TNO innovation for life

Different perspective?
A view from the safety II domain

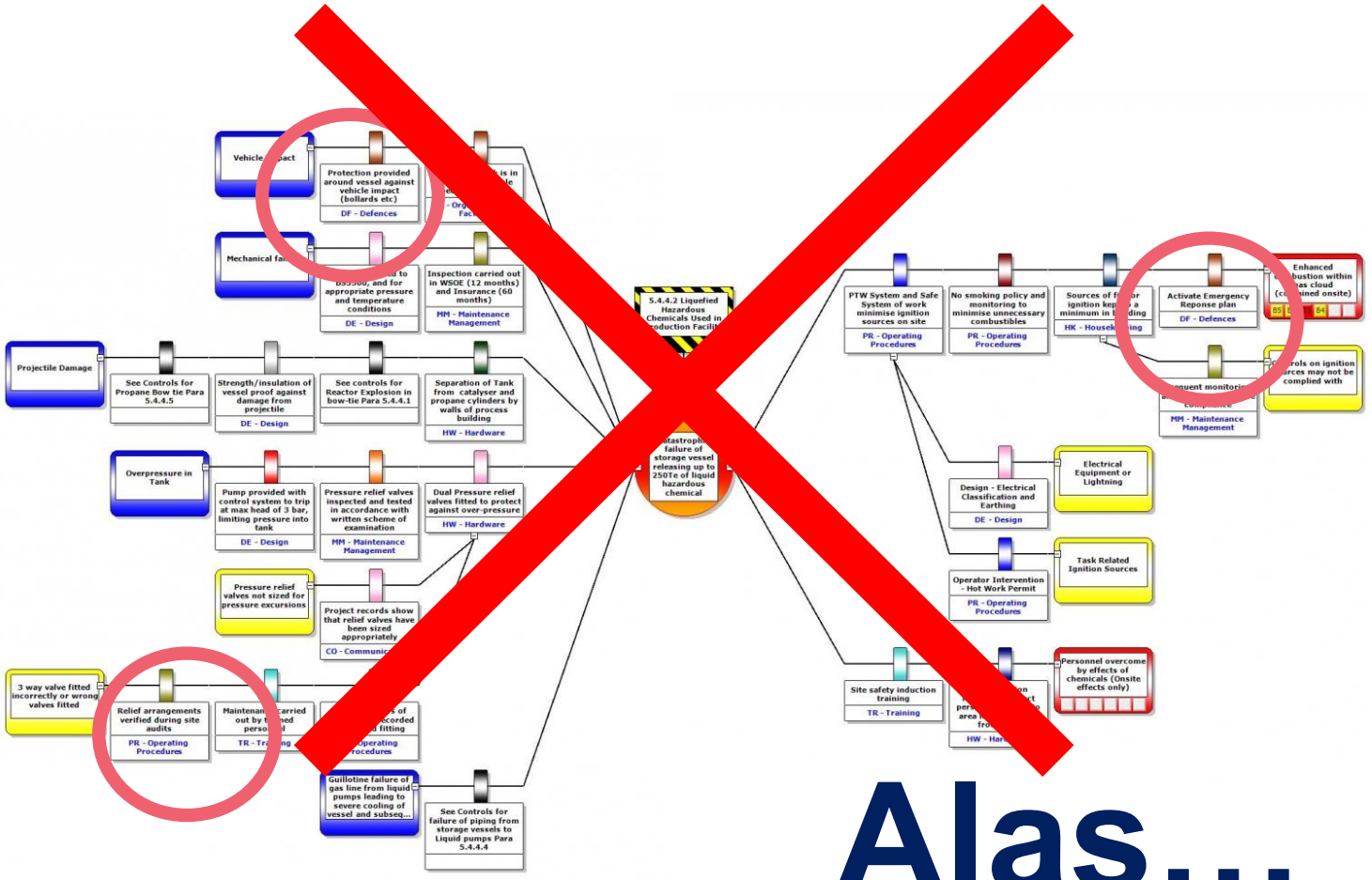
Raphaël Gallis


Aim

Still confused but on a higher level

(Enrico Fermi)

