



Different perspective?

A view from the safety II domain

Raphaël Gallis





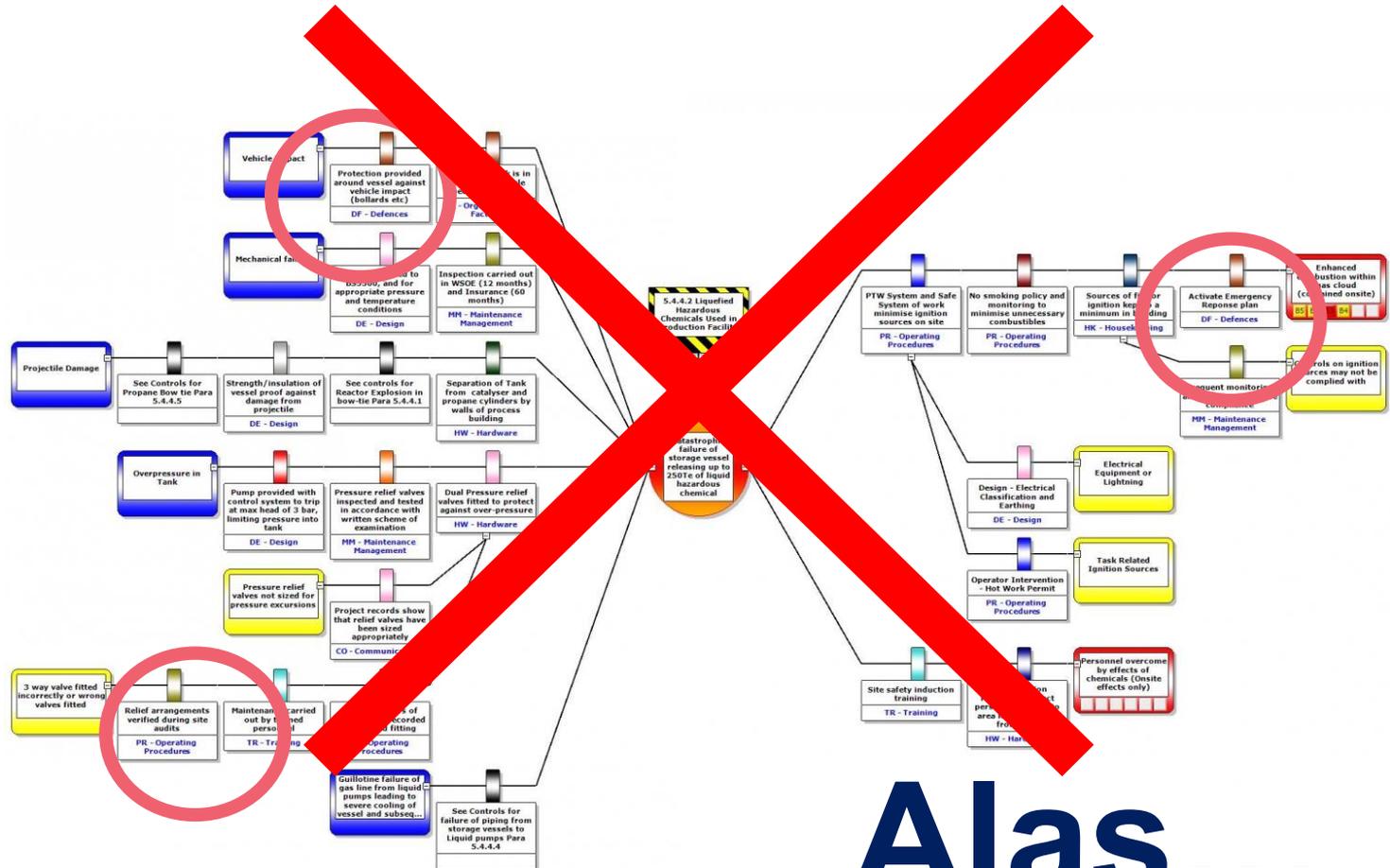
Aim

Still confused but on a higher level

(Enrico Fermi)



