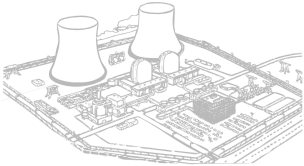
RISK ENGINEERING



Safety models & accident models

Eric Marsden

<eric.marsden@risk-engineering.org>

Mental models

- A *safety model* is a set of beliefs or hypotheses (often implicit) about the features and conditions that contribute to the safety of a system
- An *accident model* is a set of beliefs on the way in which accidents occur in a system
- Mental models are important because they impact system design, operational decisions and behaviours

RISK ENGINEERING

Accidents as “acts of god”

- Fatalism: “you can’t escape your fate”
- Defensive attitude: accidents occur due to circumstances “beyond our control”
- Notion that appeared in Roman law: reasons that could exclude a person from absolute liability
  - *e.g.* violent storms & pirates exempted a captain from responsibility for his cargo

Simple sequential accident model

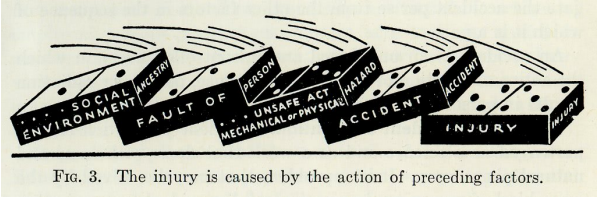


Fig. 3. The injury is caused by the action of preceding factors.

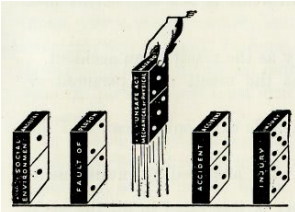


Fig. 4. The unsafe act and mechanical hazard constitute the central factor in the accident sequence.

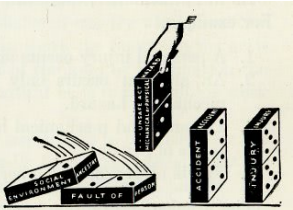


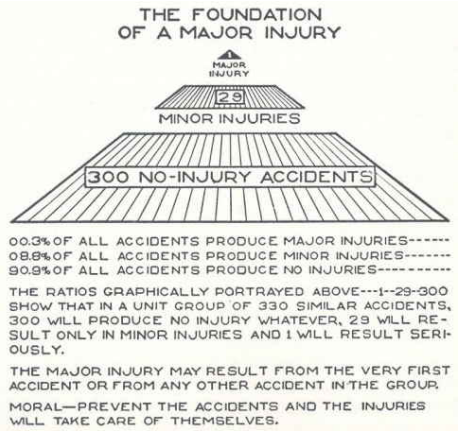
Fig. 5. The removal of the central factor makes the action of preceding factors ineffective.

H. Heinrich's **domino model** (1930)

Assumptions:

- Accidents arise from a quasi-mechanical sequence of events or circumstances, that occur in a well-defined order
- An accident can be prevented by removing one of the "dominos" in the causal sequence

Simple sequential accident model



The "**safety pyramid**" or "accident triangle" (H. Heinrich, 1930 and F. Bird, 1970)

Assumptions:

- Each incident is an "embryo" of an accident (the mechanisms which cause minor incidents are the same as those that create major accidents)
- Reducing the frequency of minor incidents will reduce the probability of a major accident
- Accidents can be prevented by identifying and eliminating possible causes

Simple sequential accident model

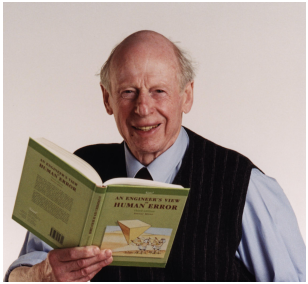
According to this model, safety is improved by identifying and eliminating “rotten apples”

- front-line staff who generate “human errors”
- whose negligent attitude might propagate to other staff

Some accidents (in particular in high-risk systems) have more complicated origins…

On “human error”

> *for a long time people were saying most accidents were due to human error and this is true in a sense but it’s not very helpful. It’s a bit like saying that falls are due to gravity...*
>
> — *Trevor Kletz*

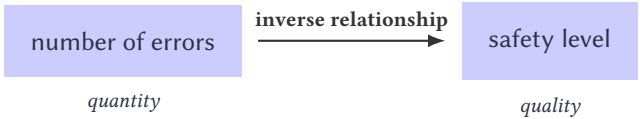


A useful alternative concept to human error is *performance variability*.