Old school



Alas…

Now

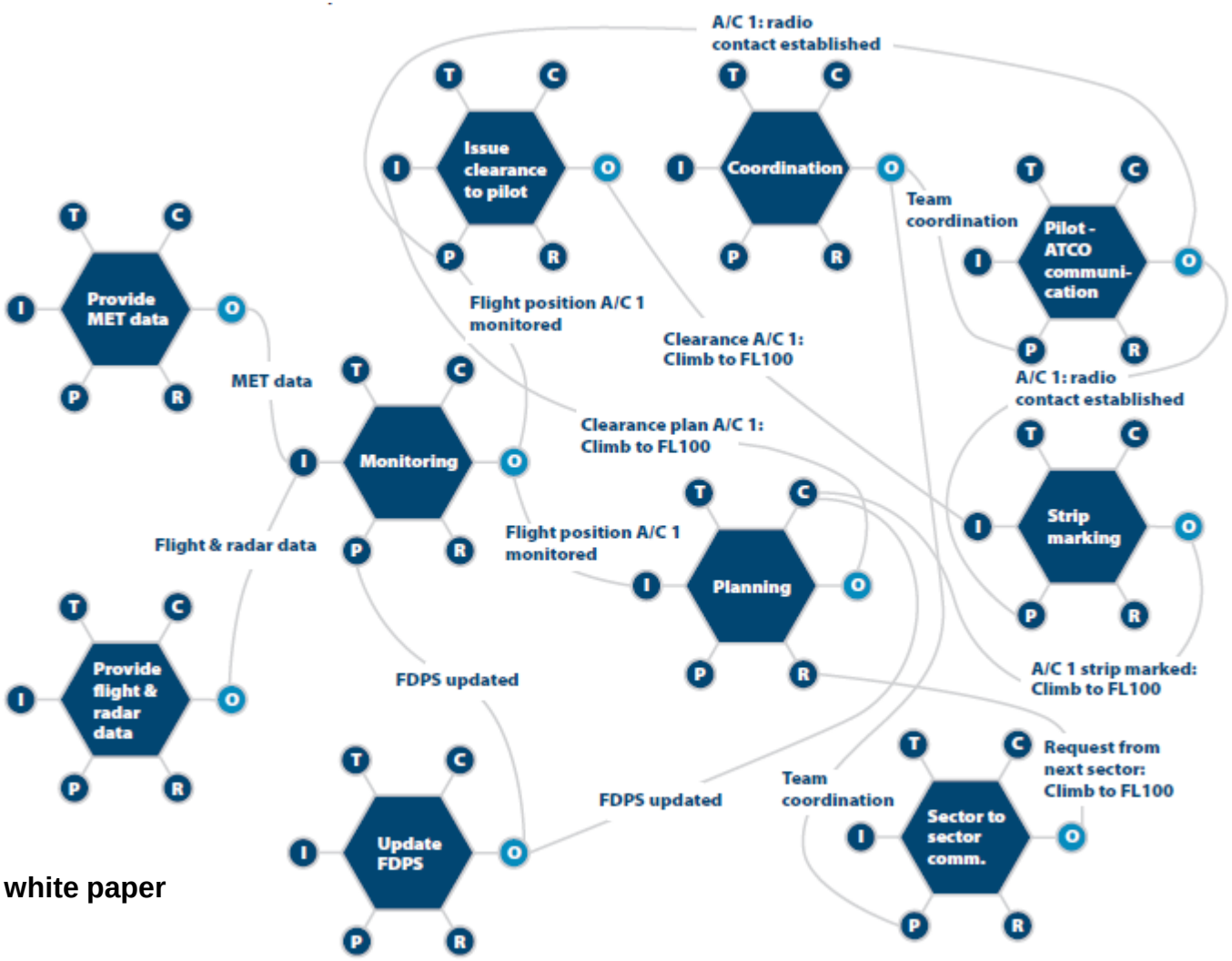


Figure 8: Instantiation of the FRAM model for the overflight scenario