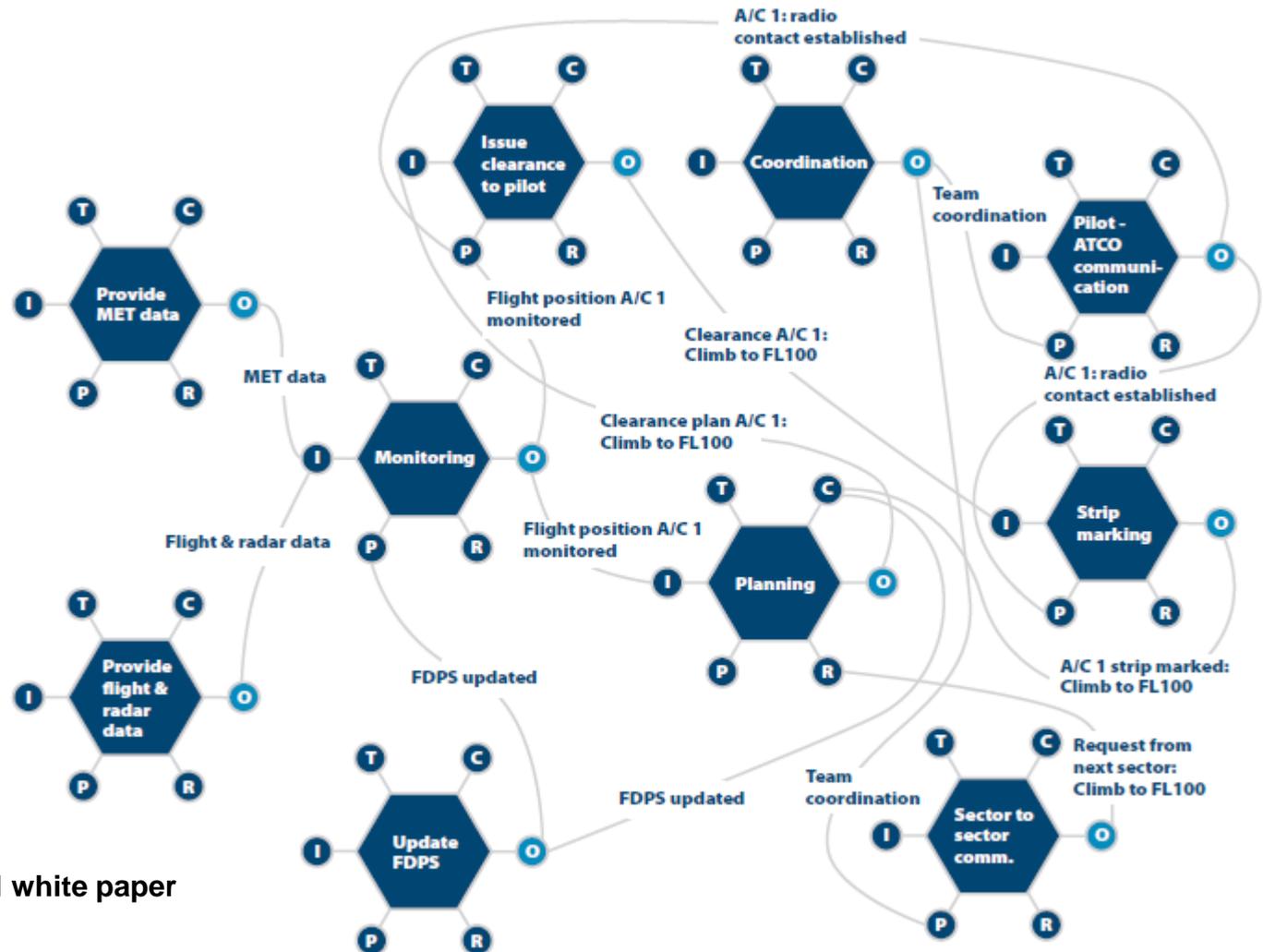
Old school



Alas...



