Willful Myopia: Cognitive Dissonance and Human Error at the Organizational Level

Graham D. Creedy, P. Eng, FCIC, FEIC
gcreedy@rogers.com

for

International System Safety Society
Canada Chapter

23 September 2020

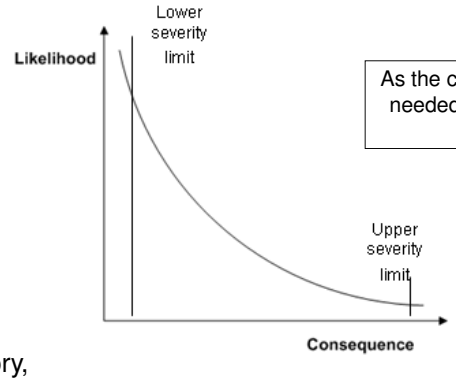
1

Willful Myopia: Cognitive Dissonance and Human Error at the Organizational Level

- Overview
  - Introductory comments
    - My background re this topic
    - Why this theme?
    - Audience
  - Discussion:
    1. Brief review of the nature of risk and risk management
    2. Issues in risk assessment and perception of risk by those making decisions on risk control
    3. Why systems fail in actual practice even in well-run organizations, and the role of motive
    4. Symptoms of vulnerability, and defences

Risk Equation

Risk = $\sum$ (probability x expected loss) for the combined range of all events studied



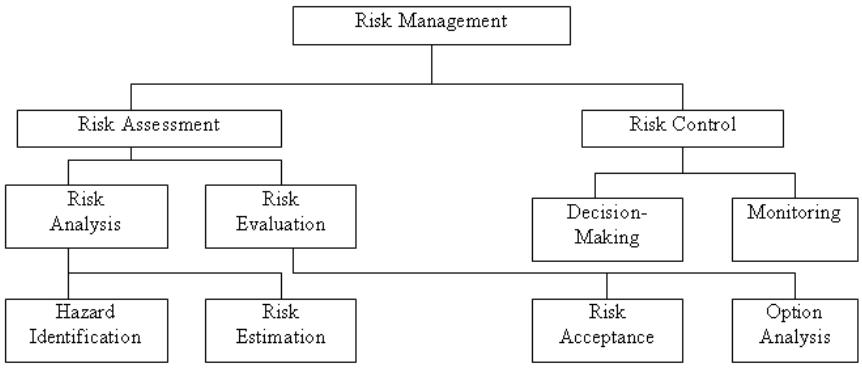
As the curves are different, a graph is needed for each scenario or type of risk being considered

In theory,

- the probability and expected benefits should be similarly estimated, and
- the result must meet criteria for risk acceptability

Risk Management Elements

- This chart shows how the various elements in risk management relate to one another:



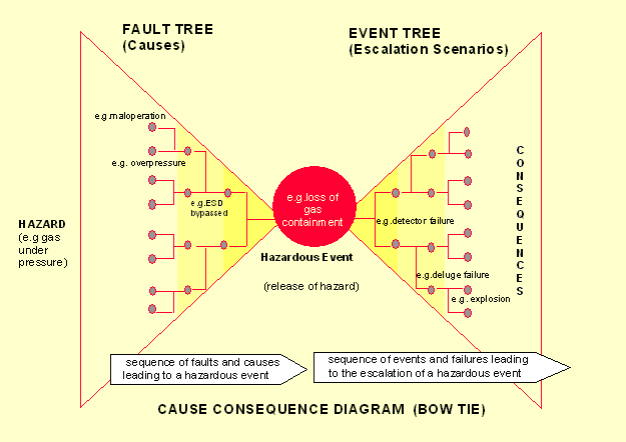
Former CSA Standard Q634 (since replaced by Q850)

Hazard Identification and Risk Assessment

- These are some of the techniques used in the process industries for identifying hazards and assessing risks. They are more relevant for acute risks:
  - What-if
  - Checklist
  - What-if/checklist
  - Risk matrix
  - Index methods (Dow fire & explosion index, chemical exposure index)
  - Hazard and operability study (HAZOP)
  - Failure mode and effects analysis (FMEA)
  - Fault tree analysis
  - Event tree analysis
  - Bow tie or cause-consequence analysis
  - Layer of protection analysis (LOPA)
  - Human reliability analysis
- It is not practical to apply all of these techniques to every situation. Some techniques need detailed information which is not available at the early stages of a project. Expert guidance is used to identify which of these should be used, and when (at what stage of a project or process)

Bow Tie Analysis

- Great for giving a quick picture of how an event develops
- Combines fault tree and event tree in one diagram



http://info.ogp.org.uk/RiskManagement/Terminology/main.html

Same principles, application varies

- These principles are valid for a range of situations, but the application can be very different as it must take into account the circumstances that could occur during the life-cycle of the project, process or product.
- For example, risk management for a nuclear power plant, an chemical plant and a propane depot must take into account the resources available at the site. For a propane depot that means minimization of risk through design of equipment and procedures, rather than relying on training and supervision of operators in the front line.

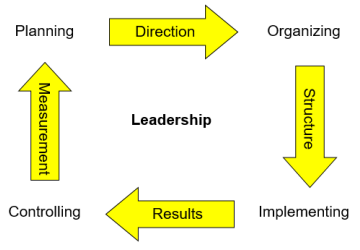
Societal Control of Risk

- To manage the issue, the organization(s) driving change must decide on the points shown on the left below, but in reverse order, i.e.:
  - The outcomes desired
  - The results needed to achieve those outcomes
  - The performance by which progress towards those results will be monitored

Management System

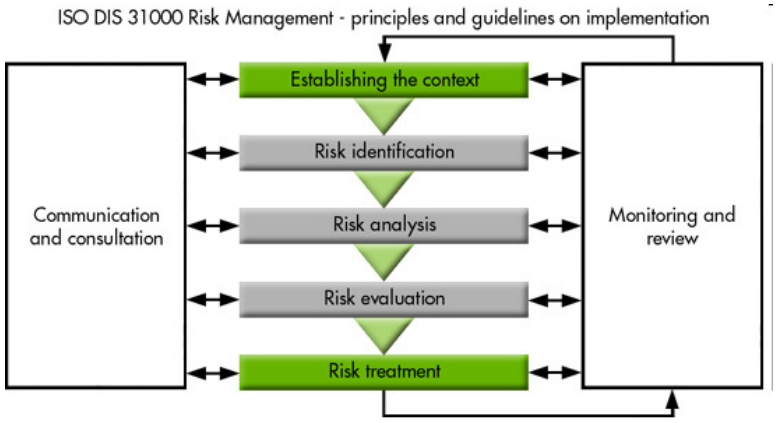
- The most important point about a management system is the *feedback loop* to ensure that the following are acceptably consistent with the design intent (= the plan):
  - ***Performance*** of people *(Equipment performance is also covered here, but typically depends on the people operating and maintaining it)* and that performance is producing
  - ***Results*** (e.g. output for resources used – can often be measured)
  - ***Outcomes*** (more related to long-term goals – may or may not be measured in quantitative terms, depending on nature)