Source: Eurocontrol white paper

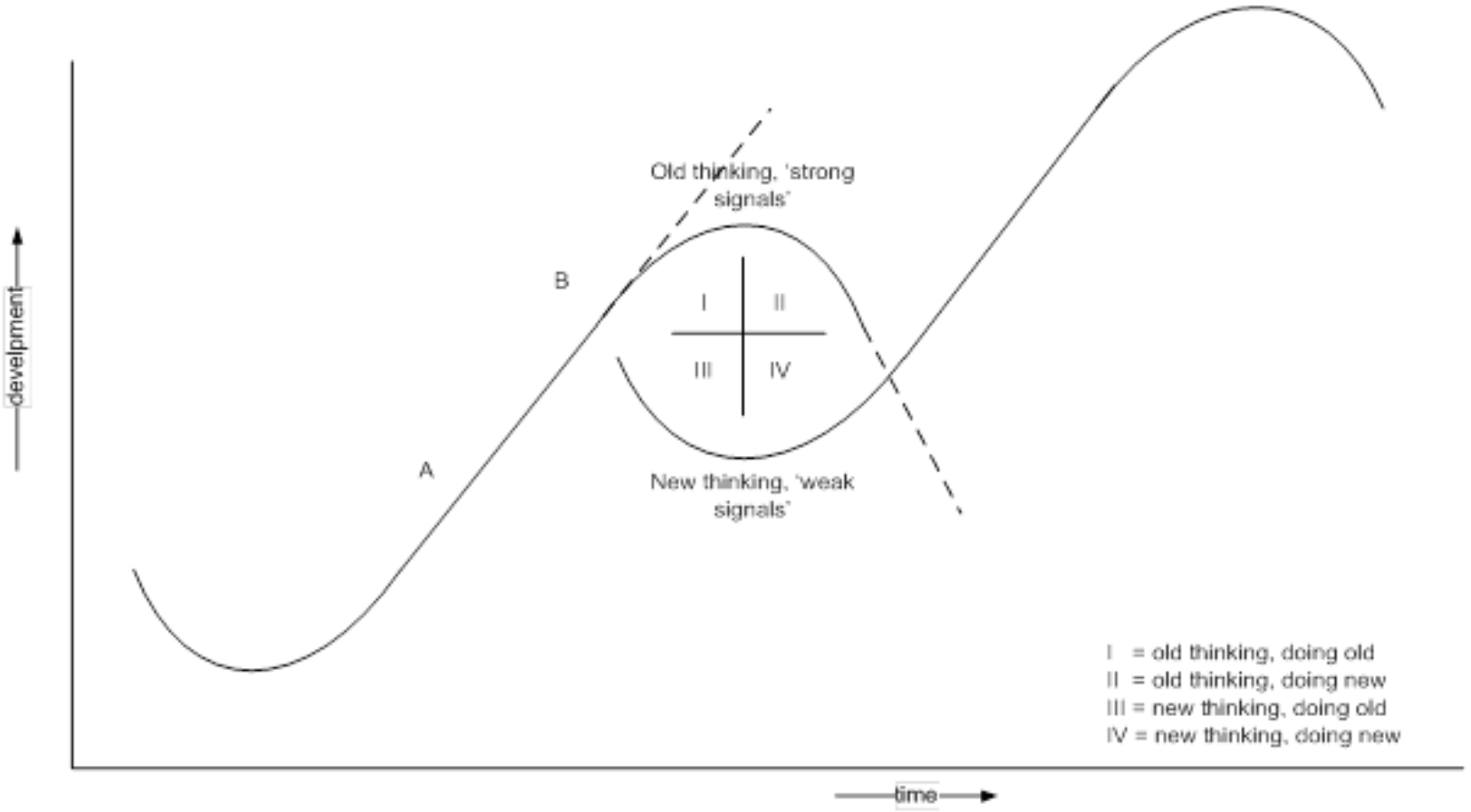

What is the difference between safety I and II?

