What if our models of risk are insufficient?

Risk modelling in complex, dynamic environments

@madplatt
www.securitydifferently.com

Where are we ? The Sociotechnical system

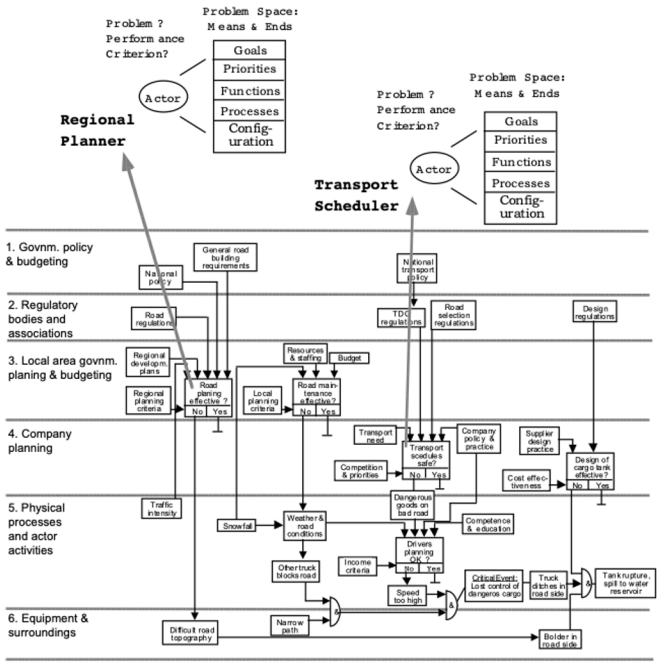


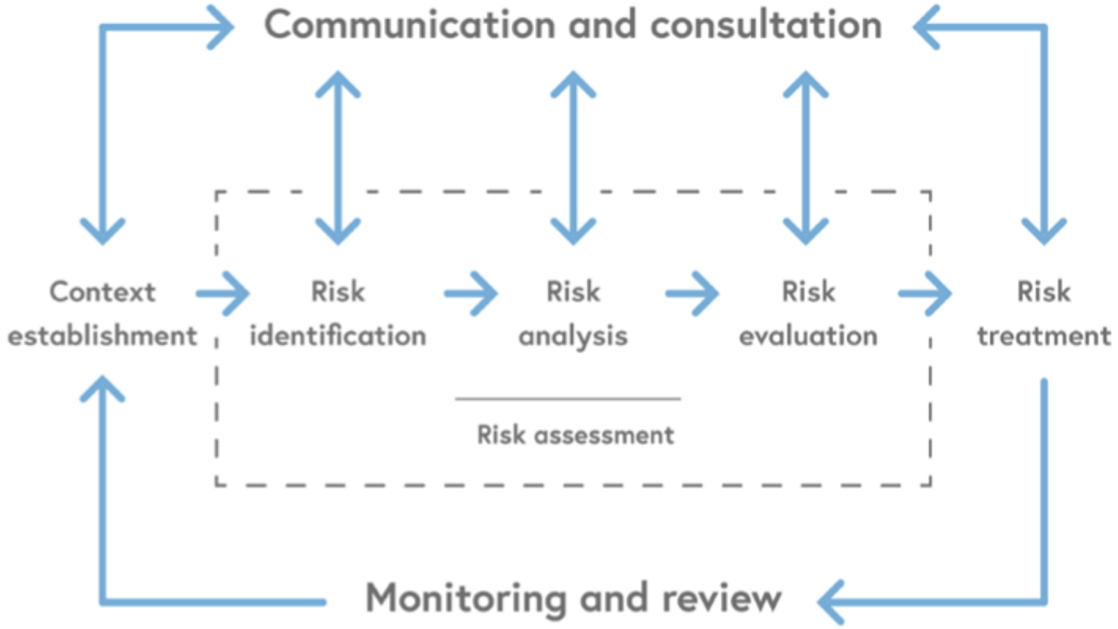
Figure 6. The course of an accidental event is created by side effects of decisions made by decision-makers busy coping with their local work requirements.