Functions of a management system



Risk Management Elements

- This version, from the international ISO 31000 Risk Management standard, is more relevant for risk assessment than for risk management, because the important monitoring and review role is shown as a general step that fits in everywhere. This is not much help in understanding why vulnerabilities occur in managing residual risk, and *caution is needed when applying this model in management of acute risk*, as we'll see later. For acute risk the model on the earlier (Q634) slide is more useful. The ISO 31000 model is, however, useful for chronic risk.



Graham Creedy, for ISSS Sept 2020

9

Chronic and Acute Risk

- Risk has chronic and acute aspects, and although the risk management principles are similar, the implications for control are very different
- **Chronic risk:** Human safety, health and environmental effects due to ***ongoing or long term exposures***
  - Delayed effects, gradual trends, causation often unclear
  - Societal attention varies over time, but societal negotiation is ongoing
  - Goals can be established, progress monitored and action plans modified as relative priority and resources change over time
- **Acute risk:** Human safety, health and environmental effects due to ***unplanned sudden, episodic events***
  - Absence of incidents is not like presence of emissions (**trying to control what isn't there**)
  - Societal negotiation is typically conducted in aftermath of major event ("smoking gun"), with an attention span that decays rapidly unless fed by vested interests
  - Risk generators and regulators think that lack of serious incidents is proof of effective controls; even near misses may be viewed as aberrations
  - Jurisdictions do not appear to learn from other jurisdictions (this also seems to be true for industries and some companies)
  - These are general categories, as the nature of the risk can vary with the context:

Graham Creedy, for ISSS Sept 2020

10

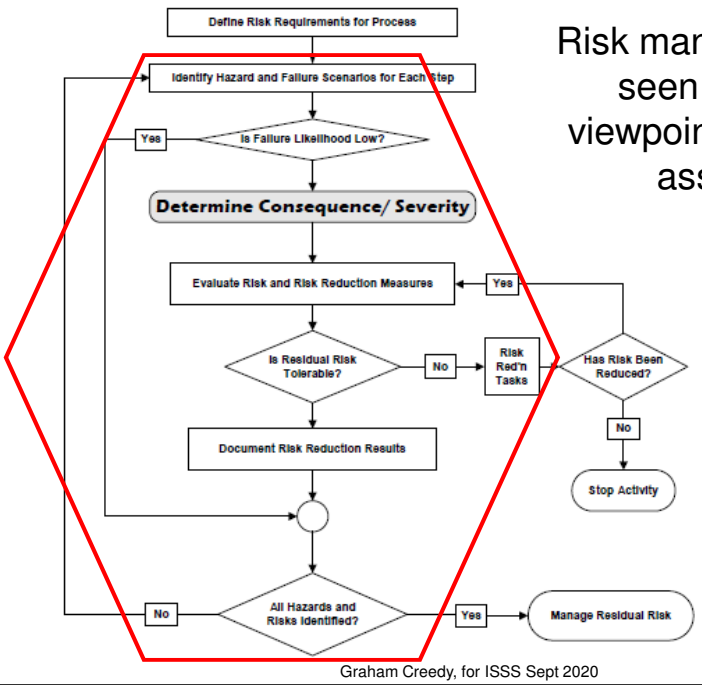
What is meant by “Risk Assessment”

- In this discussion we consider two ways of looking at risk assessment:
  - **Formal** risk assessment, done on a periodic basis according to a structured, documented format; typically performed by someone outside “line” responsibility, e.g. staff, corporate HQ, consultants. Provides advice to those making the actual decisions. This is what is usually understood by the term risk assessment
  - **Informal** risk assessment, done on an ongoing basis by those making day-to-day decisions, undocumented and perhaps even not realized by those doing it

- Note that the ones making the actual decisions are not usually the ones doing the formal assessment! However, their decisions can be strongly influenced by the perception of risk they receive from the formal assessment

- Roles:
  - the risk assessor is the person, dept or org doing the formal risk assessment
  - The risk generator is the person, dept or org actually having control, and thus making the decisions on managing risk

