Possibility Space: Understanding Risk

Patrick Hudson
Tim Hudson

Hudson Global Consulting
Delft University of Technology

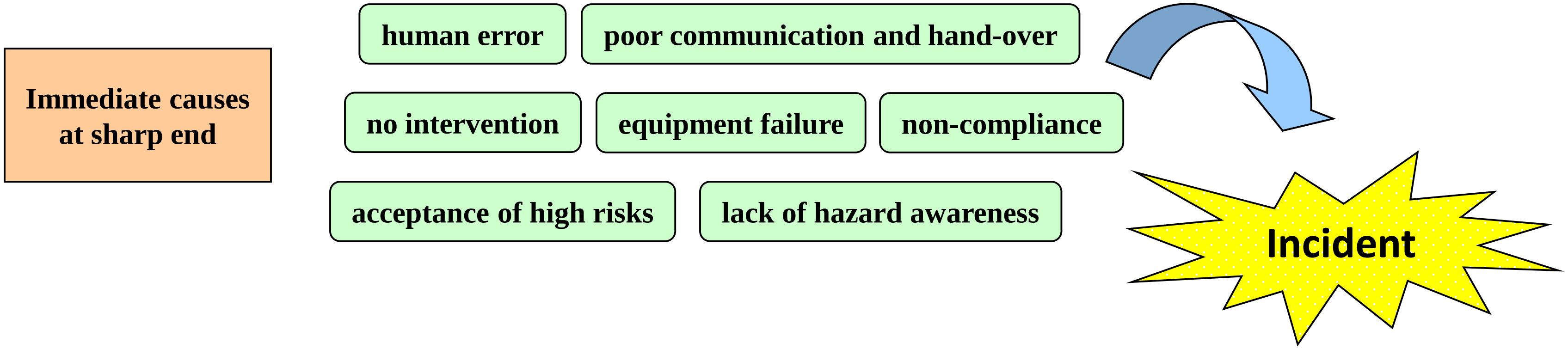
How can we manage risk?

- We can manage risk by hoping it won’t happen
- We can manage risk by offering sacrifices to the Gods
- We can manage risk by understanding what we are doing

- The first two don’t work
- The third is what a Safety Management System does
- A good safety culture makes the management system work

- Fundamental to this is an **understanding of risk**

Factors contributing to incident causation



Immediate causes at sharp end

human error

poor communication and hand-over

no intervention

equipment failure

non-compliance

acceptance of high risks

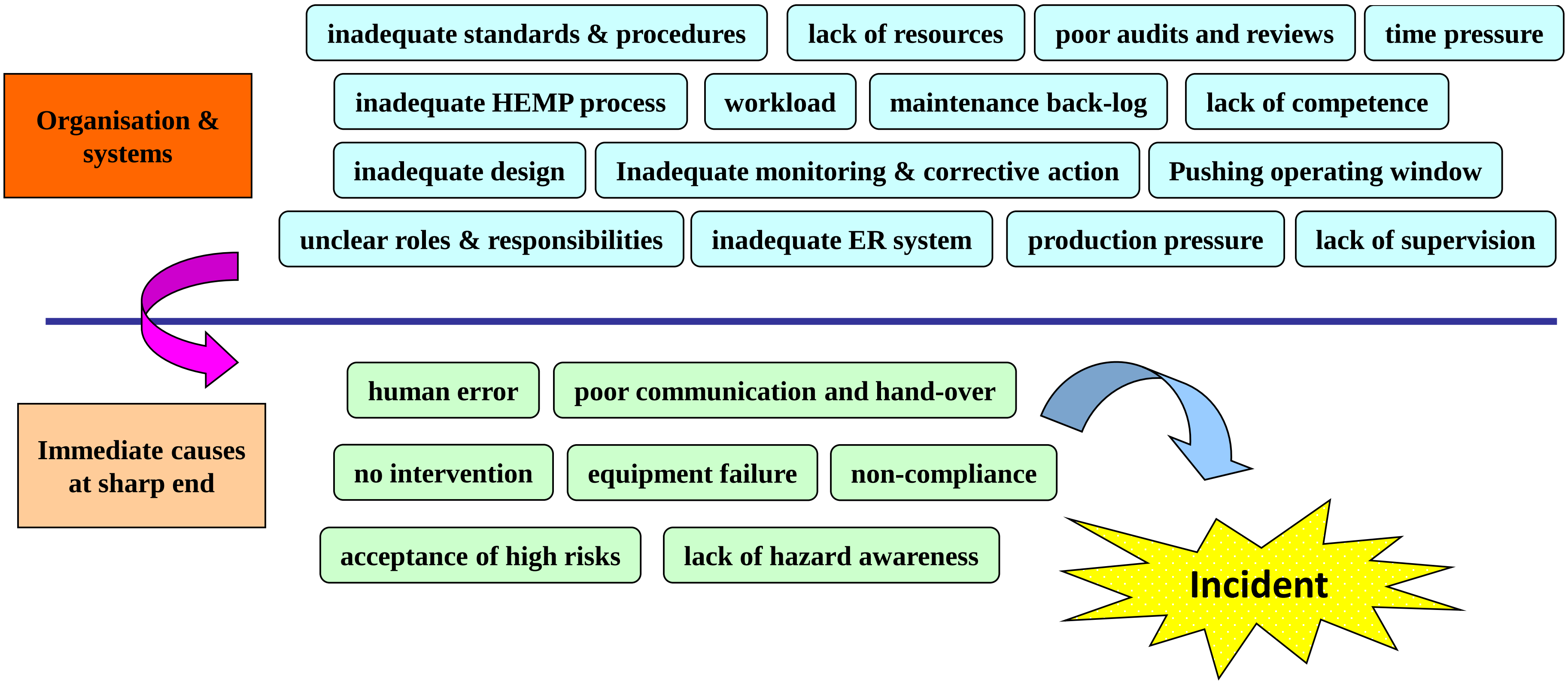
lack of hazard awareness

Incident

Theory 1
how accidents are caused

- Deterministic causes - either it is a cause or it isn’t
- Linear causation – A causes B causes C proportionately
- We can compute both backwards and forwards
- People are seen as the problem – human error etc
- Personal accidents
- Probably good enough to catch 80% of the accidents we are likely to have

