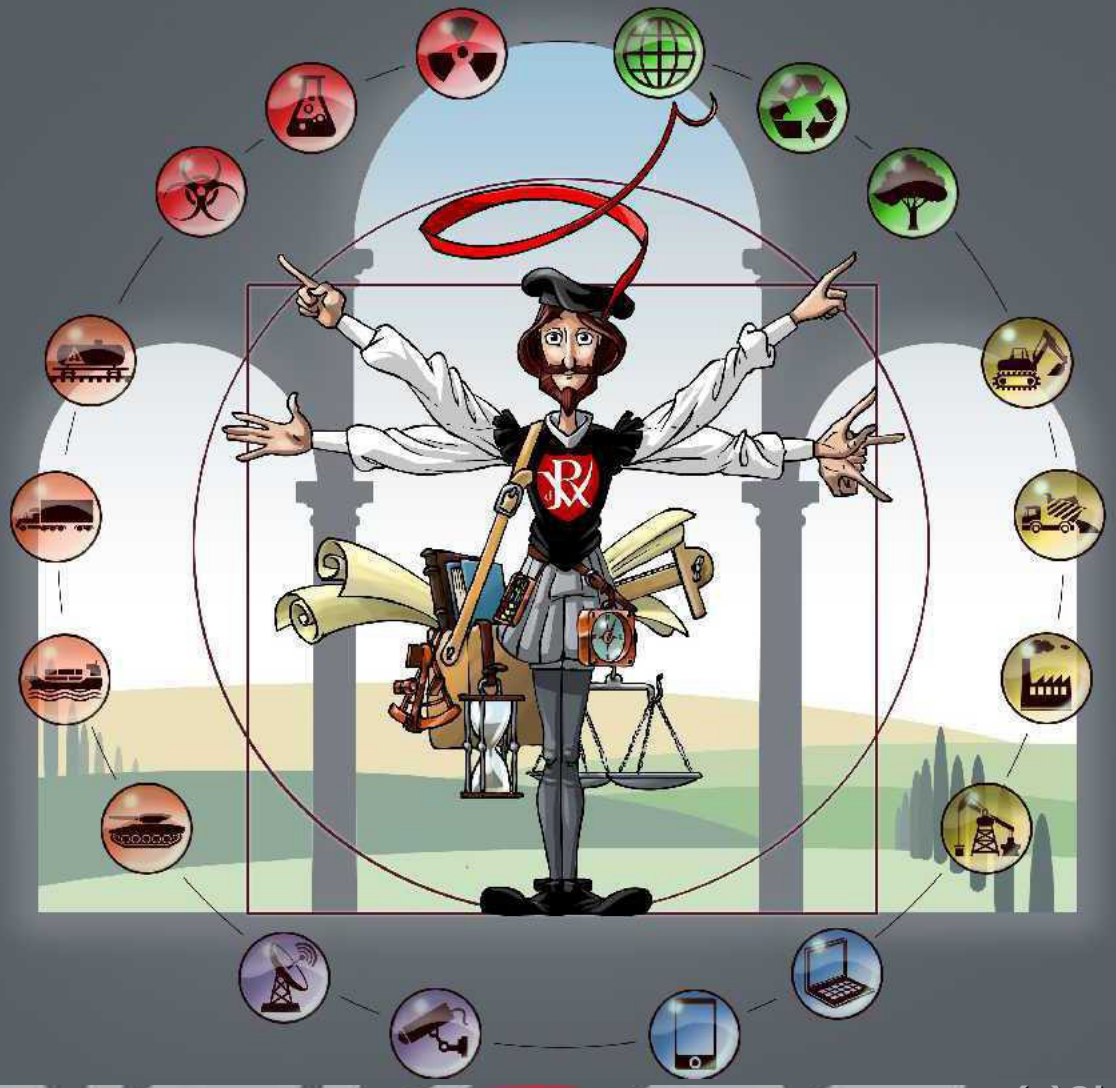
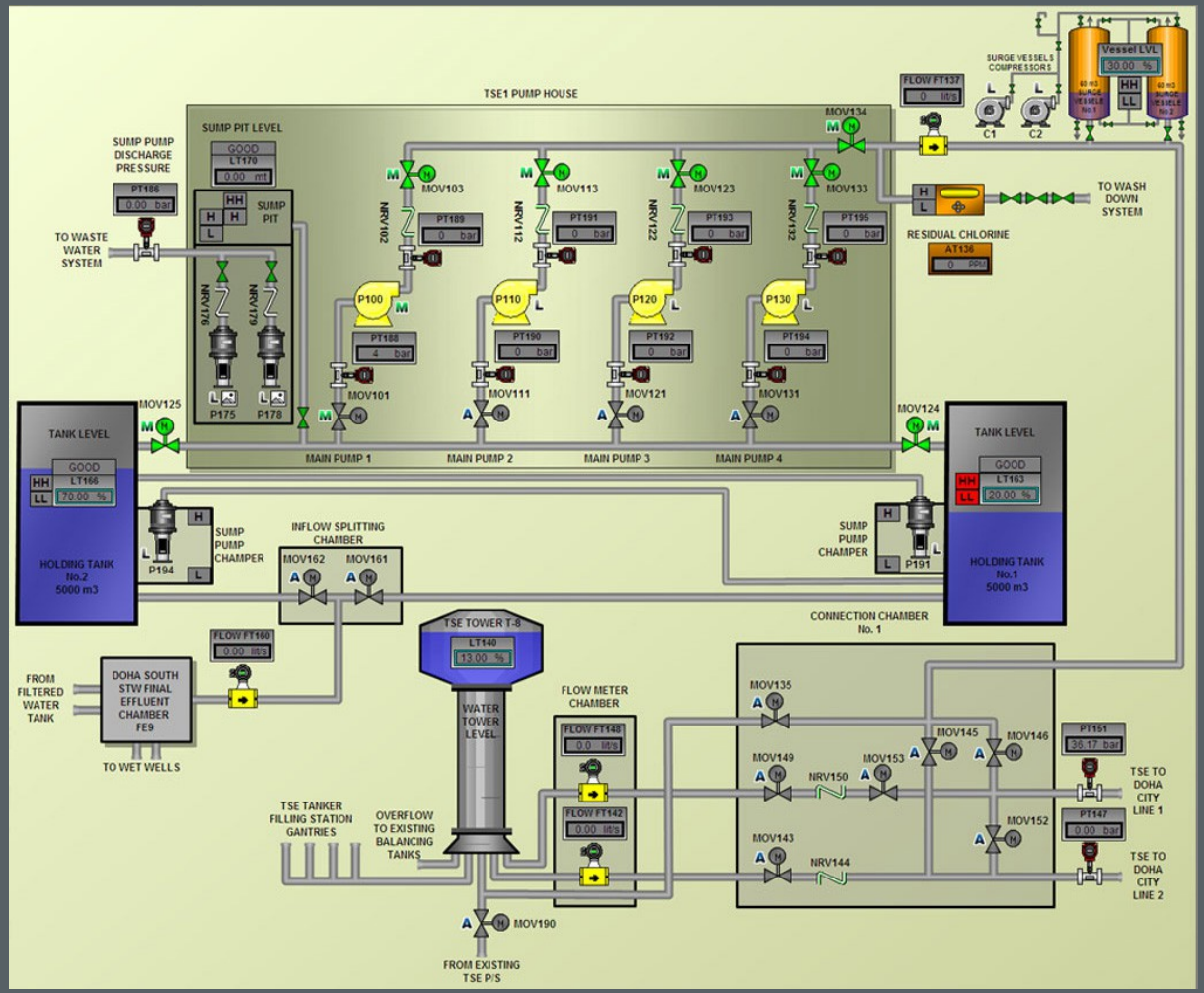
Convergent Quantitative Cyber Risk Assessment to Optimize Enterprise Reliability