The Challenges:

- **Complex network of interdependencies** across stakeholder groups
- There are many **degrees of freedom** from each actor (impossible to foresee all local contingencies)
- All actors will tend to **rationalise behaviour when making local decisions** which may affect upstream and downstream actors in unforeseeable ways, when resolving goal conflicts

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. Safety Science, 27(2-3), 183-213. https://doi.org/10.1016/S0925-7535(97)00052-0

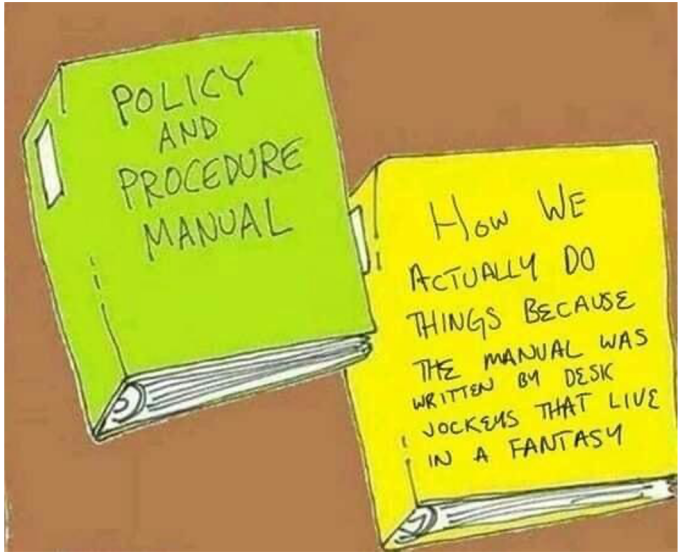
Risk-management-as-Imagined

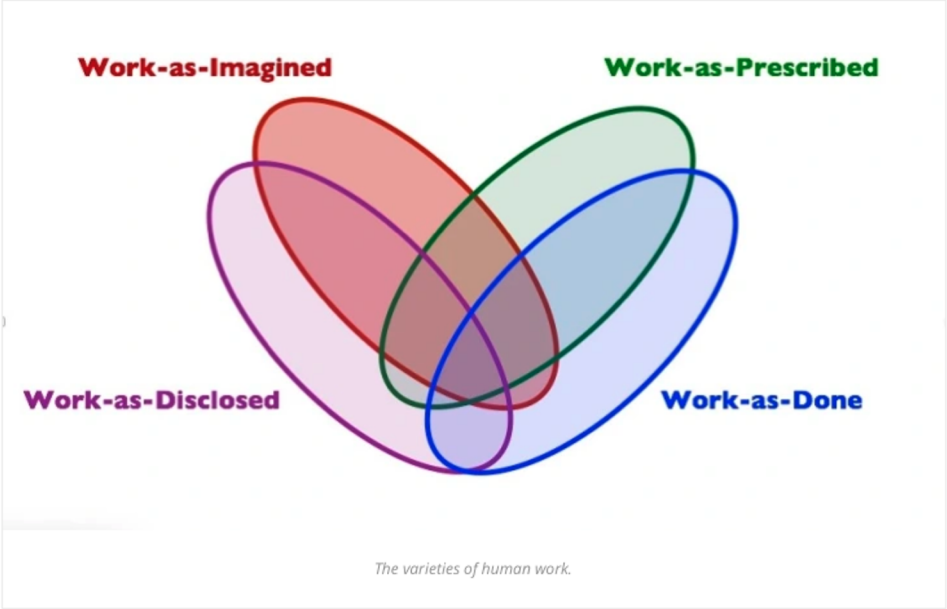


Risk Management as defined in ISO 3100 and ISO 27005

Design involves "matching an object that does not yet exist to a context which cannot be completely specified" [Rasmussen quoting Alexander]

But there's an elephant in the room





Shorrock, Steven. "The varieties of human work" https://humanisticsystems.com/2016/12/05/the-varieties-of-human-work/

Risk-management-as-Done

Org chart fence

Work as Imagined

Operation A
Team 1

Risk and
Compliance
Managers

Risk analysis
process

Controls Top Hat

Operation B
Team 2

Training and
ingrained patterns
(bias)