RISK ENGINEERING

Is it relevant to count errors?

- Counting errors produces a quantitative assessment of the “safety level” of a system
- Allows inter-comparison of systems
- Can constitute the point of departure for a search for the underlying causes of incidents



This simplistic model is very criticized

Is counting errors relevant?

Who is more dangerous?

Is counting errors relevant?

- ▷ 700 000 doctors in the USA
- ▷ between 44 000 and 98 000 people die each year from a medical error

→ between 0.063 and 0.14 accidental deaths per doctor per year

Is counting errors relevant?

- ▷ 700 000 doctors in the USA
- ▷ between 44 000 and 98 000 people die each year from a medical error
- ⟶ between 0.063 and 0.14 accidental deaths per doctor per year

- ▷ 80 million firearm owners in the USA
- ▷ responsible for ≈1500 accidental deaths per year
- ⟶ 0,000019 accidental deaths per firearm owner per year

RISK ENGINEERING

Is counting errors relevant?

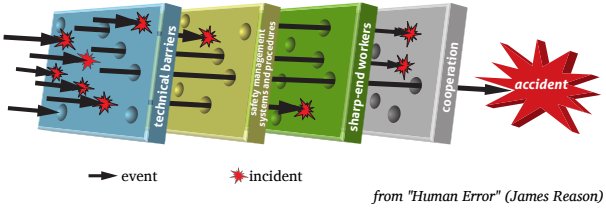
- ▷ 700 000 doctors in the USA
- ▷ between 44 000 and 98 000 people die each year from a medical error
- ⟶ between 0.063 and 0.14 accidental deaths per doctor per year

- ▷ 80 million firearm owners in the USA
- ▷ responsible for ≈1500 accidental deaths per year
- ⟶ 0,000019 accidental deaths per firearm owner per year

The probability that the human error of a doctor kills someone is 7500 times higher than for a firearm owner. [S. Dekker]

RISK ENGINEERING

Epidemiological accident model



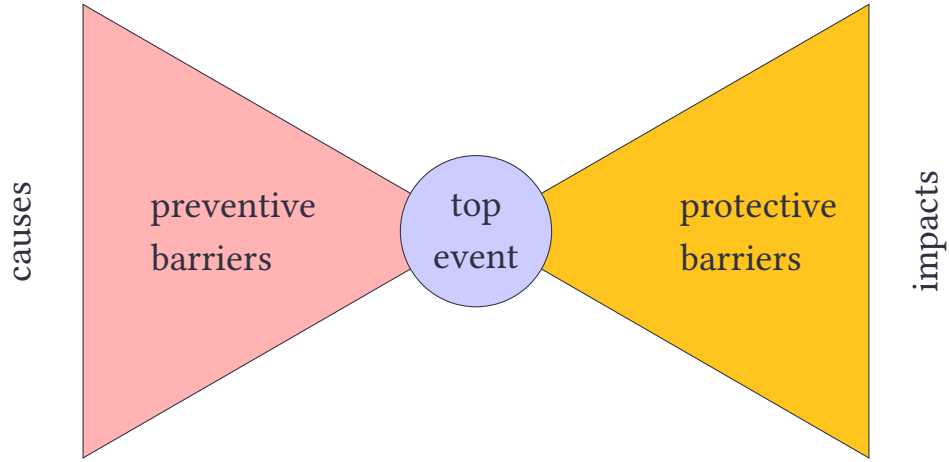
from "Human Error" (James Reason)