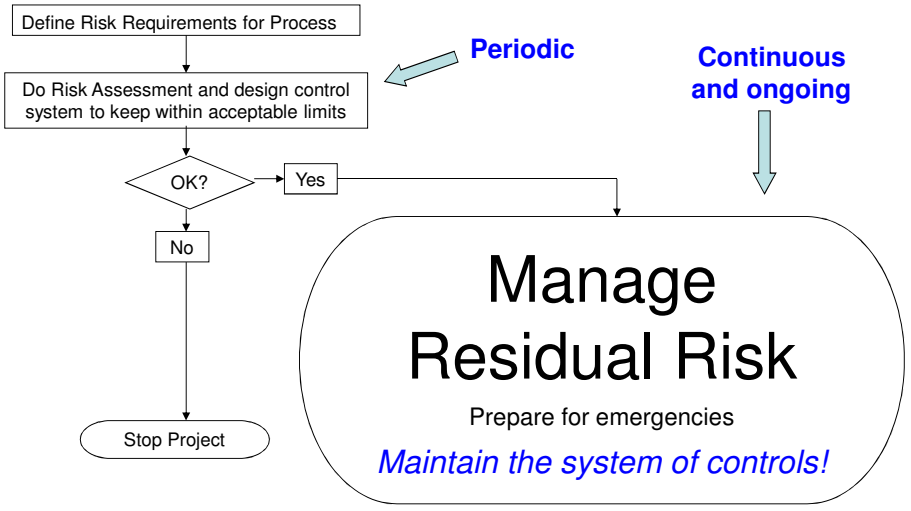
Graham Creedy, for ISSS Sept 2020 11



Risk management as seen from the viewpoint of the risk assessor

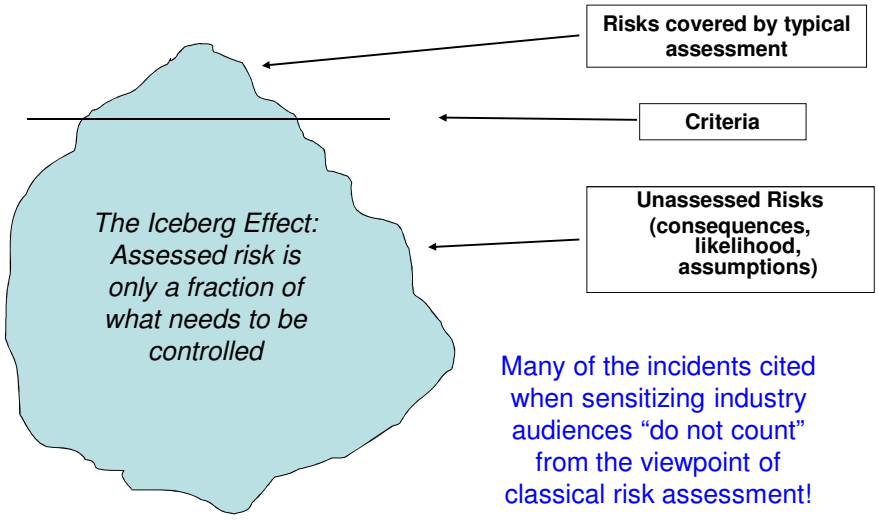
Graham Creedy, for ISSS Sept 2020 12

Risk management as seen from the viewpoint of the risk generator (those making the decisions on risk control)



Graham Creedy, for ISSS Sept 2020 13

Deficiencies in the way risk assessment is typically conducted



Many of the incidents cited when sensitizing industry audiences "do not count" from the viewpoint of classical risk assessment!

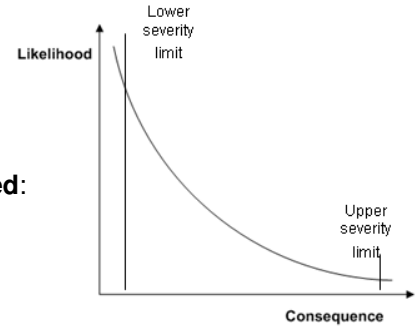
Graham Creedy, for ISSS Sept 2020 14

Deficiencies in the way risk assessment is typically conducted

Aspects commonly ignored or assumed:

Consequences
- "Unexpected" scenarios and environmental effects
- "Knock-on effects where initial incident triggers secondary scenarios
- Unusual effects due to concentration of release affected by local characteristics, e.g. surface features
- "Unexpected" level of protection or behaviour of those in the affected zone
- Non-linear effects, e.g., psychological harm (and related physical harm), financial effects (e.g. cutoff of credit), public outrage

Likelihood
- Human error (at sharp end)
- ***Management system failure***
- Distribution assumed for High Consequence-Low Probability event prediction



Criteria for acceptability
- Death or irreversible harm
- Offsite or onsite
- Individual or societal risk
- Unwritten criteria of those at points of control

Human role in assessment itself
- Decision-making and behavioral biases
- Biases in probability and belief
- Social biases
- Memory errors

15

Deficiencies in the way risk assessment is typically conducted

- The human role in the assessment itself
  - Even where a competent risk assessor is acting in good faith:
    - budget or time constraints may push to deliver results based on techniques or data not really up to the task – for example,
      - using information from earlier studies by others rather than checking to verify that it is indeed valid,
      - limiting the range of scenarios under study
      - discounting the likelihood that a system will not work exactly as intended.
  - There are never enough resources to study everything, so judgment is used to narrow the field to manageable proportions.
  - This is why risk assessment is still as much an art as a science, despite the apparent rigour at first sight.

Graham Creedy, for ISSS Sept 2020

16

Deficiencies in the way risk assessment is typically conducted

- Overconfidence in risk assessment
  - Now a recognized characteristic in the financial and economic field, and has become a specialized subject of academic study in its own right (e.g. Kruger)
  - Not yet appreciated by the process industries
  - Convenience is addictive. Economists can become seduced by their models, fooling themselves that what the model leaves out does not matter (Economist, 2009)
  - More information does not necessarily lead to better decisions – although the confidence level rises, the accuracy of prediction may well be worse! (Mauboussin)

Deficiencies in the way risk assessment is typically conducted

- False precision and reckless approximation

An actuary and a farmer are looking at two fields of sheep. The farmer asks the actuary how many sheep he thinks there are:

"1,007", is the quick and confident reply.

The astounded farmer asks how the actuary reached that number.

"Easy, there are seven sheep in that field and about 1,000 in the other."

The Economist

Deficiencies in the way risk assessment is perceived and acted on by the risk generator

- A recent risk assessment: "Worst imaginable scenario … catastrophic failure … tank of (toxic reactive chemical liquid) … event frequency for this is of the order of 10^{-10} events per year"
- On the other hand, a personal, informal assessment suggests there are situations where a catastrophic failure rate could be as high as once in a century
- This would give a frequency ***range*** of up to 10^{8}, depending on how the site is run – yet this is typically not considered in the assessment nor is it communicated to the site operator!

Deficiencies in the way risk assessment is perceived and acted on by the risk generator

- "Where a quantitative matter is being discussed, the greatest clarity of thought is achieved by using numbers instead of avoiding them, *even where uncertainties are present*. [emphasis in the original] … Systems analysis takes problems that are not defined and attempts to define them …. Rather than trying to select a precise maximum or minimum, it is better to be roughly right than exactly wrong."

A.C.Enthoven, quoted in Thomas B. Allen, *War Games*, 1987

Deficiencies in the way risk assessment is perceived and acted on by the risk generator

- To do otherwise is not simply to produce assessments based on false precision and reckless approximation – it can significantly increase the actual likelihood of the events under study, by suggesting that the missing factors are irrelevant and thus do not need to be considered in the system for control

Deficiencies in the way risk assessment is perceived and acted on by the risk generator

- Be clear about what is unclear!
  - "Tell me what you know. Tell me what you don't know. Then tell me what you think. Always distinguish which is which." Colin Powell
  - Predictions must be as transparent as possible; assumptions, model limitations, and weaknesses should be forthrightly discussed; and uncertainties must be clearly articulated. Sarewitz et al.