In order to answer that question we need to answer to following:

- What is a paradigm shift
- What is complexity
- What are Complex Adaptive Systems (CAS)
- Link to Deepwater Horizon

- Why is this important
- Safety II in a nutshell
- Take home message

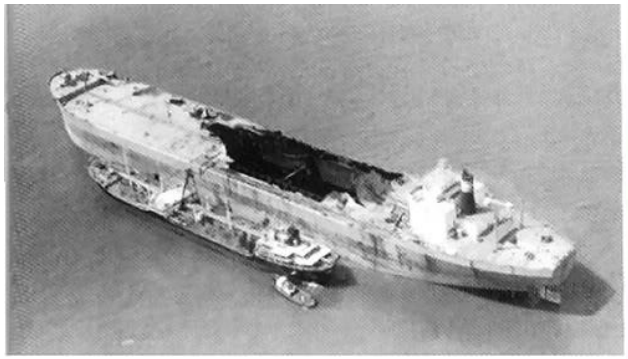
Paradigm shifts



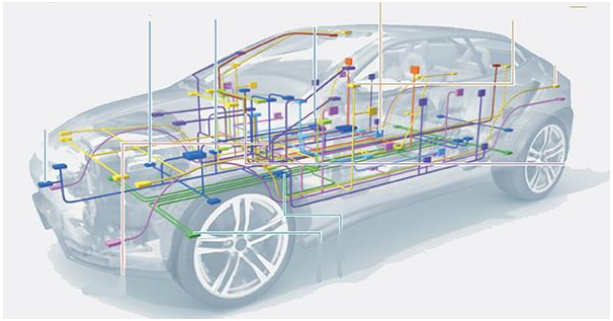
Model by Frans van Eijnatten / TUE

Examples

- Jet airliners (De Haviland Comet)
- VLCC's (Mactra, King Haakon VII, Marpessa)