Accepted Industry
best practices

"We see what we expect to see"

A Functional abstraction approach

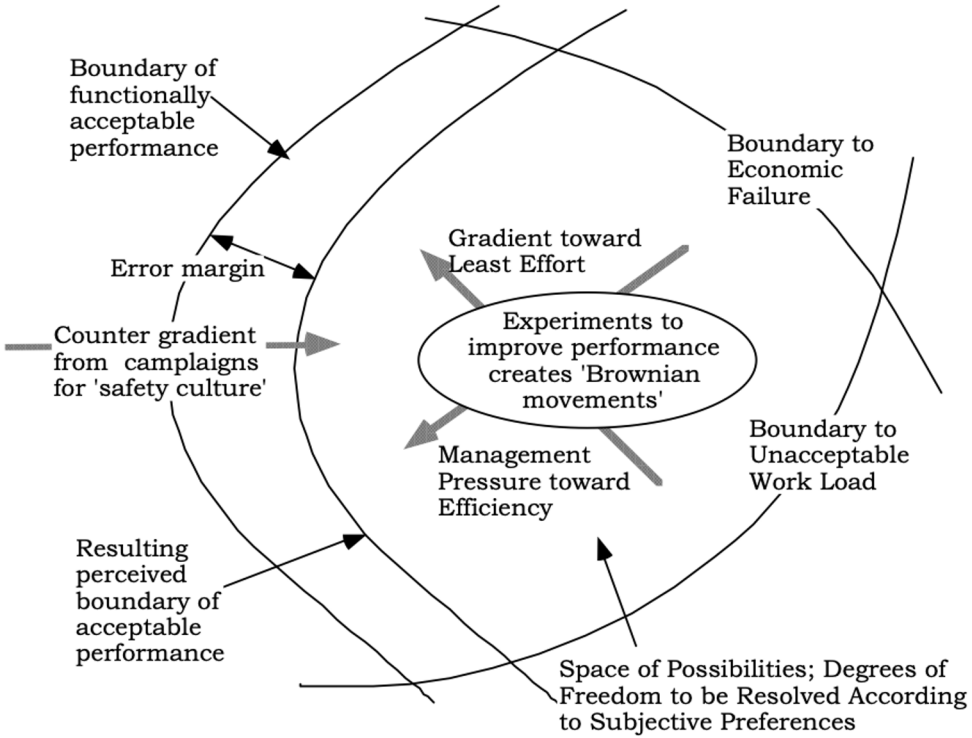
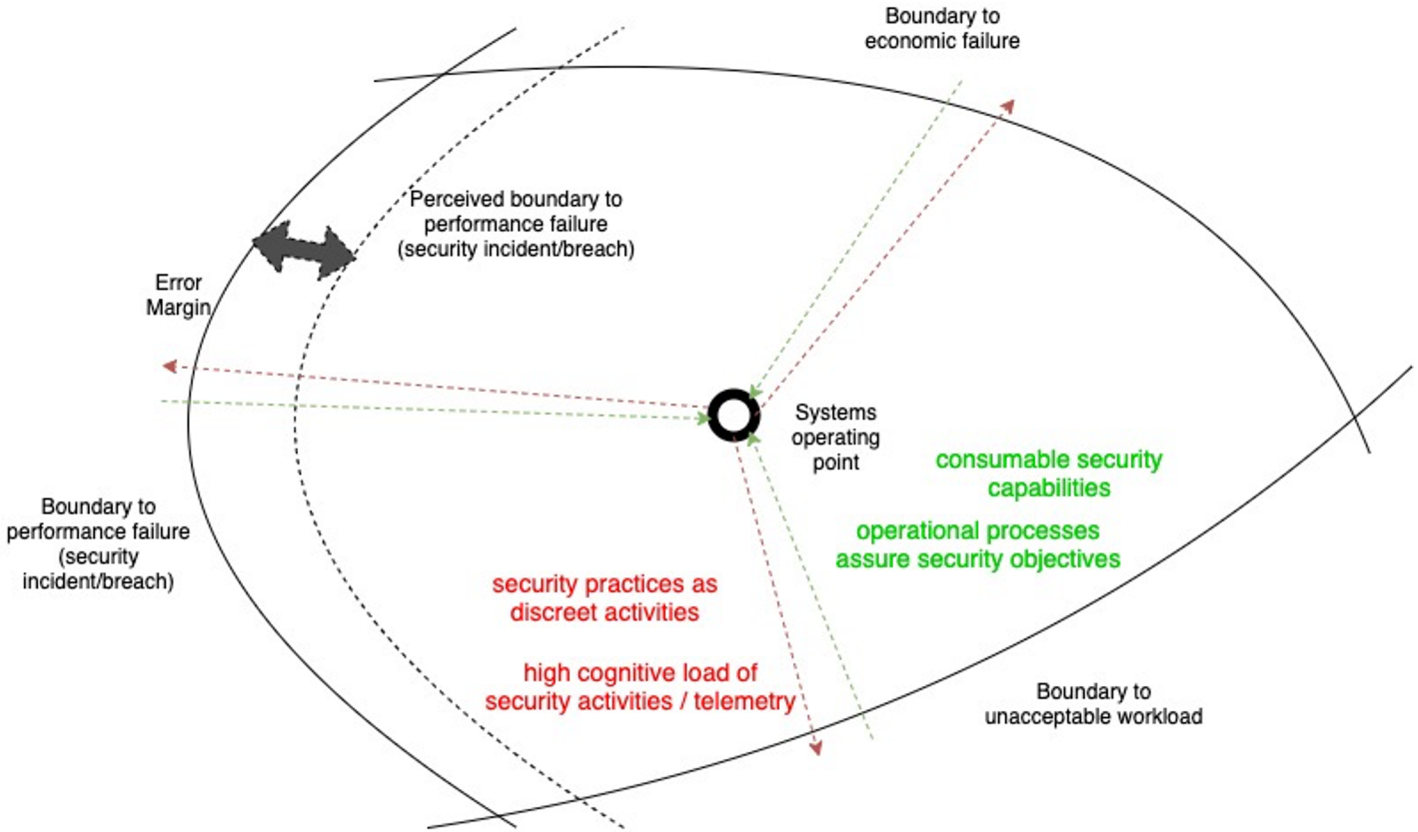