Quoted in *Communicating uncertainties in natural hazards research*, by Judith Curry
http://judithcurry.com/2012/10/10/communicating-uncertainties-in-natural-hazards-research/

Deficiencies in the way risk assessment is perceived and acted on by the risk generator

- The main issue
  - Likelihood of undesired consequences is not simply an equivalent part of the equation –

    the very way it is treated in the assessment process can have a major influence on the likelihood of events and thus on the risk itself.
  - A decision maker might be unwilling to devote much attention to control of an event that is expected to happen only once in 10^{10} years, when he or she expects to have moved on in 10 years!

History of safety philosophy in the process industries

- Four phases:
  - **Late 19th – early 20th century** ← Protection of assets, business continuity and reputation
    - Origins of much of basic safety thinking in the explosives industry
    - Focus on protection of capital and markets (assets and production for profit)
  - **Second world war through 50s and 60s** ← Protection of people, property and the environment from risks that are generally well understood
    - Concepts of loss prevention and investment in people
    - Focus on worker-equipment interface and personal safety
    - Well covered by regulatory and other guidance
    - Regulatory philosophy limited to this stage in Canada in most sectors including process industries
    - Philosophy mainly rule-based, and often prescriptive
  - **70s and 80s (Process Safety Management)** ← Protection from acute risks whose nature may not be clear without specialized knowledge
    - Recognition of seriousness of consequences and mechanisms of causation lead to focus on the process rather than the individual worker
    - Sector specific due to nature of hazards (structural/civil, aerospace, nuclear, chem eng)
  - **90s and beyond** ← Protection from risks due to individual/organizational behaviour and complex systems
    - Realization of significance of sociocultural factors
    - System safety
- Later phases do not replace earlier views, but build on them to give new perspectives (PSM can't supersede traditional workplace safety, and system safety can't supersede PSM for identification of hazards and control of risk in process industries

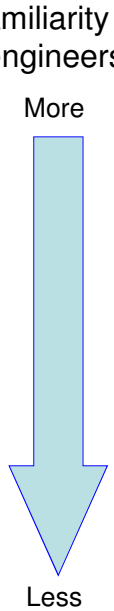
Why management systems fail

- The systems are designed and operated by humans!
- Realization of significance of sociocultural factors in human thought processes and hence in behaviours
- People, and most organizations, don't intend to get hurt (have accidents)
- To understand why they do leads us eventually into understanding human behaviour, both:
  - At the individual level
  - At the organizational level

Boeing 737 Max

Human behaviour aspects

- Physical interface
  - Ergonomics
- Psychological interface
  - Perception, decision-making, control actions
- Human thought processes
  - Basis for reaching decisions
  - Ideal versus actual behaviour
- Social psychology
  - Relationships with others
  - Organizational behaviour



Why problems with management of residual risk lie at the heart of major incidents

- The "Risk Reduction/Control" step in a risk assessment flowchart refers to the *design* of risk reduction and control measures, but not their *execution*
- Consider risk generators as:
  - **don't care** (rare in high-hazard industries)
  - **don't know** – and perhaps don't know that they don't know (often smaller or less-technical companies or sites, where regulatory guidance is weak)
  - **do (or did) know**
- "Don't knows" often fail in proper risk assessment and design of control system (apart from execution errors)
- "Do knows" tend to fail in execution of the control system

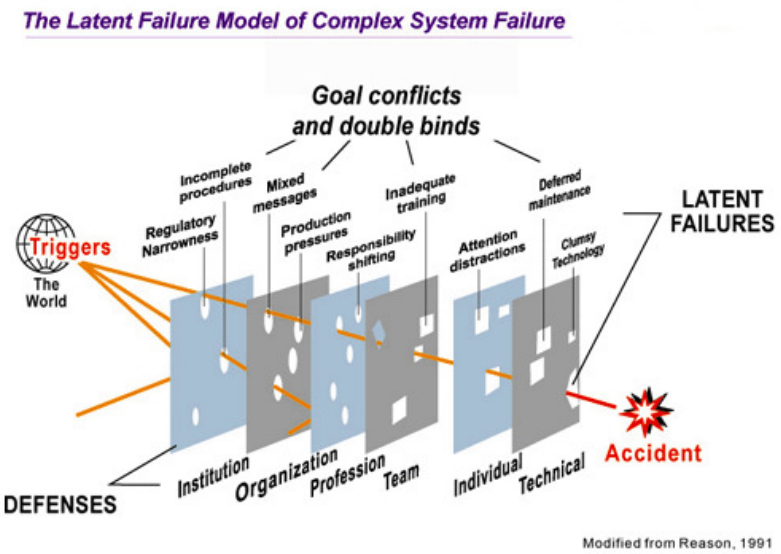
Why problems with management of residual risk lie at the heart of major incidents

- Organizations that do know what could go wrong:
  - Design for risk controls, but are then
  - Vulnerable to failures in execution
- Management system failure is especially insidious because of its "common cause" effect on multiple assumptions in the risk assessment, e.g.
  - Staffing levels, knowledge base, capability, training in operations & maintenance (and also design & construction)
  - Equipment integrity, inspections, testing, preventative maintenance
  - Perception of relative priorities when resources are insufficient for scheduled activities
  - etc., etc.
- The actual risk is then *far* greater than the assumed risk

Why problems with management of residual risk lie at the heart of major incidents

- Major accidents occur in companies that have excellent management systems for personal safety
- The personal safety performance created a false sense of security; managers did not realize that major accidents have different causative mechanisms from personal safety incidents
- The major event happened <u>despite</u> the existence of the management system, and subsequent investigation typically reveals:
  - There were multiple causes
  - Warning signs were apparent long before the incident, but were filtered out by the system

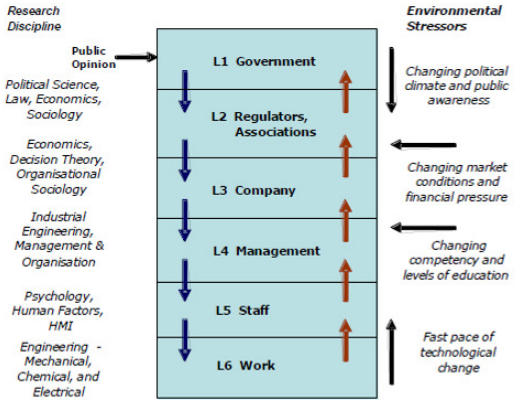
- Reason's cheese model shows how holes in defences can develop and grow



Source: http://csel.eng.ohio-state.edu/productions/pexis/conceptualize/view.html -- has useful info

Societal Control of Risk

- Control of risk doesn't just depend on the person directly operating equipment, or even the org's CEO
- It is affected by a host of decisions by many people, in many organizations, at many levels, as in Jens Rasmussen's diagram shown here.
- Those decisions are strongly influenced by the relative <u>perception</u> of risks and benefits, both from:
  - formal assessment and
  - an informal sense of potential consequences and likelihood.
- Some of this informal sense may be subconscious and not even recognized by the decision maker.