Now



Source: Eurocontrol white paper

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



What is the difference between safety I and II?

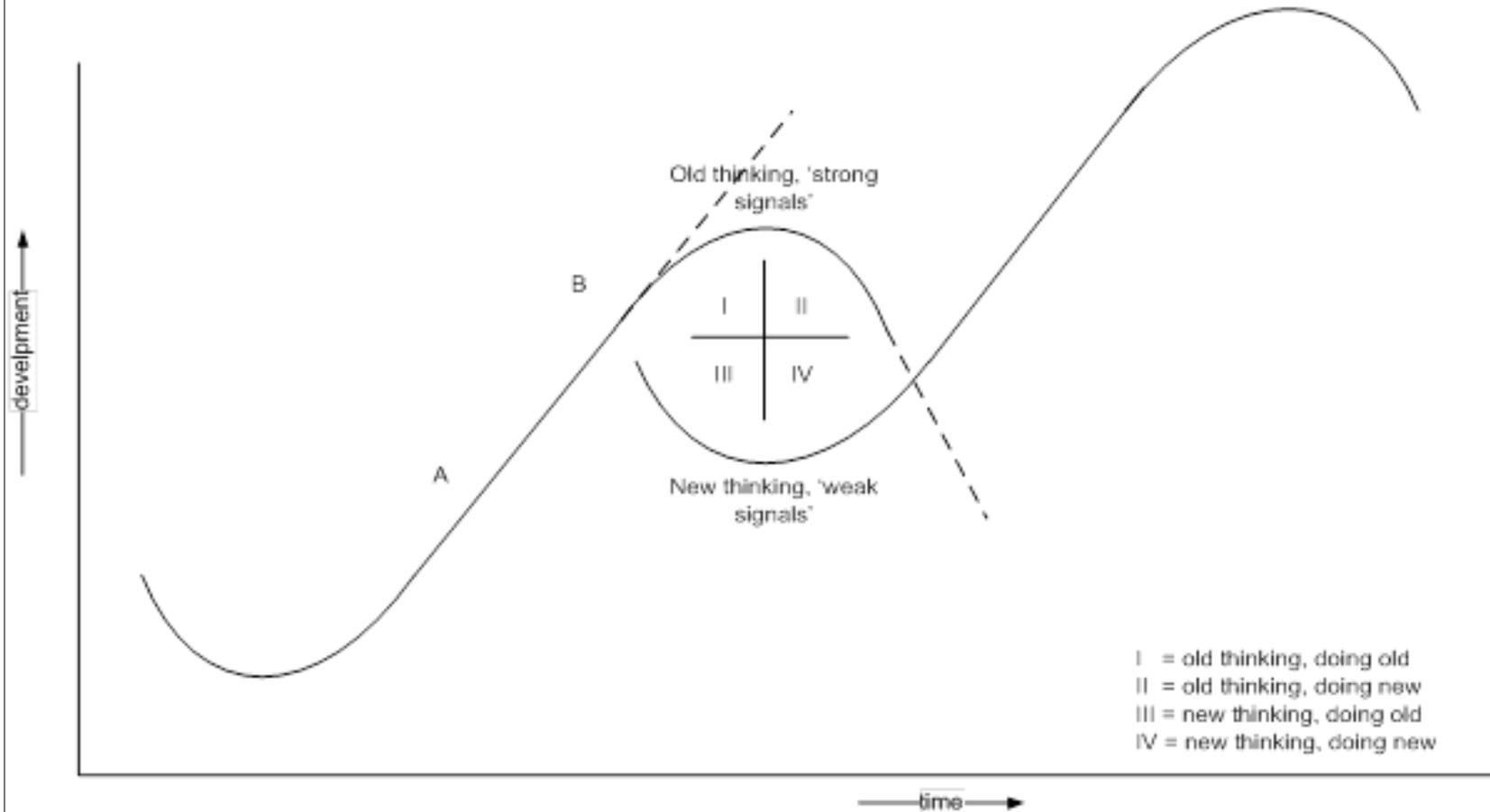
In order to answer that question we need to answer to following:

- › 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

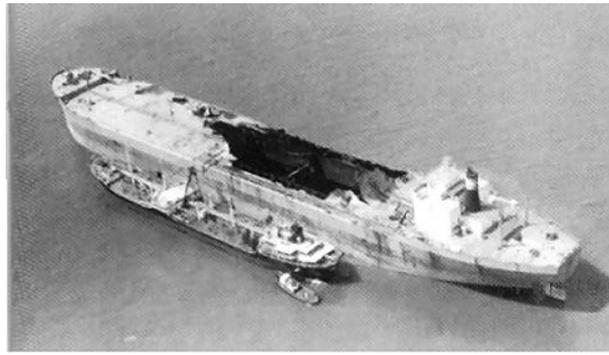


Examples

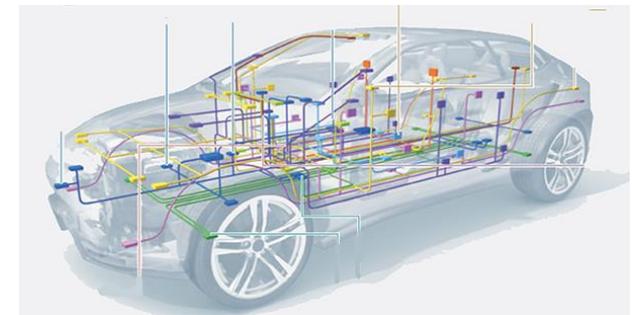
- › Jet airliners (De Havilland Comet)
- › VLCC's (Mactra, King Haakon VII, Marpessa)



Mactra (2) at Durban after the explosion. (Photo by Henry van den Heever)



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





Complexity

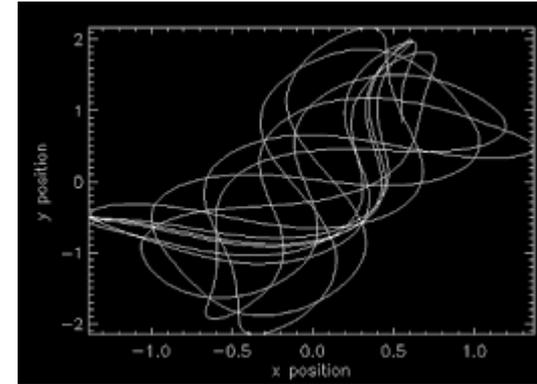
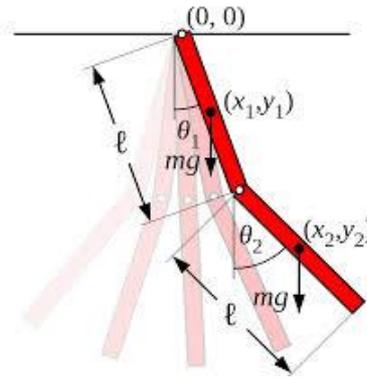