Figure 3. Under the presence of strong gradients behaviour will very likely migrate toward the boundary of acceptable performance.

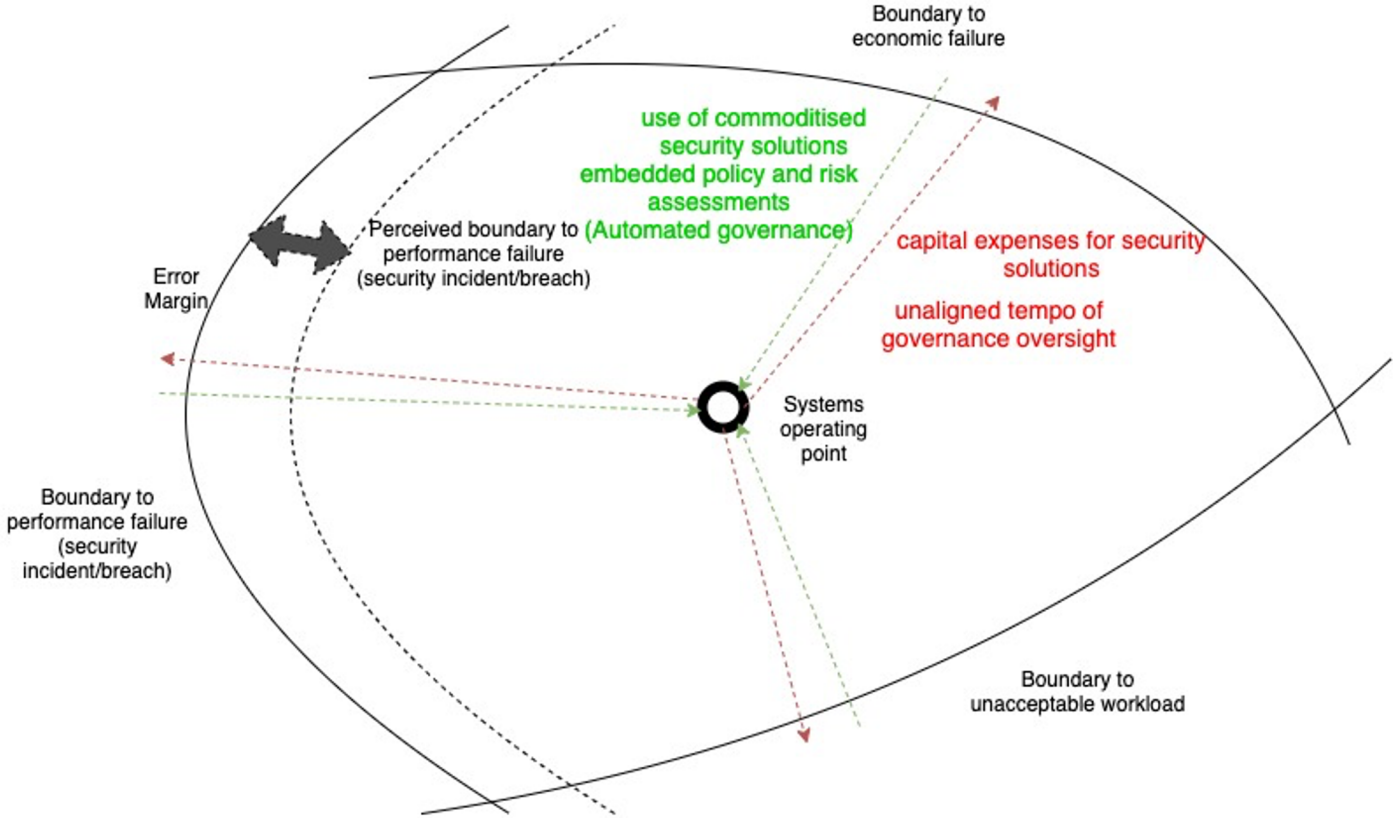
Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. Safety