Factors contributing to incident causation



Organisation & systems

inadequate standards & procedures

lack of resources

poor audits and reviews

time pressure

inadequate HEMP process

workload

maintenance back-log

lack of competence

inadequate design

Inadequate monitoring & corrective action

Pushing operating window

unclear roles & responsibilities

inadequate ER system

production pressure

lack of supervision

Immediate causes at sharp end

human error

poor communication and hand-over

no intervention

equipment failure

non-compliance

acceptance of high risks

lack of hazard awareness

Incident

Theory 2
how accidents are caused

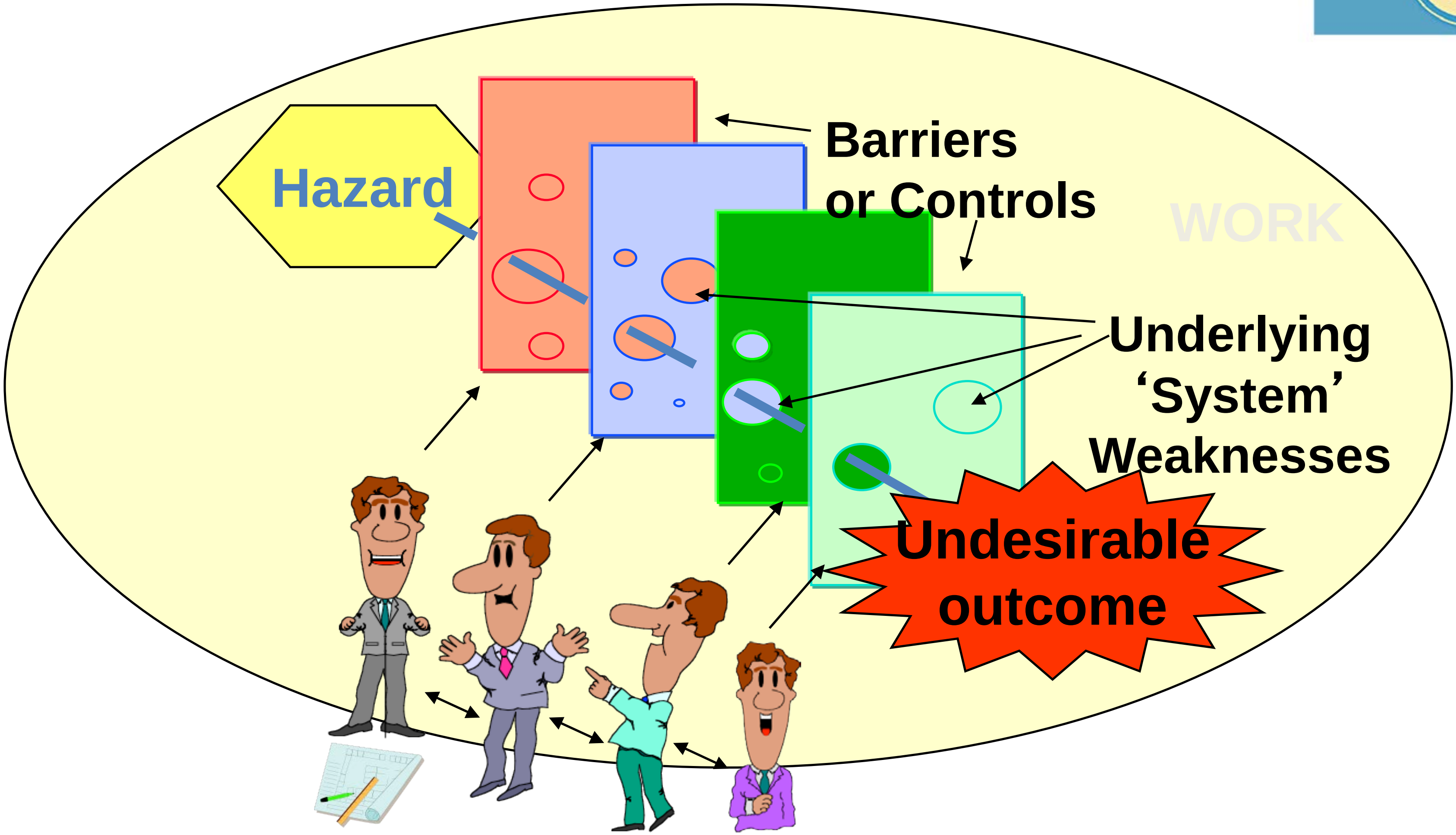
- Non-Linear causes
  - Cause and consequence may be disproportionate
  - These causes are organizational, not individual
- Deterministic dynamics- either it is still a cause or it isn’t

- We can still compute both backwards and forwards
  - Increasingly difficult with non-linear causes

- This is the Organizational Accident Model – Swiss Cheese

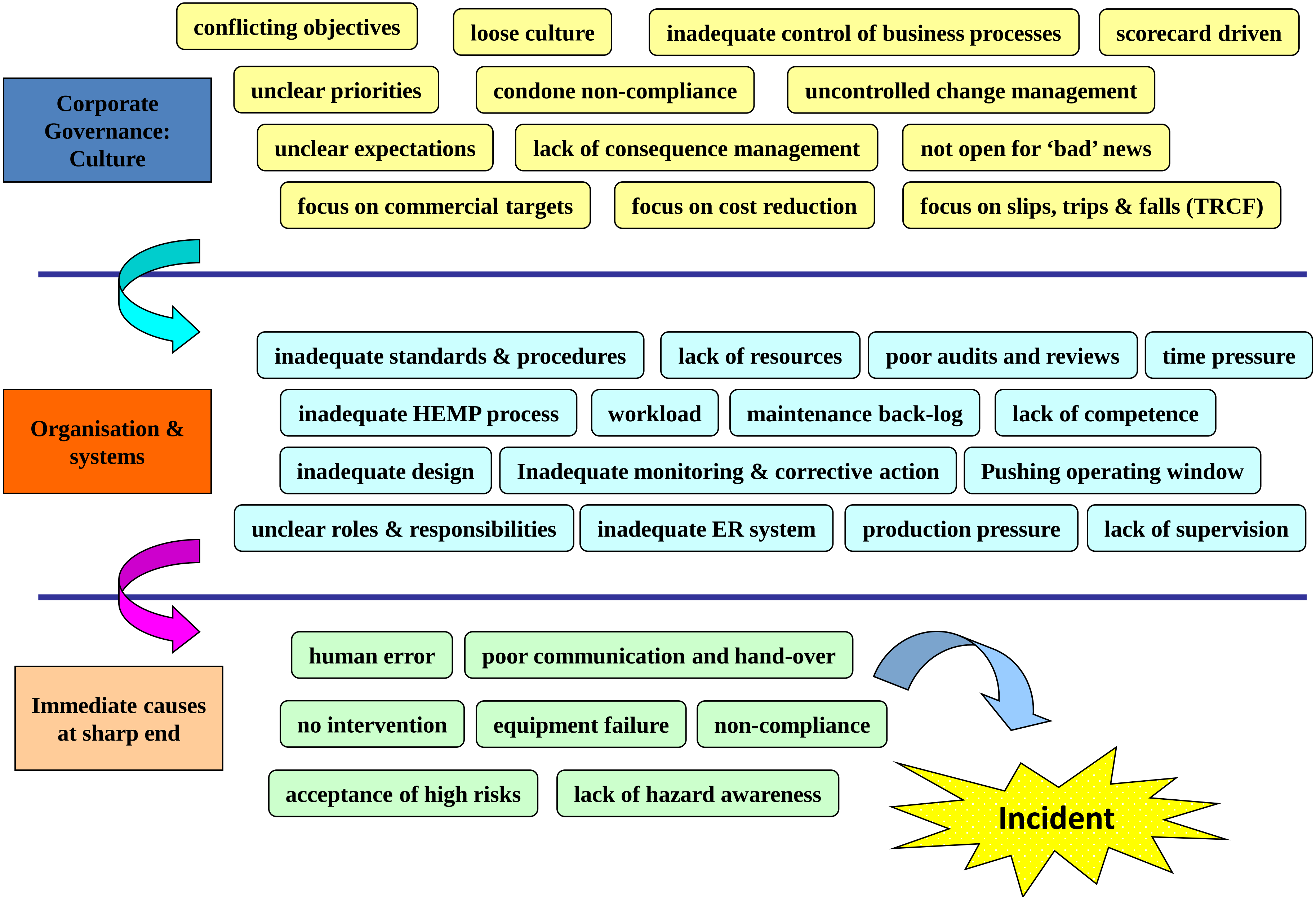
- Probably good enough to catch 80% of the residual accidents = 96%

Swiss Cheese



Is this good enough?

Factors contributing to incident causation



Corporate Governance: Culture

- conflicting objectives
- loose culture
- inadequate control of business processes
- scorecard driven
- unclear priorities
- condone non-compliance
- uncontrolled change management
- unclear expectations
- lack of consequence management
- not open for ‘bad’ news
- focus on commercial targets
- focus on cost reduction
- focus on slips, trips & falls (TRCF)

Organisation & systems

- inadequate standards & procedures
- lack of resources
- poor audits and reviews
- time pressure
- inadequate HEMP process
- workload
- maintenance back-log
- lack of competence
- inadequate design
- Inadequate monitoring & corrective action
- Pushing operating window
- unclear roles & responsibilities
- inadequate ER system
- production pressure
- lack of supervision

Immediate causes at sharp end

- human error
- poor communication and hand-over
- no intervention
- equipment failure
- non-compliance
- acceptance of high risks
- lack of hazard awareness

Incident

Theory 3
how accidents are caused

- Non-Linear causes
- Non-Deterministic dynamics
  - Probabilistic rather than specific
  - Influences on outcomes by people and the organisation
- We cannot compute both backwards and forwards
- Prior to an event there may be a multitude of possible future outcomes

- 80% of the residual 4% (80 – 96 – 99.2) leaves 0.8%
- 90% of the residual 1% leaves (90 – 99 – 99.9) 0.1%

Types of accidents

- Type I
- Simple models may cover 80% of all accidents
- These are the simple personal accidents

- Type II
- The next step gets 80% of the remainder = 96%
- These are the complex personal accidents and some organizational accidents