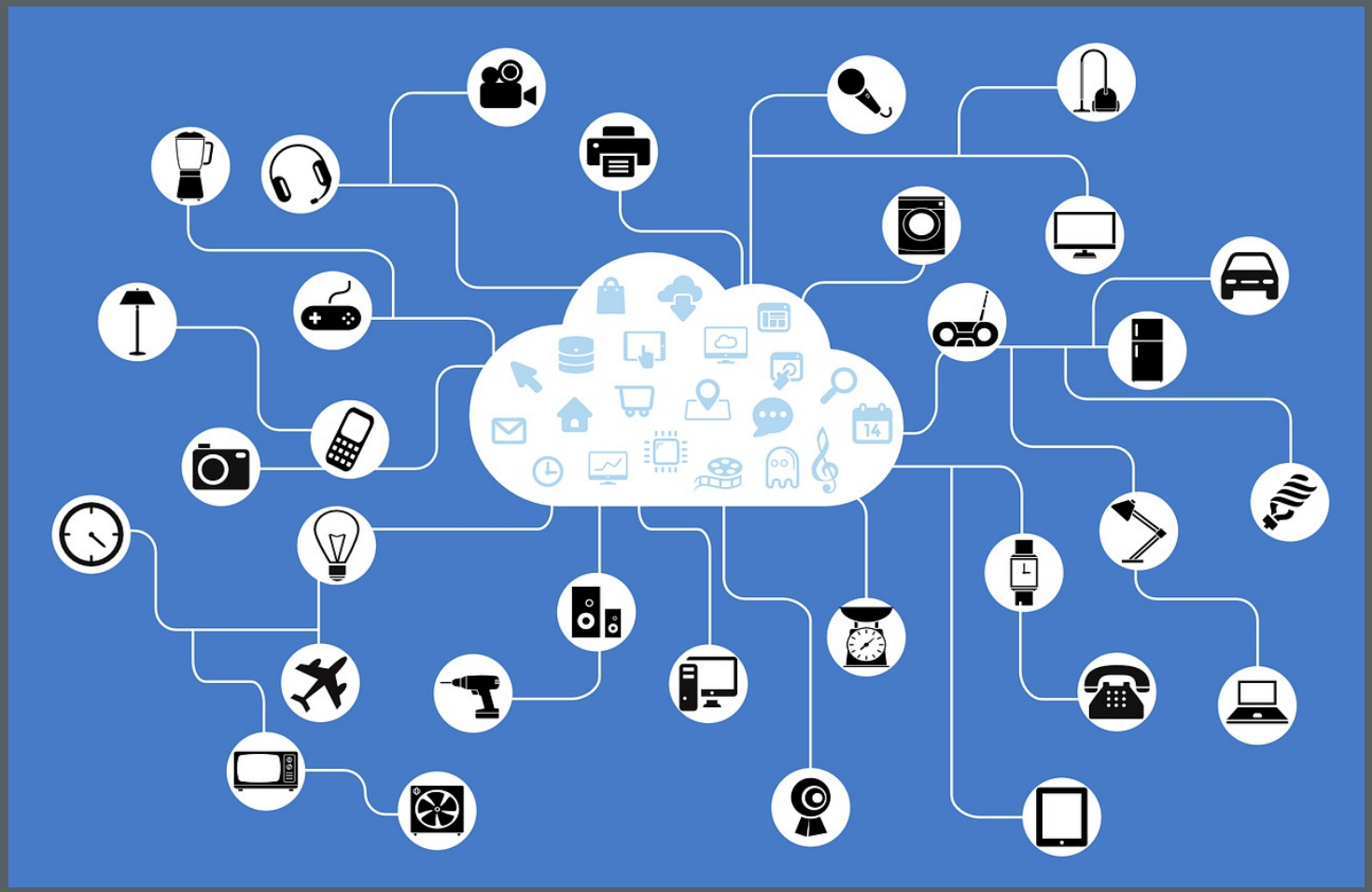
Mining is information dependent though its life cycle

As margins are becoming thinner, proper information and adequate analytics are paramount.



Information technology (IT), Internet of Things (IoT), connectivity bring significant benefits...

streamlined operations, higher efficiency.

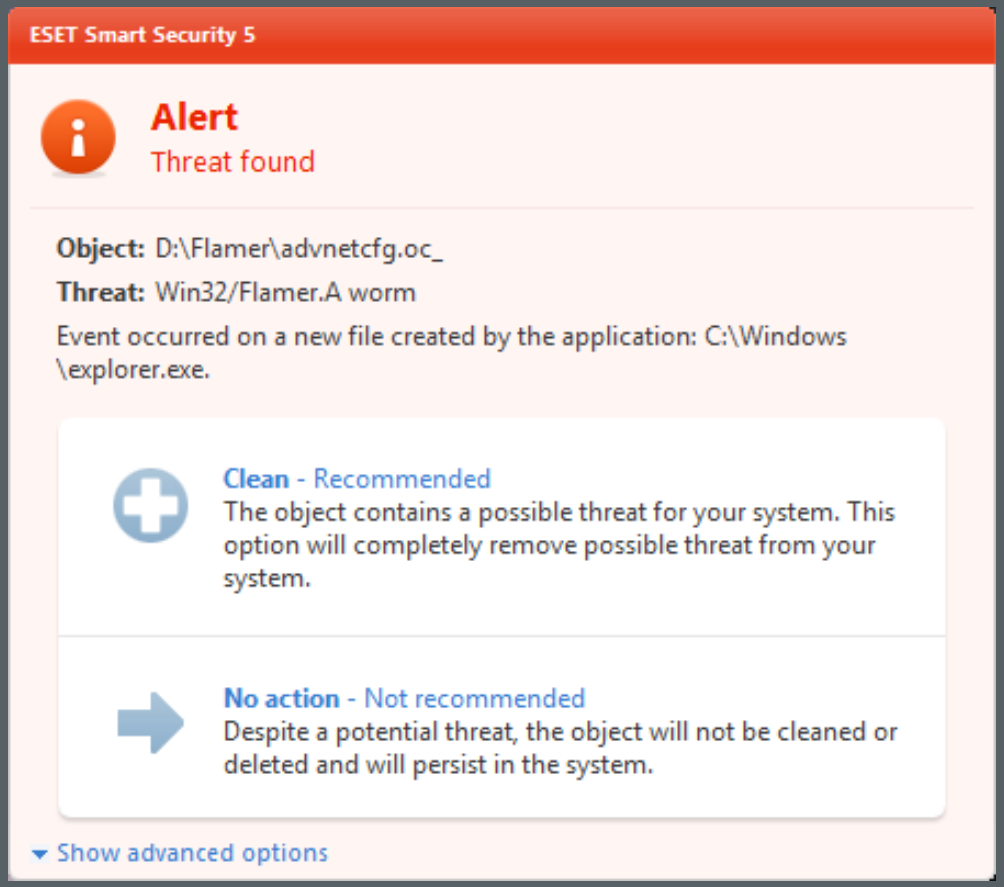


However, their ubiquitous deployment increases cyber-exposure

Cyber criminals and possibly terrorists lurk on industries, critical infrastructures and service space, not only in mining.

