Thoughts on Software Dependability in O&G

Challenges and opportunitets

Statoil

Challenges

Statoil

megaproject culture

Langeled pipeline:
- World's longest subsea pipeline (1200KM)
- 17 Billion NOK (2,2 Billion EUR)
- 4 years development time
- On stream 9 years after discovery

Snøhvit (Snow White) field & LNG Plant:
- Subsurface field produced from land
- 35 Billion NOK (4,5 Billion EUR)
- 7 years development time
- On stream 25 years after discovery

Prestige or failure

Statoil

big physical machines

Troll A, 472 meters high, the largest man made structure ever moved

Software an alien concept

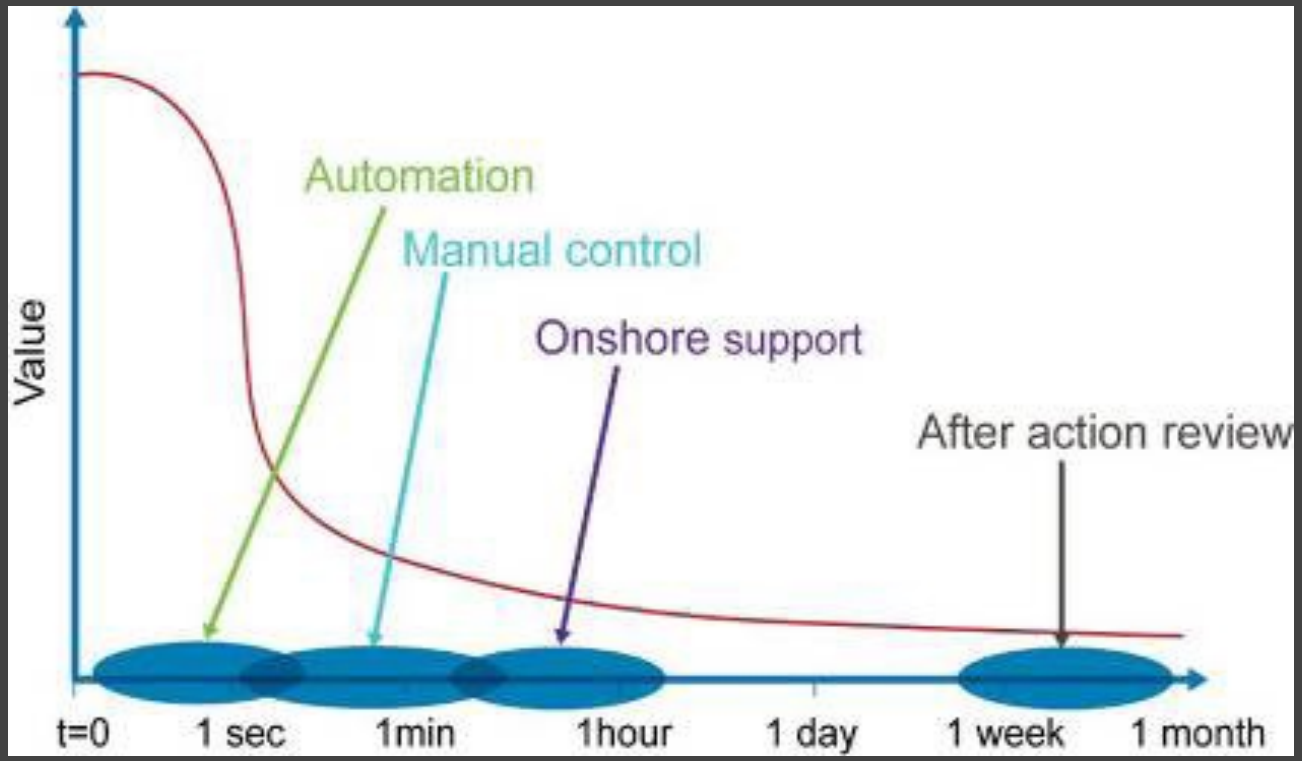
Statoil

strong belief in human expertise

Driller is king

Statoil

but time is precious



Problem severity = function(time)

Statoil

Failed Safety Critical Decisions

- Situational awareness
- Trustworthiness
- Culture
- Decision quality

Statoil

the weakest point

Human brain - planets most sophisticated and vulnerable decision maker

- Emotions trumps facts (irrationality)
- Limited processing capacity
- Need to rest, easily bored
- Inconsistency across exemplars
- Creative, easily distracted
- Values (ethics and morale)
- Mental illness (irrationality)

How to avoid clusterfucks?