Science, 27(2-3), 183-213. https://doi.org/10.1016/S0925-7535(97)00052-0

Unacceptable workload boundaries



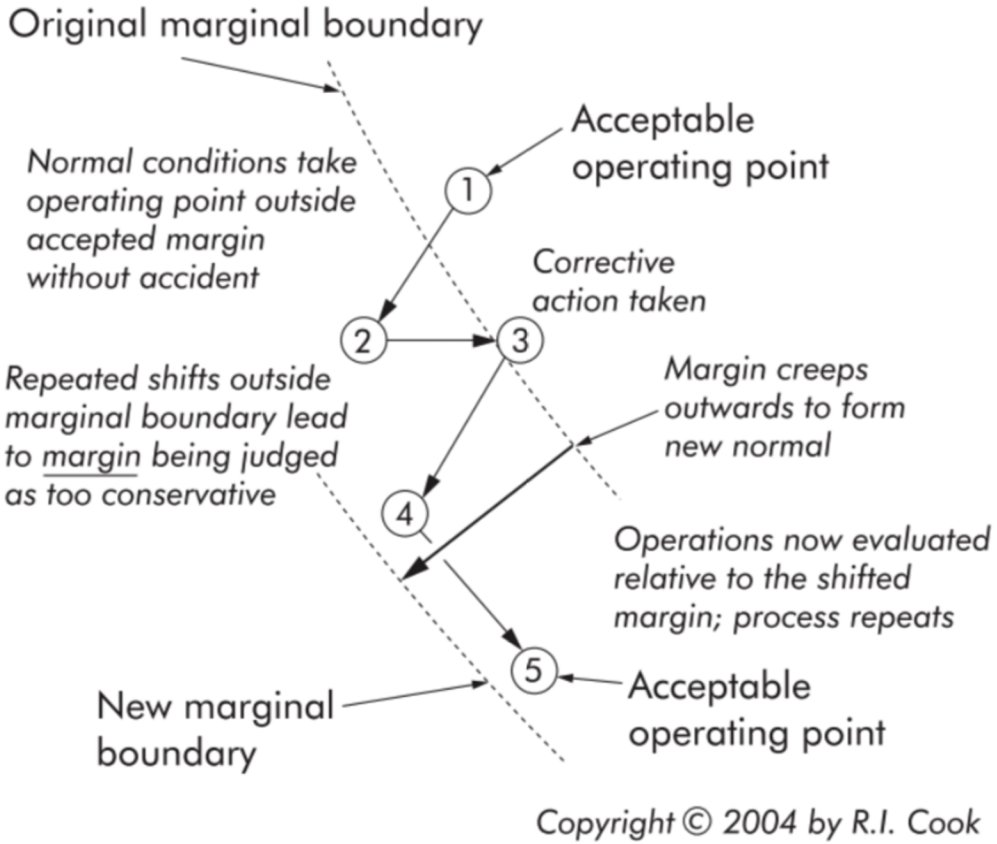
Adapted from Jens Rasmussen
Risk management in a dynamic society - a modelling problem