James Reason's Swiss cheese model

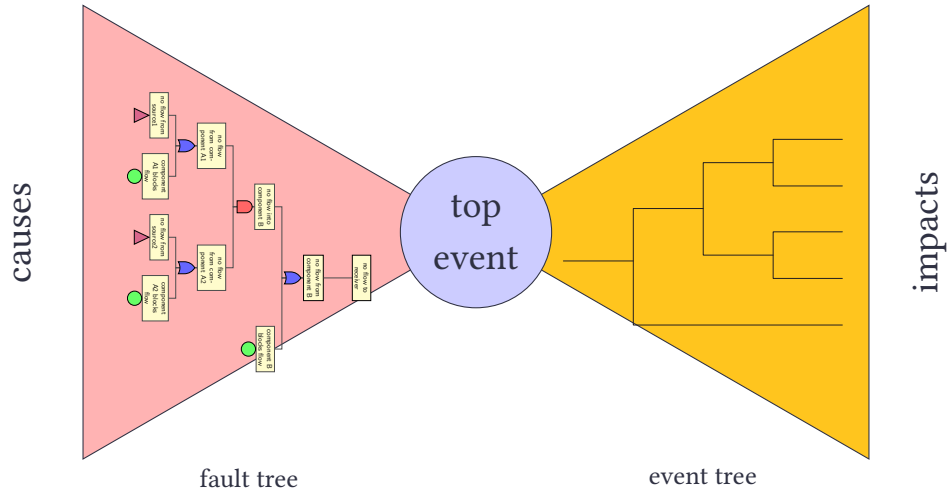
Assumption: accidents are produced by a combination of active errors (poor safety behaviours) and latent conditions (environmental factors)

Consequences: prevent accidents by reinforcing barriers. Safety management requires monitoring via **performance indicators**.

