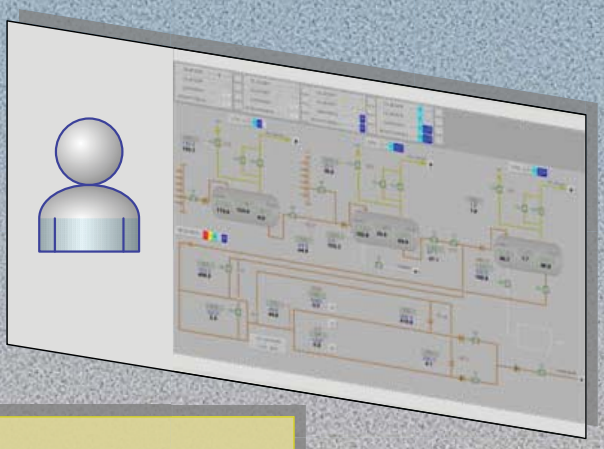
What are the problems?

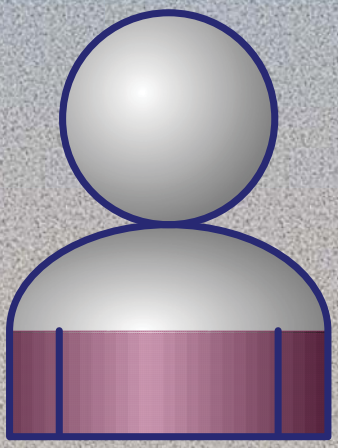
Inefficient mouse gestures

Poor readability

Missing information

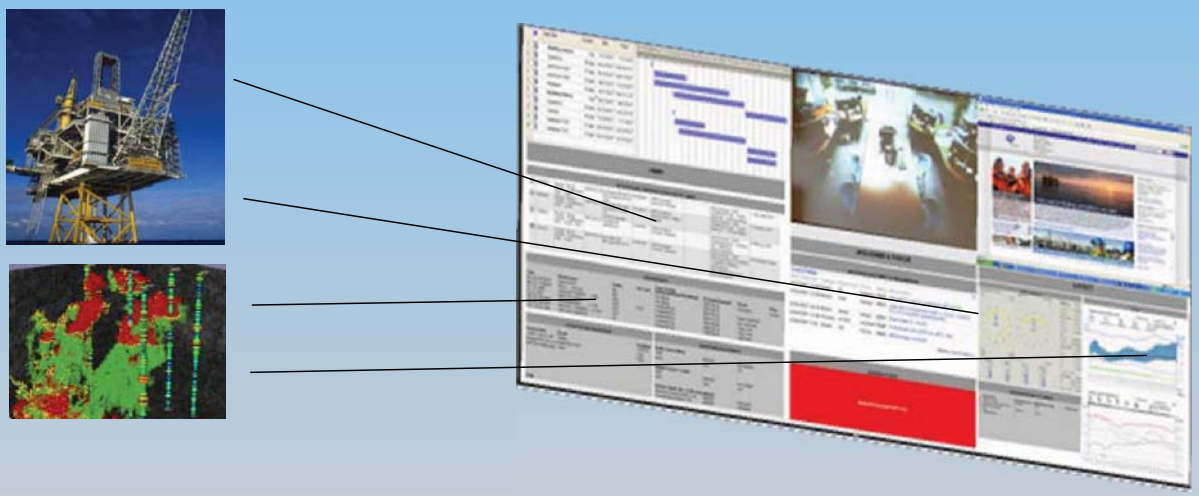
Inappropriate level of detail





Lack of referrability

Interdisciplinary collaboration surface



Fundamentally multi-user:

- Multiple perspectives mapped onto a common surface
- Easy to refer to verbally
- Part of a shared visual culture

Design is <u>situated</u> in current

- Physical environment
- Set of actors/disciplines involved
- Type of meeting
- ...

Theory

- Representation aiding
- Common ground

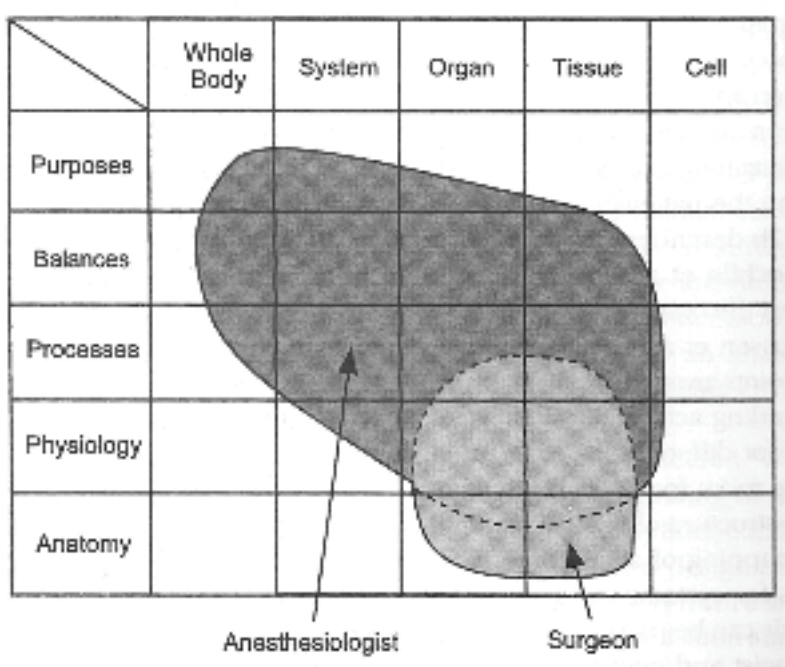
Representation aiding

- Turn a cognitive task into a perceptual task
- Offload human working memory onto an external representation

- Two main design activities
  - Content mapping
  - Form mapping

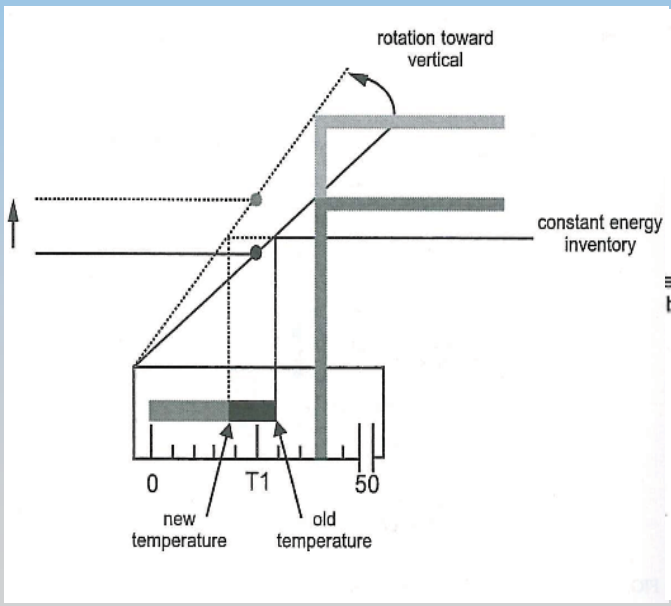
Representation aiding

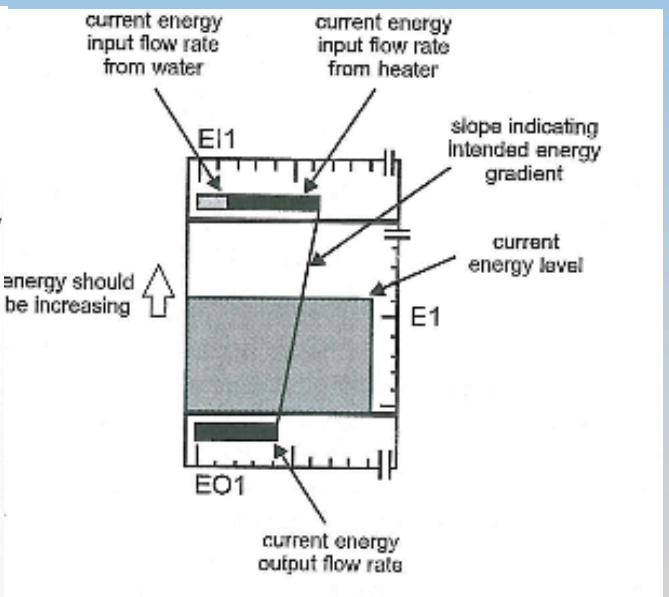
- Content mapping



Representation aiding

- Form mapping





Common ground

- Common ground (H. Clark): knowledge, assumption and information we know we share with other people
- Important elements of the theory
  - Shared basis
  - Grounding
  - Principle of least collaborative effort

Common ground

- Existing research indicates
  - CG is essential for distant collaboration
  - can explain failures of collaborative environments
  - can explain success of data-centric distant collaboration
- How can we use this theory?
  - A framework for analysis of collaboration
  - As a complement to existing theories on representation aiding (e.g., visual forms should minimize the effort needed for grounding)

Drifttagning av tekniska system

HFN intern workshop januari 2009

Domäner

- Flyg – flygtrafikledning, flygplatser, flygbolag, flygplanstillverkare
- Fordon allmänt
- Sjöfart
- Processindustri
- Verkstadsindustri
- Ledningssystem
- Medicinsk teknik

Intressanta frågeställningar

- Vilka aktörer påverkar HF vid driftsättning av tekniska system?
- Hur kan man stödja träning med inbyggd funktionalitet i tekniska system?
- Hur kan man stödja drift och underhåll med inbyggd funktionalitet i tekniska system?
- Hur kan man stödja en operatör som hamnat utanför ”loopen” (ex pga ouppmärksamhet eller blackout)?
- Vad bör man tänka på vid upprättandet av en designprocess för att stödja beslutsfattande som påverkar driftsättningen av system?

Förslag till kurs/workshop: Utveckling, drifttagning och utvärdering av tekniska system

- Inledande case från flera domäner (konkret)
- Från teknikutveckling, drifttagning till utvärdering (inkl ekonomisk alternativkostnad)
- Nya system och/eller förändring av gammalt
- Drivkrafter bakom system, design av system och interaktionsdesign i ett organisatoriskt perspektiv
- Metodik (för beställare och utvecklare), CRIOP m fl
- Varva teori och praktik
- Workshop, samarbete med HFC?

”Budskap”

- Systemtänkande: MTO
- Human Factors: framgångsfaktor
- HF: sunt förnuft men kräver expertis
- Det sista man ska behöva göra är att utbilda för att systemet är dåligt
- Tydliggöra processen, transparens för alla inblandade (input till beslutsfattande, aktiviteter etc)

CRM

Crew Resource Management

Bakgrund

- 1970-talet: Fler än 70% av flygolyckor beror på mänskligt felhandlande och inte teknik eller väder
- En NASA workshop konstaterade att majoriteten av besättningsfelen beror på brister i ledarskap, besättningssamordning och beslutsfattande
- Detta leder till utveckling av Cockpit Resource Management med träning i gruppdynamik, ledarskap, kommunikation och beslutsfattande
- I dag: Crew Resouce Management, CRM

CRM i dag

- Krav från ICAO på obligatorisk CRM-träning i flygbolag (f n i 185 länder)
- CRM-träning har börjat införas inom sjukvården (KI, Stockholm)
- Stort intresse från andra områden som sjöfart, industri (speciellt processindustri och kontrollrumsarbete)

Krav på innehåll i CRM-utbildning för piloter enligt JAA (2006)

- Human error and reliability, error chain, error prevention and detection
- Company safety culture, standard operating procedures, organisational factors
- Stress, stress management, fatigue and vigilance
- Information aquisition and processing, situation awareness and workload management
- Decision-making
- Communication and co-ordination inside and outside the cockpit

Krav på….. forts

- Leadership and team behavior synergy
- Automation (for type of aircraft)
- Specific type-related differences
- Case based studies

Exempel på kursmål för CRM-träning vid KI

Kursdeltagaren ska
-kunna kommunicera effektivt med patienten och övrig vårdpersonal
-kunna agera i rollen som ledare och följare i ett team
-kunna bidra till att genomföra etablerade rutiner och guidelines
-kunna understödja sviktande vitalfunktioner
-kunna tillkalla hjälp vid resursbrist

HFN CRM-seminarium 2008

Bo Johansson, Luftfartsstyrelsen : *Nya regler och riktlinjer*
Eric Wahren, Lunds universitet : *I huvudet på en CRM-instruktör*
Åsa Ek, Lunds universitet: *Säkerhetskultur – är det mätbart?*
Stefan Jern, Lunds universitet: *Grupper och gruppdynamik*
Ingrid Anderzen, Uppsala universitet : *Vardagsstress: Hur påverkar Vardagsstress min arbetssituation?*
Carl-Johan Wallin, Karolinska universitetssjukhuset: *Projekt att införa CRM i hälso- och sjukvården*

BORESIMULATOR - HVORDAN KAN DEN BIDRA TIL VARSLING FØR KRITISKE HENDELSER

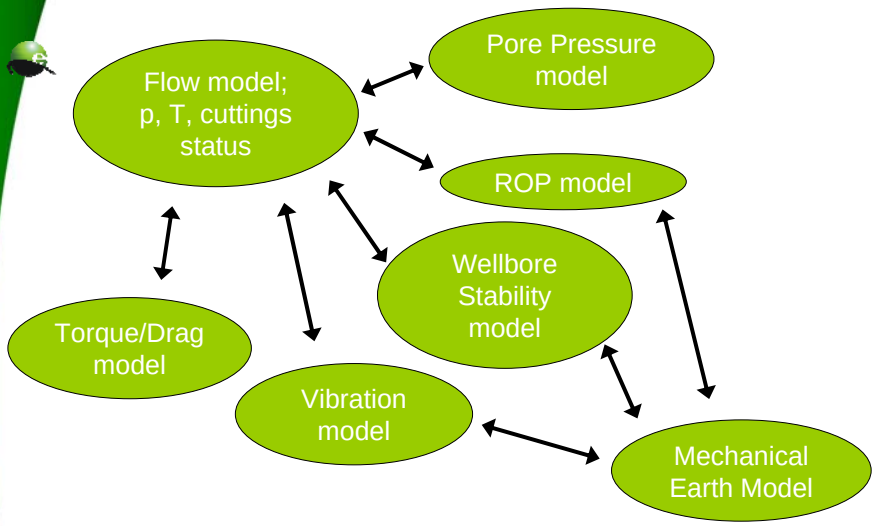
ROLV ROMMETVEIT, EDRILLING SOLUTIONS AS

«Make the invisible, visible»
«Make the impossible, possible»