Cynefin model by Dave Snowden



Examples of complexity

› Double Pendulum



› The butterfly effect





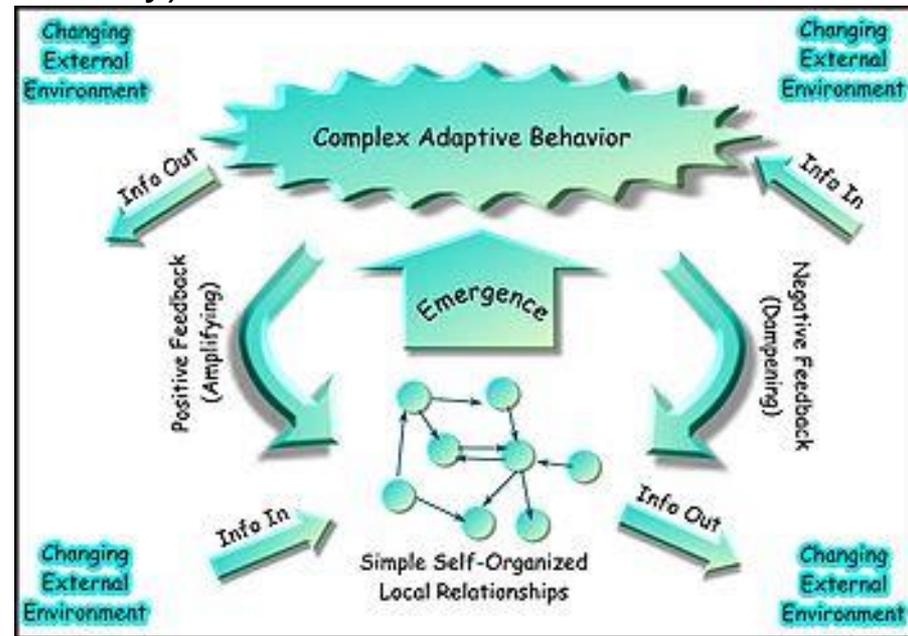
Complex Adaptive Systems (CAS)

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

The end of Newtonian Models

Characteristics:

- › Emergent properties
- › Agents
- › Self organisation
- › Adaptive
- › There is NO helicopter
- › Local control
- › not 'bi-model'
- › Non linear cause – effect relationships





Over to the Deepwater Horizon



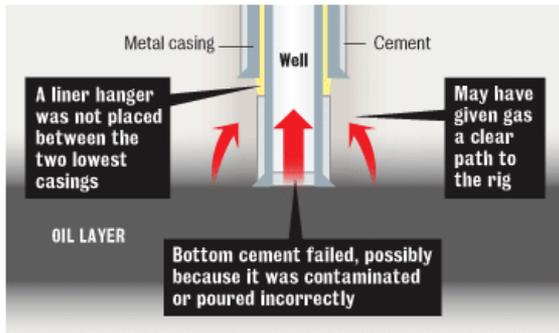


True, however.....

SIX STEPS THAT DOOMED THE RIG

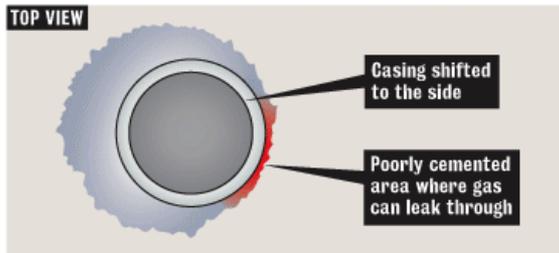
1 FEWER BARRIERS TO GAS FLOW AT WELL BOTTOM

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.