- PLC assisted automobiles
- Electric cars, king size structures, etc

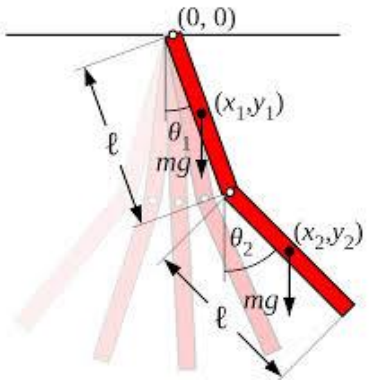


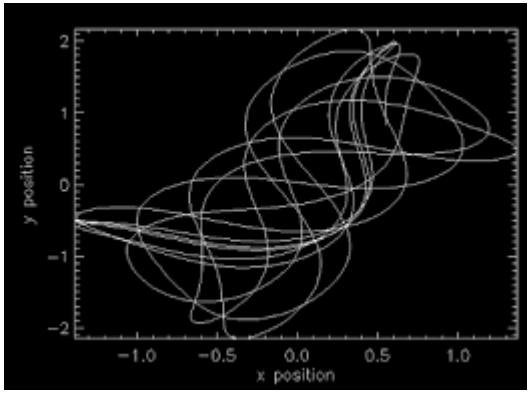
Complexity

Cynefin model by Dave Snowden

Examples of complexity

- Double Pendulum



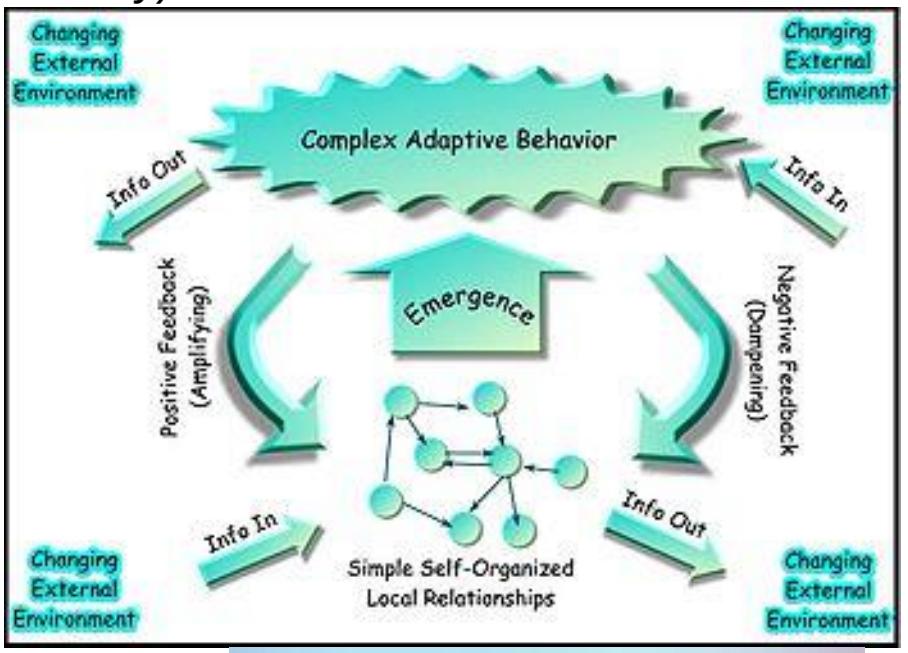


- The butterfly effect

Complex Adaptive Systems (CAS)

- From small to large (OR team – society)
- Human body

The end of Newtonion Models



Characteristics:

- Emergent properties
- Agents
- Self organisation
- Adaptive
- There is NO helicopter
- Local control
- not ‘bi-model’
- Non linear cause – effect relation ships

Over to the Deepwater Horizon

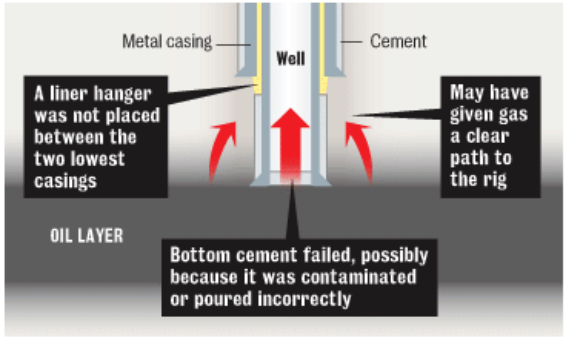
TNO innovation for life

True, however…..

SIX STEPS THAT DOOMED THE RIG

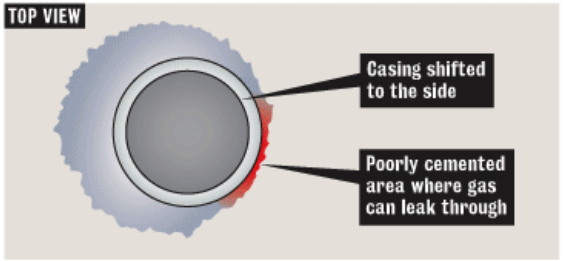
1 FEWER BARRIERS TO GAS FLOW AT WELL BOTTOM

BP used a single, long string of casing in the middle of the drill hole, one designed for later use in extracting oil.



2 FEWER CENTRALIZERS TO KEEP CEMENT EVEN

BP used six of the devices for keeping tubes centered, ignoring models calling for 21. It's important to have the casings centered in the well hole for the cement pumped in around it to set evenly.



3 NO BOND LOG TO TEST CEMENT INTEGRITY

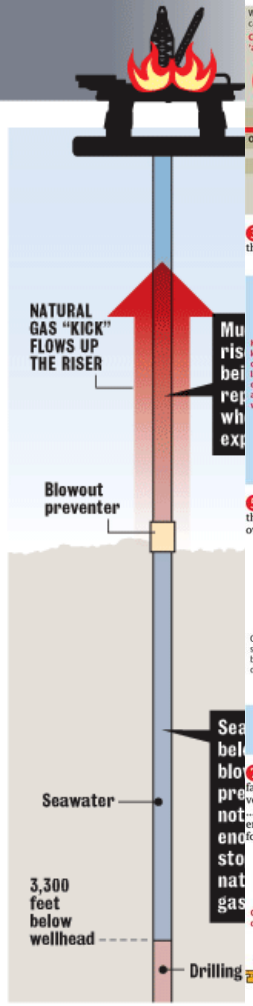
BP had hired contractor Schlumberger to run tests on the newly cemented well. But BP sent Schlumberger's crew home on a helicopter without having it run the test, called a cement bond log.