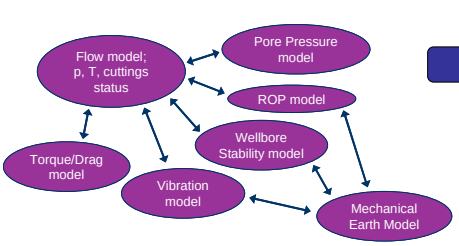
Business Case

- Goal
  - Reduce costly well problems (several billion NOK per year only in Norway!)
  - Lost circulation, reduction by 30%
  - Back reaming problems (stuck pipe, etc), reduction by 20%
  - Kick situations, reduction by 20%
- Tools:
  - Advanced visualization
  - Drilling “flight” simulator (test, train, analyze, perform)
  - Smarter use of drilling data
  - Diagnosis and advisory tools

Integrated Drilling Simulator IDS



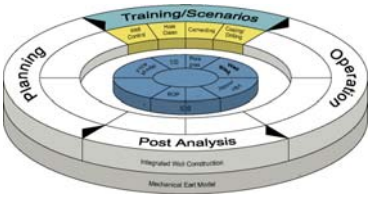
IDS is basis for drilling process modeling



Jarring
Well Control
Fishing
Casing drilling
TTRD
MPD
Interventions
Cementing
Drilling
ECD management
UBD
Tripping
Completions
Casing running

Integrated Drilling Simulator Vision

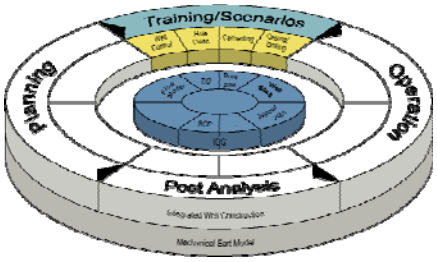
- Integrated Drilling Simulator
  - Integrated state-of-the-art drilling process models, transient and steady state
- Use
  - Planning and training:
    - *Testing of drilling plan*
    - *Drill the well on computer first*
  - Real time link to operations:
    - *Drilling supervision & control*
    - *Forward simulations*
    - *Diagnosis and advice*
  - Post analysis
    - *Efficient use of experience*
    - *Update model for future wells*
  - Advanced visualization; look downhole, virtual drilling
  - Link to earth model

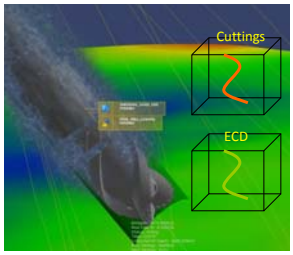


eDrilling Solutions

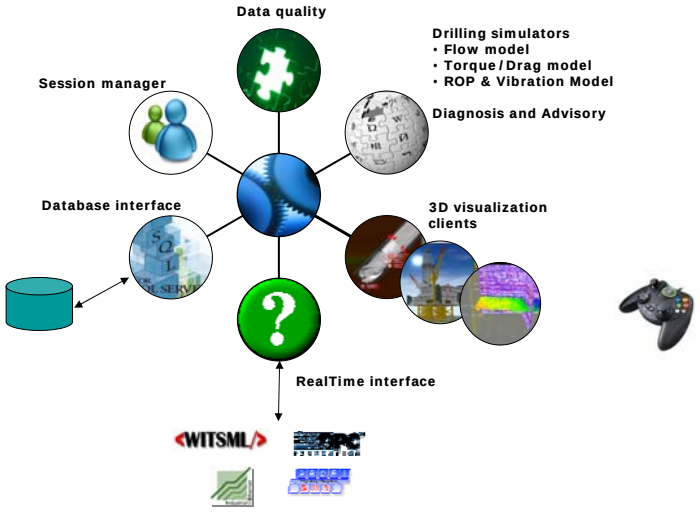
- Shall commercialise Integrated Systems within Intelligent Drilling & Well Operations
- Close R&D cooperation with SINTEF
- Integrated Drilling Simulator IDS is a key basis technology for the company

- Products in eDrilling Solutions:
  - **eDrilling (decision support)**
  - iTraining (Virtual Training)
  - eControl (drilling automation)
  - Complex Operations Control
  - ePlanning
  - Integrated MPD Systems



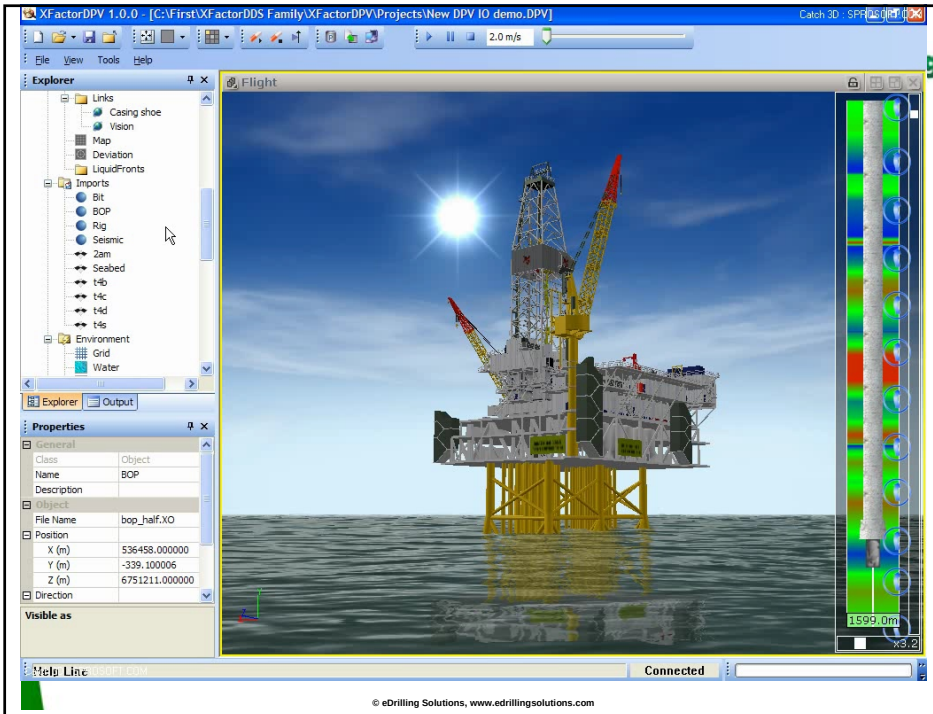


Game technology

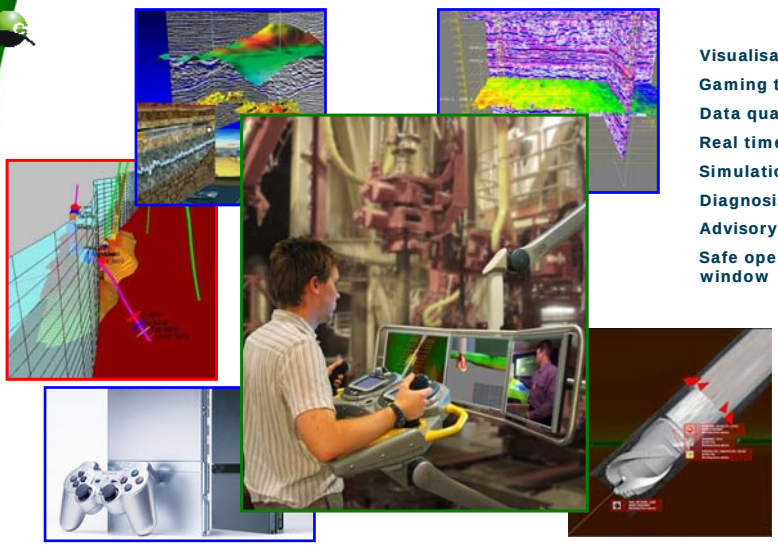


BENEFITS

- Significant reduction in Non Productive Time
  - Technical sidesteps cost Statoil Hydro >1 Billion NOK per year
  - Stuck pipe and well stability; keep hole clean!
  - Train to identify early severe proplems, and prevent them!
  - Train how to solve problems optimally
- More efficient implementation of new work processes
- More optimal well construction
- More professional problem handling
- Improved HSE through training and simulation



eDrilling; RT Decision support



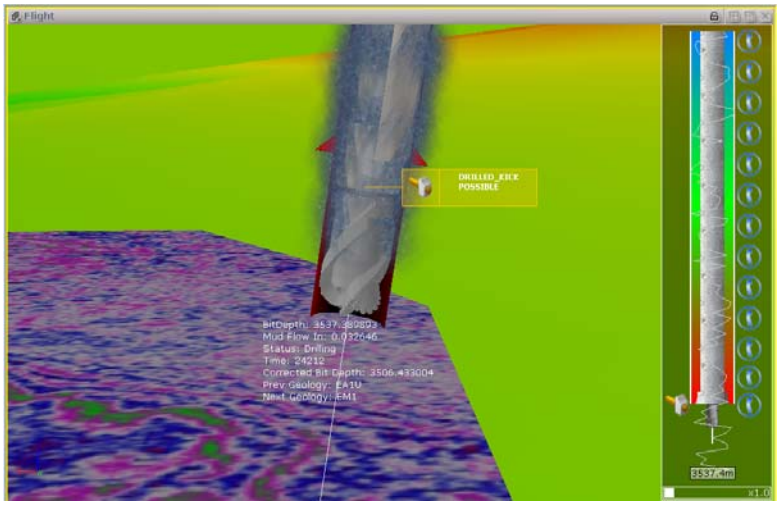
- Visualisation
- Gaming technology
- Data quality models
- Real time modelling
- Simulation
- Diagnosis
- Advisory technology
- Safe operating window

Diagnosis and Advisory

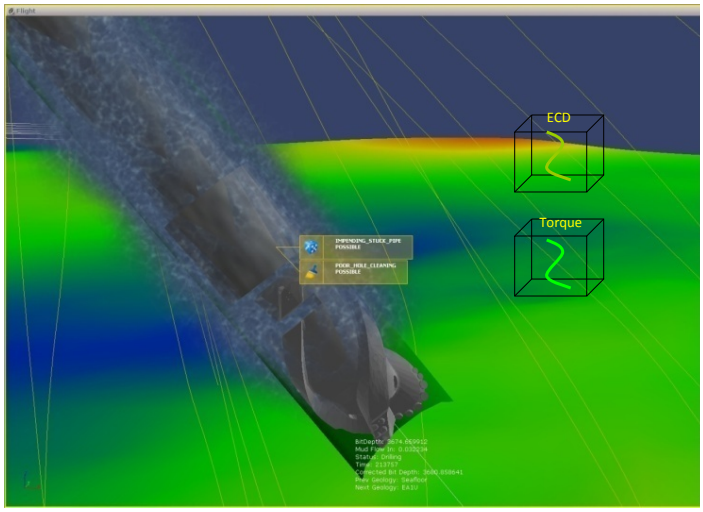
- Advisory based on:
  - Forward looking
  - Feedback from the well.
  - Diagnostics modules
  - Optimization algorithms

Diagnosis Warnings	Symbol
Unexpected sensor values	
Kick	
Loss	
Tripping velocity limit	
Impending stuck pipe	
Poor hole cleaning	
Washout	
Tight spot	
Instability	
Low ROP	
Non optimal WOB	

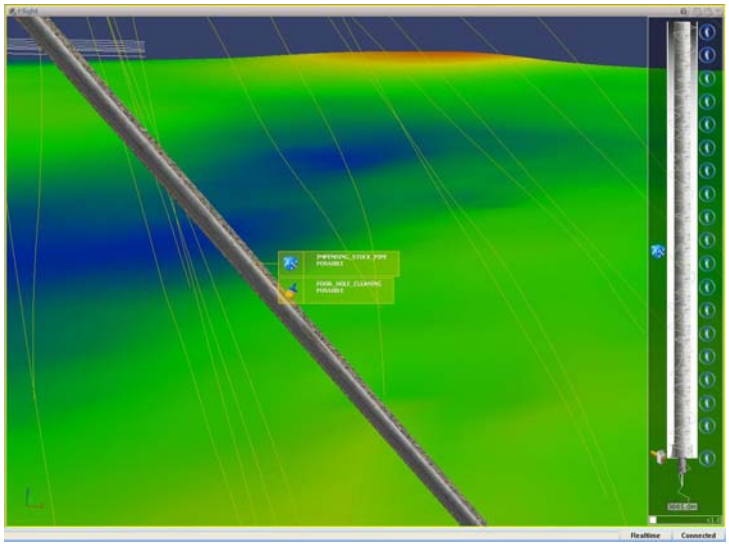
Decision support (Virtual)