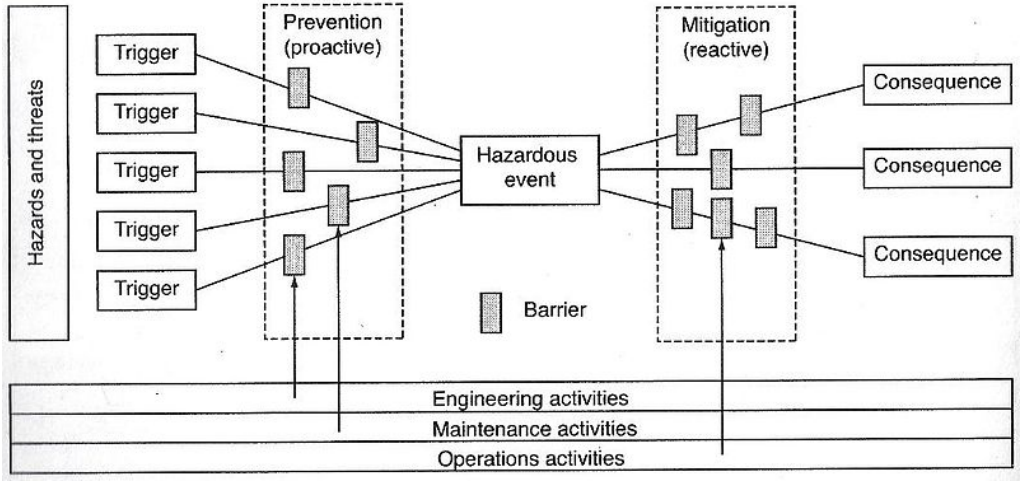
Bow-tie model



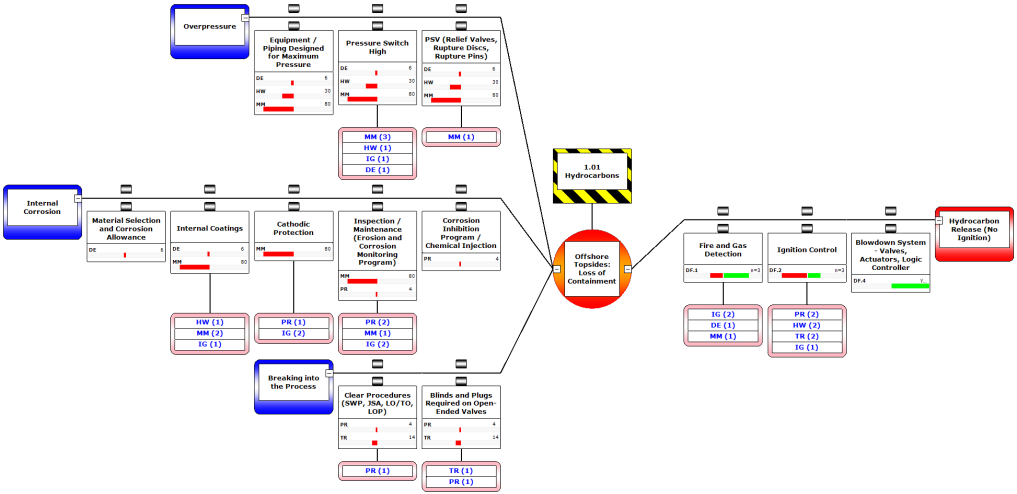
Bow-tie model



Bow tie diagram



Bow-tie: example



RISK ENGINEERING

Loss of control accident model

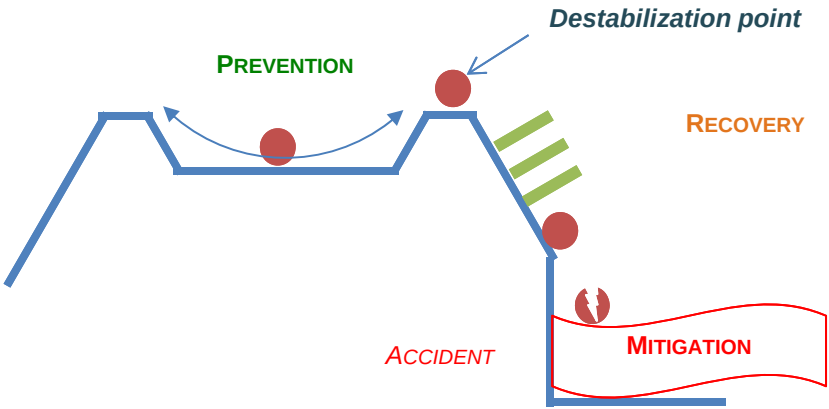
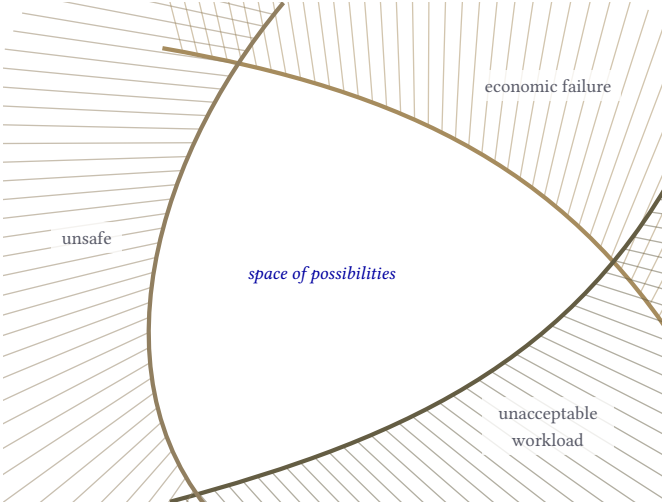