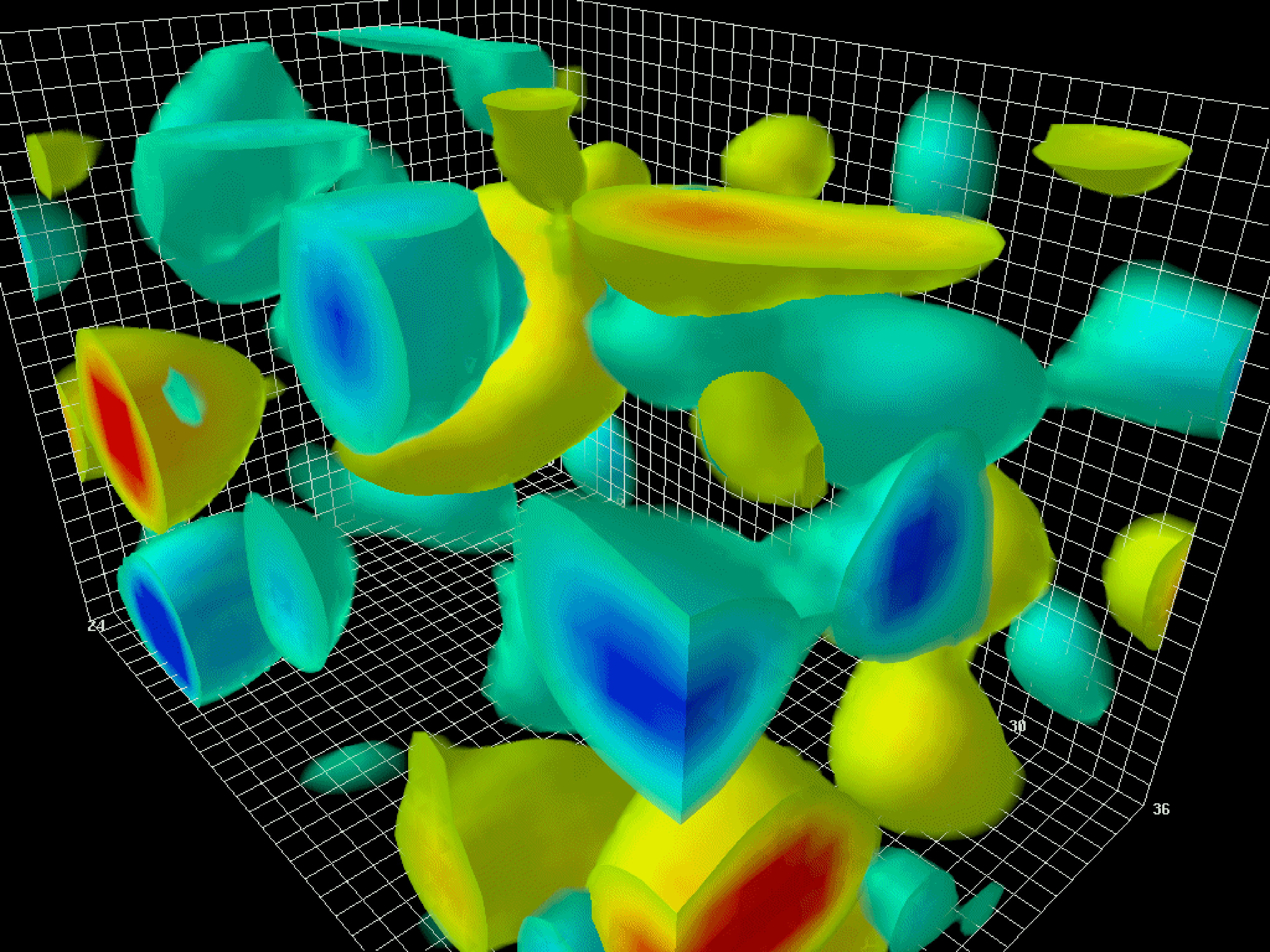
- Type III
- The probabilistic approach may net the next 80% = 99.2%
- These are the complex process accidents

Swiss Cheese

- Swiss Cheese is a metaphor for Type II accidents

- The holes were always dynamic
  - We couldn’t show this with acetate sheets!

- Extending to Type III really requires dynamics


24
30
36

The models are all approximations

- Types I, II and III are not actually different
- Type I is an approximation to II and III that works most of the time
  - classic OHS personal safety
- Type II is an approximation to Type III smoothing out the uncommon and rare details
  - Organisational accidents still primarily personal
- Type III is the best model but the hardest to work with
  - You need to be advanced to handle this level

Unusual or WEIRD Accidents

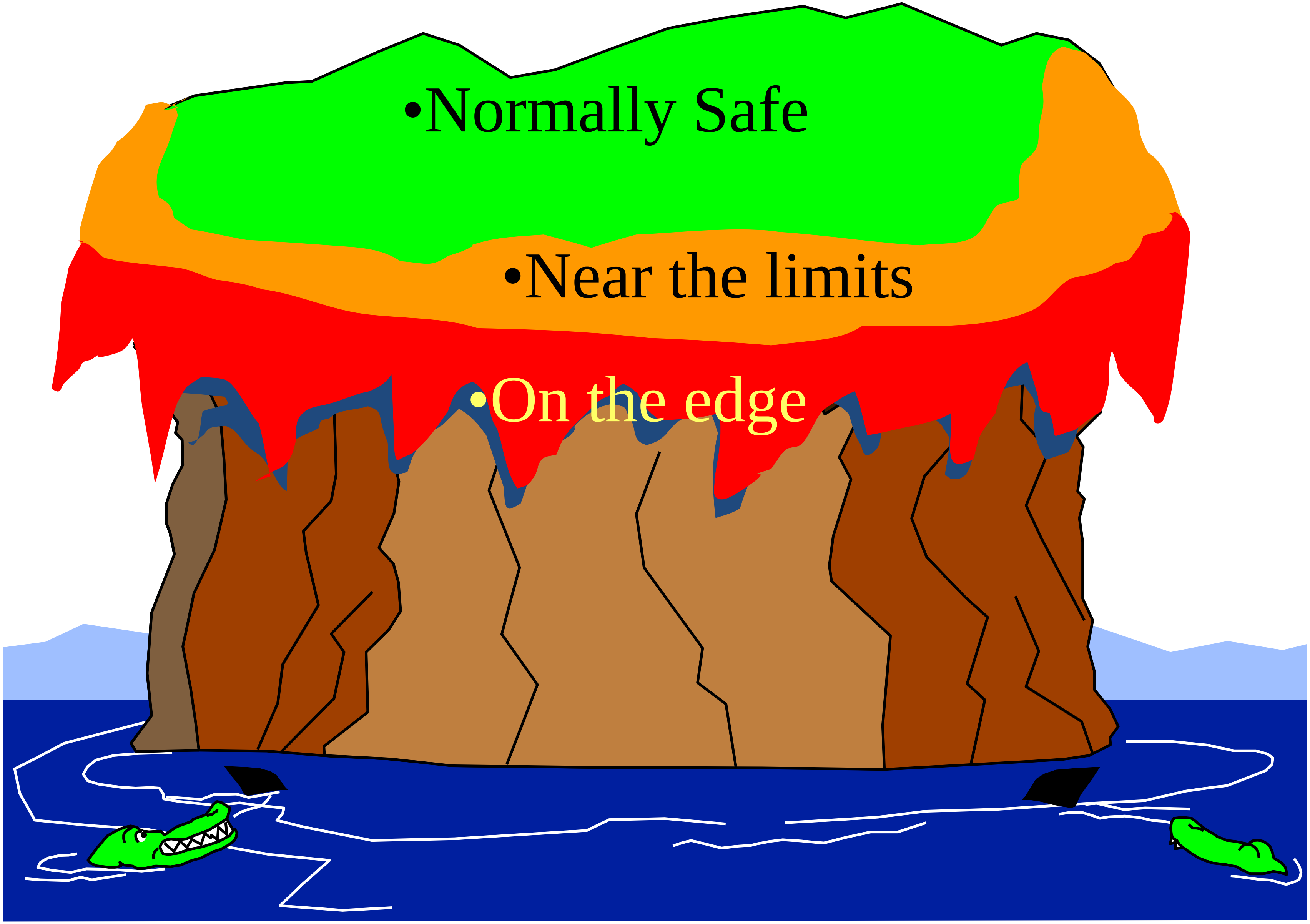
- In commercial aviation and some other industries major accidents are now extremely rare
- WEIRD – Wildly Erratic Incident Resulting in Disaster
- Simple risk assessment and analysis models often fail to capture how these accidents are caused
- We need to understand our risk space better
- The *Rule of Three* is an example of how to do this

The Rule of 3

- Accidents are complex events, with more than 50 immediate and contributory factors
- Preventing a single factor would prevent an accident
- BUT, there may be 49+ other factors waiting –
    - An Accident Waiting to Happen
- The Rule of Three helps develop Situation Awareness for organizations and individuals
- Situation Awareness tells us how close we are to ‘The Edge’

Examples of complex accidents

- Fixed wing and helicopter accidents
- Tanker incidents
- Oil-field disasters
- Many things going wrong at the same time
- No single reason to stop the activity
- Obvious with hindsight that people should have stopped earlier



- Normally Safe
- Near the limits
- On the edge

Why didn’t they stop?