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

3 NO BOND LOG TO TEST CEMENT INTEGRITY

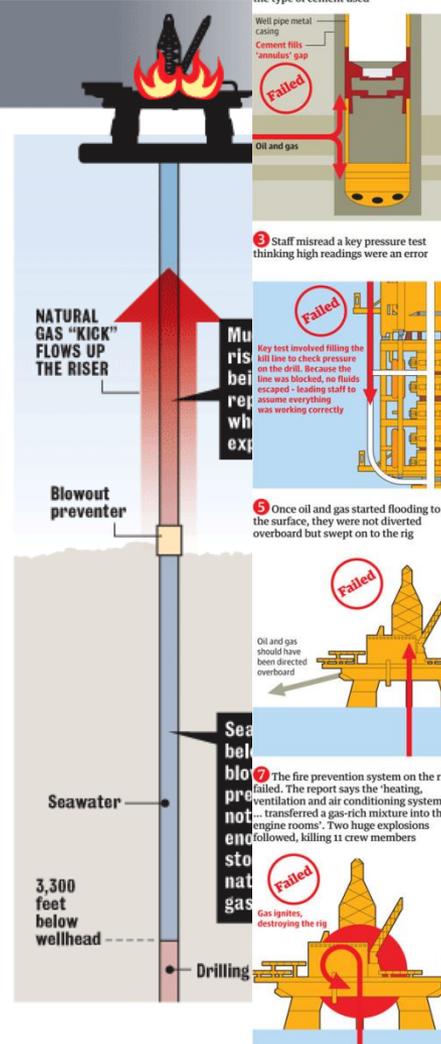
BP had hired contractor Schlumberger to run tests on the newly cemented well. But BP sent Schlumberger's crew home on a helicopter without having it run the test, called a cement bond log.

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

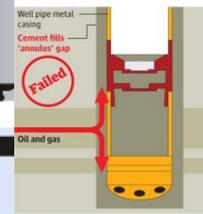
BP decided to take heavy drilling mud out of the system, to 3,000 feet below the normal point, and earlier than usual. The barrier wasn't there to stem the gas kick that destroyed the rig. The mud is used to keep any upward pressure under control.



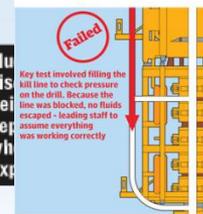
What went wrong?

The BP report identifies eight key elements in the Deepwater Horizon drilling operation - each of which could have prevented the disaster

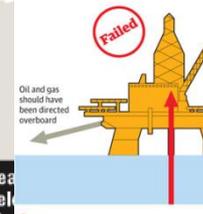
1 The cement that was supposed to stop oil and gas reaching the well pipe casing did not work. The report blames the type of cement used



3 Staff misread a key pressure test thinking high readings were an error



5 Once oil and gas started flooding to the surface, they were not diverted overboard but swept on to the rig



7 The fire prevention system on the rig failed. The report says the "heating, ventilation and air conditioning system ... transferred a gas-rich mixture into the engine rooms". Two huge explosions followed, killing 11 crew members



The key times

20 April 9.40pm

Report: 'This overwhelmed the ... system'

20 April 9.45pm

Report: 'The fire and gas system did not prevent ... ignition'

20 April 8.50pm

Report: 'Rig crew did not recognise the influx'

20 April 7.55pm

Report: 'Site leaders reached the incorrect view'

20 April 9.56pm

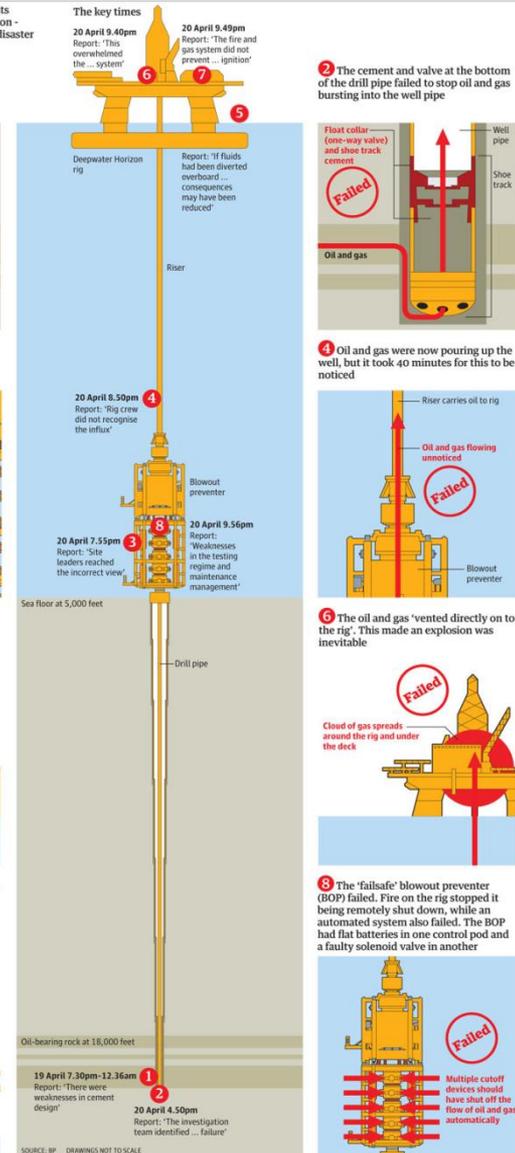
Report: 'Weaknesses in the testing regime and maintenance management'