Possible stuck pipe



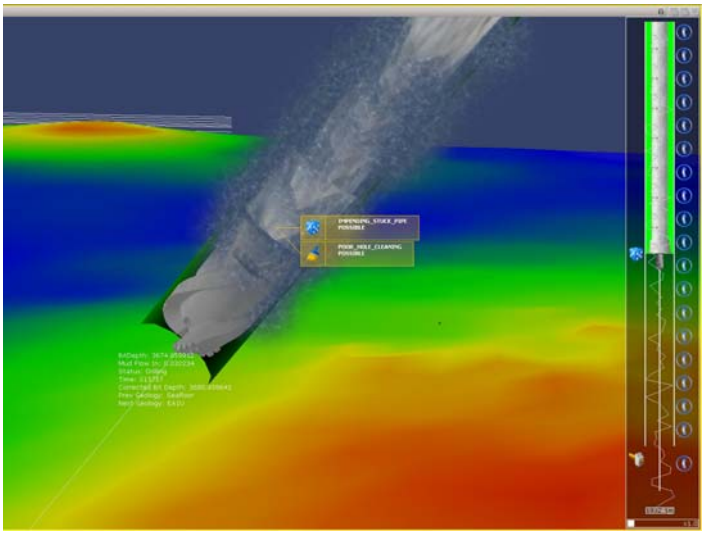
Possible stuck pipe



Simulator training environment

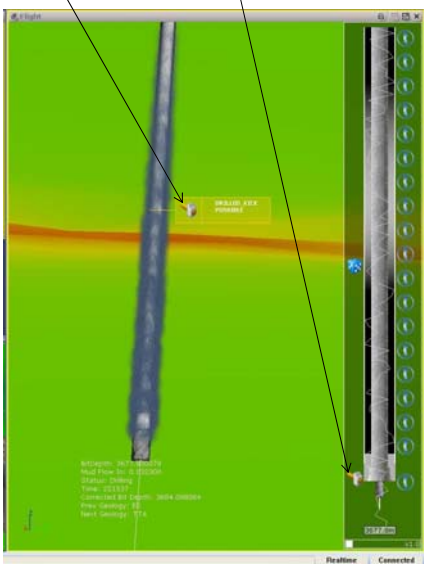
BHA element passing shoe

Possible stuck pipe



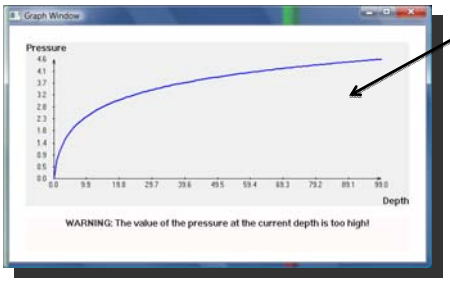
Hich Cuttings concentrations

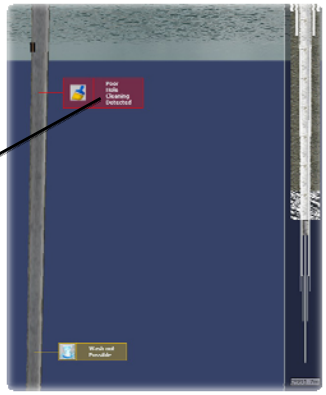
Kick warnings



Supervision and diagnostics

- When clicking an icon in the 3D view, it will bring up a window containing reason for the warning. It can be a short report or trends etc.

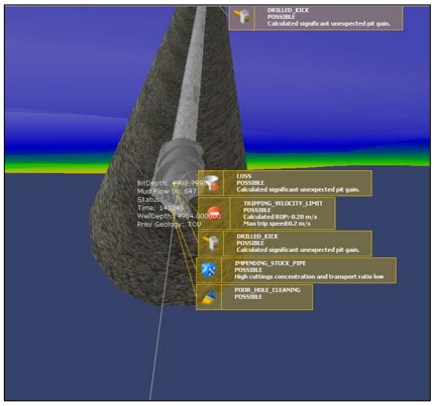




2D for analysis

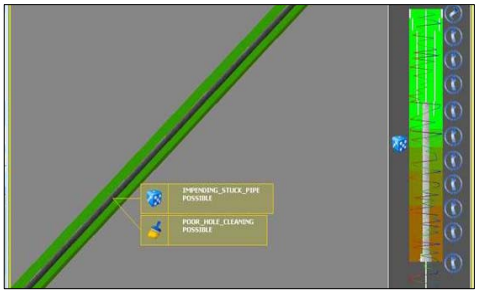
Warnings on Kick

- Kick experienced on June 16, at 13:00
- eDrilling gave one warning at 11:15
- eDrilling gave a series of warnings on kick starting at 13:00



Warnings on Poor Hole Cleaning

- eDrilling gave several warnings on poor hole cleaning in the time before May 14
- Warnings were based on calculated concentration of cuttings, and cuttings transport ratio

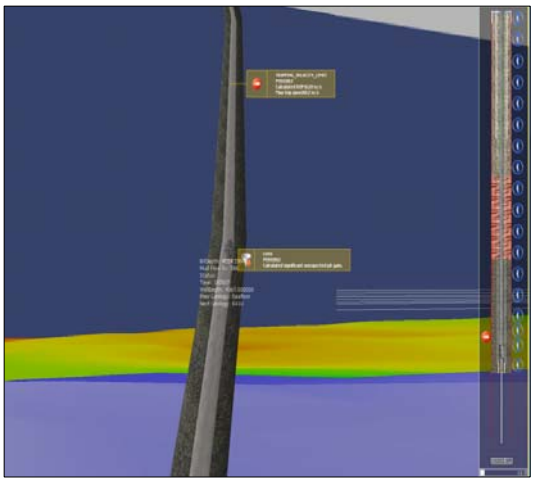


Impending
Stuck pipe possible

Pore
Hole cleaning

Detection of Loss

- Formation pore pressure data was updated manually with pressure points from drilling
- eDrilling gave warnings on loss while drilling in reservoir around June 23



Virtual PWD

- 17.06.2008: Problems with MWD during crucial phase of reservoir drilling due to tool failure
- Resulted in POOH (one day delay)
- eDrilling had accurate real-time simulations running all the time
  - Calculated properties had been verified against measured values before tool failure
  - Static calculations were very accurate
  - Dynamic calculations suffer slightly from configuration data of varying quality, but deviation is constant

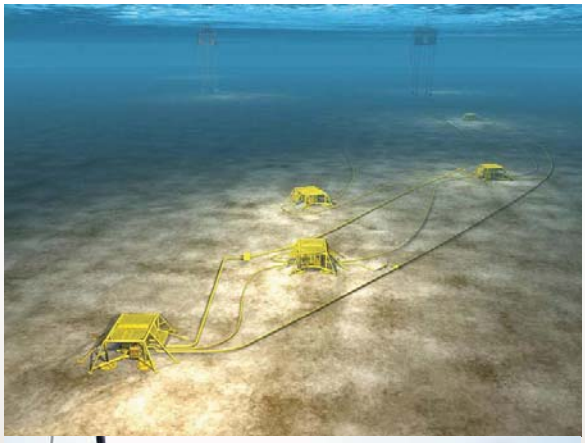
→Save one trip (30 hours saving)

Pilot Activity Summary

Use of eDrilling during replay with correct input data

- WOB significantly improved
- ROP problem not analyzed
  - ROP Module needs improvement
- Gas influx
  - **Early detection**
- Lost Circulation
  - **Early detection**
- Hole cleaning problems
  - **Correct early warnings issued**
- ECD prediction
  - **Model updated**
  - **Predictions Correct – necessary for Lost Circulation and Gas Warnings**
  - **Could have been used as ”virtual PWD” when PWD malfunctioned! 30 hours of tripping could have been saved**

Human Factor in Subsea Controls



Roald Loug Hansen
Leading Adviser Subsea Control Systems
roloha@statoilhydro.com

StatoilHydro

Topics

- Subsea ➔ Integrated Operations and other reflections
- Condition monitoring ➔ Subsea perspective
- Condition monitoring ➔ Subsurface perspective

StatoilHydro

Mission

Enable limitless Subsea

Communication and Control

for maximum, safe and environmentally

friendly field life value.

Strategic Fit

Subsea and Integrated Operations

Real time competence sharing is necessary in a complex and demanding industry. It is all about integrated operations and people in a seamless collaboration, independent of organisation, time and place.

H. Lund, 25th February 2008

Is the E-Field-/Integrated Operations and automation, challenging for Subsea Fields?

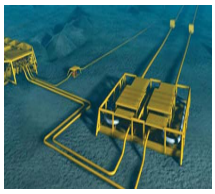
Taking subsea technology further

- Subsea processing
- Subsea wet gas compression
- Long-distance well stream transport

Lufeng 1996
subsea boosting

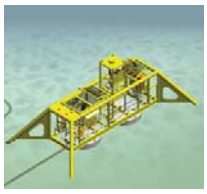
Troll Pilot 1999
subsea separation

Ormen Lange Snøhvit 2007
subsea to shore



Tordis 2007
subsea processing

Tyrihans 2009
seawater injection



Åsgard 2013
Ormen Lange 2015
subsea compression

StatoilHydro

IO-Challenges for the Subsea control system

To reach IO-goals and to drive change for the Subsea control system we have to focused both on:

a)Technology change

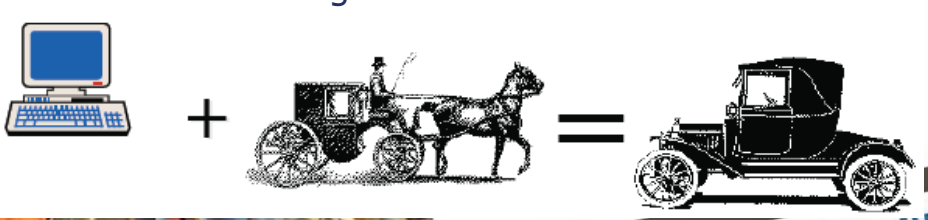
b)Human factor change

Be aware of:

History driven organisation

New technology

Limited results

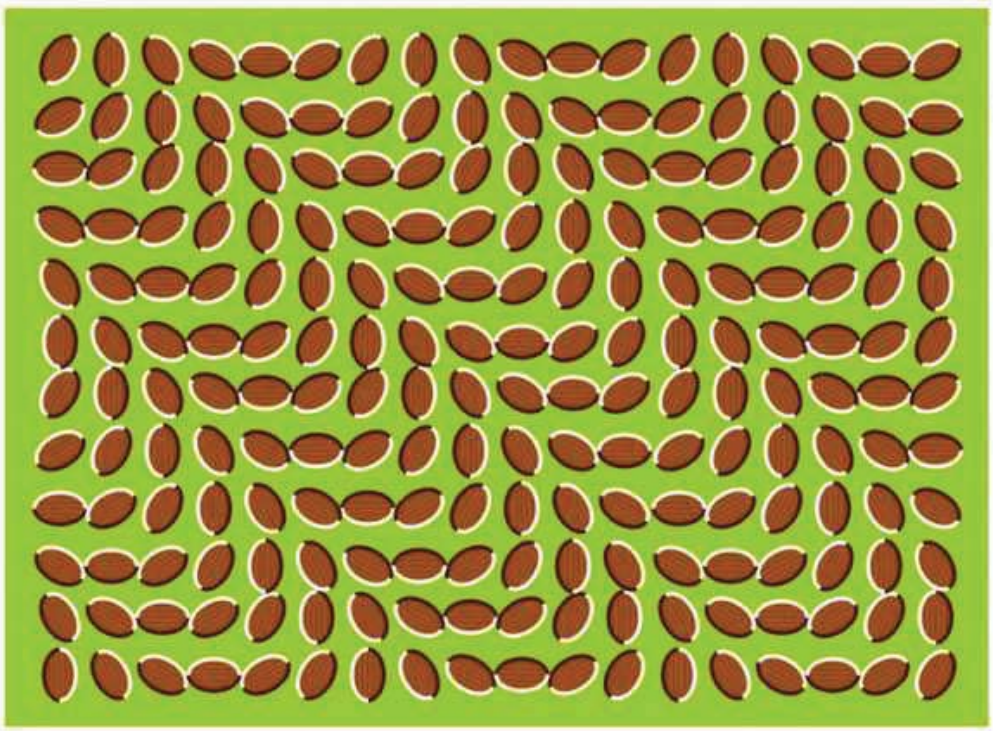


StatoilHydro

Fact of life

- We observe 10000000-15000000 bit/s
- Bandwidth interpretation is 10-30 bit/s
- We are extreme good at selection, presuming,

Interpretation



Keywords

- Subsea ➔ Integrated Operations and other reflections
- Condition monitoring ➔ Subsea perspective
- Condition monitoring ➔ Subsurface perspective

What do we mean by condition monitoring?

Some statements from the World Wide Web…

".. techniques to maximise equipment performance and throughput.."

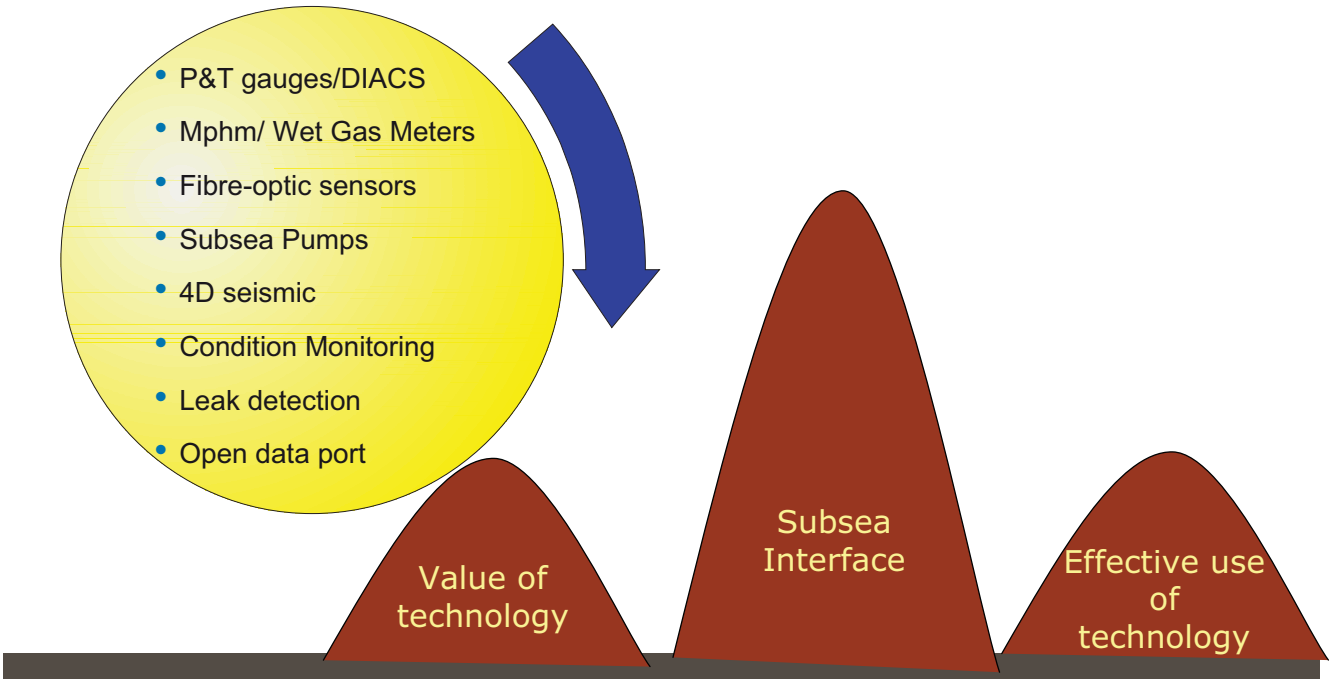
"…the use of advanced technologies in order to determine equipment condition.."