4 PRESSURE TEST MISINTERPRETED

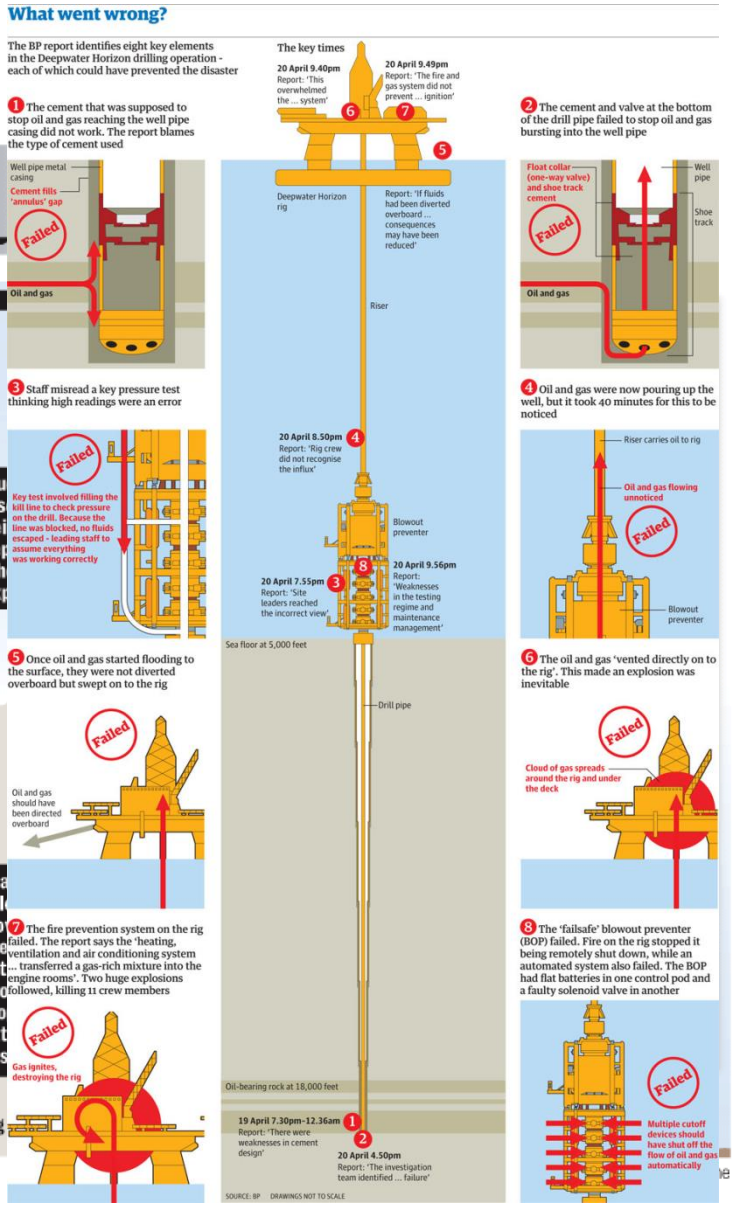
Rig workers reported confusion over the negative test, which measures upward pressure from the shut-in well. It is a key test of whether the well is stable.

5 MUD BARRIER REMOVED EARLY

BP decided to take heavy drilling mud out of the system, to 3,000 feet below the normal point, and earlier than usual. The barrier wasn't there to stem the gas kick that destroyed the rig. The mud is used to keep any upward pressure under control.