19 April 7.30pm-12.36am

Report: 'There were weaknesses in cement design'

20 April 4.50pm

Report: 'The investigation team identified ... failure'



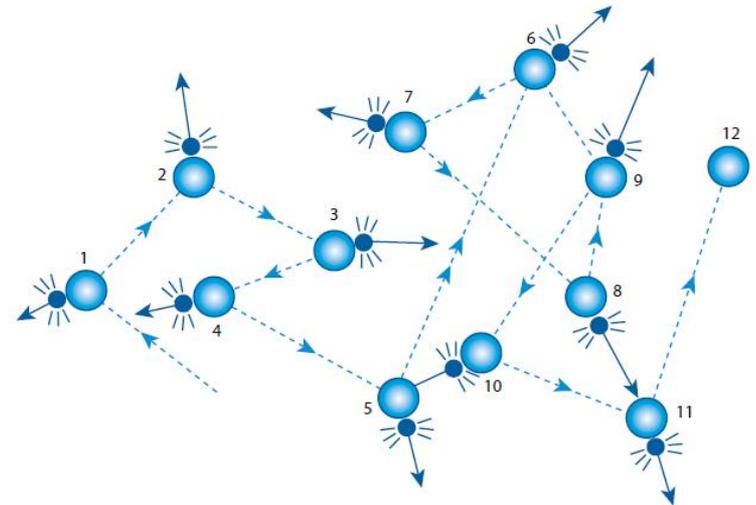
SOURCE: BP. DRAWINGS NOT TO SCALE



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 acknowledge complexity

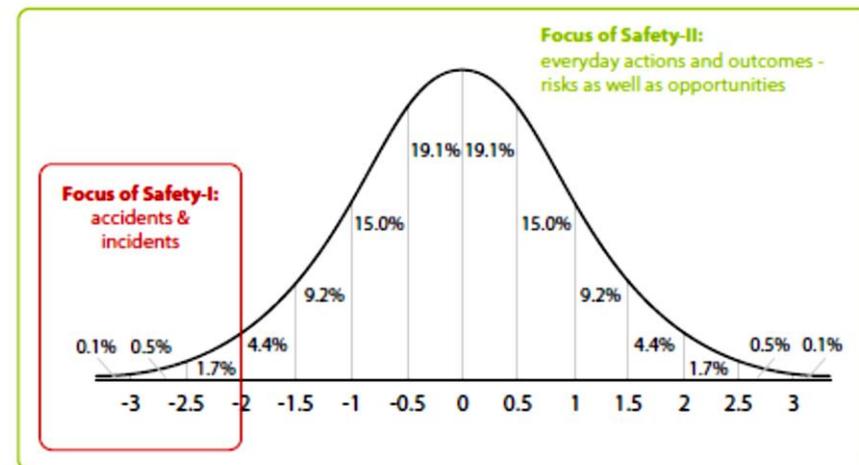
We try to apply tools from one system for another: → does not work