".. capable of determining and locating any evolving error.."

".. A major component of predictive maintenance"

".. allows maintenance to be scheduled .."

Urgent Interface requirements for Subsea Production Control Systems



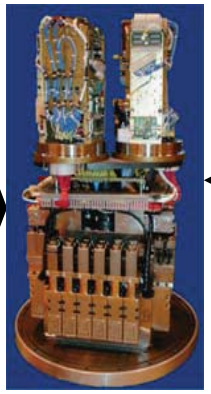
StatoilHydro

Technology gap example

Advanced 3rd party IOR Systems

Broadband Comm. Open Protocols

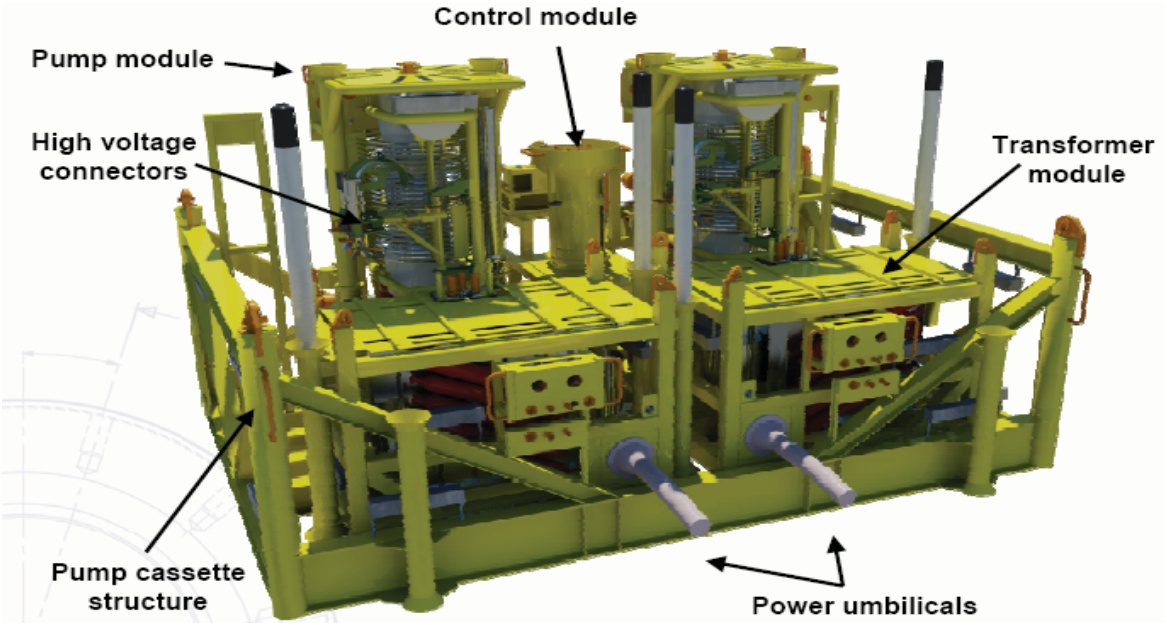
Subsea Control Module



What?
When?

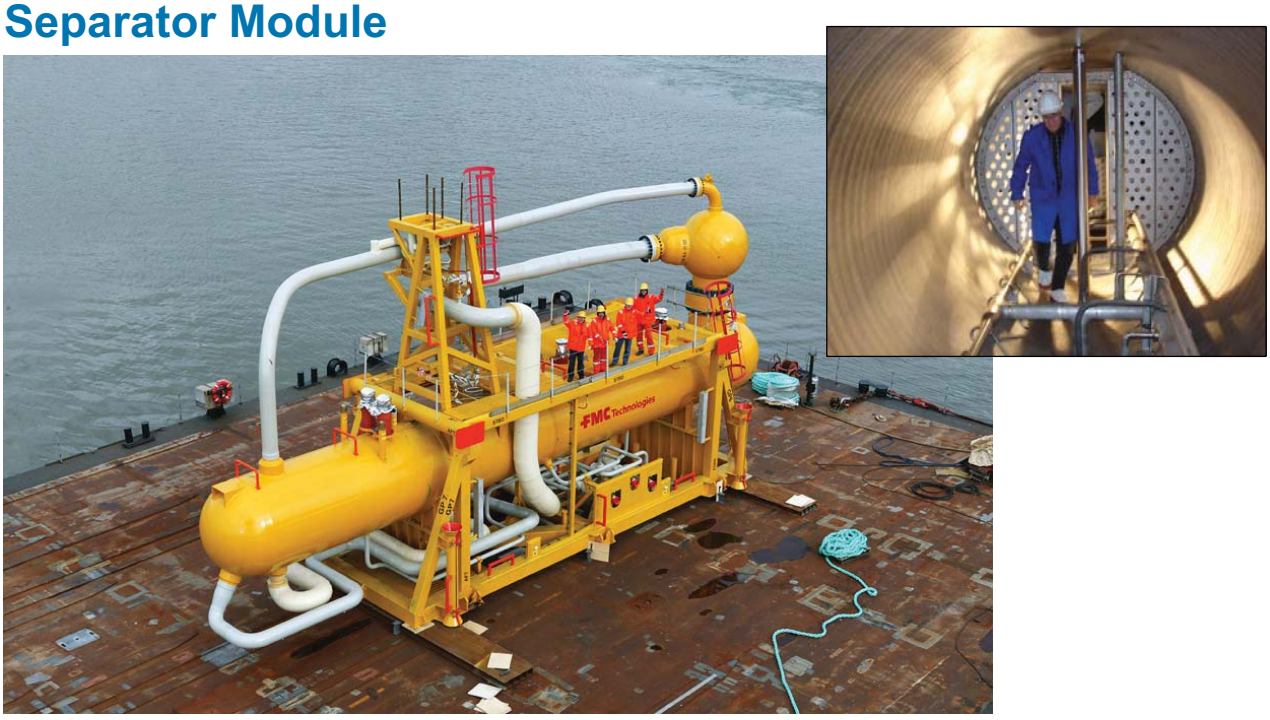
- Limited bandwidth 2400 Bit/s
- Proprietary protocols

Raw seawater injection system



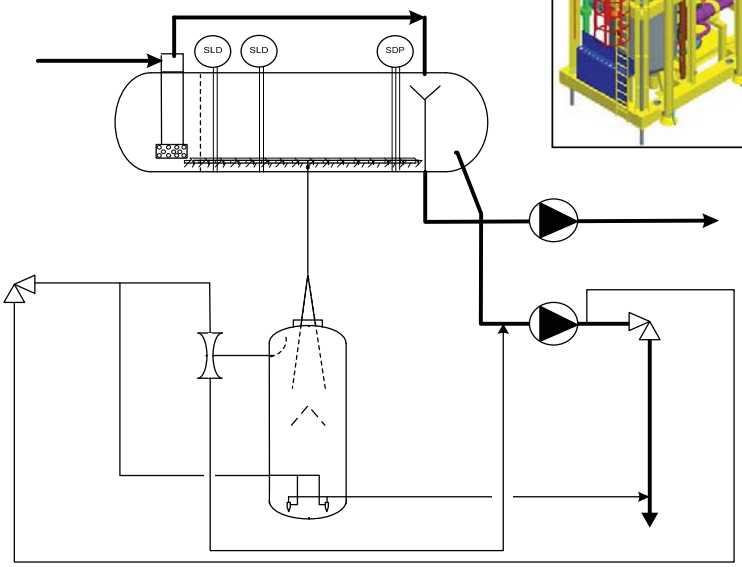
StatoilHydro

Separator Module



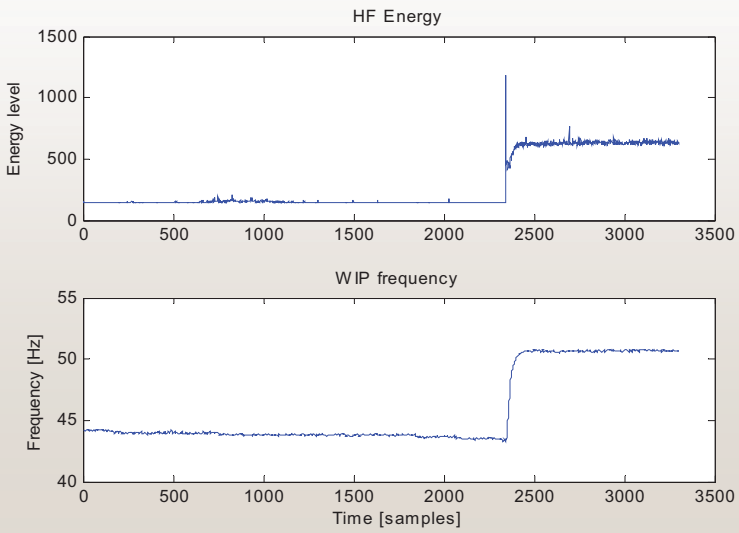
StatoilHydro

Desander Module



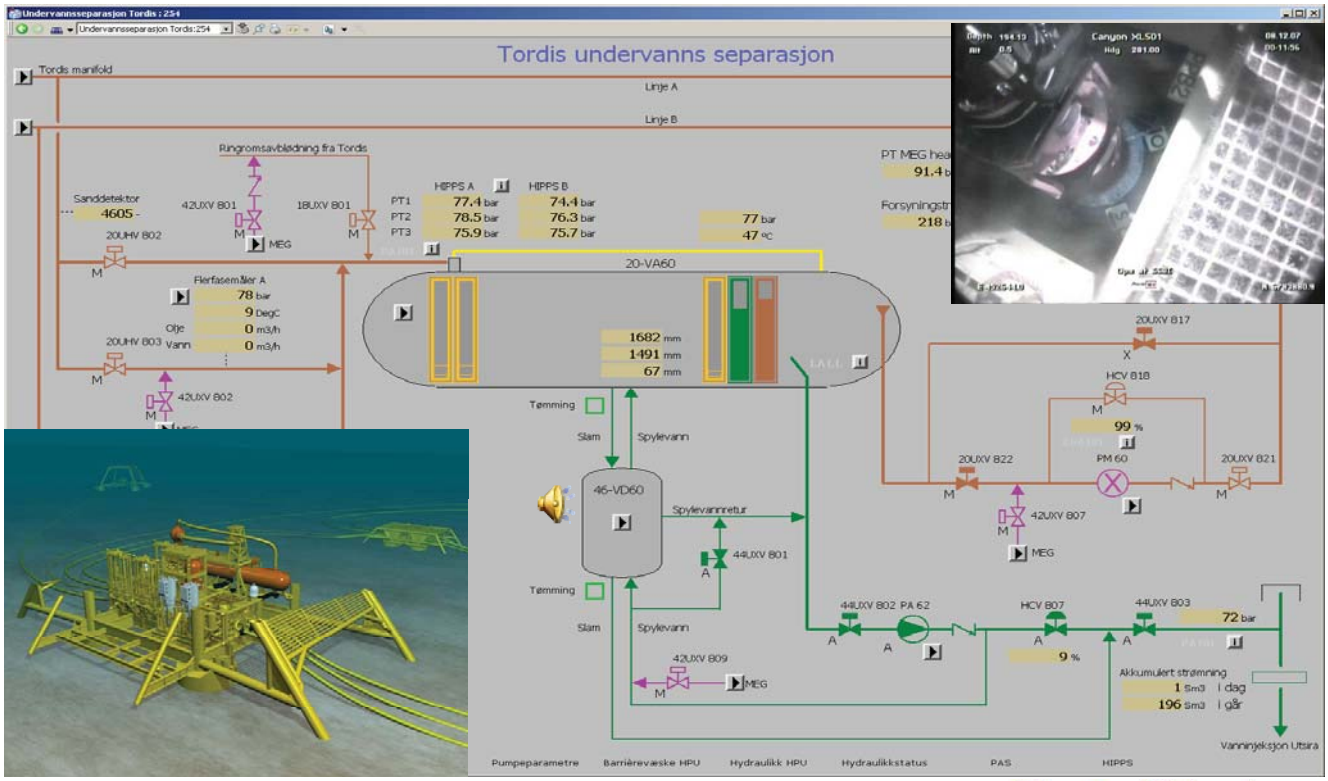
StatoilHydro

28.01.2008 kl. 21:30
Oppstart av ?