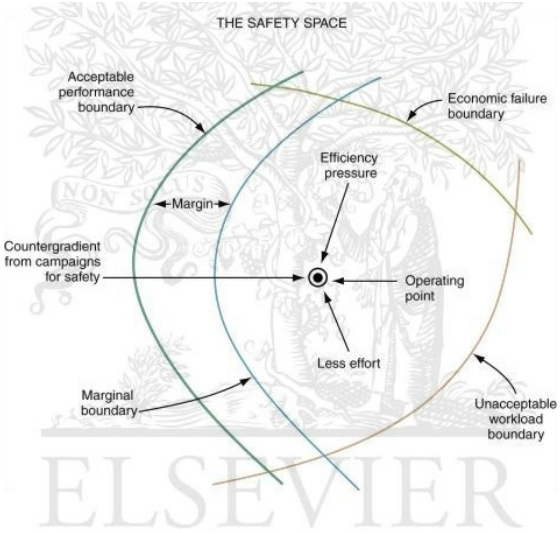


Hierarchical Model of Sociotechnical System involved in Risk Management (Rasmussen, 1997)

Normalization of deviance

- Definition by Vaughan, developed from a concept proposed earlier by Rasmussen:

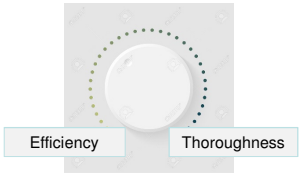
  "the systematic organisational performance deteriorating under competitive pressure, resulting in operation outside the design envelope where preconditions for safe operation are being systematically violated"



Rasmussen's diagram

Efficiency & thoroughness

- Erik Hollnagel
  - There is a trade-off between efficiency and thoroughness (you can't have both)
  - It is not possible to follow all the rules; people therefore make decisions on where the balance should be, based on their perception of what is important in the circumstances for the organization, their boss and themselves
  - Rather than assuming ideal behaviour with occasional lowering of standards as an anomaly, it is better to design for the likely range of behaviour



Systems are more complex than Reason's model suggests

- Nancy Leveson
  - The risk management process is far more complex than in Reason's linear model, involving a multitude of actors at many levels, as in Rasmussen's hierarchical model but much more extensive.
  - The characteristics of this network are not constant, but subject to change which then causes ripple effects through interactions throughout the system

STAMP Accident Causation Model

- Accidents arise from unsafe interactions among humans, machines, and the environment (not just component failures)

~~"prevent failures"~~

↓

"enforce safety constraints on system behavior"

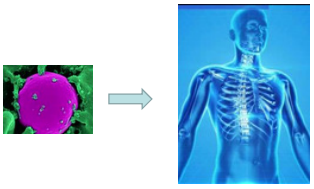
- Losses are the result of complex dynamic processes, not simply chains of failure events
- Most major accidents arise from a slow migration of the entire system toward a state of high-risk
  - Need to control and detect this migration

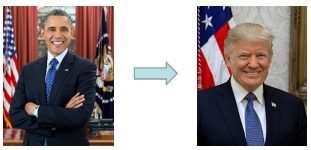
Hierarchy and Emergence

- Leveson:
  - Complex systems can be modeled as a hierarchy of organizational levels
    - Each level more complex than one below
    - Levels characterized by emergent properties
      - Irreducible
      - Represent constraints on the degree of freedom of components at lower level
  - Safety is an emergent system property
    - It is NOT a component property
    - It can only be analyzed in the context of the whole

Emergent Properties

- Emergent properties are those which arise through interactions among smaller parts that alone do not exhibit such properties
  - You cannot model human behaviour by summing the properties of a single cell
  - or model a city by examining the properties of a single citizen and multiplying by the population of the city
  - You cannot switch one person for another as you could a component, and assume that the system will behave in the same way



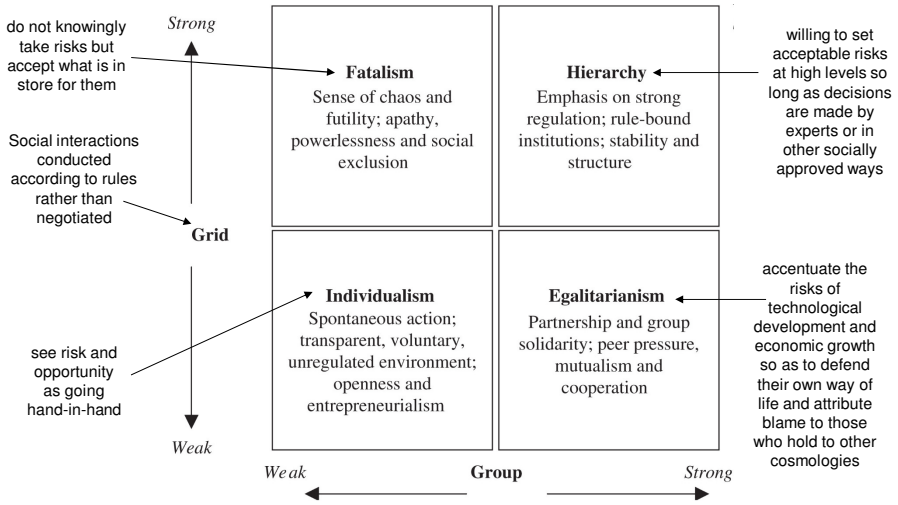


Likelihood: Human error

- Humans are not “black boxes”, interchangeable and behaving reproducibly until failure; theories and models based on those theories allow no role for human intention or choice
- Human failure modes and effects analysis
  - Individual and group behaviour
  - Operator and manager/executive level
- Technical disciplines such as engineering tend to focus on the item that failed, and how to make it more robust to prevent future failures
- Lessons from commercial aviation and finance show the relevance of human and organizational failure; these aspects are also present in engineering, but are typically ignored in risk assessment for process industries