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



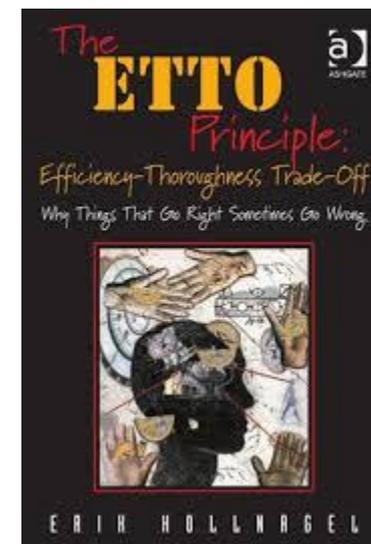
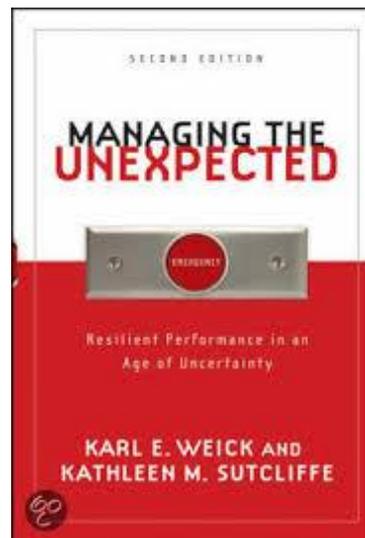
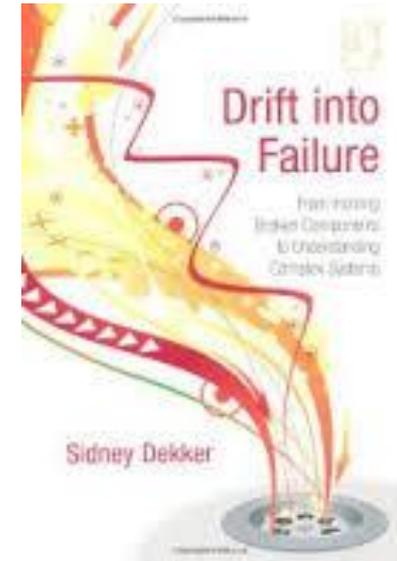
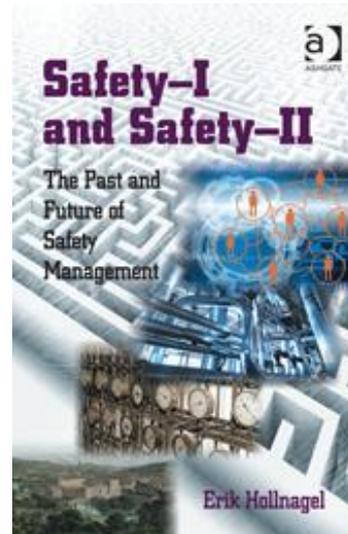
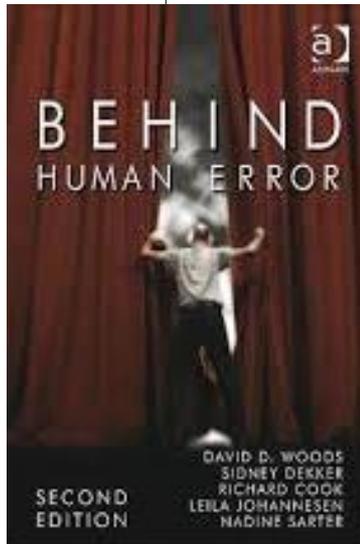


High reliability organisations (HRO)

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



Suggested reading





18
December 16, 2014
Raphaël Gallis
A different perspective?

TNO innovation
for life

6TH SYMPOSIUM ON RESILIENCE ENGINEERING

Managing resilience, learning to be adaptable
and proactive in an unpredictable world



22-25th June
2015 | Lisbon, Portugal

Rio de Janeiro, Brazil 5 | (1750) 285111
Tel: +351 21 251 27 00 | 861 33 65 43
Fax: +351 21 251 29 65 | joao.pedro@tno.nl



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 your kind attention