Economic failure boundaries



Adapted from Jens Rasmussen
Risk management in a dynamic society - a modelling problem

Marginal boundaries and Normalisation of Deviance



Risk and Compliance functions don't share a model of where the marginal boundary is or where it should be with Engineering / Operations

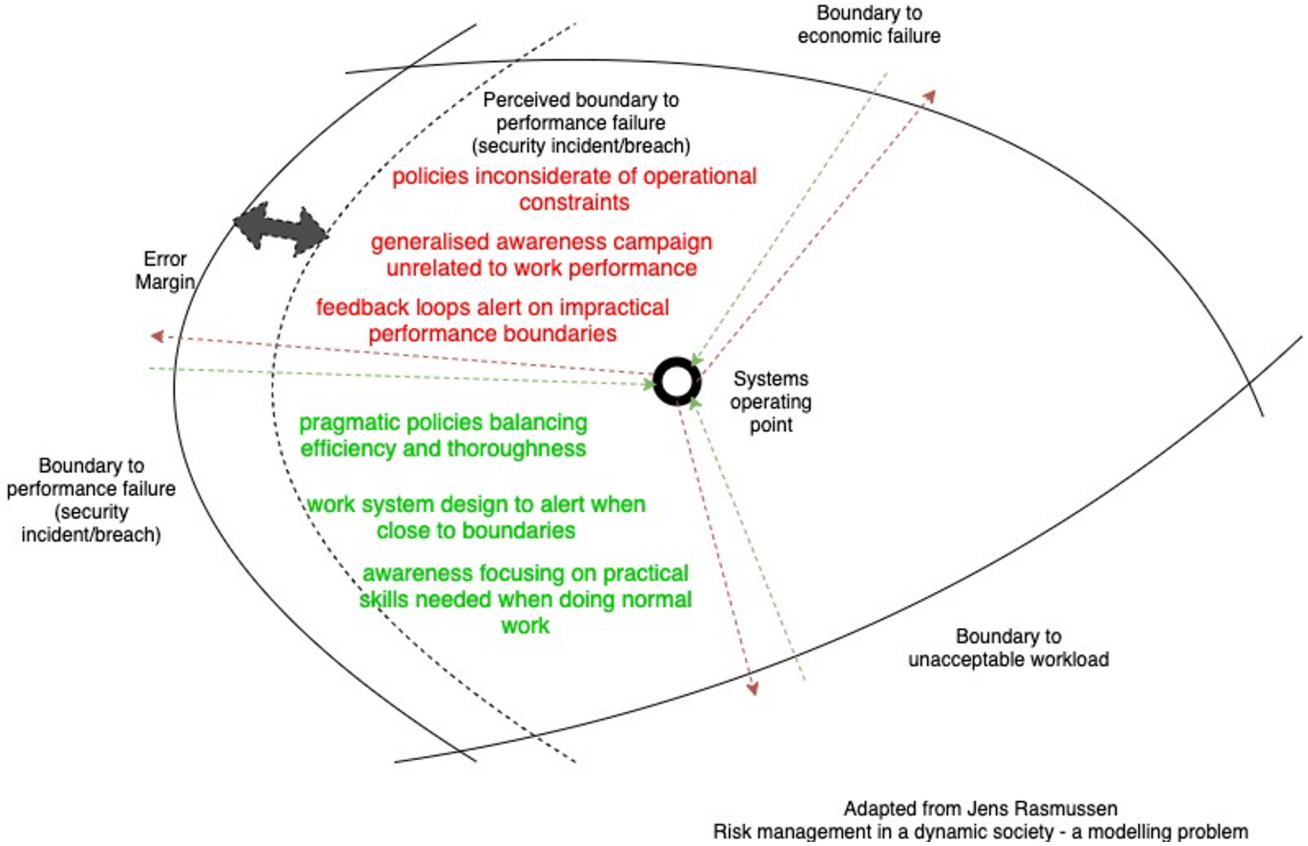
Unrealistic policies set the tone for normalisation of deviance which deteriorates over time