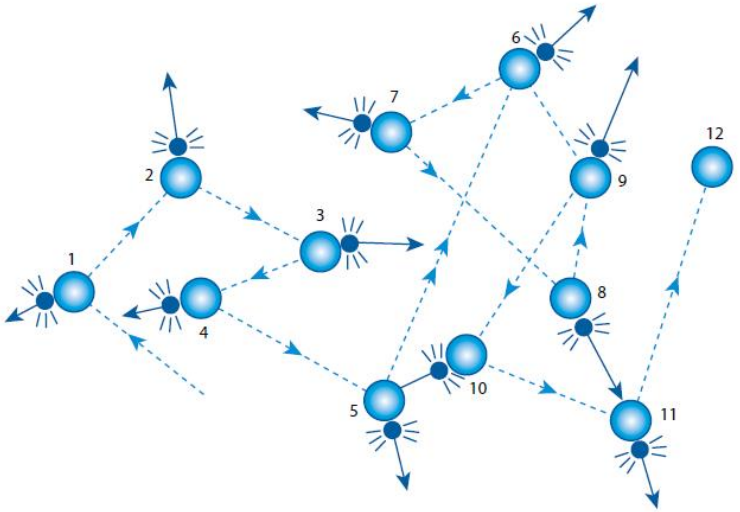


Source: Det Norske Veritas, Halliburton, BP e-mails, testimony, Times-Picayune investigation



Apply our new insights to the Deepwater Horizon incident:

- Paradigm shift not recognized:
  - from 250 to 1500/6000m
  - Old technologies
  - Old frame, new environment



- Complex adaptive system (not recognized)
  - Hyundai, Transocean (Triton asset leasing), BP, Halliburton, Anadarko, MOEX offshore, Minerals Management Service, ….

Why is this important?

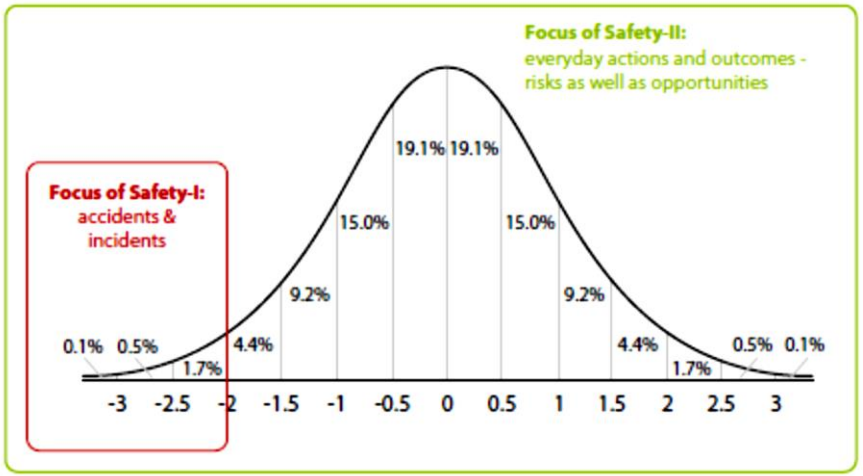
- We love simple, tend to rationalize (after the fact)
- We are notoriously bad in recognizing paradigm shifts
- We attempt to linearize
- We attempt to determine simple cause – effect relationships
- We suffer from hind sight bias
  - If only…..
  - Golden rivets
- We do not recognize nor acknowlegde complexity

We try to apply tools from one system for another: → does not work

Thus: we need something else

Safety II (in a nutshell)

- Things basically happen in the same way, regardless the outcome
- Zero risk is not possible (ETTO principle)
- Variation is inevitable and needed
- Humans are seen as resource necessary for system flexibility and resilience
- Risk assesment: to understand the conditions when performance variability can become difficult or impossible to monitor and control
- Safety management: proactive, continiously trying to anticipate developments and events
- Definition of safety:
- As much as possible goes right