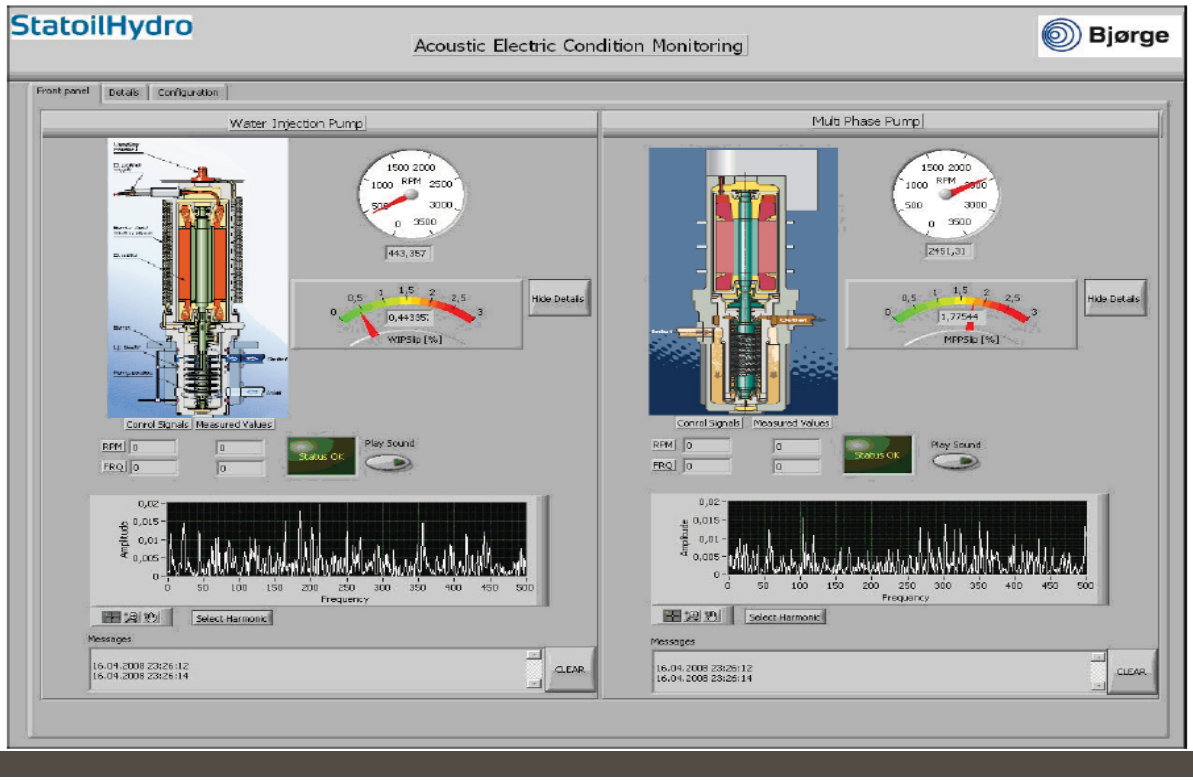


StatoilHydro

Limitless remote monitoring and control



StatoilHydro

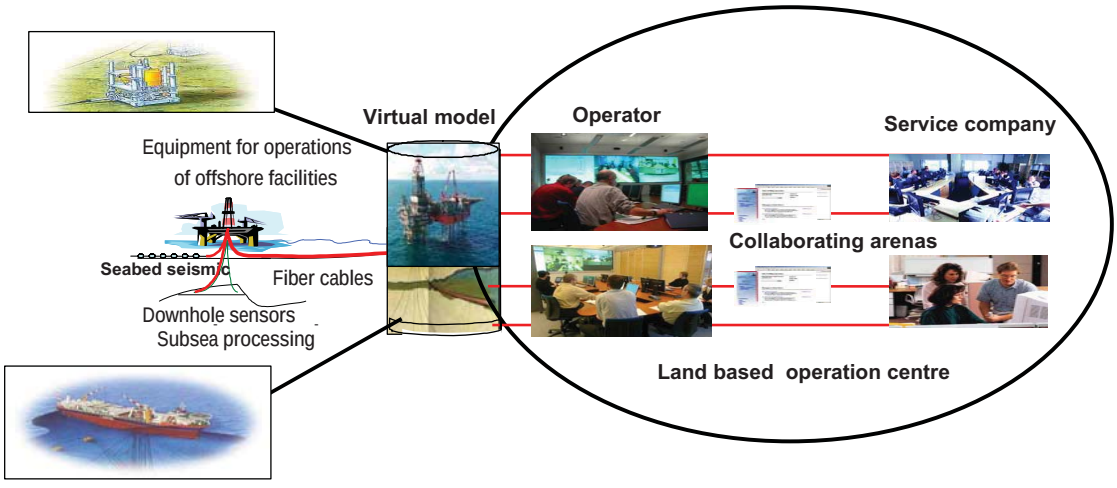


StatoilHydro

Keywords

- Subsea ➔ Integrated Operations and other reflections
- Condition monitoring ➔ Subsea perspective
- Condition monitoring ➔ Subsurface perspective

Remote Operation of wells and subsea facilities

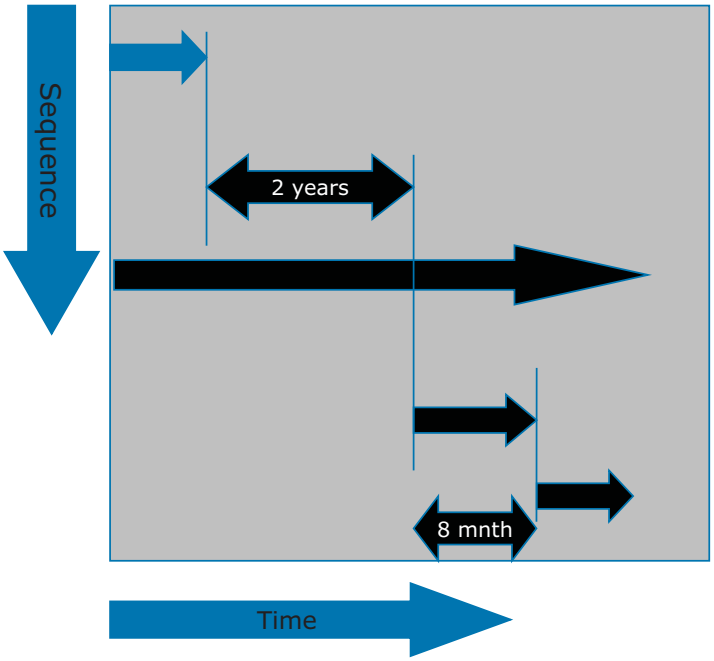


Mission

Enable limitless Subsea
Communication and Control
for maximum, safe and environmentally
friendly field life value.

Typical equipment purchase schedule – Subsea projects

- Subsea equipment purchase
  - B&B personnel consulted
- Subsurface well planning
- Completion equipment purchase
- Install completion

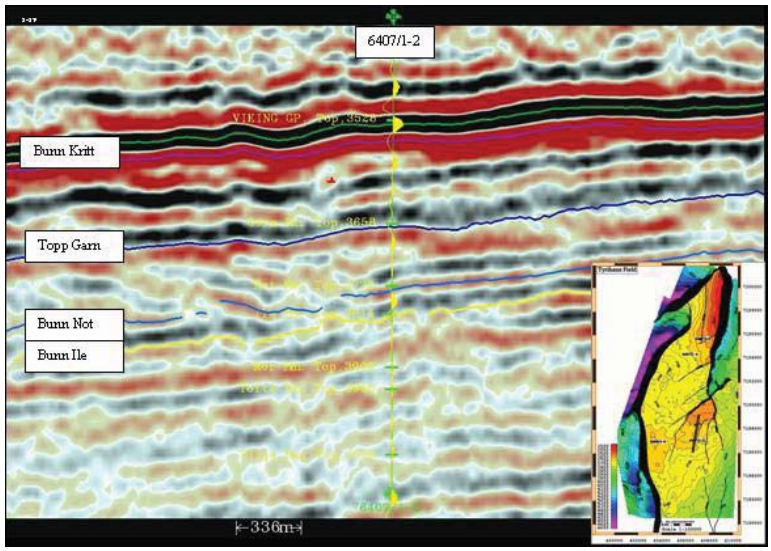


Why Control System Upgrade, an Example

Seismic data
– a clear picture of what to produce?

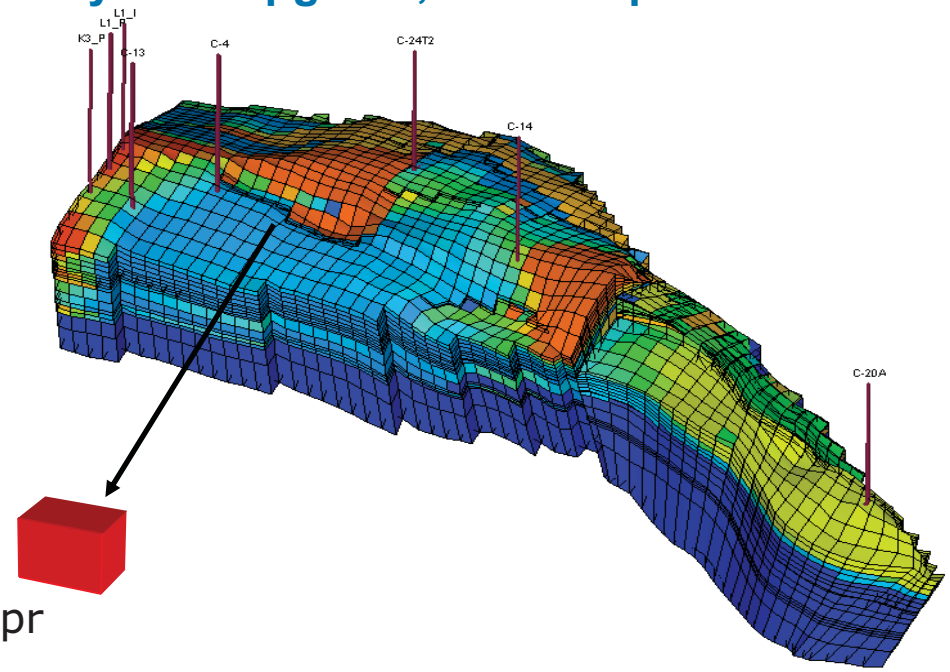
Why Control System Upgrade, an Example

- Exploration well data



Why Control System Upgrade, an Example

Modell of reservoir



Parameters pr element

Why Control System Upgrade, an example

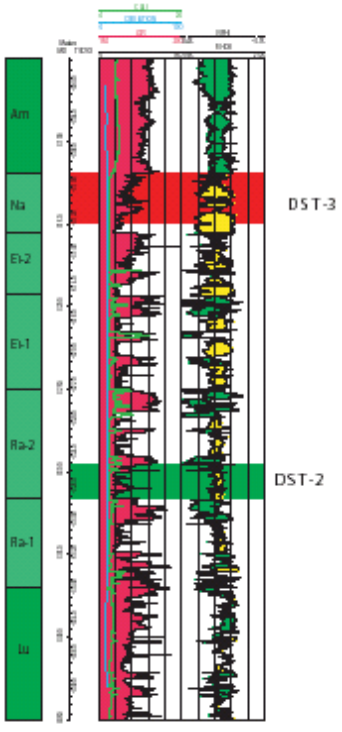
The model ends up with one answer

High Low

- Parameters are assumed and based on seismic experience and exploration well data.

- A log in the model will look like this.

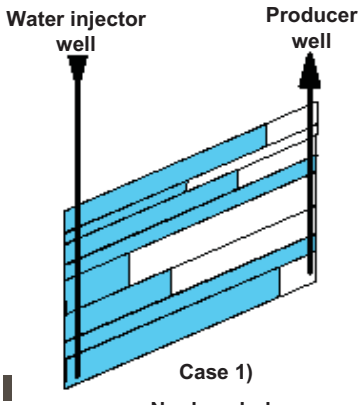
- But the reality is like this



Subsea well condition monitoring

Goal: Optimal drainage

Conventional
No downhole control

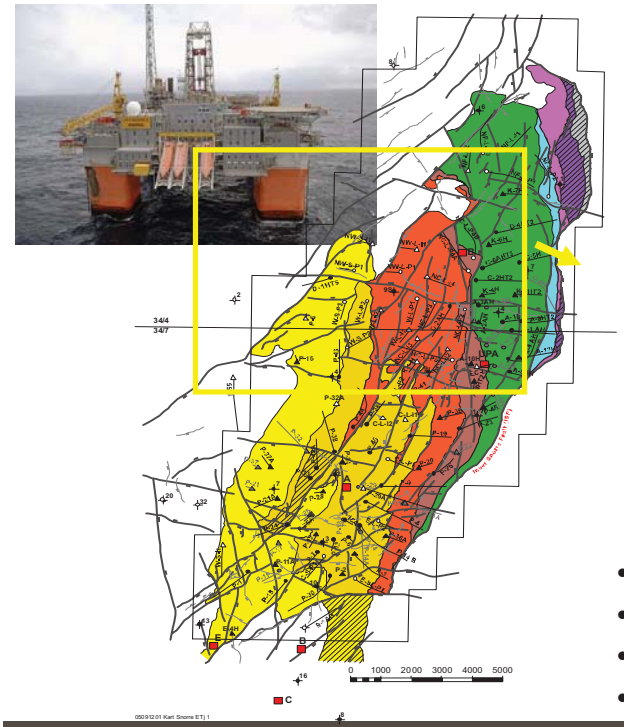


Case 1)

No downhole instrument & control

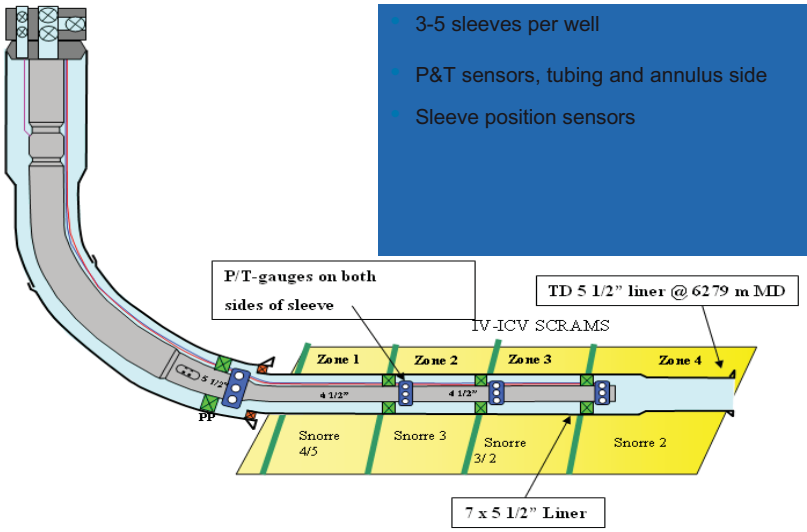
StatoilHydro

Map of the Snorre Field



- Production vessel with drilling facilities
- 4 templates: 26 slots (16 Prod +10 Inj)
- 17 planned smart well completions
- Production start 2001