Covert work systems emerge

Eventually… drifts into failure

Cook, R. (2005). "Going Solid": a model of system dynamics and consequences for patient safety.Qual Saf Health Care 2005;14:130–134. doi: 10.1136/qshc.2003.009530

Unacceptable performance boundaries



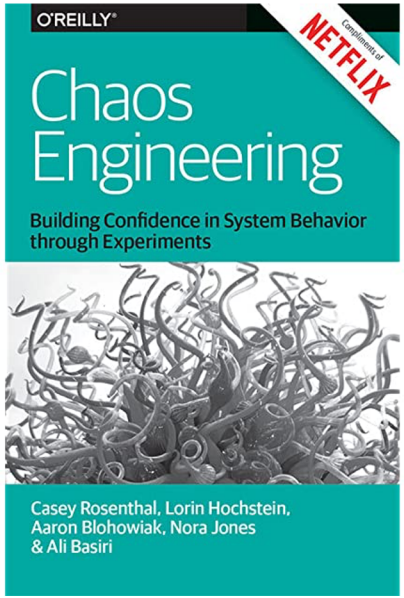
Adapted from Jens Rasmussen
Risk management in a dynamic society - a modelling problem

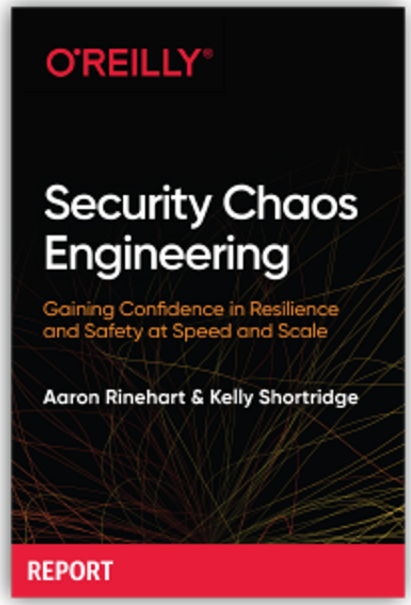
"It's the design that creates behavior change. Not rules and decrees from the top-down. It's the design"

- Sidney Dekker

Coping skills at boundaries

- Chaos Engineering
- Security Chaos Engineering
- Game Days / Storm Drills
- Disaster Recovery exercises (with surprises)





"all systems, however successful, have boundaries and experience events that fall outside these boundaries—model surprise" (Woods 2015), "theory of graceful extensibility"