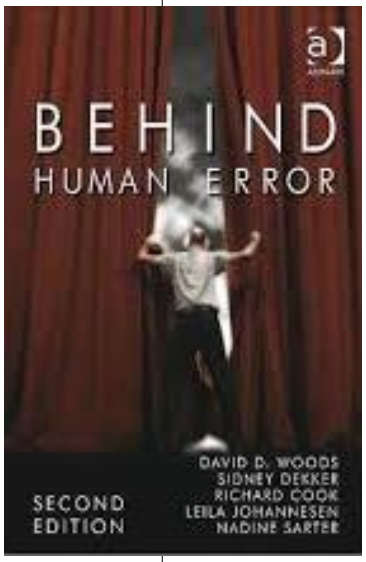


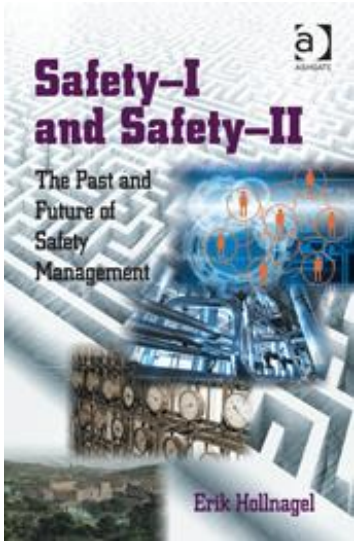

TNO innovation for life

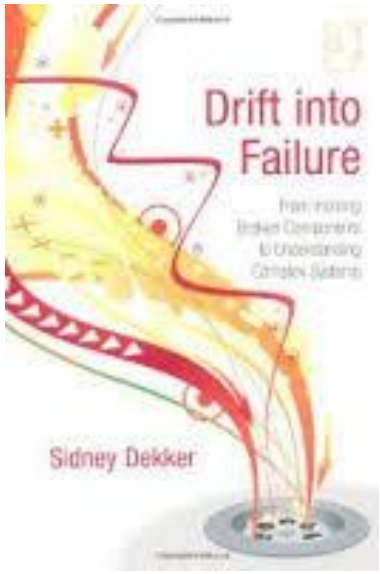
High reliability organisations (HRO)

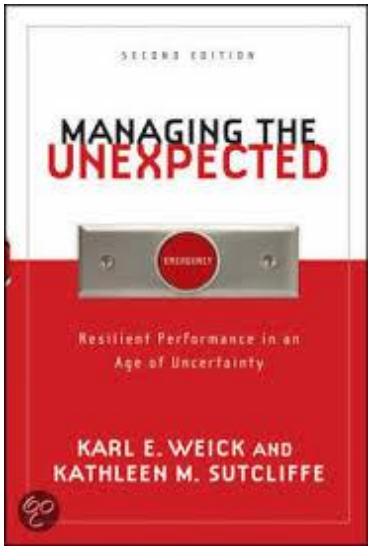
- Preoccupation with failure
- Reluctance to simplify interpretations
- Sensitivity to operations
- Commitment to resilience
- Deference to expertise
- Redundancy built in

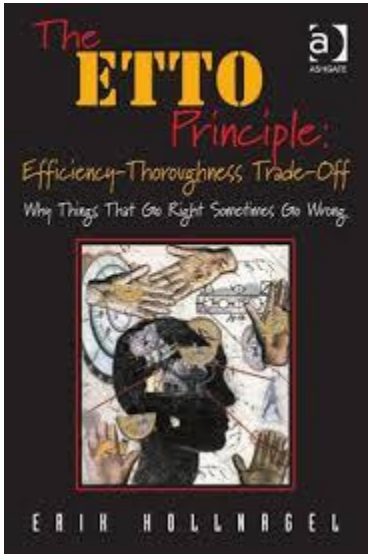
Suggested reading











TNO innovation for life


TNO innovation for life

Conclusions

This is not the final verdict

Take home message:

- Be vigilant: is what we do today sufficient for the challenges of tomorrow?
- Try to recognize weak signals
- You cannot engineer complexity out of a system, however, you may tame it (slightly)
- Learn from things that go well
- In CAS there is no point in looking back for the ‘golden rivet’ (emergent properties)
- Maybe we need to apply the precautionary principle more

- Good luck!
- Thank you for you kind attention


time for discussion