At least one major mining company has been the target of a massive hack

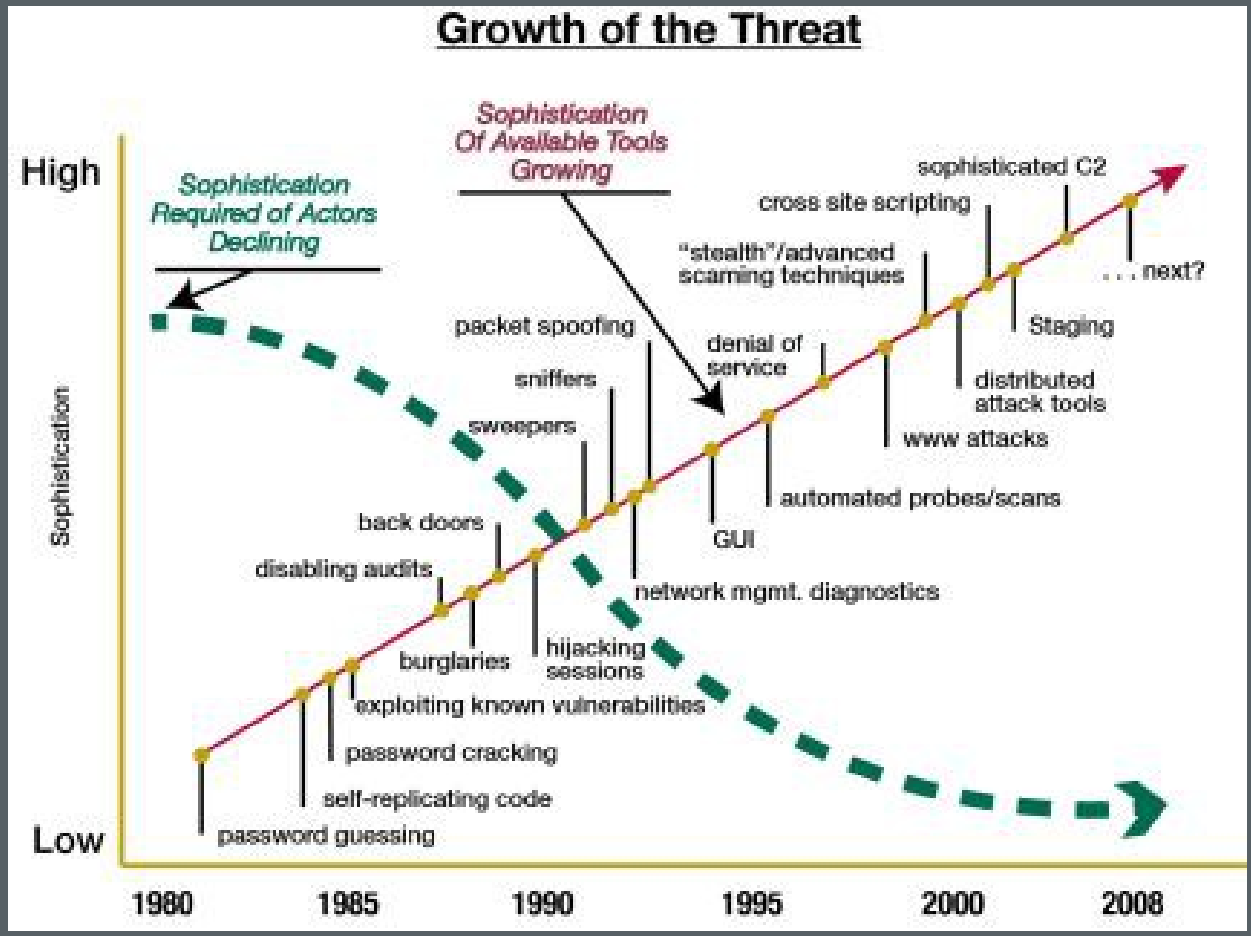
Serious infrastructural damages have only seldom been inflicted to date, and not in mining (as far as we know).



Flame (malware) affecting Iranian Oil Ministry computers.

Techniques and sophistication of cyber attacks evolve continuously

The distinction between actors and threats are blurred and attack prospects more worrying.



The speed and sophistication of cyber attacks have been increasing over time. Source : NATO

Consequences of an attack are always multidimensional

They span from physical to psychological and have strong indirect components.

Direct	Indirect
Health & Safety	• Regulatory compliance (fines) • Public relations/crisis communications • Attorney fees and litigation • Insurance premium increases • Lost value of customer relationships • Value of lost contract revenue • Devaluation of trade name • Loss of intellectual property (IP) • ...
Business Int.	
Environmental	

Given the rapid escalation in the number and sophistication of cyber attacks

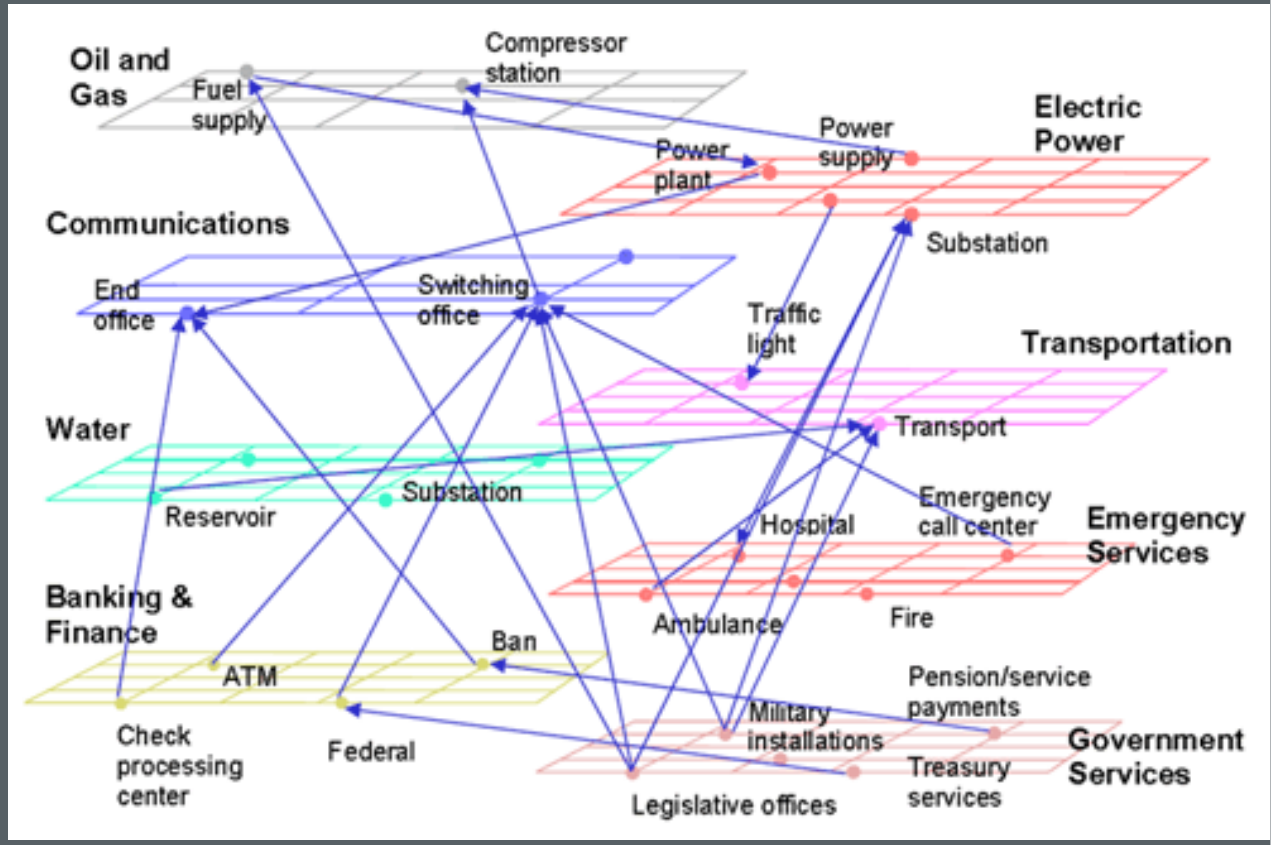
infrastructural damages are to be expected “any time”, anywhere.
A shift in mentality has to occur from threat-from to threat-to.

The « threat-from » is almost impossible to know !

Interdependencies, common cause failures and "long chain events" make things worse

This happens in any of the consequences dimensions

(in)-direct, H&S, BI, environmental, etc..



Source: FCC (Federal Communications Commission)

Any infrastructural damage, especially those with environmental consequences or harm to people...

will lead to significant crisis potential, reputational damages and legal consequences.