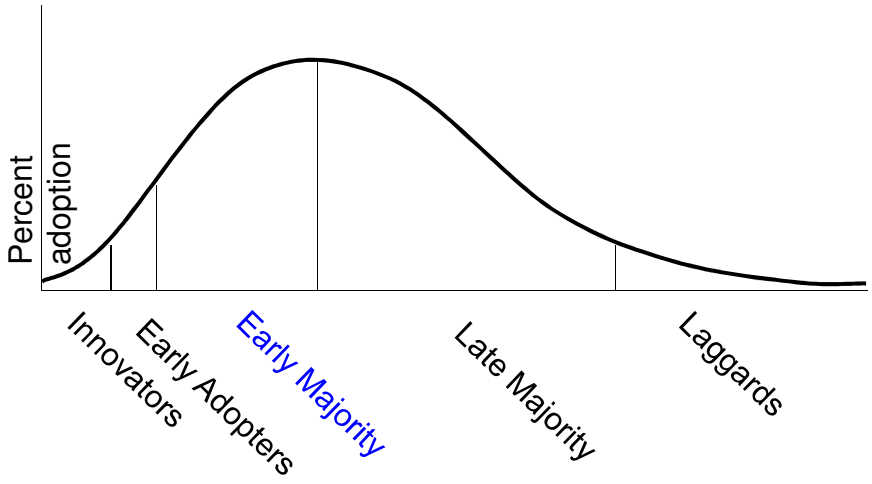
Douglas’ Cultural Bias Grid

(Although challenged by some sociologists, it can be useful in understanding ways in which different people may view risk decisions)



As referred to in *Lees’ Loss Prevention in the Process Industries*, 4th ed.,vol. 1, p4/8

The New Product Introduction Curve



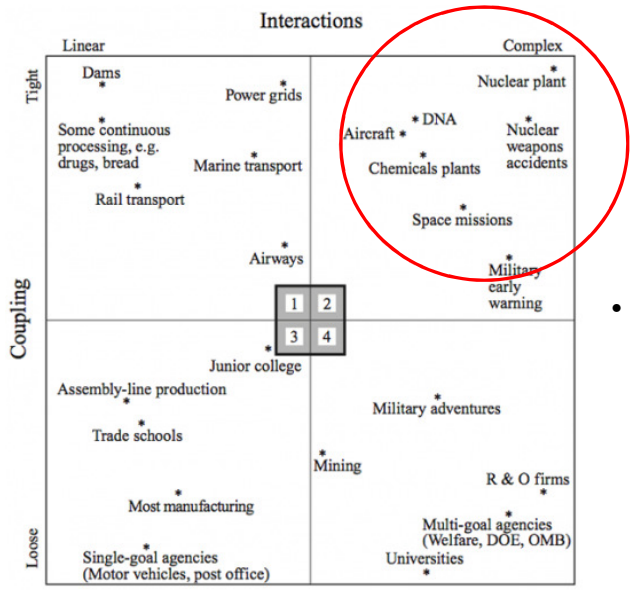
- Can be applied to adoption of new ideas, e.g. PSM
- Categories differ by ability and more importantly, motivation

The New Product Introduction Curve

- This diagram, a concept from "Marketing 101", shows how a new product or idea is not taken up with immediate enthusiasm by the whole target market, but is adopted at different rates by different categories of users.
- **Innovators** don't need outside persuasion to get going – they are capable of moving by themselves and indeed will have developed many of the techniques described in this lecture.
- **Early adopters** are not able to develop many of the techniques by themselves, but are alert and constantly looking for ideas they can use to get their job done easier and more effectively. They read newsletters, attend conferences, research the web and often participate on technical working groups and committees.
- The **early majority** is a large group, typically with the right attitude but lacking the time or resources to learn by themselves. A combination of instruction and motivation is needed for this group, showing what tools and assistance are available and putting them in touch with innovators and early adopters who can explain and suggest to them what to do next.
- The **late majority** is also a large group, but differs from the previous group in having a much lower motivation to adopt the new practices or techniques. There may be a variety of reasons, from a well-run organization with other priorities to a poorly-run one lacking an effective process for establishing and meeting objectives. This group typically follows the early majority, doing something new mainly because everyone else is doing it, and can be brought in once the techniques, etc. have gained wide acceptance are and becoming well-known. Motivation is far more important than instruction with this group.
- **Laggards** are a smaller group, consisting of those who refuse to move unless the consequences of not doing so are close to threatening. Very strong peer pressure, the imminent cut-off by suppliers and customers or sanctions by insurers or regulatory agencies are likely to be necessary, and it is this group at whom regulations are primarily targeted.

Relevance of the curve for strategy when introducing a change or new idea

- When trying to change behaviour, don't worry about the large number and lack of enthusiasm of the late majority. Concentrate on the early majority, and use the innovators and early adopters to show them the way. Deal with laggards only if you need to make an example at this stage, or if behaviour is clearly unacceptable.
- Once you have worked out the problems with the early majority and have their "buy-in", then you can look for group commitment to bring in the late majority.
- As the late majority move, you can then think about graduated options to deal with laggards.



Charles Perrow's chart of complexity and coupling, From his book *Normal Accidents*

You don't want "Move fast and break things" as a guiding principle when you're up in this corner!

- See David Woods on Resilience Engineering for principles of managing risk and complexity

"Managing risk is never the top priority!"

Graham Creedy

- People don't go into work in the morning with the primary objective of managing risk
  (there are "risk managers", but these are typically staff roles, providing recommendations to the actual decision makers)
- Offence and defence analogy:
  - How to bring about what you **intend** to happen (offence)
  - How to prevent and be ready for what you **don't intend** to happen (defence)
- Some of the considerations:
  - Scope (limited, or "lifecycle"? From whose viewpoint?)
  - Design vs operations & continuity
  - Potential changes in external & internal environment
  - Balance (competition for resources, likelihood of success, etc.)
  - "Office politics"

The importance of Narrative

- Issues of technical complexity are typically considered in the form of narratives, or story lines connecting a series of events in a way we can relate to. This is characteristic of journalism, but also of the way even experts summarize complex information in their minds and present to others
- Narratives are often used to influence thought by presenting selected information in a way that directs the reader or listener to a particular conclusion
- We also construct our own narratives, which influence our behaviour – perhaps subconsciously – when assessing and making decisions about potential risks
- Such narratives can be highly subjective ("what does this imply for me?"), and can have a strong influence on motive