An Incident occurs when 2-4 of the signs meet

The Rule of Three

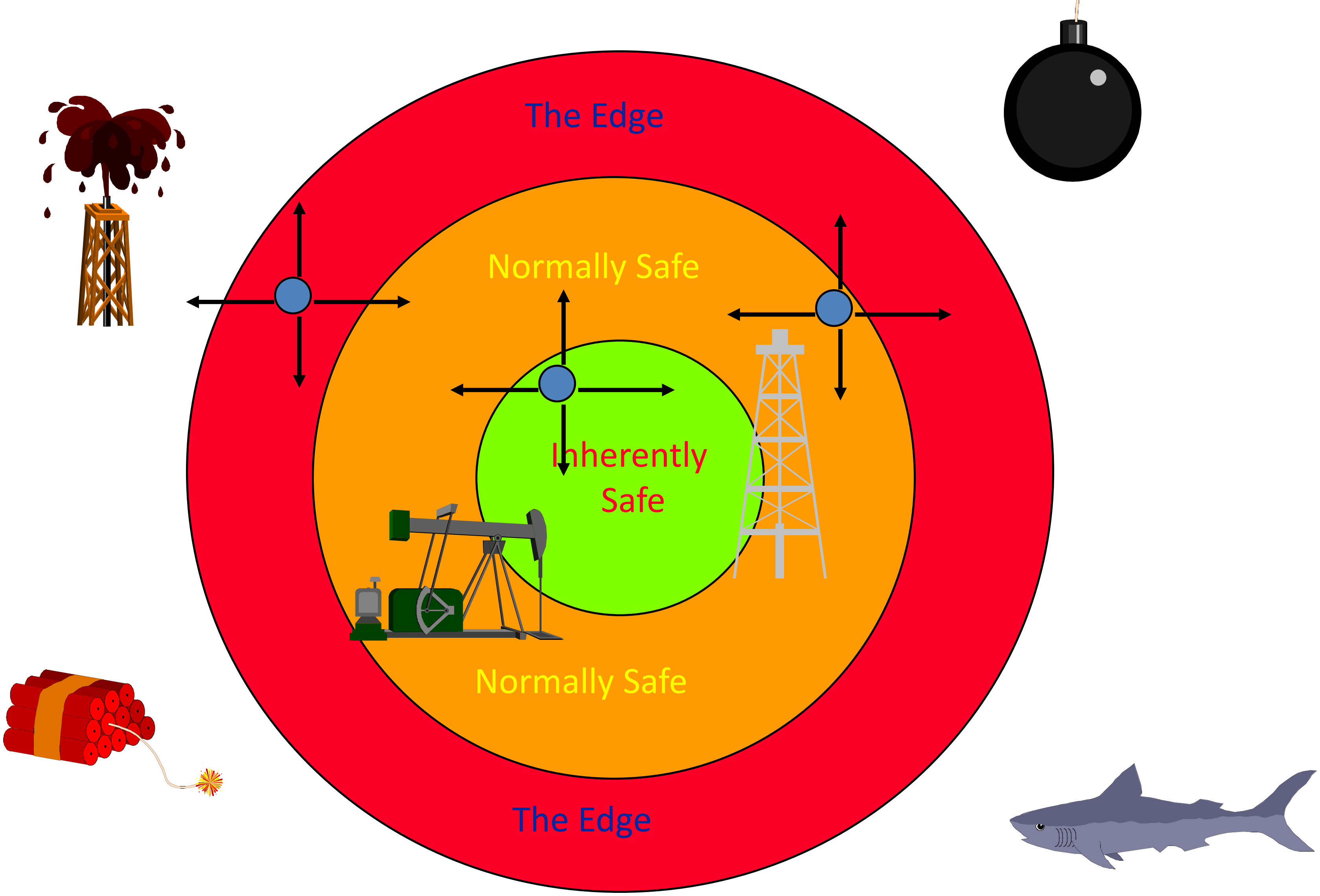
- A Rule based on two levels of threshold
- Green = OK
- Orange = Proceed with caution
- Red = Stop
- Three Oranges = 1 Red = STOP
- Levels defined in terms of Dimensions
- Dimensions made up of sub-dimensions

Aircraft Operation Dimensions

- Crew Factors Experience, Duty time, CRM
- Aircraft Perf. Category, Aids, Fuel, ADDs
- Weather Cloud base, wind, density alt, icing, wind
- Airfield Nav Aids, ATC, Dimensions, Topography
- Environment Night/day, Traffic, en route situation
- Plan Change, Adequacy, Pressures, Timing

- These dimensions are all orthogonal - uncorrelated

The Edge


The Edge
Normally Safe
Inherently
Safe
Normally Safe
The Edge

Testing the Rule of Three

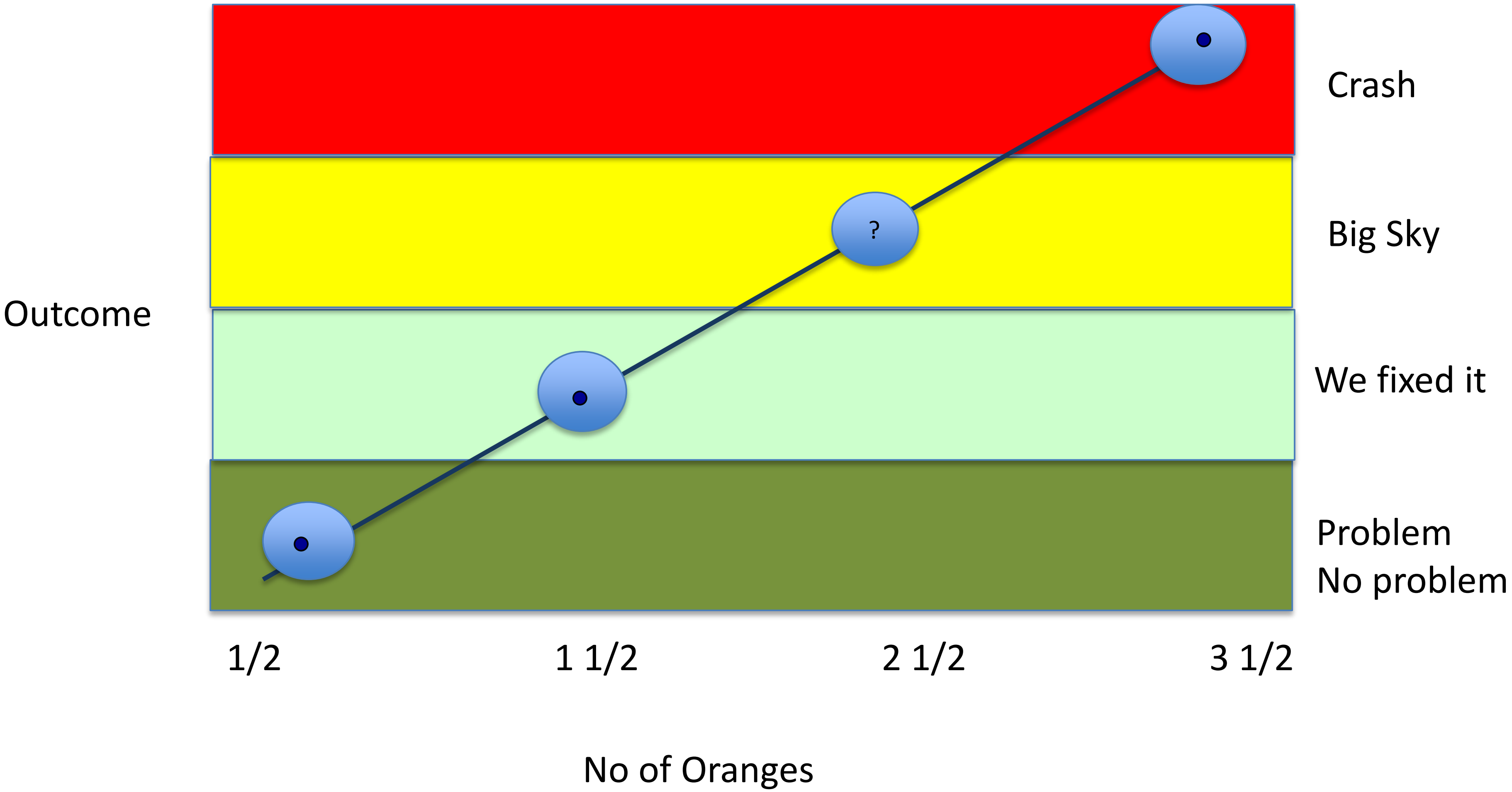
- Stephens(1996) analysed UK AAIB reports
- Found 4.4 factors per accident for aircraft > 2000 kg
- British Airways provided access to the BASIS database in Heathrow
- Analysis concentrated upon the last 12 months