We cannot ignore or censor that!

The wide spectrum of threats and potential consequences...

… shows that siloed approaches do not work.

Integrative ones are only slightly better.

Poorly prioritized mitigations are not efficient as they are limited in scope by other operational requirements.

Investments based on "simplistic" hazard analyses do not help making optimum/good decisions.

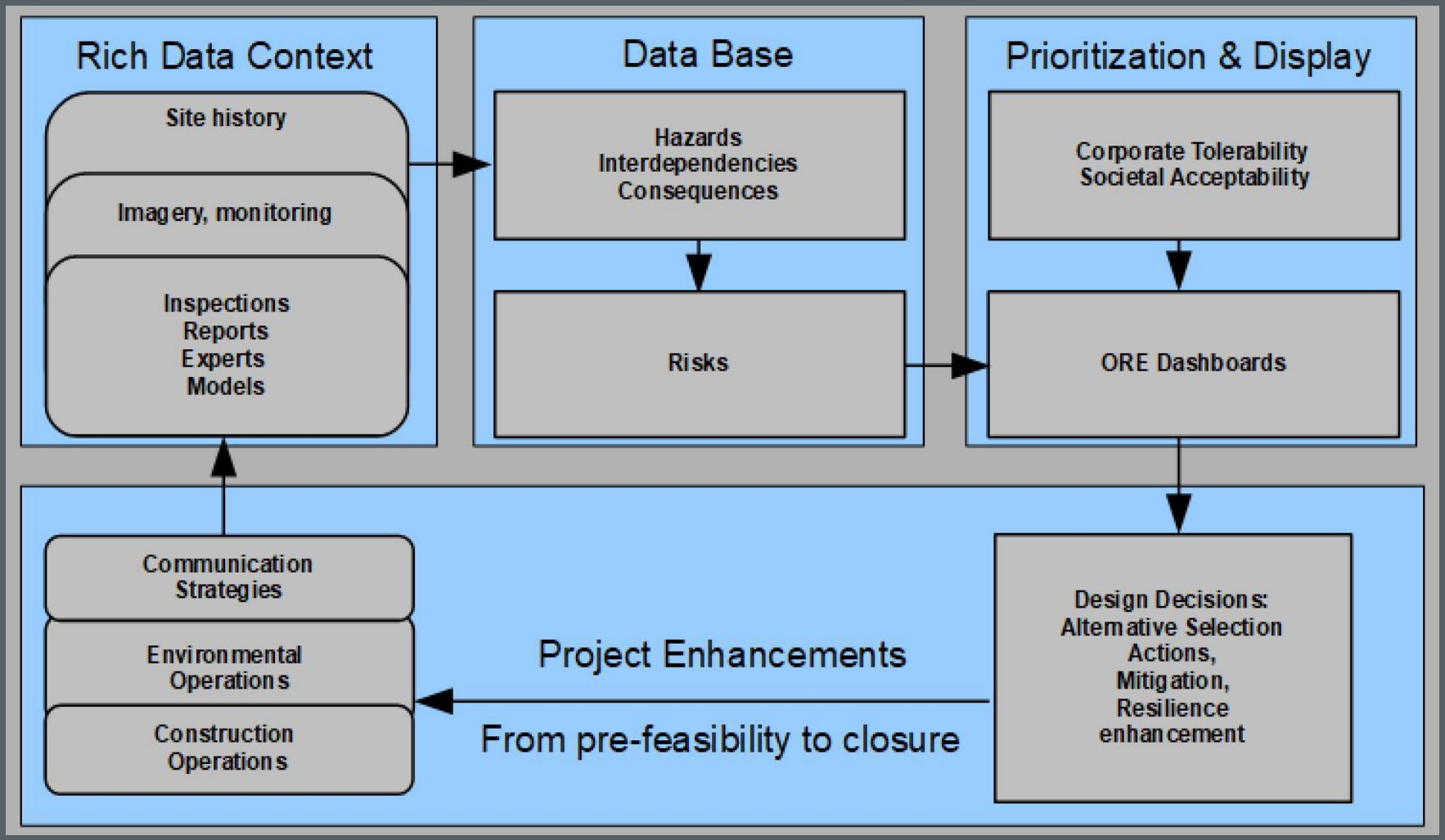
Encouraging information reports « from the trenches »

In some cases, two-thirds of the overall capex on the cyber risk mitigation strategies was non-technology driven.

The idea that cyber risk is not only an IT issue is finally sinking.

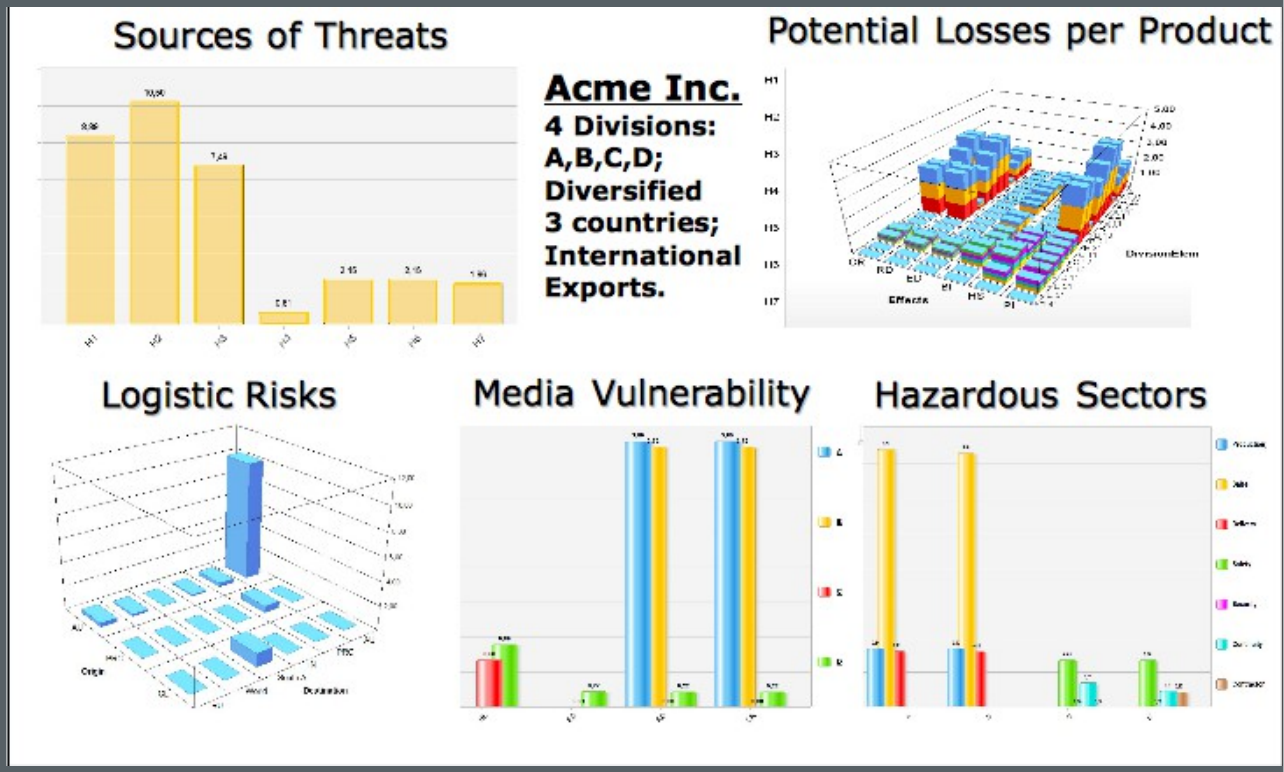
This, however, does not necessarily mean the capex is allotted in the most efficient way at all, unless proper prioritization was performed and silo-culture is replaced by a “horizontal” thinking.