Statoil

Opportunities

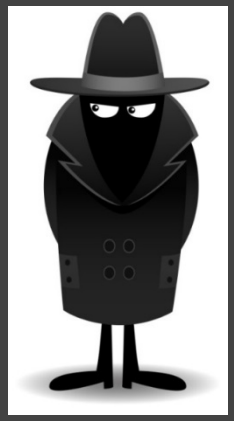
Statoil

a drillers perspective

What is the best action to take?

- I have to make frequent decisions and many of them depend upon readings from sensors that can be correct, noisy, random, unavailable, or in some other state.
- The decisions I have to make often have safety consequences, they certainly have economic consequences, and some are irreversible.
- At any point in time there may be three or four actions I could take based on my sense of what's happening on the rig
- I would like better support to determine how trustworthy my readings are, what the possible situations are and the consequences of each action.

systems of action



Computer systems that

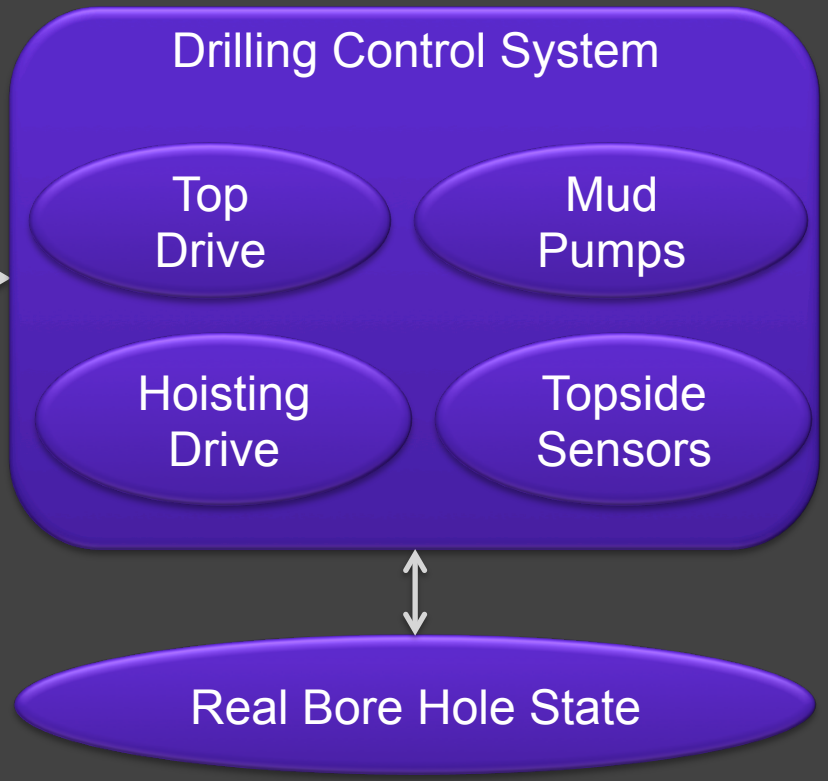
- Can sense or observe a phenomena, process or machine
- Process observations and search for anomalies, undesired state changes and other deviations that must be dealt with.
- Plan and execute / (recommend execution of) actions to bring the observed phenomena, process or machine back to its desired operational state.
- Monitor effects of actions and re-plan if action did not have intended effect on process state