Types of outcome

- There were no accidents but many incidents
  - Problem but no problem
  - Problem that we sorted eventually
  - It’s a big sky

  - Accident (AAIB)

The Rule of Three



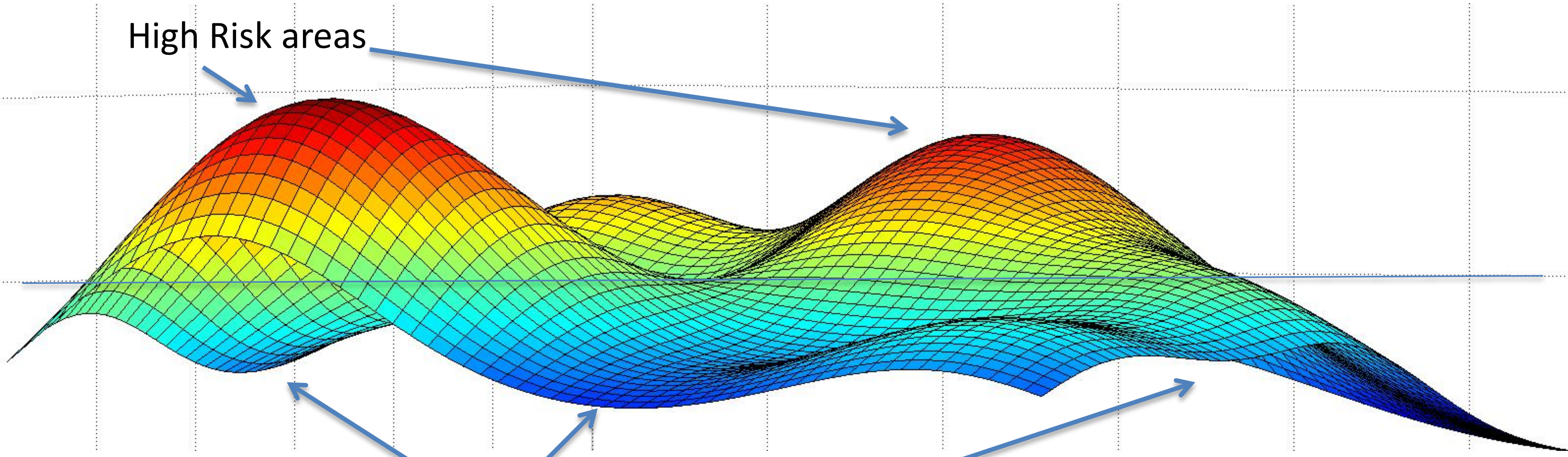
Why does the rule work?

- People use cognitive capacity to allow for increasing risk
- As the oranges increase the remaining available capacity is reduced
- At 3 oranges there is little available capacity remaining
- Any trigger can de-stabilize the system
- An accident suddenly becomes very likely
- This sensitivity exists for any combination over dimensions
    - NOT Human plus 2 other dimensions

So what does this mean for risk?

- What about triggers?