Convergent, scalable, quantitative approaches are necessary to increase reliability while mitigating risks



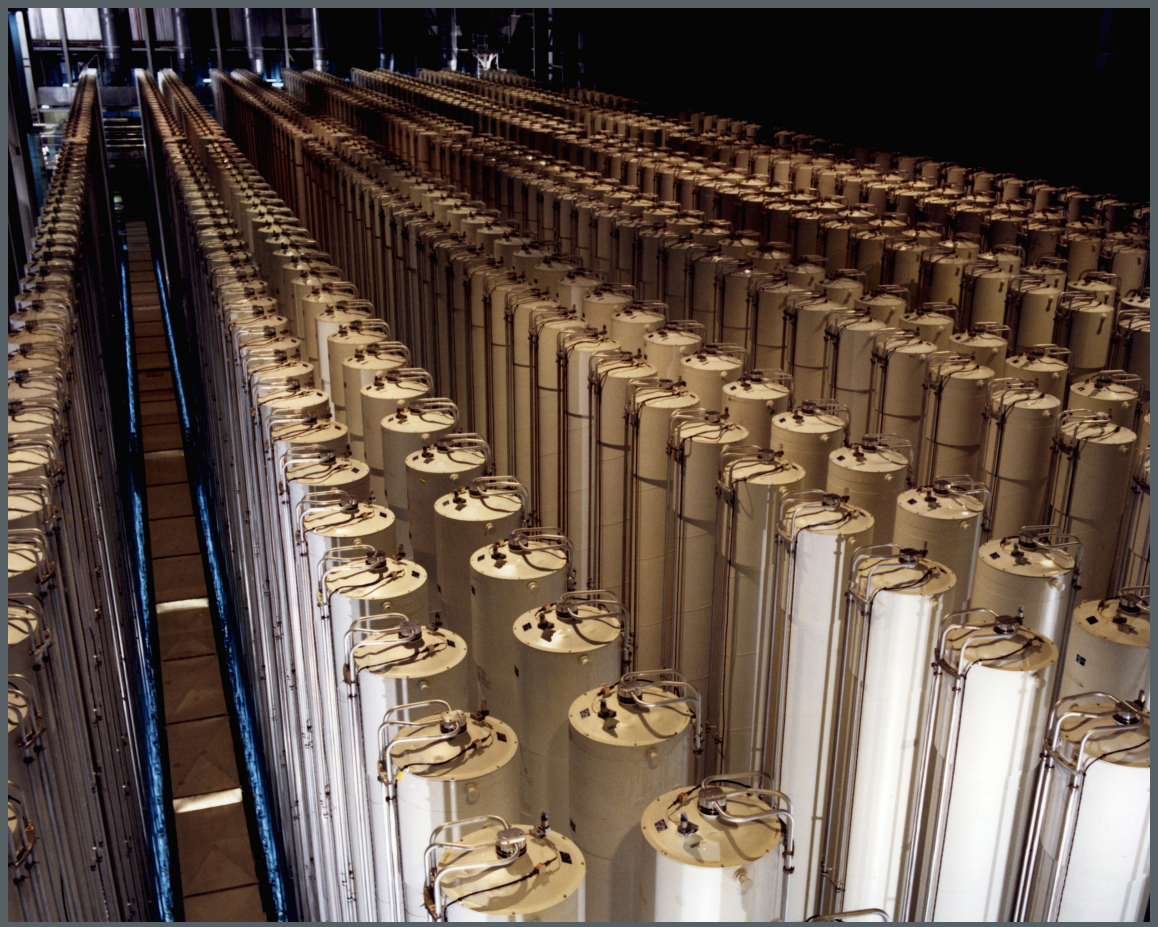
Cyber risks in mining companies are a reality that cannot be ignored and requires appropriate tools

Tools have to be refined enough to grasp the complex reality, yet operable enough to avoid paralysis by analysis.



Insurers cannot help as they lack the necessary knowledge, tools and even more importantly actuarial data.

Statistics cannot help, probabilities and solid risk assessment platforms do.

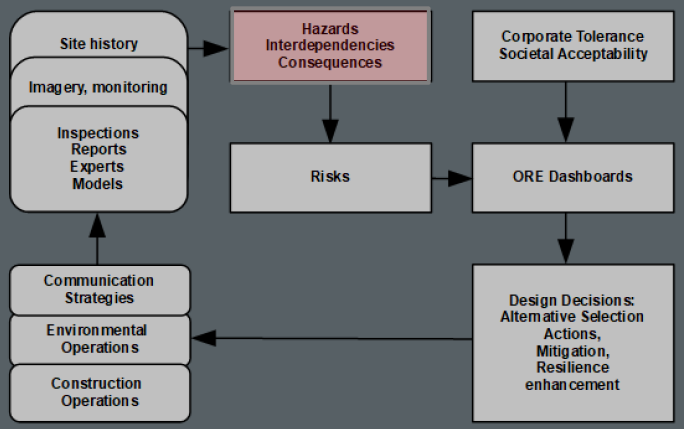


Centrifuges affected by stuxnet

Case history of convergent quantitative prioritized risk assessment for risk informed decisions

The goal is to optimize mitigative investments and increase reliability through a mining portfolio, including cyber-risks in the best possible way.

We will look at the mineral wharves sub-system.



Hazards Interdependencies Consequences

Plant Office

Main Substation

Railway

Dumper Indexer

Conveyor

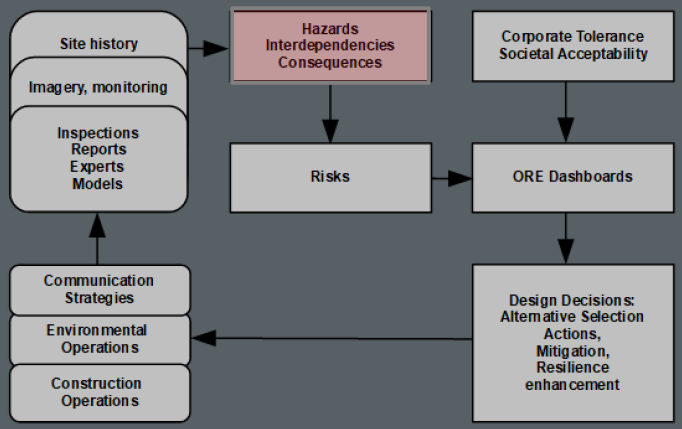
Stacker Reclaimer

Loader

Ship

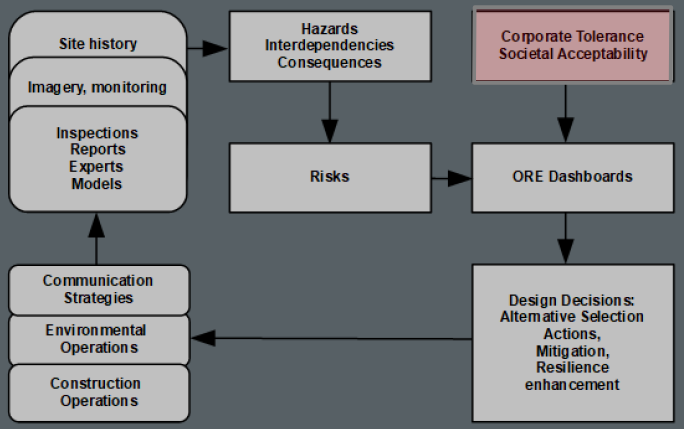
Waste Water

Sludge System



Hazards

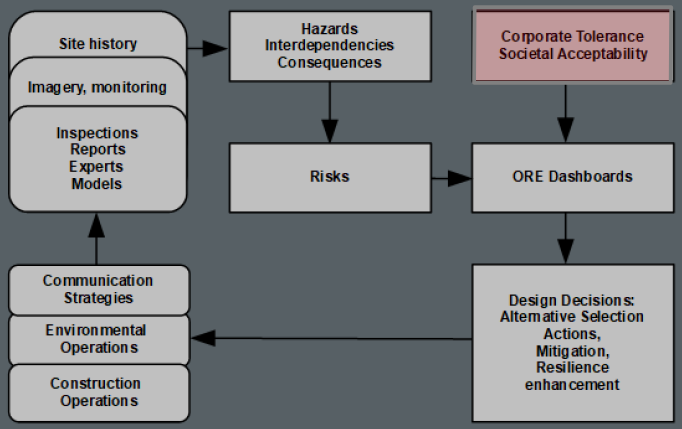
Earthquake
High wind (Windstorm & Hurricane)
Lightning
Snowstorm
Volcano Ash
Extreme cold, freezing rain
System of communication
Power electric
Power hydrocarbons
Equipment Failure
Fire, explosion
Spill Hydrocarbons
Spill Chemical
Succession Planning
Pandemic
Employees' Dishonesty
Riots
Arson
Cyber attacks