Figure source: French BEA

Drift into failure

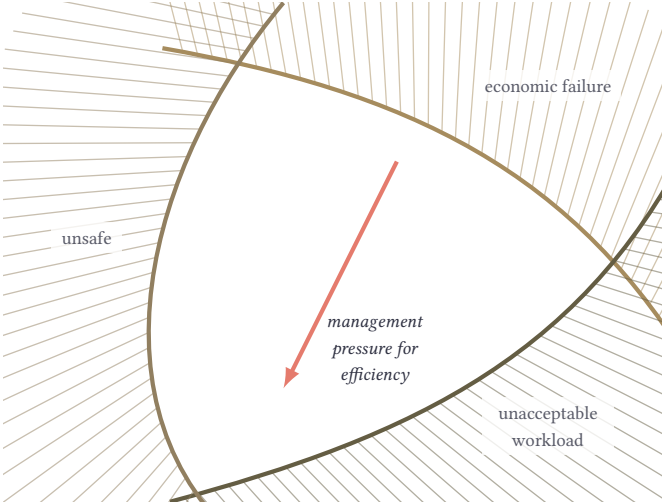


Human behaviour in any large system is shaped by constraints: profitable operations, safe operations, feasible workload. Actors experiment within the space formed by these constraints.

Figure adapted from *Risk management in a dynamic society*, J. Rasmussen, Safety Science, 1997:27(2)

RISK ENGINEERING

Drift into failure



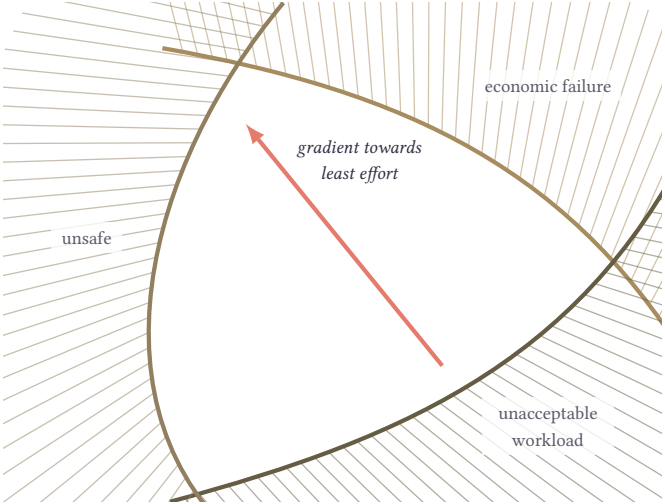
Human behaviour in any large system is shaped by constraints: profitable activity, safe operations, feasible workload. Actors experiment within the space formed by these constraints.

Management will provide a "cost gradient" which pushes activity towards economic efficiency.

Figure adapted from *Risk management in a dynamic society*, J. Rasmussen, Safety Science, 1997:27(2)

RISK ENGINEERING

Drift into failure



Human behaviour in any large system is shaped by constraints: economic, safety, feasible workload. Actors experiment within the space formed by these constraints.

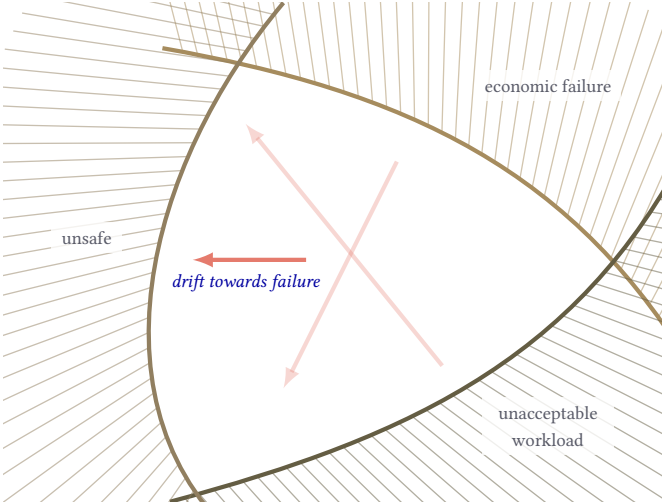
Management will provide a "cost gradient" which pushes activity towards economic efficiency.