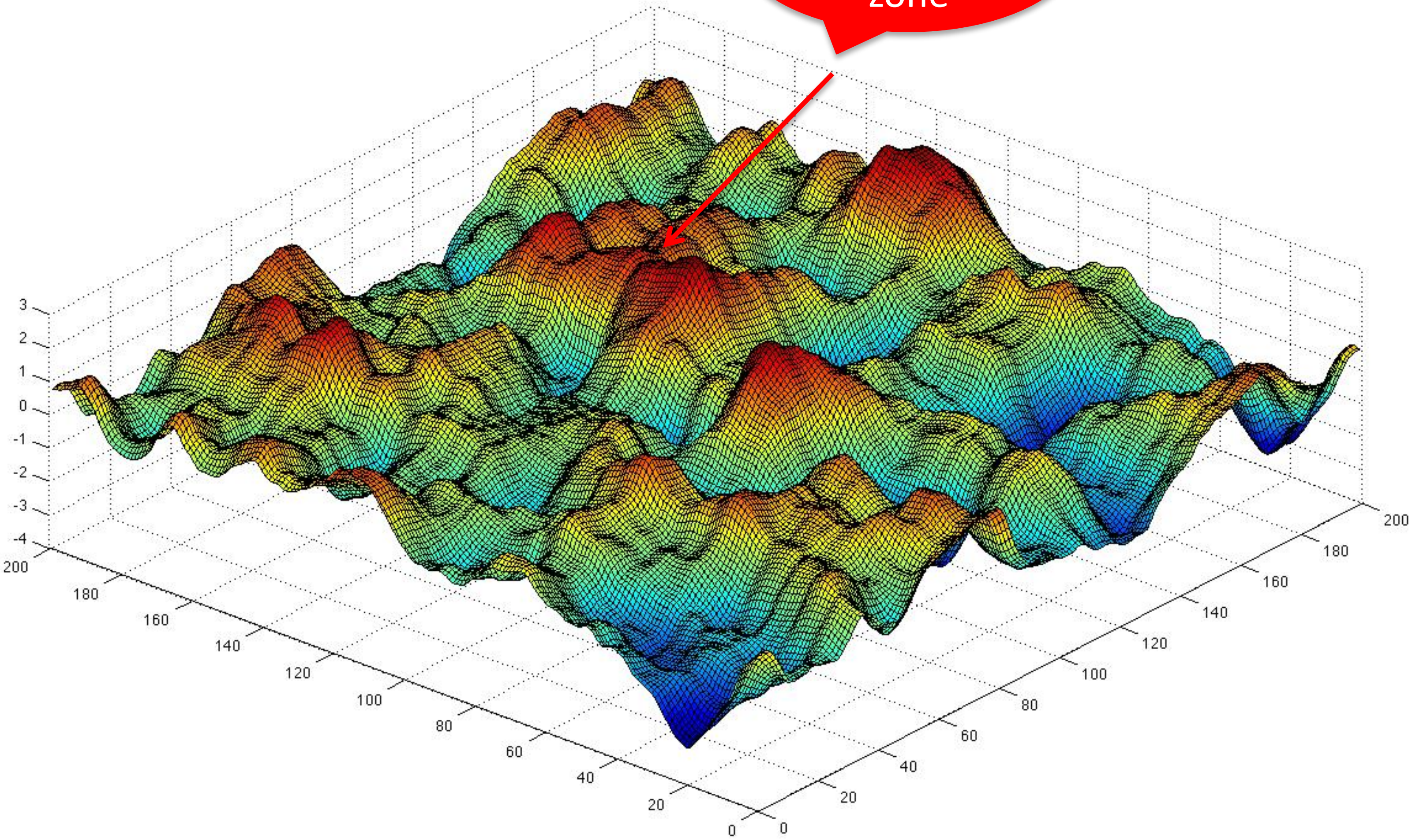
Risk Space



High Risk areas

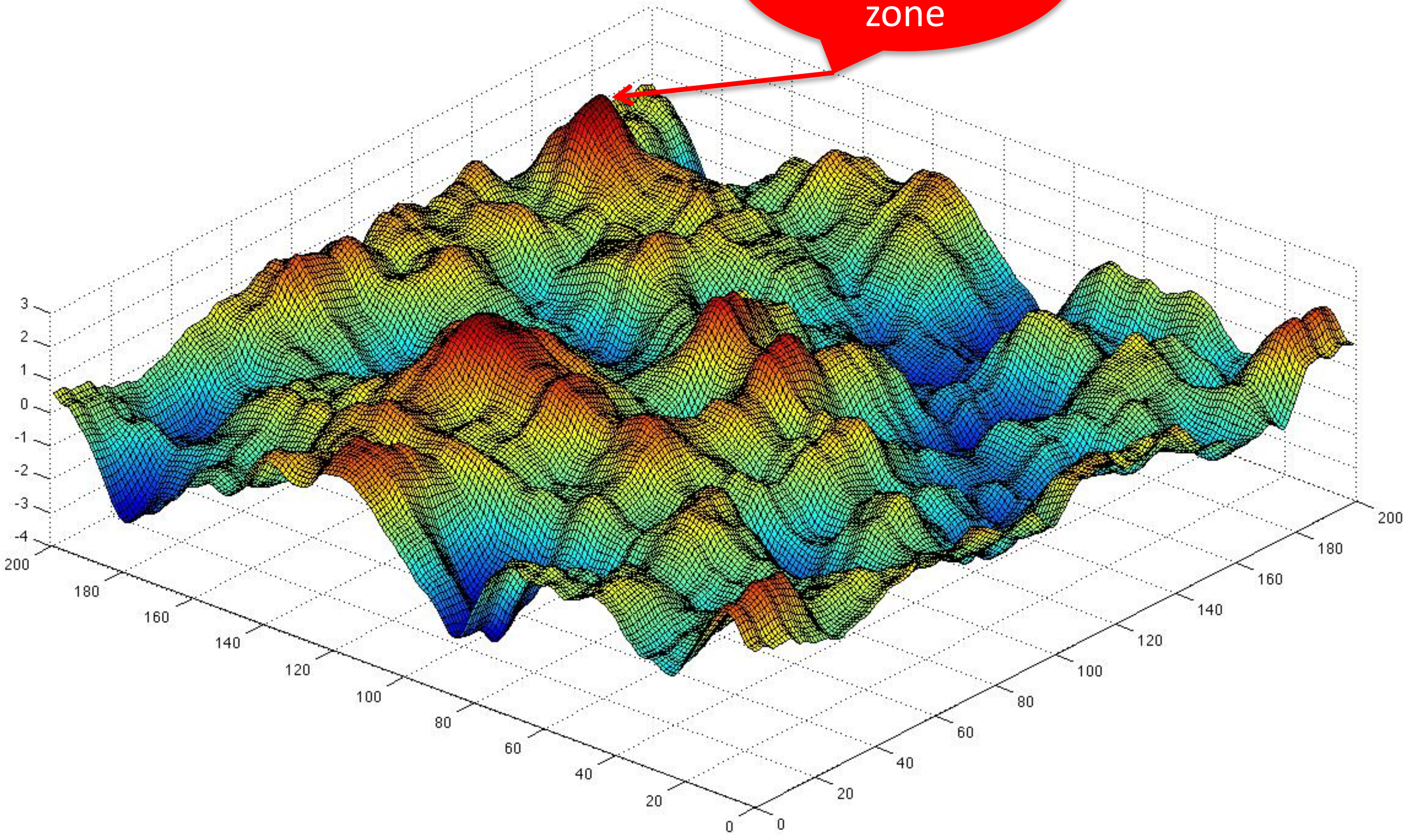
Low risk/resilient areas

Single distribution A



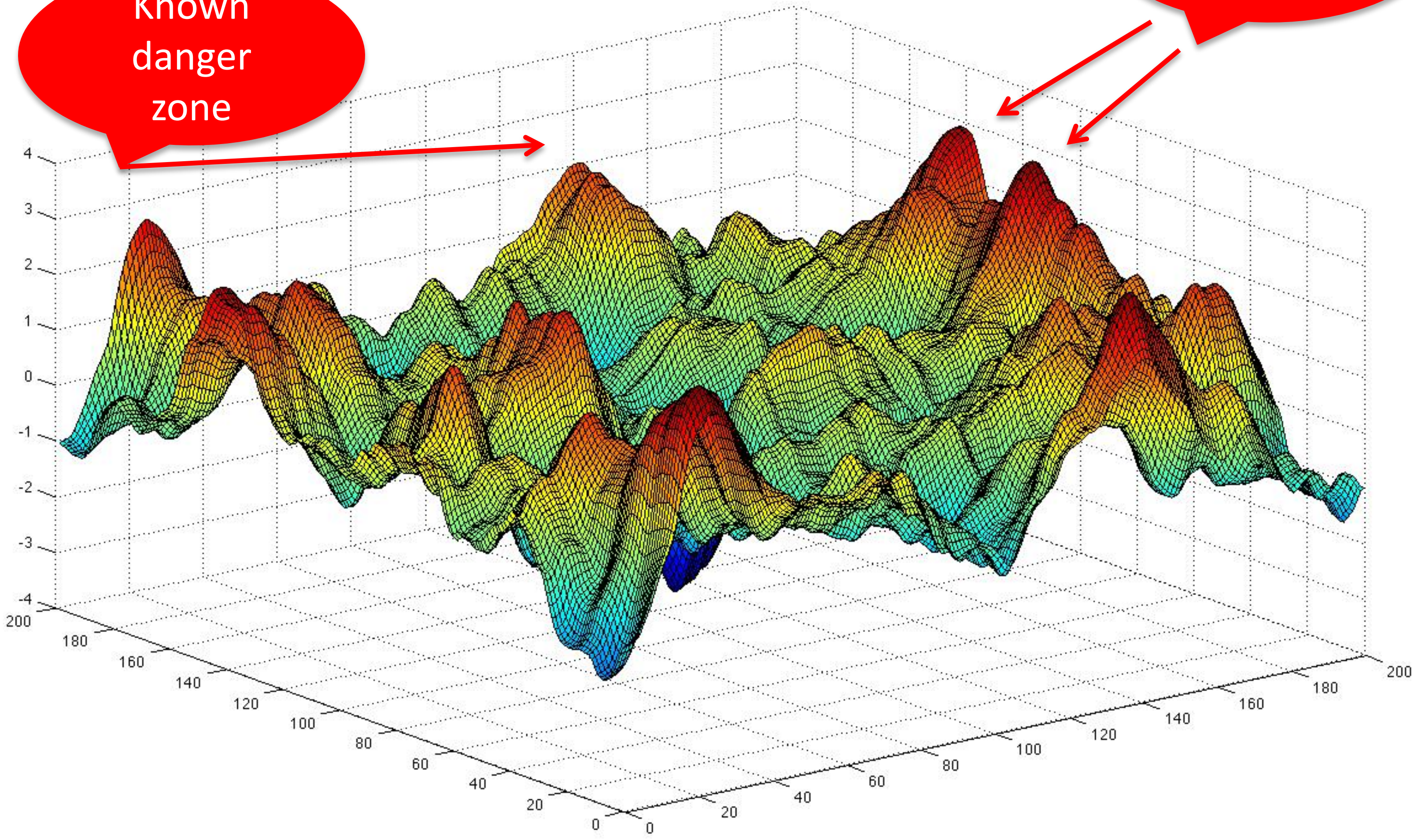
Known danger zone

Single distribution B



Known danger zone

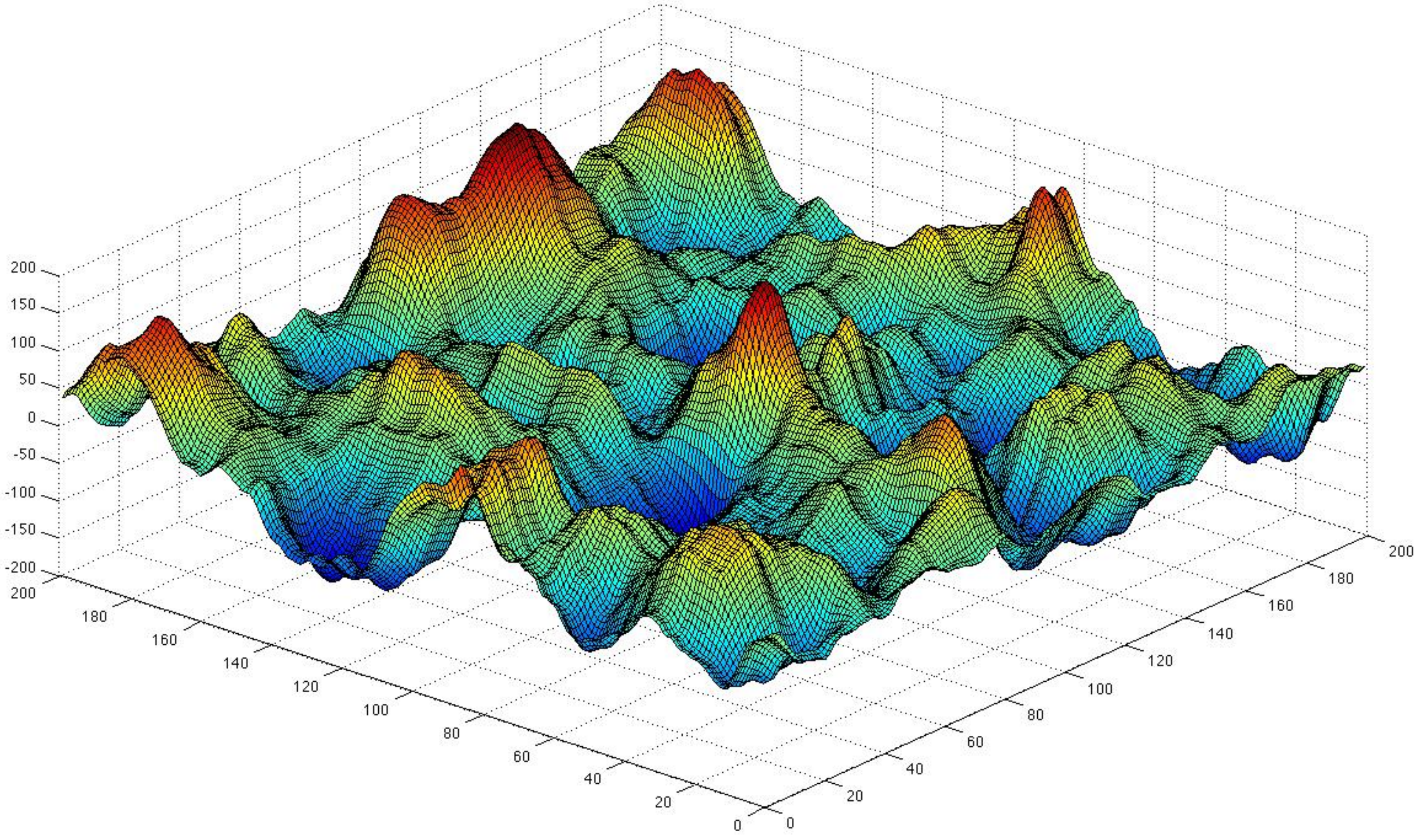
Single distribution C