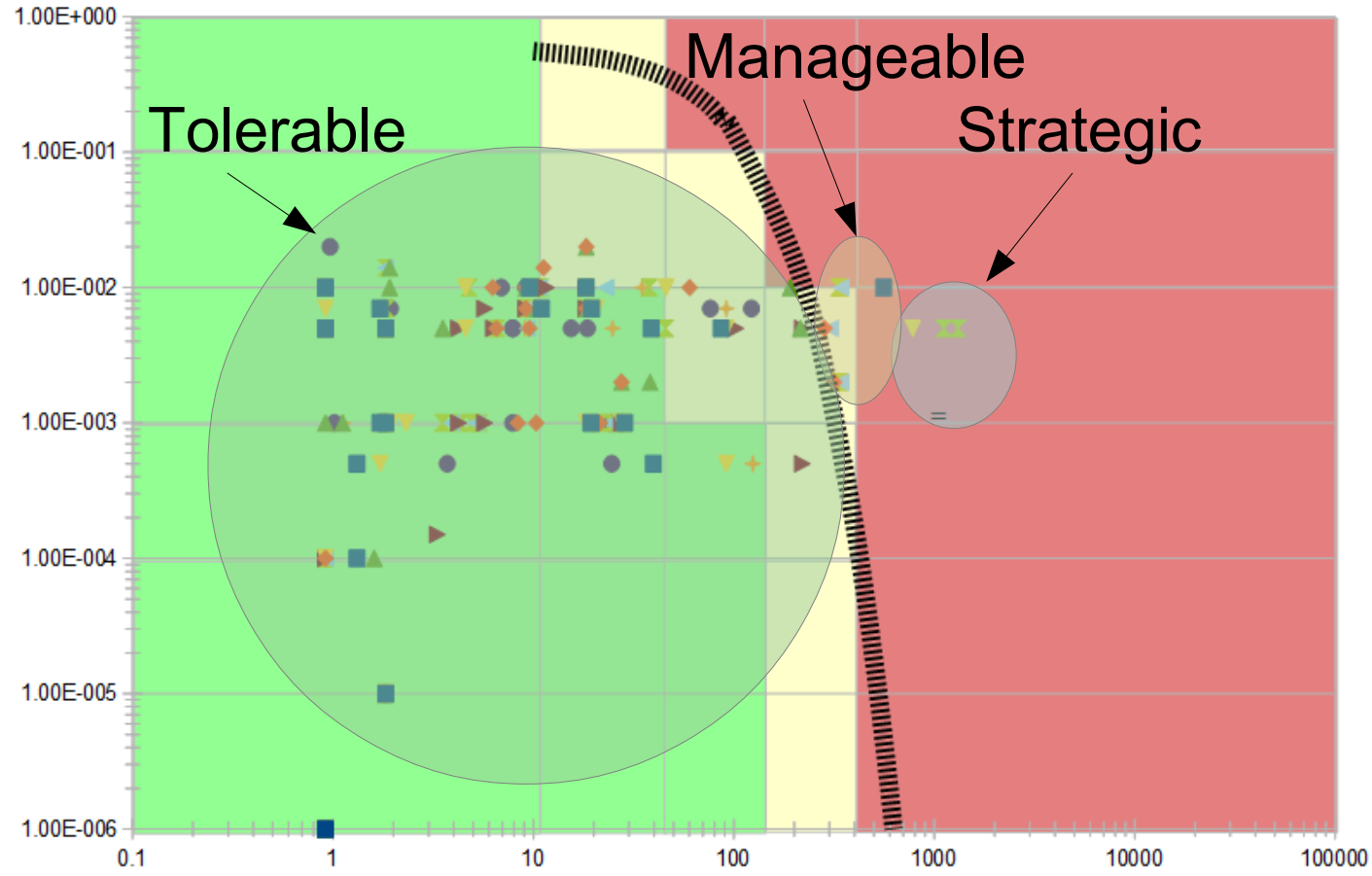
Instead of the classic matrix, the plot showing risk and tolerance (next slide) allows the analysis to:

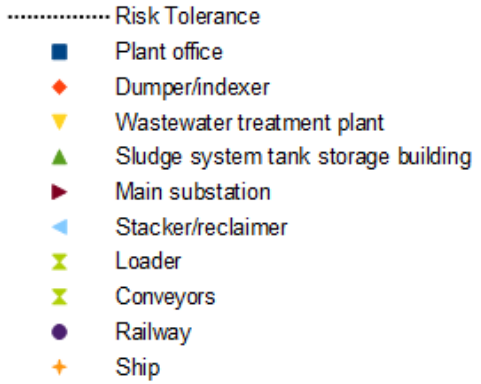
- prioritize risks based on their intolerable part, which focuses attention on those risks that actually have the potential to hurt; this enhances the focus and the value of the assessment;

- determine which risks are:
  a) tolerable;
  b) manageable, i.e. which are under the responsibility of management;
  c) strategic, i.e. which might require upper management to shift their objectives