making better decisions under stress and uncertainty

Statoil

drilling - a case study

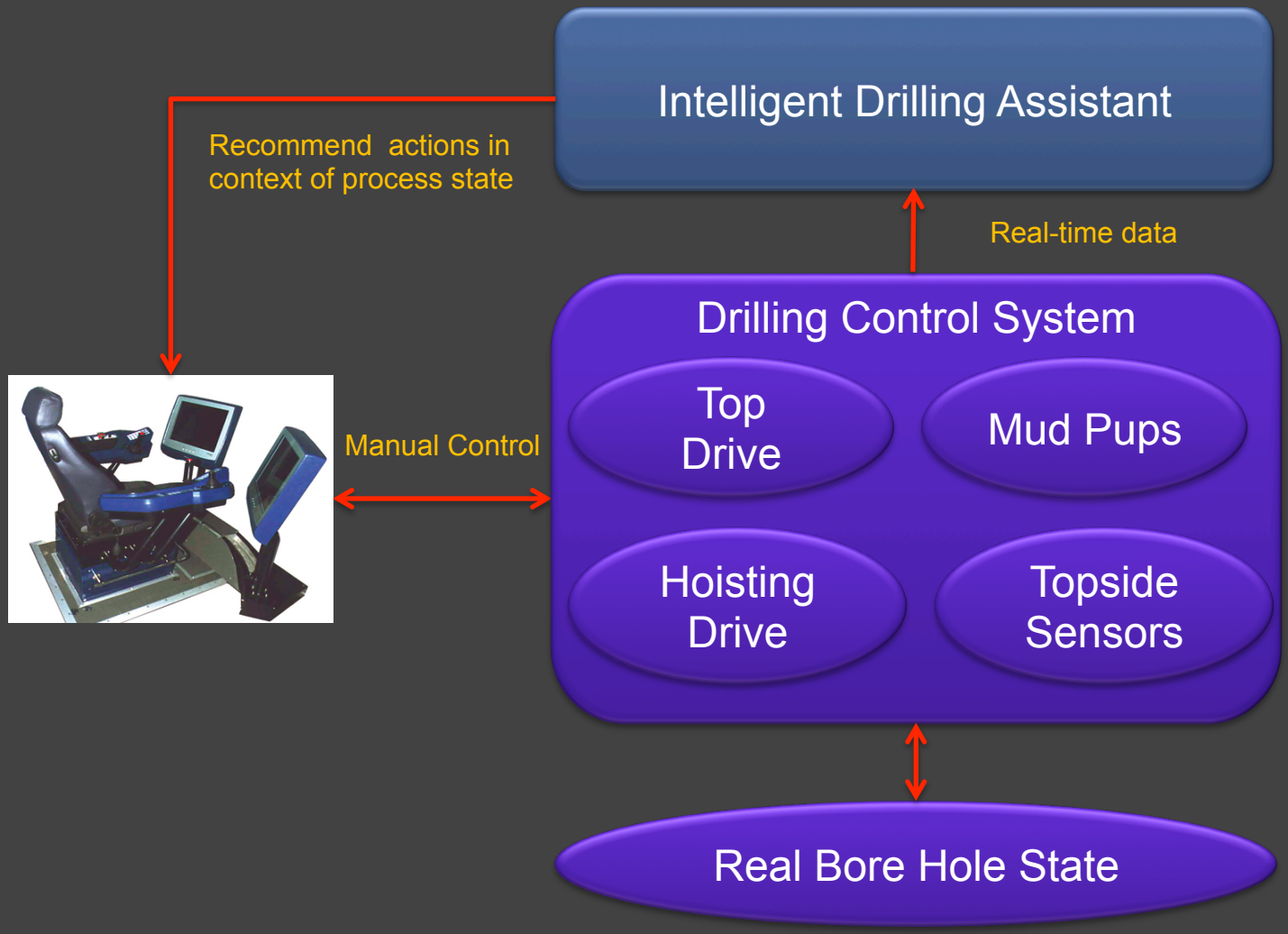
Manual Control
- Interpret data
- Perform tasks