Typical Snorre B Smart Well



- 3-5 sleeves per well
- P&T sensors, tubing and annulus side
- Sleeve position sensors

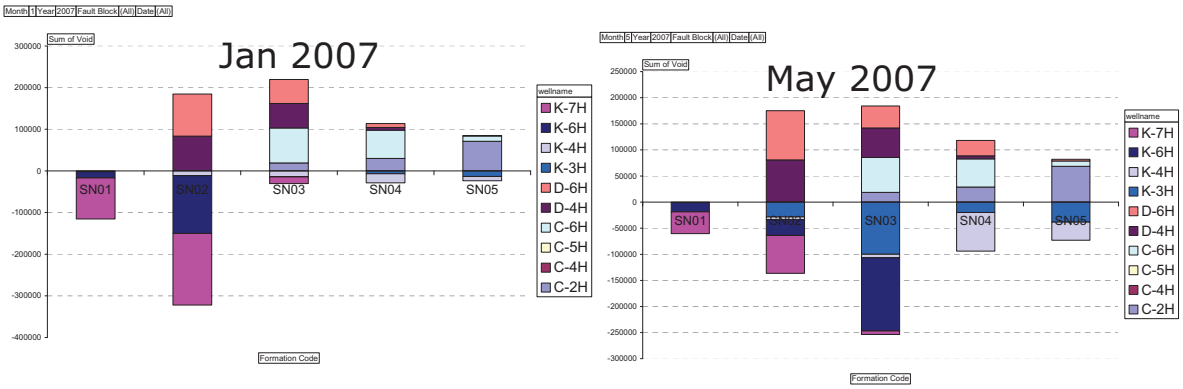
The 11 installed smart wells have in total 40 sleeves

- Monitoring challenge equal to that of 40 wells

StatoilHydro

From Analysis to Action SnB

Able to change injection profile to improve voidage:

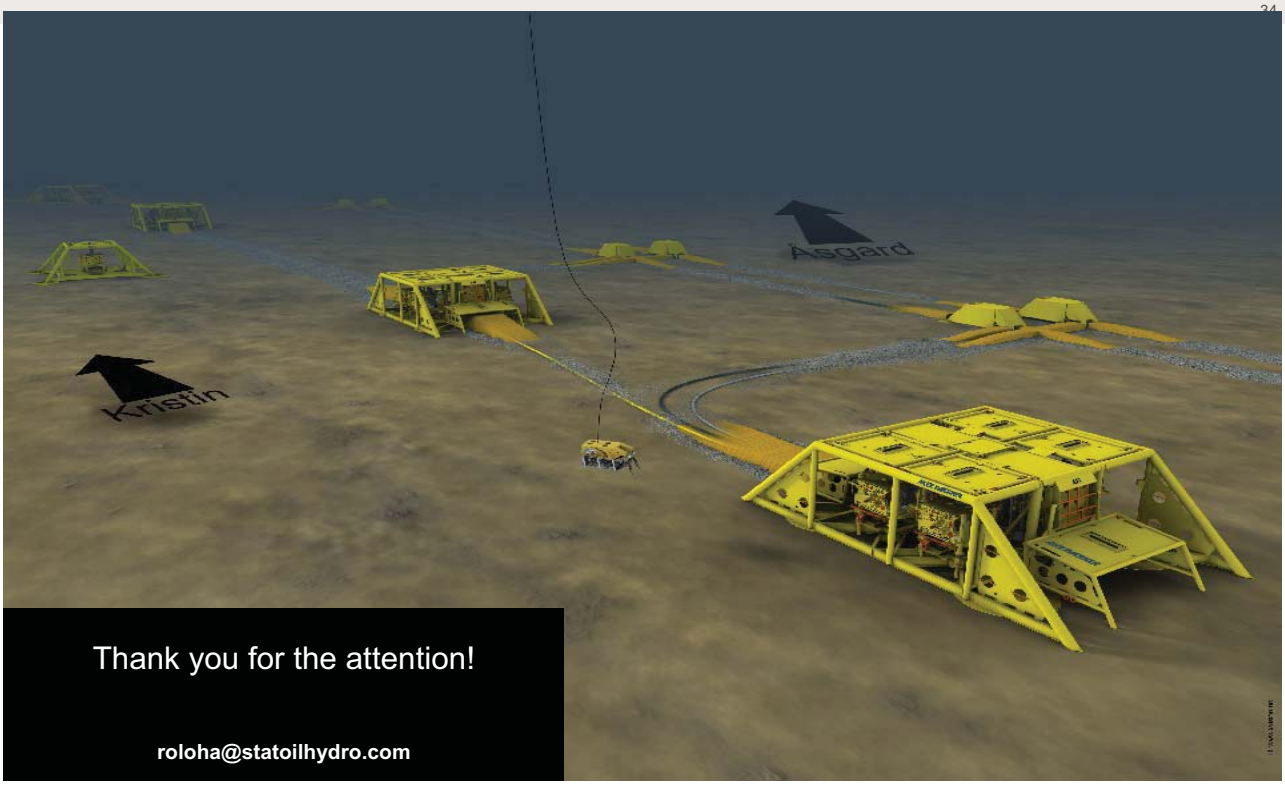


Difference between Snorre B and a typical subsea field

StatoilHydro

“Urgent” enabling features for robust Subsea control

- Segregation of PSD/ESD from process control
- Ethernet Backbone, “from office to subsea”
- Use of managed switches to control traffic
- Standard interface with no protocol conversion subsea system to SAS
- Transparent links from subsea and downhole sensor systems to topside expert applications
- High bandwith communication from subsea to topside (min 100 Mbit/sec)



A case study of HF methodologies in Norwegian O&G

Andreas L. Aas, Stig Ole Johnsen and Torbjørn Skramstad
Dept. of Computer and Information Science, Norwegian University of Science and Technology (NTNU), Trondheim, Norway
{andreaas, stigolj, torbjorn}@idi.ntnu.no

NTNU
Innovation and Creativity

Outline

- Introduction
- CRIOP and HFAM
- About the study
- Results
- Conclusion and future work

NTNU
Innovation and Creativity

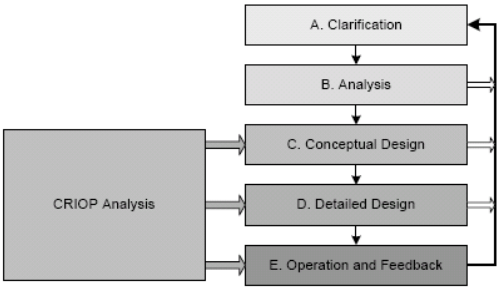
Introduction

- Case study of HF methodologies in Norwegian O&G
  - ISO 11064
  - CRIOP
  - Human Factors Assessment Method (HFAM)
- Objectives:
  - Map the use of the methodologies
  - Map the experiences and attitudes of the users
- Motivation:
  - Collect industrial feedback
  - Identify potential areas for improvements

NTNU
Innovation and Creativity

CRIOP

- Methodology to verify & validate Control Centre designs.
- Checklists and scenarios
- Assumes ISO 11064 is used



NTNU
Innovation and Creativity

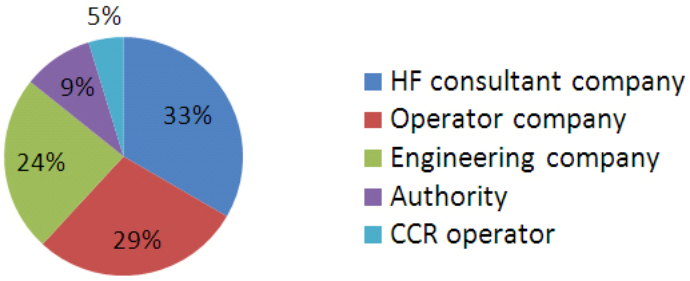
HFAM

- Human Factors Assessment Method (HFAM)
- V&V tool that "*can be used for systematically reviewing both the **process** of how Human Factors has been integrated into the design and operation of control rooms and for evaluating the **results** of this process*"

About the study

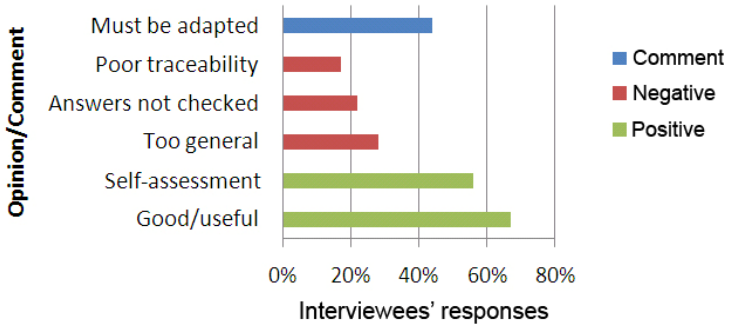
- Interviews:
  - 18 interviewees familiar with CRIOP Checklists
  - 17 interviewees familiar with CRIOP Scenario analysis
- Survey:
  - 22 respondents familiar with CRIOP Checklists
  - 20 respondents familiar with CRIOP Scenario analysis
  - 9 respondents familiar with HFAM

Interview stakeholders



NTNU
Innovation and Creativity

Results - Interviews

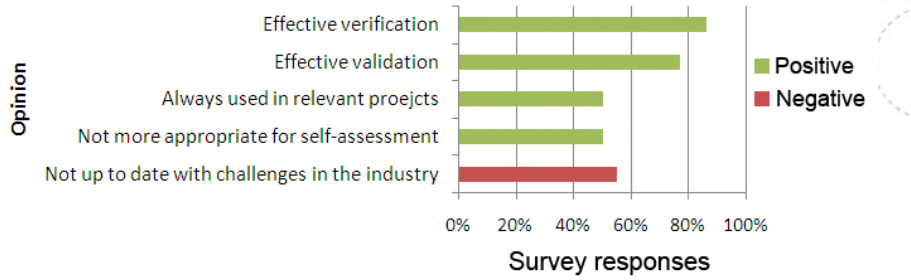


NTNU
Innovation and Creativity

Survey stakeholders

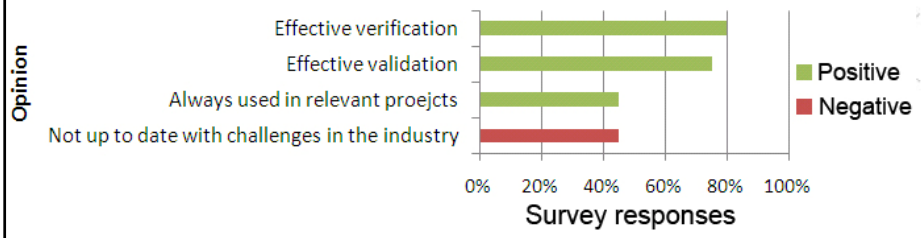
NTNU
Innovation and Creativity

Results - Survey Checklists



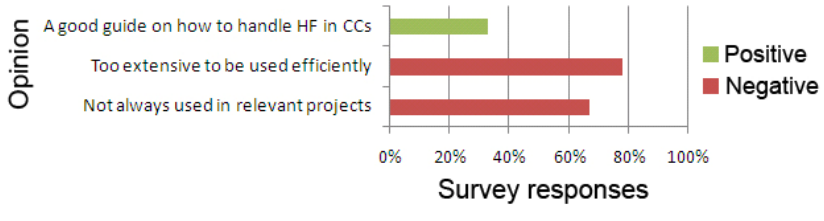
NTNU
Innovation and Creativity

Results - Survey Scenarios



NTNU
Innovation and Creativity

Results - HFAM



NTNU
Innovation and Creativity

CRIOP - Suggested improvements

- Guide for the CRIOP adaption process.
- Domain specific CRIOP checklists:
  - CC/CCR
  - Driller's cabins
  - Crane cabins
- Improve dialouge with the industry (users).
  - Contact criop@sintef.no
- Improve linking between CRIOP and relevant standards where possible.

NTNU
Innovation and Creativity

Conclusion

- CRIOP is used and appreciated by the Norwegian O&G industry.
- The majority of both interviewees and survey respondents were positive to CRIOP checklists and CRIOP scenarios.
- We have suggested some areas for improvement

NTNU
Innovation and Creativity

What do **you** think?