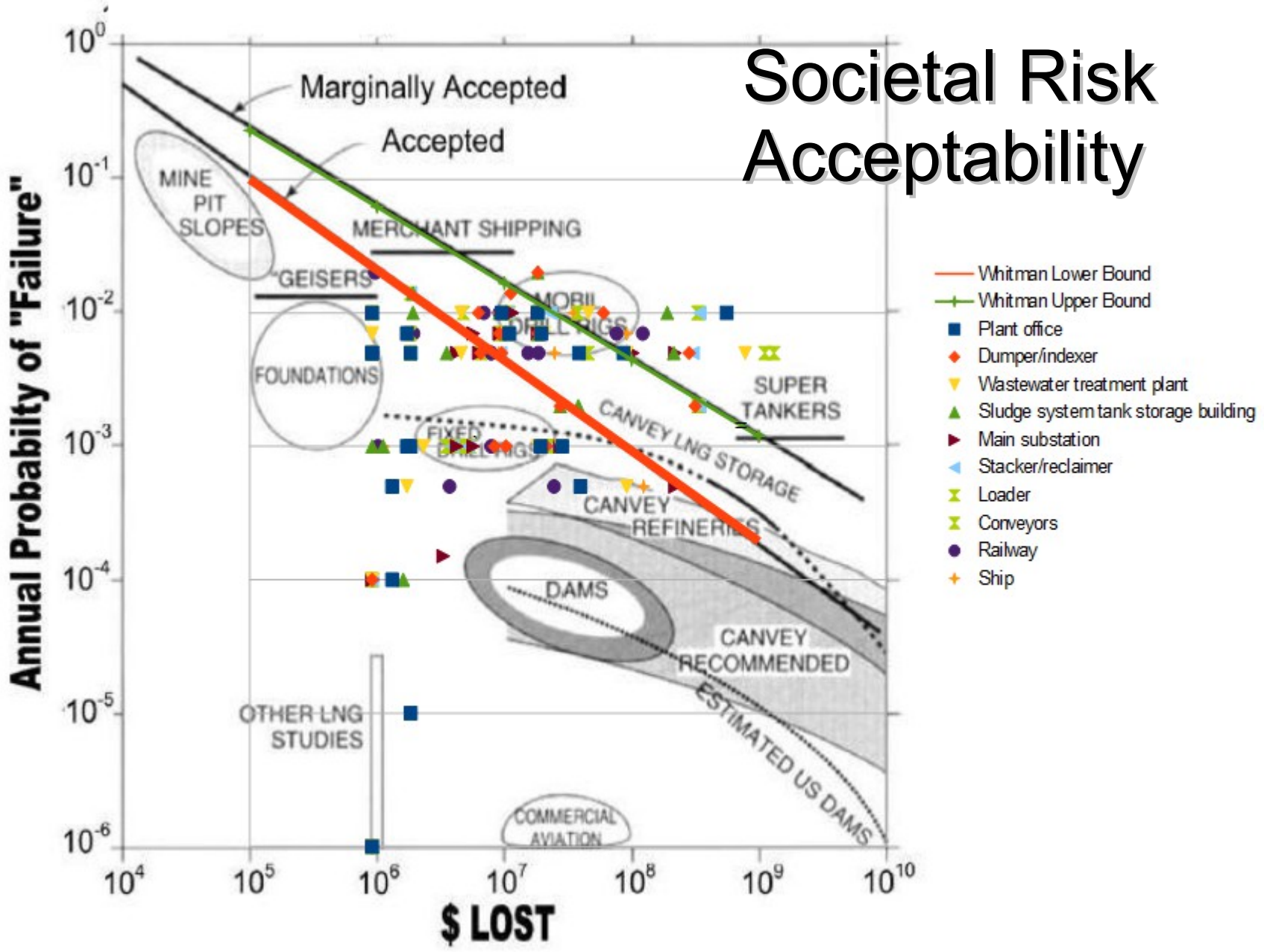


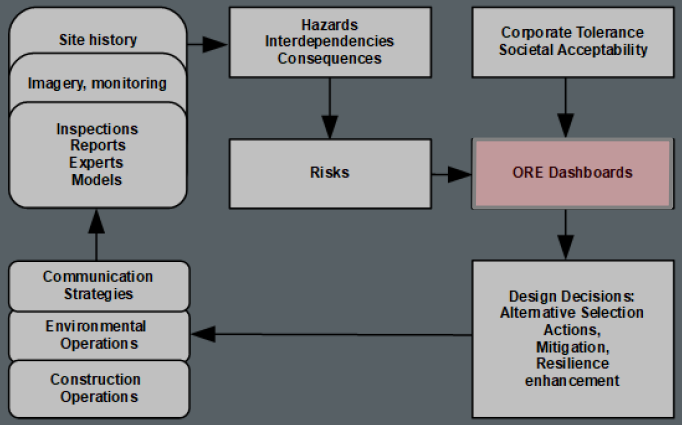
Corporate Risk Tolerance allows to define tolerable, manageable, strategic risks