Real-World Risk Management requires multiple strategies

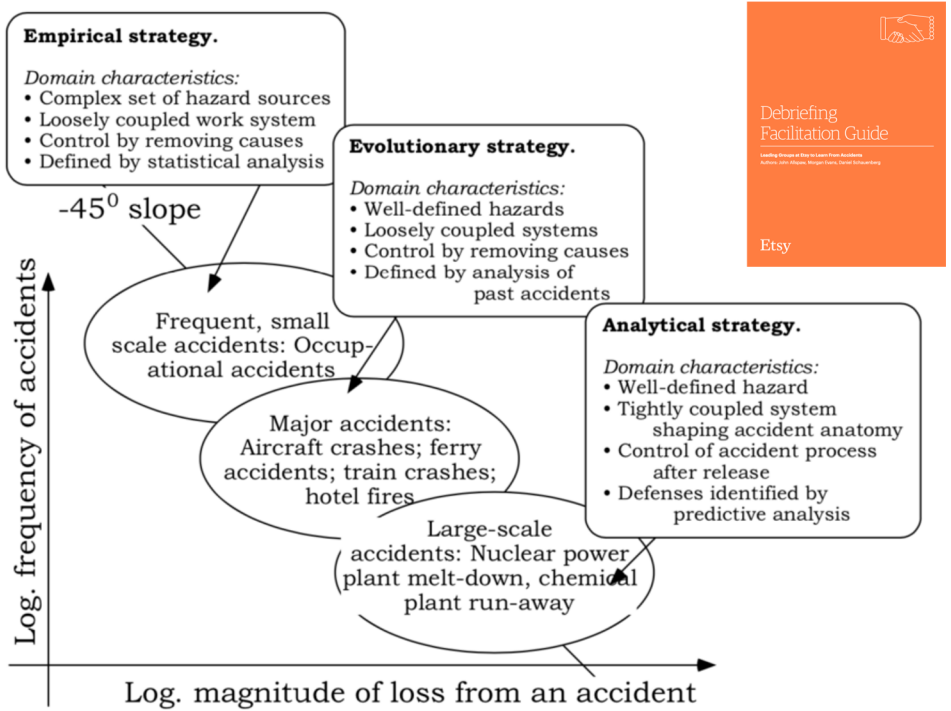


Figure 7. Hazard source characteristics and risk management strategies.

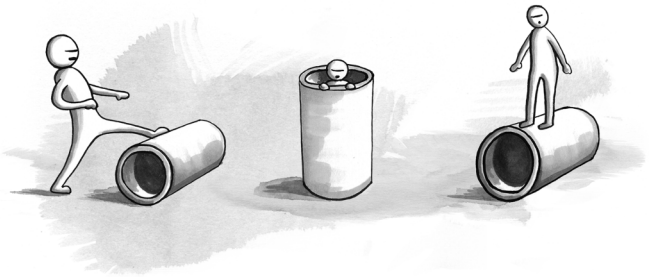
Empirical strategy - where we can **apply simple controls (automated governance)**, things happen often so it's simple to study and discuss with operators best approaches and heuristics to control them

Evolutionary strategy - we can analyse past events and understand how **different parts of sociotechnical system interacted to produce conditions** which led to incidents

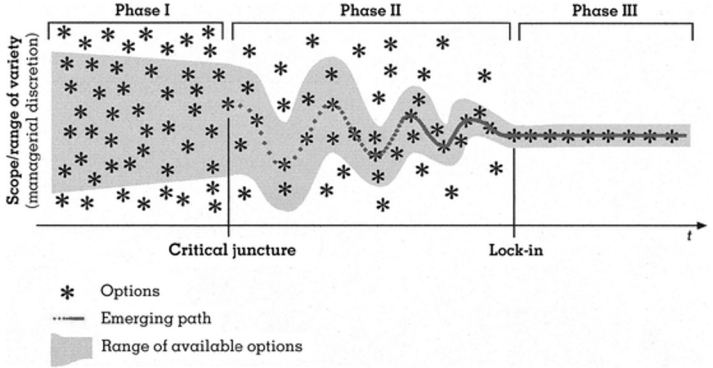
Analytical Strategy - well-defined hazards but entanglements of systems are numerous, **requires appreciation and understanding of entanglements** and how failures in one part of the system can affect other parts

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. Safety Science, 27(2-3), 183-213. https://doi.org/10.1016/S0925-7535(97)00052-0

Managing IN complexity - Muddling through



"Affordance is what the environment offers the individual"
James J. Gibson



Complex systems have a history (path dependency)

https://quotefancy.com/quote/1160460/W-Edwards-Deming-It-is-not-necessary-to-change-Survival-is-not-mandatory

Mario Platt

Twitter: @madplatt
Linkedin: marioplatt
Email: mario.platt@privacybeacon.io

Blog & Talks:
www.securitydifferently.com