A manually controlled process

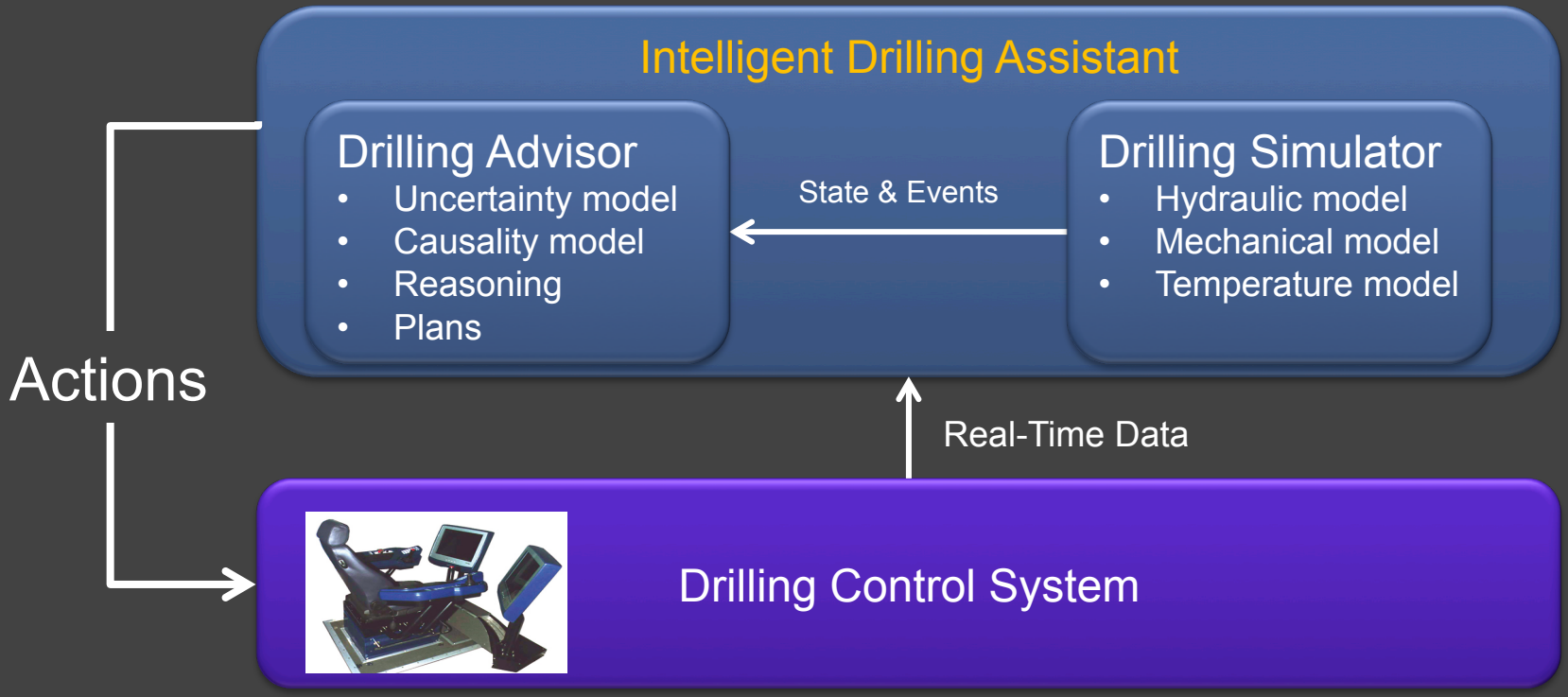
Statoil

add active computer support



Statoil

the drilling assistant



Action to be executed by human, but concept opens up for more computer control in the future.

i.e. Drilling advisor can be turned into “synthetic driller”.

Statoil

expressed in capabilities

Global Action Optimization	What is the best action to take for the business?
Local Action Optimization	What is the best action to take for control or safety?
Situational Awareness	What is the process state and where is it heading?
Uncertainty and Validation	What do we know for certain and what are we estimating?
Physical System Behavior	What can we infer about performance and changes in the physical system?
Physical System Sensing	What are we measuring directly, with what accuracy?

Thanks to Dr. Matthew Barry, www.softisms.com and Dr. Andrew Lucas AOS www.aosgrp.com for valuable contributions

Statoil

more sophisticated technology

Global Action Optimization

Local Action Optimization

Situational Awareness

Uncertainty and Validation

Physical System Behavior

Physical System Sensing

Automated planning and scheduling

Machine learning (Bayesian) + Physics (Cyb)

Decision / game theory

Rational agent

- has goals
- models uncertainty
- chooses action with optimal expected outcome for itself
- Examples:
  - human (on a good day)
  - intelligent software agent

Statoil

new challenges

Industry become software dependent

What parts are safety critical?

What parts are only business critical?

How to assess and protect against cyber threats?

How does failure in non-safety part influence safety and security?

What dependencies do we have?

How to design software that tackles mechanical failures?

Boundary between safety and business critical functions blurred

Statoil

summary

Increased software dependency in critical functions

Software used in critical control loops, beyond traditional safety systems

Must understand 2nd and 3d order failure effects

System behaviour is not linear

Software to be used to mitigate human weaknesses

Must be designed to enhance human capabilities

High Integrity System thinking needed

For more software than we traditionally think

Statoil

Thank you

Statoil