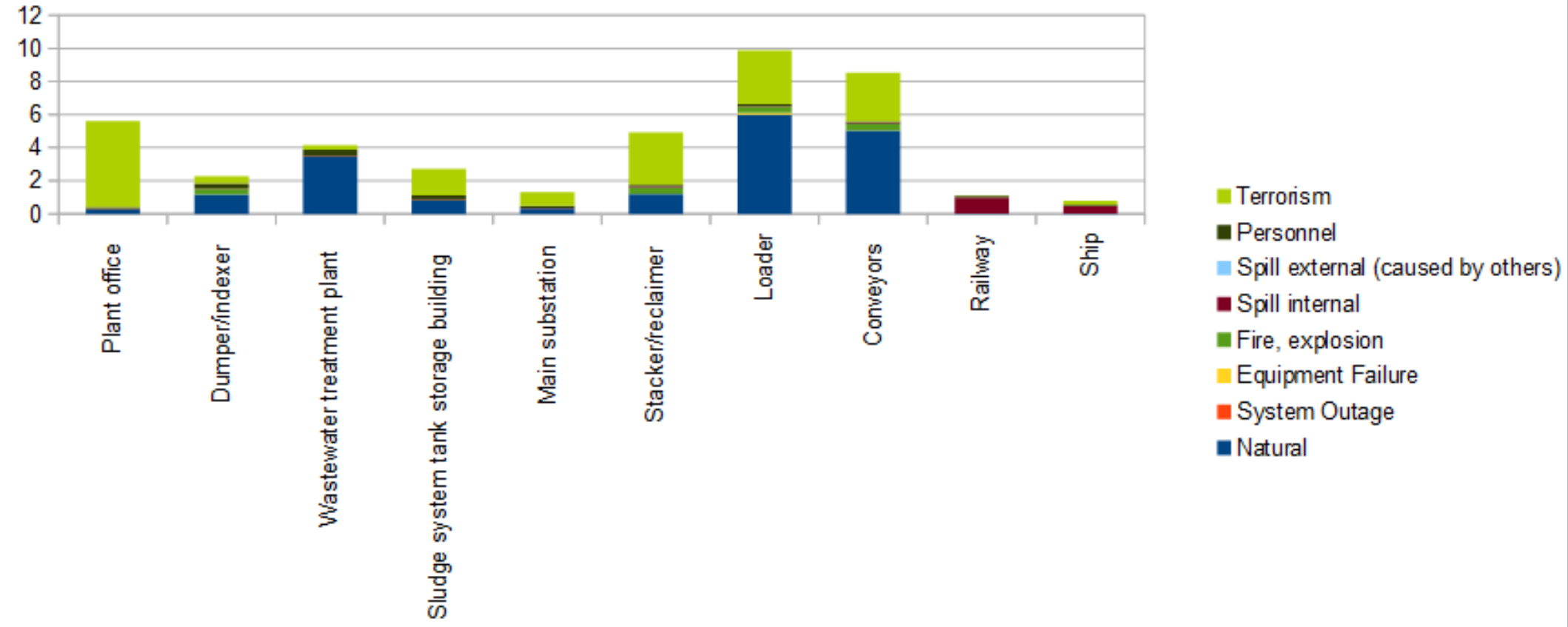


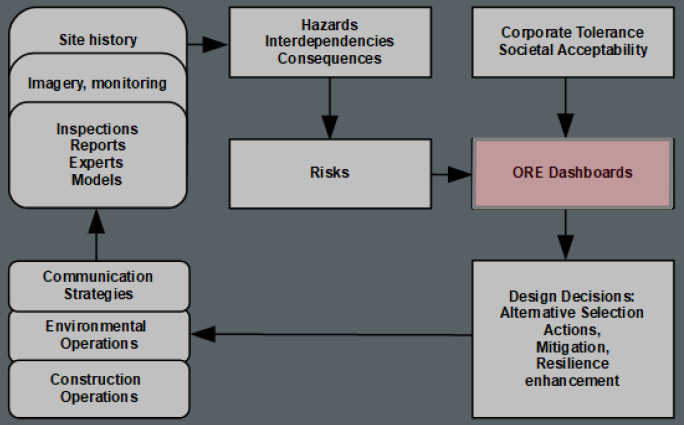
Societal Risk Acceptability



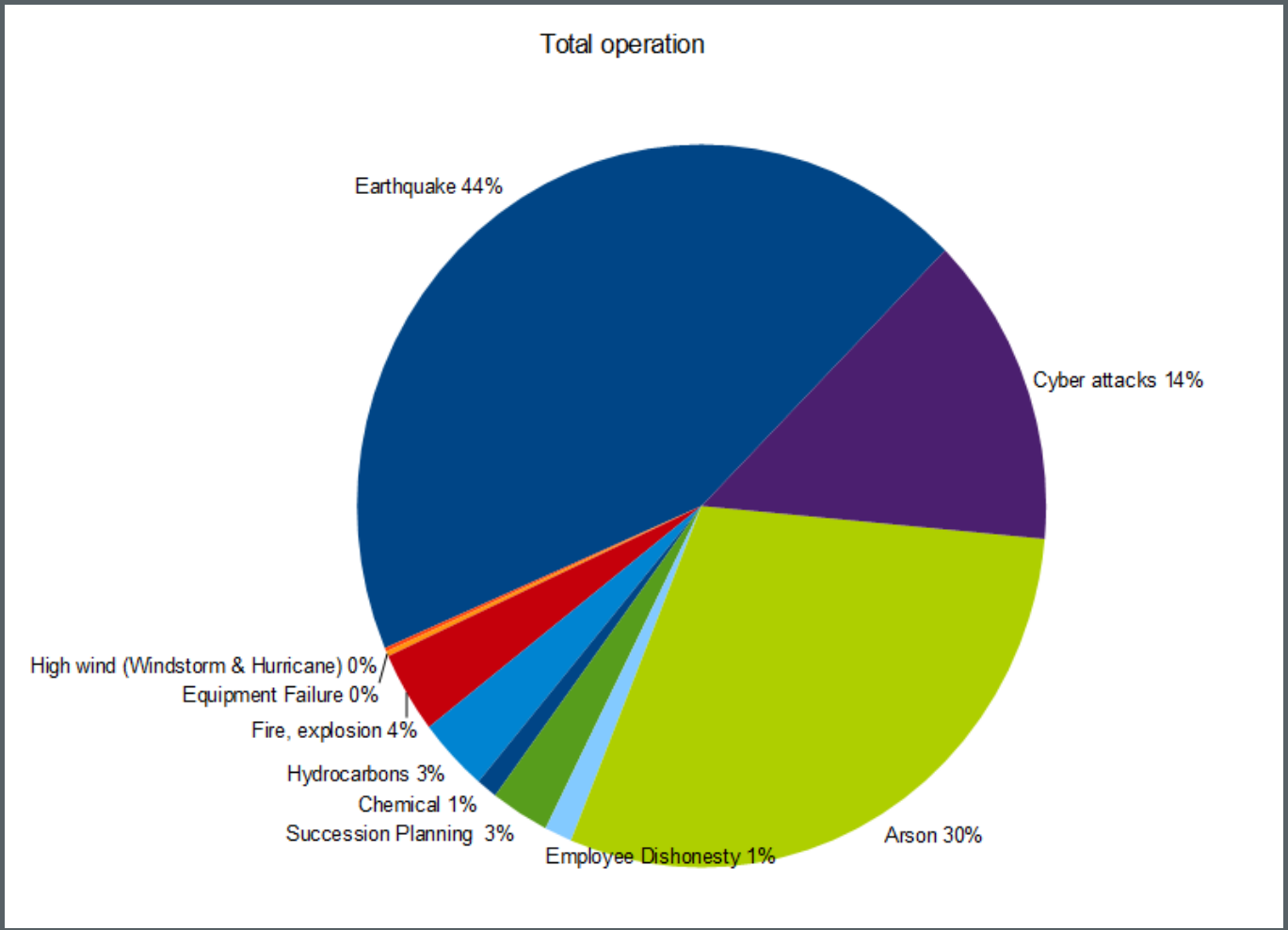


ORE roadmap per system's elements and Risk Triaging by hazard

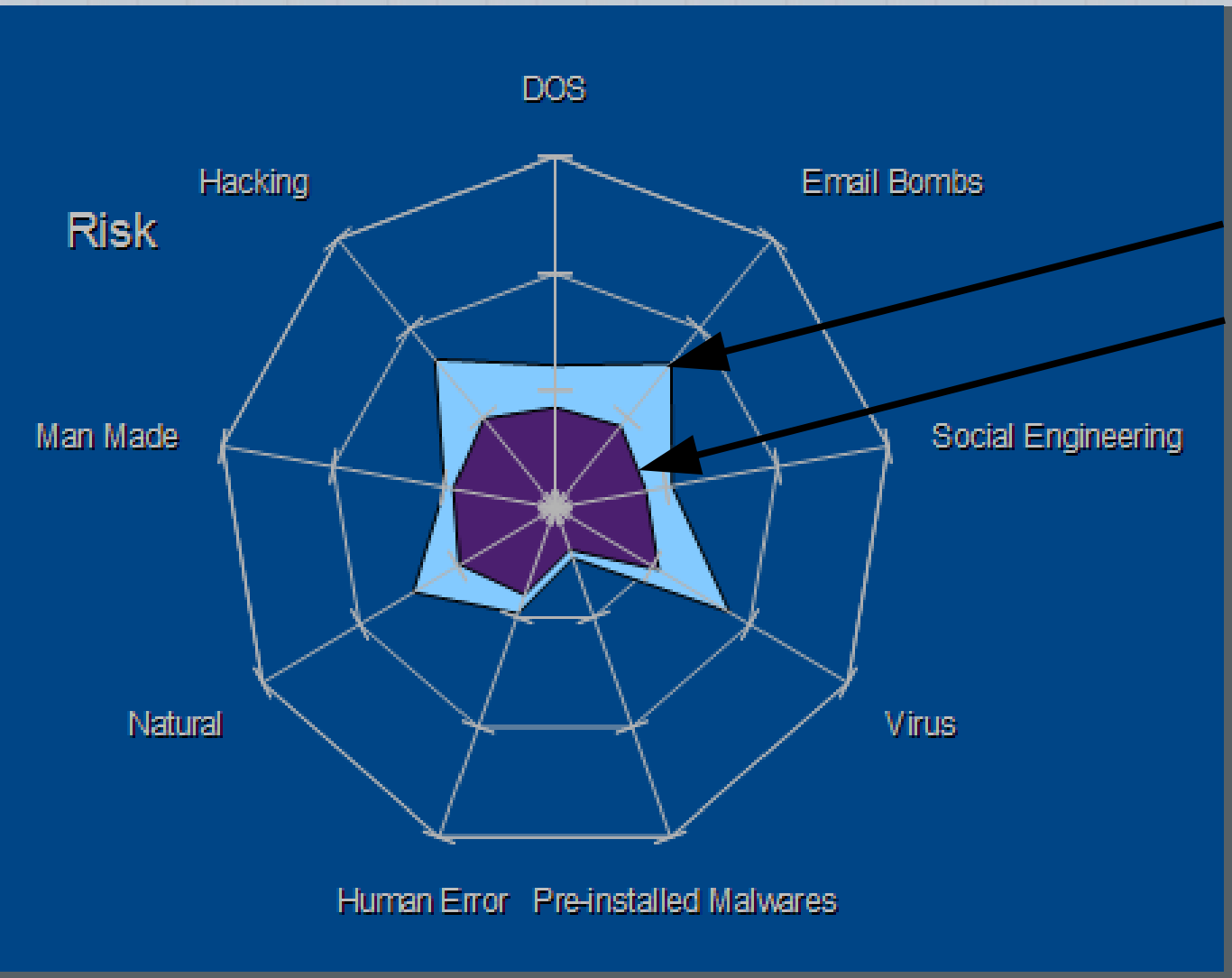




ORE roadmap for the entire system : risks prioritized by hazard



Residual risk evaluation



Pre Mitigations
Post Mitigations

Because it is simply not possible to protect each property from each threat.

Cyberdefense must be rooted on convergent prioritized rational Risk Management

and not

on standardized audits and practice of indolent regulations, written a priori,
or
the biased advice of fear monger solutions sellers.

Cyber risks in mining companies are a reality

The deployment of an adequate siloes-busting convergent analysis methodology will eliminate capex squandering and increase overall enterprise reliability.

Risk informed technical support to projects, operations, corporations helps to define:

- Sensible quantitative scalable risk assessments.
- Interdepedencies, global uncertainties, near misses inclusion, efficiency of existent or future mitigations.
- Contract clauses, insurance limits, mitigative road-map, avoidance of decision-makers' overwhelming syndrome.
- Deployment of a consistent risk reporting tool across one or many operations/projects at any geographic scale.