Workers will seek to maximize the efficiency of their work, with a gradient in the direction of reduced workload.

Figure adapted from *Risk management in a dynamic society*, J. Rasmussen, Safety Science, 1997:27(2)

RISK ENGINEERING

Drift into failure



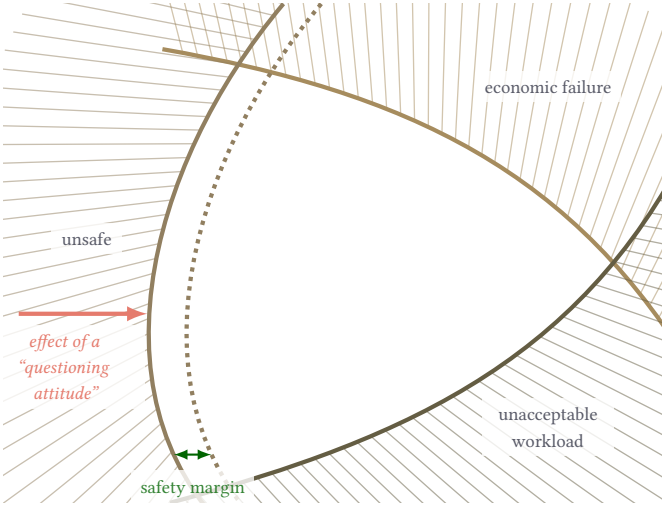
These pressures push work to migrate towards the limits of acceptable (safe) performance. Accidents occur when the system's activity crosses the boundary into unacceptable safety.

A process of "normalization of deviance" means that deviations from the safety procedures established during system design progressively become acceptable, then standard ways of working.

Figure adapted from *Risk management in a dynamic society*, J. Rasmussen, Safety Science, 1997:27(2)

RISK ENGINEERING

Drift into failure



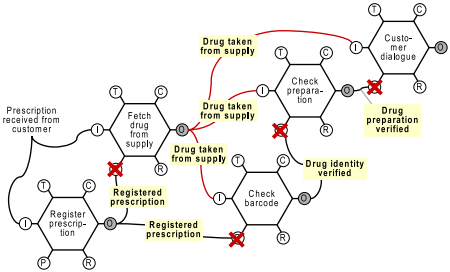
Mature high-hazard systems apply the *defence in depth* design principle and implement multiple independent safety barriers. They also put in place programmes aimed at reinforcing people's *questioning attitude* and their *chronic unease*, making them more sensitive to safety issues.

These shift the perceived boundary of safe performance to the right. The difference between the minimally acceptable level of safe performance and the boundary at which safety barriers are triggered is the *safety margin*.

Figure adapted from *Risk management in a dynamic society*, J. Rasmussen, Safety Science, 1997:27(2)

RISK ENGINEERING

Non-linear accident model



Systemic models

- ▷ FRAM (Hollnagel, 2000)
- ▷ STAMP (Leveson, 2004)

Assumption: accidents result from an unexpected combination and the resonance of normal variations in performance

Consequences: preventing accidents means understanding and monitoring performance variations. Safety requires the ability to anticipate future events and react appropriately.

Image credits

- Sodom and Gomorrah burning (slide 26): Picu Pătruţ, public domain, via Wikimedia Commons
- Dominos (slide 27): H. Heinrich, *Industrial Accident Prevention: A Scientific Approach*, 1931

For more free content on risk engineering, visit `risk-engineering.org`

RISK ENGINEERING

Feedback welcome!

Was some of the content unclear? Which parts were most useful to you? Your comments to `feedback@risk-engineering.org` (email) or `@LearnRiskEng` (Twitter) will help us to improve these materials. Thanks!

`@LearnRiskEng`

`fb.me/RiskEngineering`

For more free content on risk engineering, visit `risk-engineering.org`