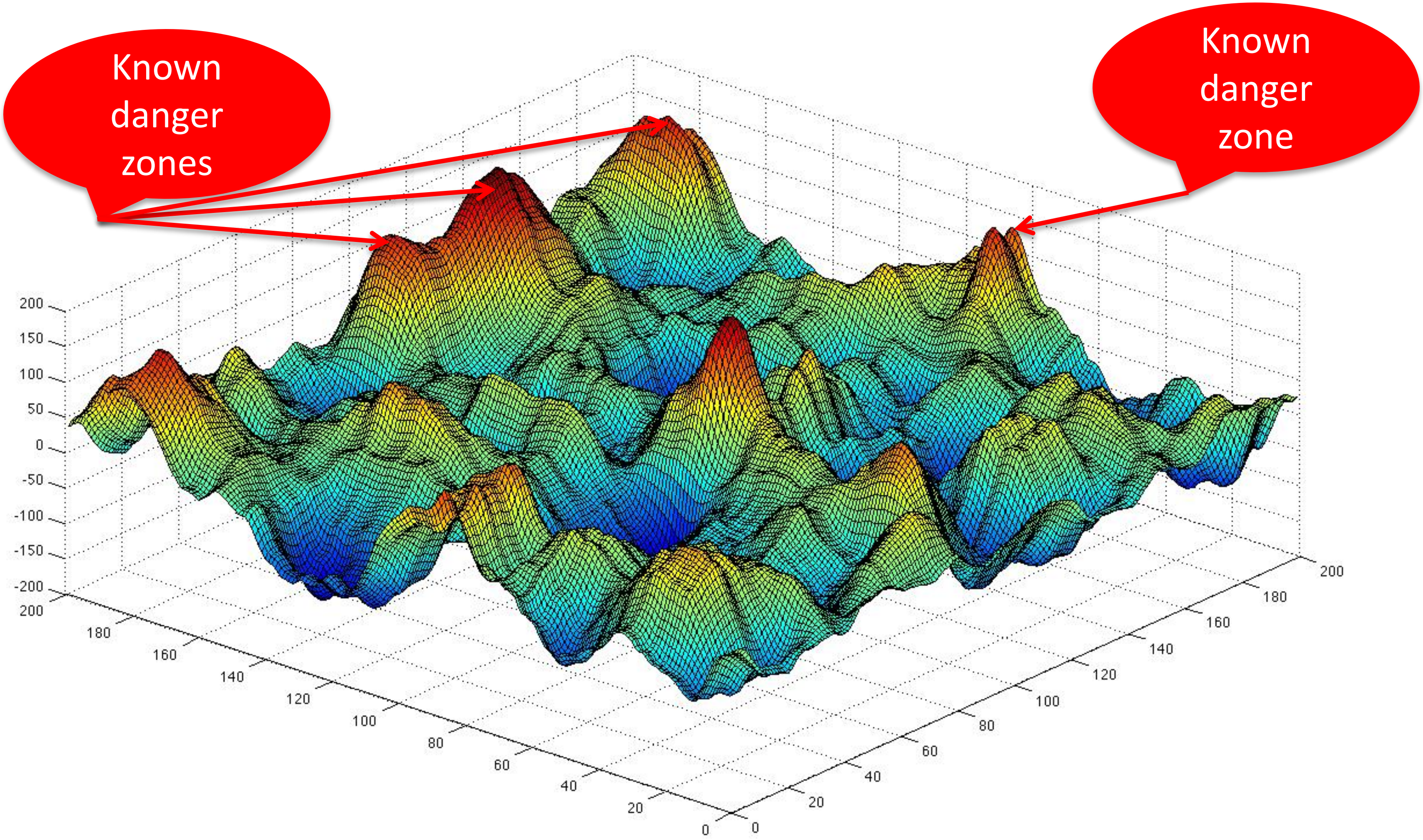
Known danger zone

Known danger zones

Combined distribution (A,B,C)



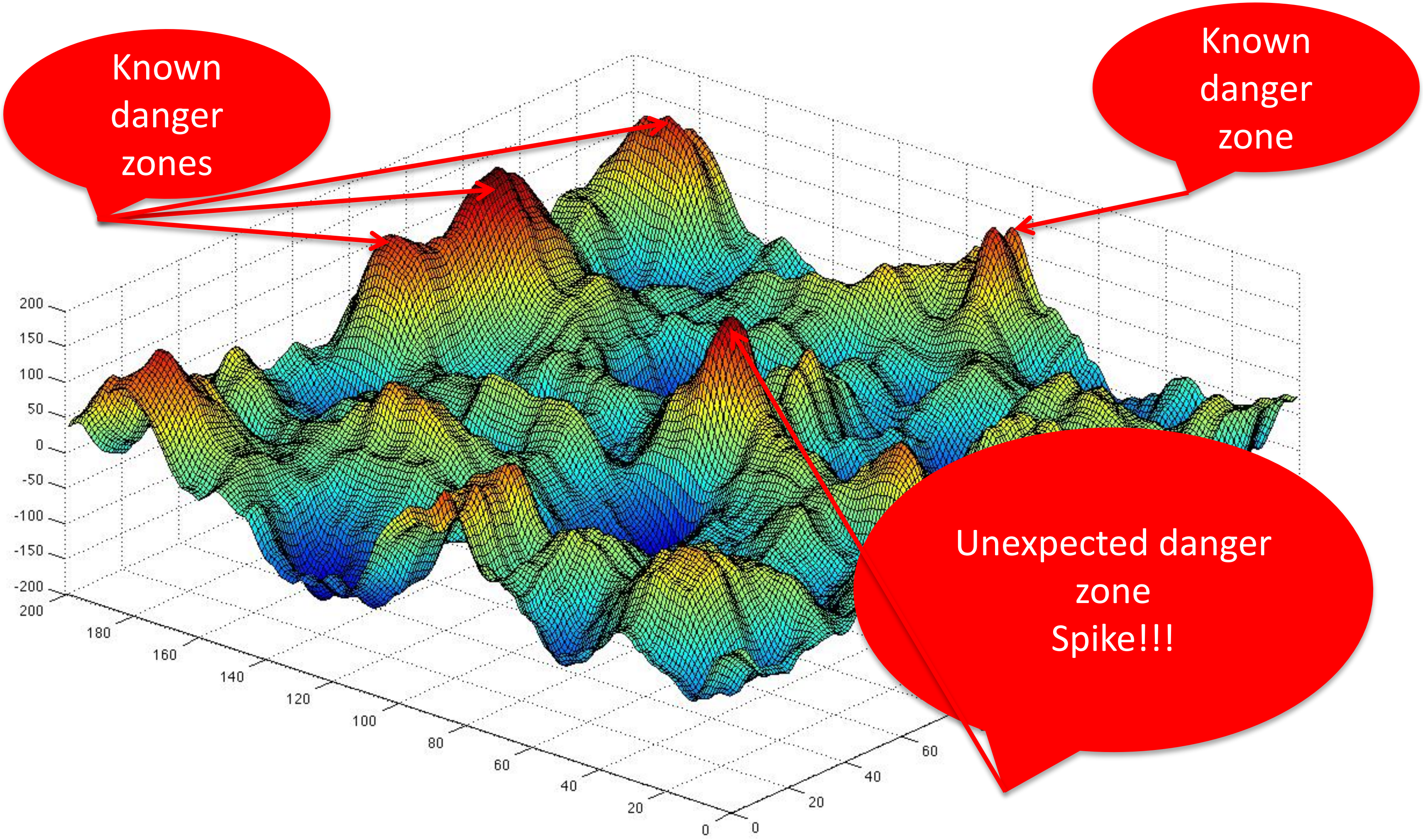
Combined distribution (A,B,C)



Known danger zones

Known danger zone

Combined distribution (A,B,C)



Known danger zones

Known danger zone

Unexpected danger zone
Spike!!!