NTNU
Innovation and Creativity

HFC-forum

Punkter:

- Regnskap/Budsjett
- Planer
- Organisering
- Rekruttering

Regnskap/Budsjett

Regnskap 2008:

- Inntekter 412,000
- Utgifter 412,000
  - Justert CRIOP 95´
  - HFC møte Stavanger 85´, HFC møte Oslo 85´
  - Administrasjon 141´
  - Overskudd 6

Budsjett 2009

- Inntekter 350,000
- Utgifter 350,000
  - Søknad/forarbeid forskningsrådet 50´
  - HFC møte i Stavanger 85´ og Trondheim 85´
  - Administrasjon 130´

Planer HFC forum

- Øke inntektene i HFC forum ved å få inn brukerinitierte prosjekter
  - Retningslinjer (&forståelse) samhandling
  - Oppdatering CRIOP (forenkling, modernisering)
- Human Factors kurs NTNU (og UiS), eks: ”Introduksjon til HF og IO”
- Samarbeid med Human Factors Nettverket i Sverige (HFN)
- Diskusjon av tema HFC fremover?
  - Høst 2009: HFN og Team Cognition/Org. Cognition E.Salas/K.Weick
  - Vår 2010: HF i ulykkesgranskninger
  - Høst 2010: HF i endringsprosesser; design for resilience
  - Vår 2011: Inntog i det globale
  - Høst 2011: HF i andre land – USA, SørøstAsia, ..etc

Organisering og rekruttering

- Referansegruppe
  - Leder : Thor Inge Throndsen/Statoilhydro (Gjenvalgt 13/2-08)
  - Atoosa Tunem/IFE,
  - M. Green/HCD,
  - Ole Klingsheim/ConocoPhillips,
  - Stig Ole Johnsen; (Camilla Tveiten; Irene Wærø)/SINTEF.
- Rekruttering
  - Arbeide for å få inn flere medlemmer

Utviklingsprosjekter

- Referansegruppen i HFC fungerer som styringsgruppe

Søknad til PetroMax programmet:
- Retningslinjer for samhandling
- Oppdatering av CRIOP

HFC aktiviteter

1. Criop brukermøte (2005.04.27)
2. Etablering av HFC forum (2005.10.26)
3. Human Factors erfaringer og utfordringer med ISO 11064 (2006.04.19)
4. Kompetansebehov og erfaring innen Human Factors (2006.10.25)
5. God praksis for Human Factors i kontrollrom og IO (2007.04.18)
6. Læring fra feil /HF i fjernstyring av prosessanlegg (2007.10.17)
7. Praktisk erfaring fra samhandlingsrom (2008.04.23)
8. Error Tolerance in complex settings (2008.10.01)

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

HFC status og planer

SAK, FORMÅL

Status for 2008 og planer fremover for HFC forum

	DISKUSJON	ORIENTERING
Går til		
Arbeidsgruppen i HFC:		
Thor Inge Trondsen (StatoilHydro)	X	
Athoosa Thunem (IFE)	X	
Mark Green (HCD)	X	
Ole Klingsheim (ConocoPhillips)	X	
Stig Ole Johnsen (SINTEF)	X	
[Irene Wærø (SINTEF)		
Camilla K. Tveiten (SINTEF)]		

PROSJEKTNR.	DATO	SAKSBEARBEIDER/FORFATTER	ANTALL SIDER
	08.06.2009	Stig O. Johnsen, Camilla Tveiten Godkjent av: Thor Inge Trondsen	7

Vi vil med dette presentere status for HFC forum for 2008 og videre planer fremover.

1 Status

I 2008 har det vært 12 bedrifter som har vært betalende medlemmer. (Se vedlegg 1 for en opplisting.)

1.1 Økonomisk status

HFC forum for 2008 har følgende resultat pr 20/11-2008:

Inntekter		**Utgifter**	
		Justert CRIOP	95,000
Medlemsinntekter (Medlemer vedlegg 1)	412,000	Møte 1 Stavanger april 2008	85,000
		Møte 2 Oslo oktober 2008	85,000
		Timeinnsats administrasjon	141,000
		Overskudd til 2009	6,000
Sum	**412,000**		**412,000**

Internkostnadene fra SINTEF er fakturert ut fra timesats brukt mot forskningsrådet.

1.2 Møter og tematikk i HFC forum

HFC forum ble etablert 27/4 2005 og vi har gjennomført følgende møter

1. Første brukermøte – forumet ble døpt HFC forum, 27-28/4-2005
2. **HF i eDrift, IO og tilsyn,** 26-27/10-2005
3. **Human Factors erfaringer og utfordringer med ISO 11064**, 19-20/4 - 2006
4. **Kompetansebehov og erfaring innen Human Factors (HF)** , 25-26/10 – 2006

5. **God praksis for HF i kontrollrom og Integrerte Operasjoner**, 18-19/4 – 2007
6. **Læring fra feil /HF i fjernstyring av prosessanlegg**, 17-18/10 – 2007
7. **Praktisk erfaring fra samhandlingsrom**, 23-24/4 – 2008
8. **Error Tolerance in complex settings**, 1-2/10 – 2008

To møter er tidsatt i 2009:
- Møte #9 den 22. til 23.4 – 2009
- Møte #10 den 21. til 22.10 - 2009

2 Mål for HFC forum

Visjon og målet for HFC forum er

- ” Kompetanseforum for bruk av Human Factors (HF) innen samhandling, styring og overvåkning i olje og gass virksomheten"

Hovedoppgave:
- ”Være et forum for erfaringsoverføring som bidrar til å videreutvikle HF metoder til bruk ved design og vurdering av driftskonsepter.”

Det foreslås at primærfokus beholdes, men allerede i denne perioden bør vi jobbe mot et delmål knyttet til å øke bredden slik at det også kan være et nettverksforum for Human Factors innen samhandling, styring og overvåkning generelt – ved at vi tar inn ytterligere industri som eksempelvis kraftsektoren, ulykkesgranskninger etc. Det er også ønske om å synliggjøre CRIOP bedre beskrivelse av oppgavene våre.

3 Ambisjoner HFC framover

3.1 Øke inntektene i HFC forum ved å få inn BIP eks CRIOP BIP/ ”CRIOP” – for samhandlingsrom

Forslaget er at vi søker om midler fra NFR på basis av medlemsinnskuddene vi får fra HFC forum. Ved at vi lager en relevant BIP kan vi søke om ytterligere støtte fra NFR. Vi kan bruke eventuelle overskudd i HFC forum som ”såkornmidler” for å lage en prosjektsøknad. Viktige deltakere i HFC forum vil gjerne engasjere seg for å lage prosjektsøknader. (I PDS forum har man fått ca 1 Mill via BIP søknad til NFR, ut fra en medlemsavgift på ca 0,5 Mill kr)

Følgende områder er foreslått prioritert, på basis av diskusjoner med deltakerne i HFC forum og ønske om prioritering:

Prio	Område	Innhold
1	Retningslinjer ”CRIOP” for samhandlingsrom	Basere seg på arbeidsdokumenter for samhandlingsrom laget av industrien – sette ned en arbeidsgruppe som lager forslag til ny standard, arbeidsdokument som kan benyttes.
2	Oppdatere CRIOP – 2010	Oppdatere CRIOP med nytt regelverk fra Ptil, forenkle sjekklistene for Scenariegjennomgang. Legge til regelverkskrav fra USA. Regelverkskrav innen sjøfart ifb bruk av CRIOP (når Ptil’s regelverkskrav ikke gjelder)

3.2 Human Factors kurs (HF-kurs)

"HF kurset" kom opp som aktivitet på HFC møtet i 2005 og 2006. Det ble gjennomført et planarbeid av Jasmin Ramberg (Scanpower) og Adam Balfour (HFS) basert på HF kurstilbud i utlandet (fra Cranfield/England) og industrierfaring. Kurset har deretter blitt etablert i et samarbeid med HFC forum og NTNU/IO senteret. IO senteret har støttet kursutviklingen og har tilbudt det til alle sine medlemmer. Det ble foreslått et totalt kursopplegg som kunne være et masterkurs, men man startet med en del av kursopplegget, et introduksjonskurs "Introduksjon til HF og IO. Man valgte å tilby det som et etter- og videre utdanningskurs ved NTNU. Pensum og innhold ble tilpasset IO for å møte interesse fra næringen. Første kurs ble holdt i vårsemesteret 2008.

Generelt fikk kurset en bra evaluering. Kurset justeres litt ut fra tilbakemeldinger fra deltakerne, men tilbys i hovedsak som opprinnelig planlagt. Deltakerne fra første kurs ville markedsføre kurset til sine kolleger. Det er håp om å videreutvikle kurset i retning av ordinært studietilbud ved NTNU. Per i dag er denne planleggingen overlatt til psykologisk institutt ved NTNU/Karin Lauman. Kurset videreføres for 2009 som en aktivitet ved NTNU i regi av SVT fakultetet med faglige ansvarlige Prof P.M.Schiefloe, Karin Lauman og Stig Ole Johnsen.

Neste gjennomføring planlegges i vårsemesteret 2009. Samlingene blir i uke 7 (10,11,12 februar), uke 11 (10,11,12 mars) og uke 20 (11,12,13,14 mai). Påmelding http://videre.ntnu.no.

HFC forums videre involvering i planlegging og utforming av HF kurset
HFC forum bør fungere som et ideforum og referansegruppe for HF kursoppleggene. Det kan være et alternativ at HFC forum gir økonomisk støtte til HF kurs for å sikre at kursene blir avholdt. HFC nettverket sammen med nettverket fra IO senteret skal bidra til å spre informasjon om HF kurset. Deltakere fra HF kurset får tilbud om medlemskap i HFC forum og blir en del av nettverket.

3.3 Samarbeid med det svenske HFC nettverket, som heter HFN

Thor Inge Trondsen og Stig Ole Johnsen besøkte HFN, den 7/10 ved KIT i Stockholm. Deltakere på møtet fra HFN var Arne Axelsson (styrelseordf.), Gunilla Derefeldt; Lena Mårtensson; Clemens Weikert, Kjell Ohlsson og Martina Berglund (HFN verksamhetsledare). Formålet med møtet var å styrke samarbeidet mellom nettverkene.
Agenda for møtet var:

1. Kort beskrivning/presentation av respektive nätverk, målsättning, verksamhet, styrkor och vad som kan utvecklas vidare
2. Vad vill vi uppnå med samarbetet?
3. Utväxling av information om möten, kurser och annan undervisning
4. Ytterligare steg/aktiviteter för att fördjupa samarbetet
5. Övriga frågor

Vi skal kunne delta på hverandres møter, dele erfaring, ha tilgang på informasjon fra HFC og HFN og arrangere felles møter etter behov. I tillegg til at vi ble bedre kjent med HFN nettverket, kom det opp følgende momenter:

- Vi planlegger at HFN deltar i et HFC møte i april, hvor vi kan diskutere samarbeide som er nyttig for deltakerne i nettverkene. (Workshop om dette planlegges i oktober 2009).
- Vi er enig om at medlemmene kan delta på kurs som arrangeres. For HFC er det mulig å delta på kursene hos HFN i 2009, som p.t er: "Juste culture" (mars 2009)/ "Drifttagning av tekniska system"(maj/juni 2009) / CRM-seminarium (ikke tidsbestemt).
- Dersom det er interesse for å delta i CRM kurs – kan det arrangeres etter behov fra de som er interessert i HFC nettverket.

4 Tematikk, aktiviteter og tiltak framover

4.1 Valg av tema for HFC framover

Tema for 2009 og fremover bør lages som en oversikt over flere møter for 2009 og 2010, slik at vi kan ha dette som en langtidsplan. I nedenstående tabell har vi laget en oversikt over mulige tema.

Periode	Forslag til tema og innslag
Vår 2009	Human Factors og proaktivitet -R.Westrum, J.Wreathall eller andre (Industrieksempler – bruk av proaktive indikatorer)
Høst 2009	Samarbeid med HFN i Sverige, Situational awareness (Team Cognition – E.Salas og Organisational Cognition - . K.Weick)
Vår 2010	HF i ulykkesgranskinger, hvordan forstår vi Human Factors i ulykkesgranskninger
Høst 2010	HF i endringsprosesser, ”Design for resilience”, Perspektiver som Actor-network theory (ANT) i HF granskninger.
Vår 2011	Inntog i det globale: Språk, kultur, tidsforskjell, HF i global setting.
Høst 2011	Fokus på HF i andre land, somUSA og SørøstAsia – erfaringer, muligheter og trusler

4.2 Nye medlemmer

Det arbeides med å få inn Norske Shell som medlemmer. Kontaktperson er identifisert og inviteres til neste samling i regi av HFC forum. Vi sender informasjon om medlemskap. Dette gjelder alle som deltar en gang som gjest og som vi ønsker som medlemmer.

I forbindelse med neste møte i Trondheim vurderer vi å invitere representanter fra Teekay Petrojarl som deltakere og/ eller foredragsholdere og vi vil arbeide med å få dem inn som medlemmer.

Vedlegg 1: Medlemmer og deltakere i 2008

Medlemmer betaler en medlemsavgift avhengig av størrelsen på 25.000 kr eller 12.500 Kr. Deltakere på frittstående møter betaler 6.500 kr i deltakeravgift.