How “Real-World” Decision Making Works

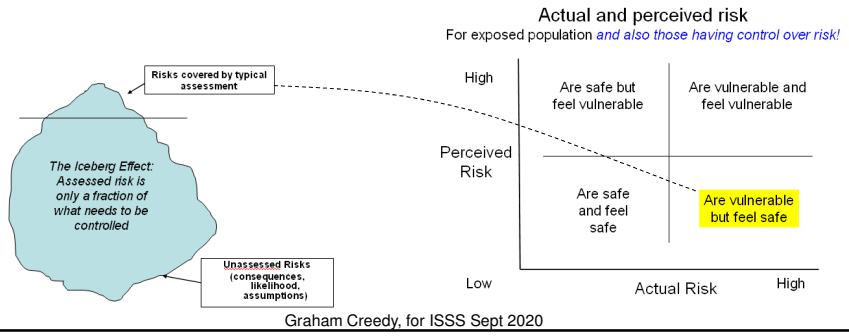
- Kahnemann & Tversky: ***Thinking fast and slow***
- Rapid decisions based on “gut-feel”, but influenced by logic, narratives and motives
- Logic and narratives often conflict when seen from different viewpoints; ***cognitive dissonance*** allows multiple conflicting influences to be taken into account without having to resolve them into a harmonious whole
- A rough sense of priorities (for the individual, boss, co-workers, organization, family, environment, common good, etc.) guides the weighting of these factors

Graham Creedy, for ISSS Sept 2020

45

Deficiencies in the way risk assessment is perceived and acted on by the risk generator

- Judgment and decisions by the risk generator at key points of control are:
  - Dependent on balancing multitude of influencing factors and this balance is influenced by the motives – conscious and subconscious – of the person making the decision
  - Strongly influenced by how the risks are perceived



Graham Creedy, for ISSS Sept 2020

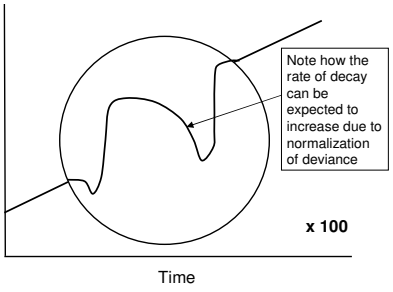
46

Why and how defences fail

- People often assume systems work as intended, despite warning signs
- Examples of good performance are cited as representing the whole, while poor ones are overlooked or soon forgotten
- Latent errors are allowed to develop, and to increase in number and intensity if their significance is not recognized
- Normalization of deviance is self-reinforcing … until a wakeup call that may be too late!
- Analysis of failure modes and effects should include human and organizational aspects as well as equipment, physical and IT systems

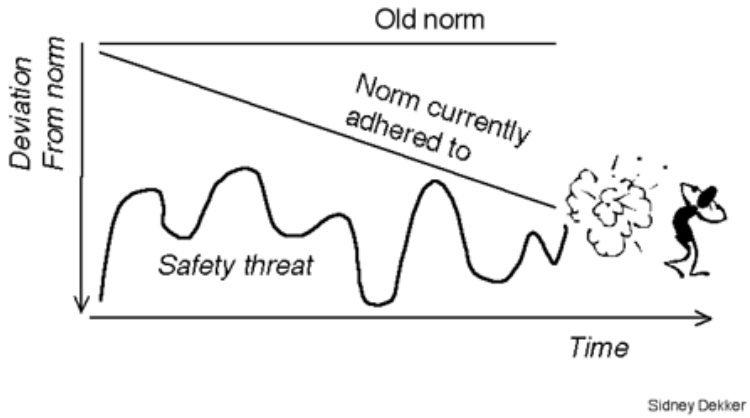
Normalization of deviance

"the systematic organisational performance deteriorating under competitive pressure, resulting in operation outside the design envelope where preconditions for safe operation are being systematically violated" (Rasmussen)



System Safety

- Drift into failure



Human Error at the Organizational Level

"The relevance of organizational factors has also been graphically and tragically revealed in the inquiry reports of recent UK transportation and offshore oil disasters.

Prior to ..., senior managers in all the organizations propounded the pre-eminence of safety. They believed in the efficacy of the regulatory system, in the adequacy of their existing programs, and in their confidence of the skills and motivation of their staff.

The inquiry reports reveal that their belief in safety was a mirage, their systems inadequate, and operator errors and violations commonplace.

The inquiry reports stated that ultimate responsibility lay with complacent directors and managers who had failed to ensure that their good intentions were translated into a practical and monitored reality. Moreover, the weaknesses so starkly revealed were not matters of substantial concern to the regulatory authorities before the accidents."

"There was an evident belief of senior managers that they were working in safe organizations. This may have been because they may not have known how to seek out, or to recognize, the symptoms of an unsafe organization. It may also be true that they would not have known what practical steps to take to turn an unsafe into a safe organization."

ACSNI Human Factors Study Group, 1993

Challenging issues

- Issue definition, drivers, points of control and plan (who is to do what and by when, resourcing, what to measure, political continuity)
- Confusion of name and purpose, e.g. defence, health care
- Different risk appetites/perception of benefits & risks by different stakeholders, e.g. finance, investment
- Human characteristics (culture, "identity", "face", etc.) and challenge of cultural change
- Plausible deniability, transfer of responsibility
- Hindsight bias and scapegoats
- Logical weaknesses of models and metrics, e.g. business case fallacy, ISO 31000, MIL STD 882
- Interface between humans and technology (AI, complexity, IT arrogance and hubris)
- Balance between imperfect rules and judgement (skill/rule/knowledge-based behaviour)
- Roles of regulation, media pressure

Examples of human error at the organizational level

- Inconsistency between goals and culture
- Balance between caution and “can do”
- Normalization of deviance
- Belief that absence of serious incidents is proof of an effective system of control
- Using risk assessment to “prove” that an activity is safe, rather than to understand how risk is caused and how to further improve defences
- Treating near-misses as outliers, not as symptoms
- Failure to define and maintain critical skill base
- Undue faith in others (trust, but without verification)
- Team sports analogy
  - Individual judgement is displaced by the desire to be seen as one of the team
- Failure to learn from experience elsewhere
- “Faith-based” risk management
  - Those who question conventional wisdom are seen as inconvenient heretics
- The wise, courtiers and fools
  - Wise: understand and recognize system vulnerabilities
  - Courtiers: know there are vulnerabilities, but tell superiors what they think they want to hear (they filter communications both up and down)
  - Fools: believe the “PR” of the org or dept, that the system works as claimed and that everything is under control

Incident Investigation

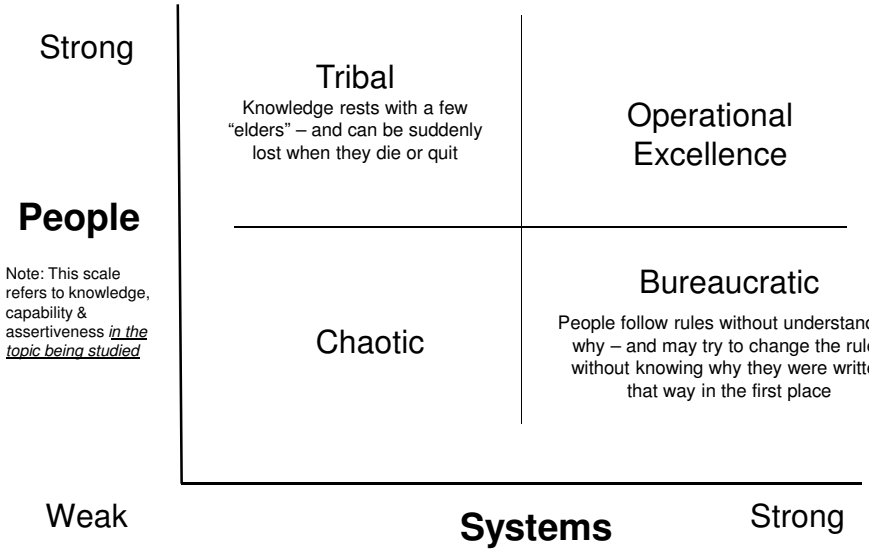
- You can learn a lot about the culture of an organization by how it investigates incidents and near-misses
- How does it:
  - Keep the focus on what happened rather than on blame
  - Avoid hindsight bias
  - Consider other possible consequences if the scenario had developed slightly differently
  - Consider broader implications and lessons, rather than narrowing the focus to a specific incident
  - Look for the root causes
  - Keep a sense of perspective
  - Follow through to ensure lessons are communicated and applied?

What does an organization's investigation of its failures reveal about its culture and management system?

- Knowledge
  - *Never realized problem could occur (benchmarking error)*
    - *was it treated as a unique deficiency?*
    - *was there a broader review of the benchmarking process to find if there are other areas where knowledge could be deficient?*
- Policy
  - *Thought situation would be acceptable but didn't realize full implications until it happened*
    - *Does it appear to be acceptable now?*
    - *Was review of policy and accountability limited or broad in scope?*
- System design
  - *Even if everything had been done as intended, problem would still have occurred*
    - *How comprehensive was analysis of system deficiencies and practicality of solutions?*
    - *How effective is action plan and follow-through?*
    - *Was review of system design limited or broad in scope?*
- System execution (management system error)
  - *Problem occurred because someone or something did not perform as intended*
    - *Did analysis consider why execution not as intended?*
    - *Was corrective action appropriate and balanced?*
    - *Was review of system execution limited or broad in scope?*

Organizational Culture Model

James W. Bayer, Senior VP Mfg, Lyondell Chemical Company



Understanding motive

- Sociology of group behaviour, e.g. sports
- Logical fallacies
- Value of role-playing
- Perception of relative priorities when resources are insufficient for scheduled activities
- Expectation of resolving problems without referring up the line
- Well-intentioned but inappropriate can-do response
- Reinforcing effect of normalization of deviance
- Role of leadership in steering control policy

55

Understanding motive

- Not so much “Black Swans & Ostriches”, but more:
- Willful Myopia:
  - Intentionally narrowing the focus to concentrate on aspects deemed important/urgent, and pushing other aspects to the background to avoid distraction, “for now”
- Leading to normalization of deviance and drift into failure

Understanding Motive: Tips

- ***How is the issue defined?***
  This is the most important step, and time spent here can save a lot later
  Does this make sense? How does the issue change when viewed from different perspectives? How does the definition relate to other issues?
- Watch out for those narratives and labels (e.g., Defence, Ukraine, green)
- Who stands to gain or lose? (orgs, groups, individuals)
- What "facts" have been selected (validity, relevance, what others could be relevant?)
- When does the story start and end? (what happened before, alongside, after?)
- What is the nature of the participants? (e.g. on Douglas' grid, the new product introduction curve, etc.)
- What conscious and subconscious motives are they likely to have?
- ***What principles are involved in addressing the issue, and what is the hierarchy?***
- If others were to apply those principles and hierarchy in their dealings with us, how would we feel?

Key defences against organizational error and normalization of deviance

- Maintain a sense of vulnerability
  - Watch for lessons from incidents and near-misses, not only from your own org/sector but also elsewhere, and how they could apply to your situation.
- Recognize economic and other constraints, and use triage:
  - We must do these things, no matter what;
  - We're going to drop these, at least until conditions improve;
  - We'll do these if we can fit them in, but they're secondary to the "musts" (allowing a little flexibility in negotiating the "drop" list can help with team acceptance).

  Recognize when and where resources are clearly not enough, handle with tact, but make your own decision about your role.
- Trust, but verify
  - Management by wandering around (keeping a "finger on the pulse" of what is really going on).
  - Learn how to handle courtiers, who can be above or below you; you have to find ways to bypass them, and to convey with tact the message you want to get through; find what's actually happening and not what people think you want to hear.
  - Lead and direct the management system re those below and at same level. You might also be able to influence the system above you once you understand how it works.

Defences don't have to be perfect!

- Herbert A. Simon, the famous economist and cognitive scientist studying how people make real-world decisions, observed that they seldom optimize.

  "Rather people seek strategies that will work well enough, that include hedges against various potential outcomes and that are adaptive. Tomorrow will bring information unavailable today: therefore people plan on revising their plans."

  In this spirit, people have developed an approach to look not for optimal strategies but for robust ones, defined as strategies which perform well when compared with the alternatives across a wide range of plausible futures.

  The approach "need not be the optimal strategy in any future. It will, however, yield satisfactory outcomes in both easy-to-envision futures and hard-to-anticipate contingencies. This approach replicates the way people often reason about complicated and uncertain decisions in everyday life."

  Quote from Malevergne and Sorette, 2005, *Extreme Financial Risks: From Dependence to Risk Management*, p285

Questions?