Medlem (25.000 eller 12.500 Kr)	**Avgift**
Aker Solution	25.000
ConocoPhillips	25.000
ENI	25.000
HCD	12.500
HFS	12.500
IFE	25.000
Kokstad BHT	12.500
Kongsberg Intellifield	25.000
National Oilwell	25.000
Scandpower	25.000
SINTEF	25.000
StatoilHydro	25.000
SUM Medlemsavgift	**262.500**
Deltakere (6.500 Kr) og Antall #	**Avgift**
BP #4	26.000
Norske Shell #1	6.500
SINTEF #2	13.000
UMOE IKT #2	13.000
StatoilHydro #10	65.000
DnV #3	13.000
Petrolink #1	6.500
SUM deltakeravgift #23	**149. 500**
SUM	**412.000**

Vedlegg 2: Ønsker og innspill fra HFC deltakerne

Vi har fått en lang rekke innspill fra deltakerne i HFC forum på områder og tematikk av interesse. I det vedlagte har vi forsøkt å gi en oppsummering av aktuelle tema:

- Kompetanseutvikling innen Human Factors
- Det var et ønske om at en person presentere et helt konkret HF-analyse som viser både prosess, resultat (positivt og negativt) og dilemmaer mellom menneskelige feilhandlinger og systemfeil– eks modifikasjon av drillerbu, kraner
- Det hadde vært fint med HF praktikere til å innlede metodediskusjon og analyser (Eks James Bunn/ StatoilHydro, noen fra Scandpower, HFS, Sintef, IFE eller HCD.
- Hendelser hvor Human Factors (HF) eller mangel på HF har vært avgjørende og eksempler på gode/dårlige HF design. Gode tabber i forbindelse med Human Factors analyser.
- HF og Alarm Management.
- HMI, typiske fallgruber, design, god praksis, erfaringer, gode retningslinjer, kognitivitet..
- Koplinger mellom HF bruk innen Olje&Gass og andre industrier som luftfart, kjernekraft slik at en fikk tilgang til erfaringer fra andre. Også fra HF nettverket i Sverige.
- Operatør som barriere for feil i IKT systemer, eller som feilkilde?
- Erfaringsoverføring med fokus også på ”Hva ble gjort feil på andre prosjekter”? Likeledes presentasjon av konkrete erfaringsdata med fokus på menneskets behov og opplevelser.
- Mer om standarder og retningslinjer, eksempelvis standarder og erfaringer knyttet til etablering og bruk av samhandlingsrom
- Oppfølging av bestemte presentasjoner eksempelvis:
    - Hvordan gikk det når man benyttet ”Hydros metode for å identifisere HF utfordringer”?
    - Mer om ”Optimisme og sikkerhet” og mer om ”Improvisasjon”

- Praktiske erfaringer knyttet til Integrerte Operasjoner og metoder som kan støtte IO, eksempelvis forholdet mellom sikkerhet, beredskap og integrerte operasjoner
- MTO utfordringer ved innføring av IO, fokus på overlappet mellom M, T og O.
- Hva er beste praksis innen IO? (Oseberg Øst er for eksempel et spennende eksempel på generasjon 3 innen boring med krysstrening.). Sammenlikne og diskutere IO strategien til de forskjellige selskapene. Bruk gjerne Workshop for å bli mer konkret.
- Reelle erfaringer fra IO løsninger. Med synspunkter fra de som anvender ulike løsninger og konsepter. Noen problemstillinger som ønskes belyst er om arbeidsoppgavene har blitt mer spennende, om det har blitt mer motiverende å jobbe eller om stressnivået er økt? Og hva med utfordringer knytte til ”Remote Control” dvs. ekte fjernstyring, er det like aktuelt eller blir det nedprioritert?
- Komparative analyser, for eksempel Brage vs Oseberg i forbindelse med utvikling og implementering av Integrerte Operasjoner eller erfaringer i STATOIL med innføring av IO på tvers av Feltenhetene
- Hvilken fagkunnskap mangler pr dag innen IO? Prosjektledelse, OU? Nye oppgaver for SKR, IO produksjonsoptimalisering.
- Hvordan filtrere og presentere relevant informasjon for IO. Informasjonsbehov i IO kan være et tema som gir god basis for teori og praksis.
- Hva er ledelsesutfordringer og utfordringer knyttet til implementering av IO?
- Hvordan jobber man i team under IO? Hvordan etableres og bygger man ut kunnskap og kompetanse i team som samhandler? Hvordan mobiliserer man i forbindelse med teamorganisering? Hvordan skal men trening på samhandling i forbindelse med IO?
- Det snakkes mye om teknologi og utforming, ikke hva vi samhandler om og hvordan. En bør derfor i sterkere grad ha fokus på de nye arbeidsformene i IO, en bør ikke bare se på design av rommene, men innholdet er like viktig.

- Diskutere endring i arbeidsprosesser i forbindelse med IO. Hvilke HMS-risikoer kan det medføre? Hvilke barrierer er viktige i et IO perspektiv?

- Flere internasjonale foredragsholdere eksempelvis med flere eksempler på metoder fra internasjonale bedrifter og selskaper. Hva med erfaring fra ”ekte fjernstyring?
- Kan vi på sikt få etablert en omvisning hos f.eks SAAB flyproduksjon eller i et CCR i et kjernekraftverk? Luftfart, besøke kontrollrom i flygeledersentraler.
- Hvordan takler samhandlingsrom krisehåndtering, overgang fra normal drift til problemløsning, eventuelt krise?
- Hva er status for CRIOP – er CRIOP relevant for samhandlingsrom? (Ønske om en mini CRIOP til intern selskapsbruk som kursdeltakerne kan bruke i praktisk arbeid. Hydro ved Jon Monsen eller Hjertaker kjenner behovene.)

- Risikoforståelse
- Kollektive dimensjoner, team, samarbeid. Etnografiske undersøkelser, Ledelsestema mer spesifikt, Organisasjonsstruktur team opp mot hierarki.
- ”Shared situational awareness in IO teams.” Viktigheten av å ha en lik situasjonsforståelse ved en overgang til kommunikasjon gjennom “nye” kanaler.
- Utfordringer med Teams of Teams” – spesielt interessant i forhold til IO.
- Inntog i det globale: Språk, kultur, tidsforskjell, HF i global setting.
- IO og HMS, hva er oppsider og utfordringer.
- Hva kan nye perspektiver som Actor-network theory (ANT) bidra med i HF granskninger.
- Diskusjon av sosiotekniske system teori (STS) som grunnlag i HF, nye perspektiver.
- Hvordan er menneskelige og organisatoriske aspekter behandlet i forskjellige risikoanalyse tilnærminger, se hvordan HRA/PSA gjør det

Hovedpunkter fra HFC workshop 23.april –

Standard for samhandling og videreutvikling CRIOP

Agenda var:

Diskutere og avgrense muligheter å søke forskningsrådet om midler til 1) utvikling av en standard for samhandling, 2) videreutvikling av CRIOP.

Deltagere: Arno Pont, Adam Balfour, Arne Jarl Ringstad, Siri Andersen, Ingrind Omland, Andreas L. Aas, Heidi Stenberg Andersen, Berit Moltu, Kristian Gould, James Bunn, Marie Green, Mark Green, Irene Wærø, Thor Inge Throndsen, Stig Ole Johnsen

e-post: (heidi.andersen@nov.com; siri.andersen@dnv.com; gislea@hrp.no; adam@hfs.no; JBUN@StatoilHydro.com; kgo@scandpower.com; marie.green@hcd.no; mark.green@hcd.no; Bmol@statoilhydro.com; ingrid.omland@kongsberg.com; apon@statoilhydro.com; ajri@statoilhydro.com ; bkr@scandpower.com ; TIT@StatoilHydro.com; Irene.Waro@sintef.no Andreas.Aas@idi.ntnu.no)

I det følgende lister vi opp momentene dere kom med, førs om samhandling og deretter om CRIOP:

A) Forslag til videre arbeid mht samhandling:

- I. Kartlegge status. Gjennomføre studier av samhandling i dag. Organisere sette ned arbeidsgruppe..Lage søknad til forskningsrådet.
- II. Definere metoder og standard. Samhandling/IO i fremtiden innebærer romløs samhandling. En standard bør fokusere på å definere mål, filosofi og prosesser for samhandling, inkludert å identifisere aktører, kontekst, krav etc. Kan bygges som et hierarki. HF må integreres sterkere i IO/samhandling.

A- SAMHANDLING- Viktigste momenter fra flipover - utdypet i det etterfølgende

1) Hvilken operasjonell filosofi (strategi) er utgangspunkt for samhandling - hva er viktige "salgs"elementer? Både overordnet filosofi og driftsfilosofi.

I fbm IO, skal vi gi et øyeblikksbilde - etablere "common Ground" ? Hva er fokus - er det kjølvannet eller fremtiden? Vi må forske på fremtiden og fremtidens løsninger.

2) Ønsker å vite hvordan en skal lage filosofi for samhandling og hvordan lage funksjons spesifikasjon (Funksjon: dvs hva skal vi samhandle om, hvem skal samhandle).

3) Ønsker beskrivelse av hvordan vi går frem for å beskrive samhandling, eks: hvilke prosesser bør benyttes, hvilke aktører bør involveres i prosessen? Resultatet kan være en metode/ prosess for utforming av samhandlingsløsninger. (Samhandlingsløsninger er mye mer enn bare rom – det kan være et nettverk av aktører).

4)Gi eksempler på (nye) løsninger for samhandling.

5) Hvilke ytelseskrav skal en benytte for samhandling - hva er mål/krav, hva er ønsker? Hvordan skal samhandling måles? Hvordan skal tilbakemeldinger og evaluering struktureres? Hvordan vet en at det virker? – ifht samhandling, HMS, IO…(Sjekklister/ scenarier for verifikasjon og validering av samhandlingsløsninger)

6) Hvordan beskrives samhandlingskulturen - og hva er det?

7) Hvordan spesifiseres forskjellige type samhandling og hvilke konsekvenser får det for utforming av forskjellige typer rom. Ulike krav til ulike rom – eks prod.støtterom har andre krav/behov.

8) Hvordan utforme arbeidsområder i et samhandlingsrom, eller ifbm samhandling?

9) Hvordan er koplingen mellom samhandling i IO i forhold til HMS? - Hvordan ivareta IO design og HMS; IO og effektivitet? Hvordan skal vi få til fleksibilitet (?)– behovene endres underveis.

11) Hvordan ivareta/samhandle med flere praksisfellesskap - eks produksjonsstøtte senter - som inngår i et nettverk av rom?

12) Hvordan spesifisere/ ivareta info.deling. Hvilke sjekkpunkter bør etableres ifbm samhandling.

13) Hvilke grensesnitt/interfaces bør en benytte? - det er grensesnittene som er viktige - ikke bare romdesignet..

14) Hvordan vurdere arbeidsbelastning i nye samhandlingsløsninger? ..

Statoilhydro har utviklet en filosofi for samhandlingsrom, men den ønsker de ikke å dele ut. Det er heller behov for å definere rammer for og verifikasjon av samhandlingsrom. Men samhandlingsrom er egentlig nåtiden, skal vi se på fremtiden må vi se på romløs samhandling og nye løsninger for dette. Det er ikke mulig å lage EN standard for alle samhandlingrom, så det er bedre å søke å definere metode/prosess for å håndtere samhandlingsproblematikk, idenitfisere aktører etc. Hvem samhandler og når? Trenger også å definere hva som er et godt samhandlingsrom; som ytelseskrav, brukerkrav og akseptkrav. Til det trenger vi operasjonell feedback fra eksisterende samhandlingsrom. Nødvendig å ta inn multikulturelle aspekter (f eks operasjonssenter i Brunei vs Norge).

Må se på IO design og HMS, IO design og effektivitet. Når er det primært en link hav-land, men trenden er et nettverk av operasjonssentre rundt omkring i verden. Definere en samhandlingsrom designprosess. Må ikke fokusere på rom. Må se på interfaces i samhandling. Det kan være en utfordring å definere en operasjonell filosofi i prosjekter. Det skal også "selges" til andre miljø. Trenger et hierarki av filosofier, inkludert filosofi for IO. IO i dag er også et øyblikksbilde, slik som samhandlingsom. Må forske bakover ved å se på samhandling i dag og måle effekten av den og forske forover på prosess for å lage en operasjonell filosofi.

Samhandlingstandard kan fokusere på mål. Dvs goal-based approach. Fokus på prosesser for operasjonell filosofi. Arbeidsprosesser vil være bidrag forskningsmessig. Mest interessant med samhandlingsdata. Må se på beslutningsprosesser og målkonflikter.

B. Forslag til videre arbeid mht CRIOP:

- Kartlegge status, samle inn behov og nye momenter. Organisere og sette ned samarbeidsgruppe. Lage søknad til forskningsrådet.
- Forbedre/utvide CRIOP konkret - Inkludere ISO 11064-5 i CRIOP (HMI), Inkludere forklaring til hvorfor kravene stilles , Forbedre sjekklistene i scenarie-delen; Forslag til å inkludere flere aspekter og perspektiver f eks systemiske modeller som normalulykker, resilience etc.

B) CRIOP - Viktigste momenter fra Flip-over

1) Fint om ISO 1104, del 5 om HMI inngår som utvidelse av CRIOP sjekklisten.

2) Benytte WEB for å legg ut og dele scenarier - få til enkel mekanisme for å dele scenarier (vurderes opp i mot lokalt eierskap og lokalt engasjement) – kan være mal som utgangspunkt for lokalt engasjement og arbeid.

3) Beskrive bruk av Maritimt regelverk. Generelt og opp mot Olje og Gass industrien.

4) Spørsmål i CRIOP - få fram muligheten for å si noe om "Hvordan" ikke bare bruke "Ja"..(Skriv hvordan punktet er ivaretatt for senere oppfølging – bør inn i metoden.)

5) CRIOP er i dag litt skjevfordelt - metoden bør gjennomgås for å sikre at det blir lik detaljering på alle områder

6) Sjekklisten i Scenariodelen bør forenkles og bli mer brukervennlig

7) Få inn mer referanser til teori og erfaring

8) Er det muligheter for å lage en kombinasjon av CRIOP og HFAM eller et sterkere samspill mellom metodene? (HFAM er utviklet for tilsynet – PTIL).

9) Diskusjon av CRIOP som verktøy for validering og verifikasjon vs designverktøy.

10) CRIOP vurdert opp mot ISO 11064 - fokus og "scope" mellom verifikasjon&validering - og design. (Ønsket fokus på CRIOP er verifikasjon og validering).

11) Hvordan øke proaktivitet vs reaktivitet ifht design

12) Hvordan få til en CRIOP av framtidens arbeidsplassdesign - spørsmål(?) Hvordan reflektere over IO/Feilhandling; IO/Human Factors?

Kan dele/legge ut scenarier på HFC web, til inspirasjon for alle. Relatere scenarier til funn i sjekklister. Bruk av sjekklister fungerer godt og gir som regel mange aksjoner. Noen bruker maritimt regelverk (Istendenfor NORSOK). Rød bok → O&G CC må tilfredsstillle NORSOK. Må sjekke kritikaliteten. Utvide CRIOP til å forklare hvorfor ting gjøres. Må også inkludere systemiske modeller (f eks normalulykker, resilience etc). Kombinere HFAM/CRIOP. HFAM er for myndighetene, et batteri å velge fra. De er laget for forskjellige grupper. CRIOP sjekker godhet i design, mens HFAM er mer prosess. Hvordan kan CRIOP komme inn i startpunktet av et design. Bruke CRIOP til å stille krav (design verktøy). Men det har man ISO 11064 til. HFAM til å styre prosess. Arno Ponts paper om Troll prosjektet anbefales å leses. NB! CRIOP må fokusere på V&V i CC.

CRIOP er god, men trenger noen oppdateringer. Integrere HF i IO. CRIOP er for en ting. Interesant med aspekter utover det fysiske.