So what is Safety?

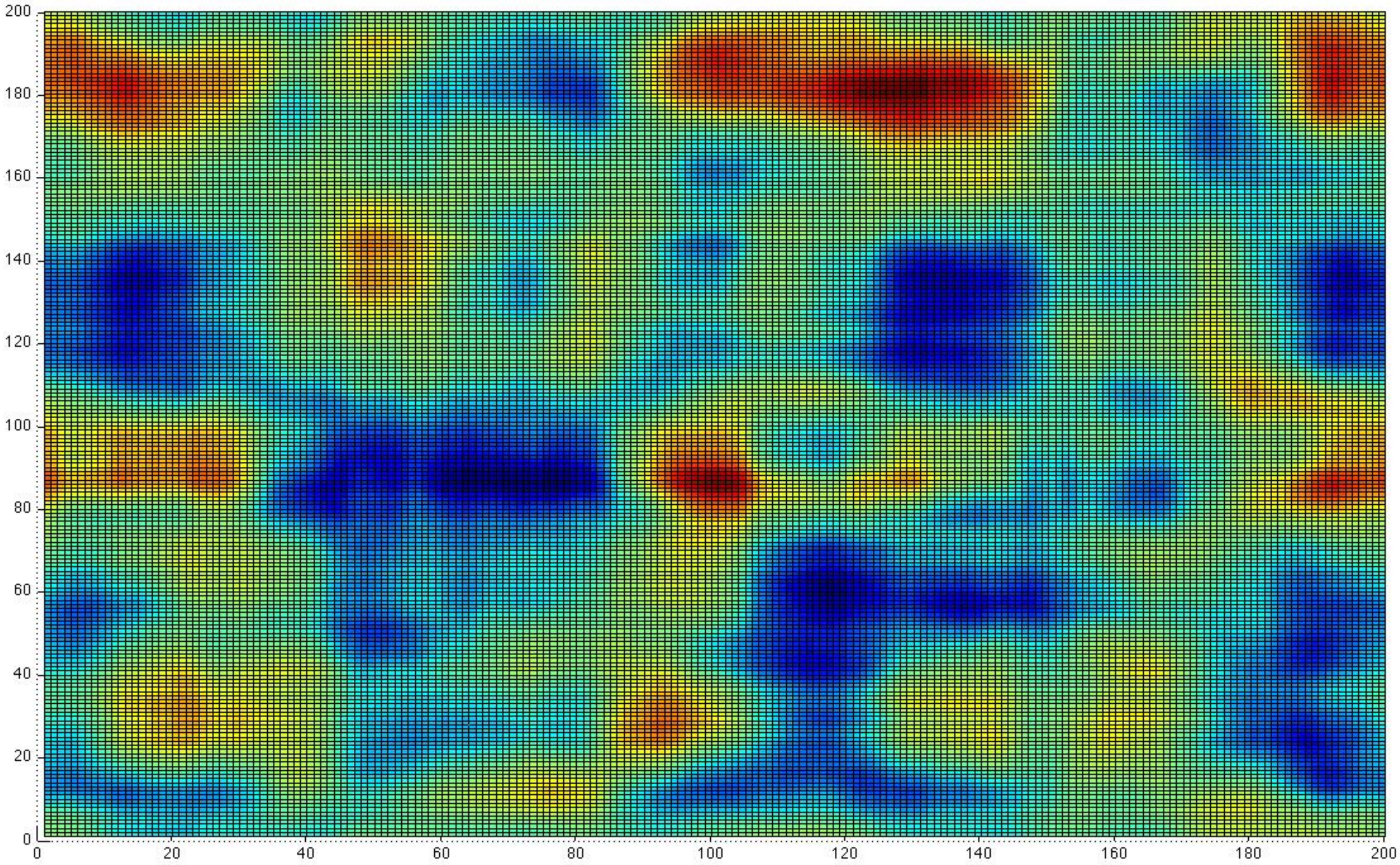
- Safety is usually defined as “not having accidents”
- This definition is being heavily criticized
- Resilience is the distance to the ceiling in risk space
  - It takes a small trigger event to make a disaster if resilience is low
  - But, with high resilience a big enough trigger can still lead to disaster
- The more resilient you are, the safer you are
- Safety is now defined as the integral of resilience over the total risk space

Safety as an integral in risk space

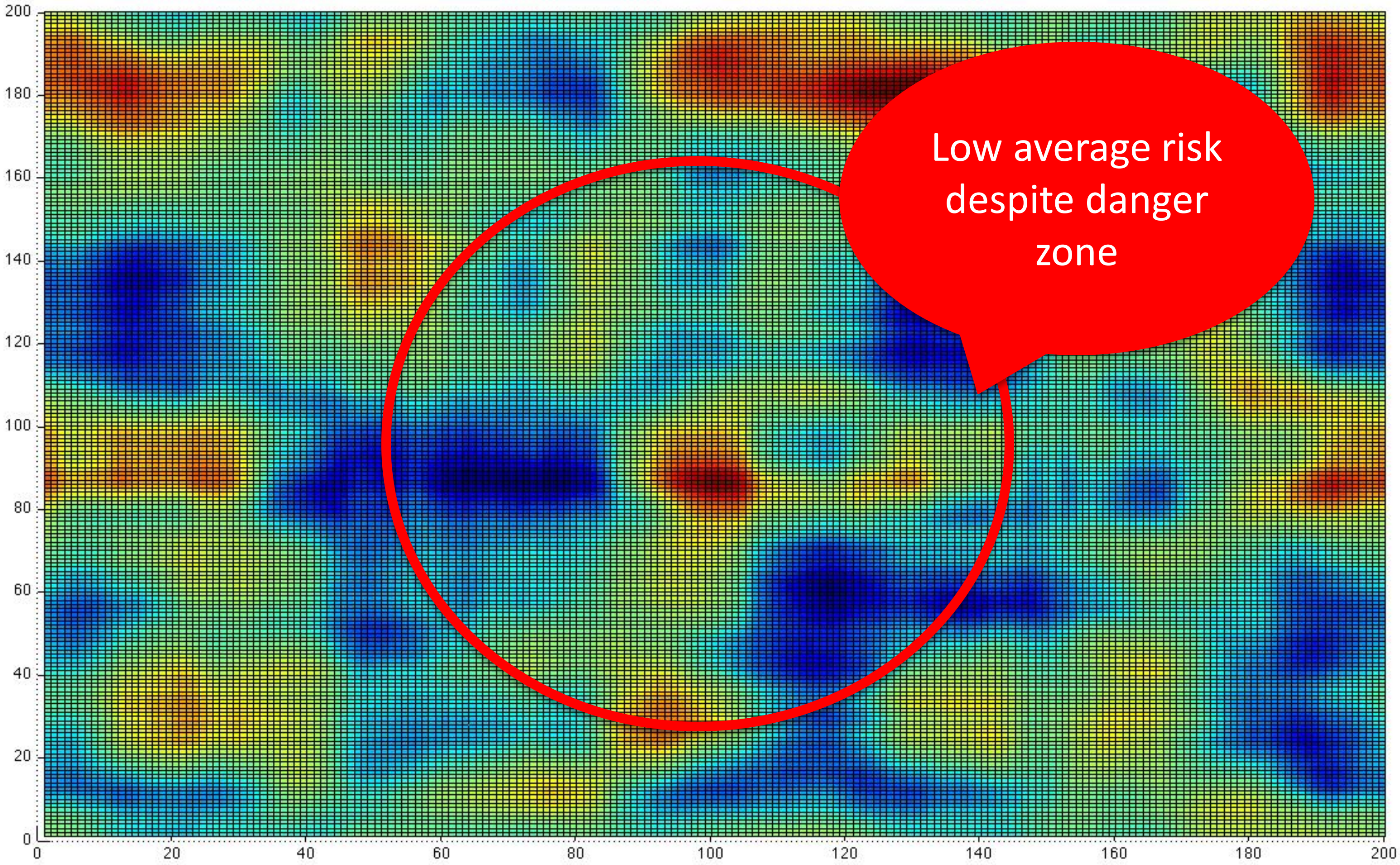
$$\text{Safety} = \int_{ops\ boundary\ a}^{ops\ boundary\ b} resilience\ d1 \ldots dm$$

For m = 1 through n

Simple view of combined distribution

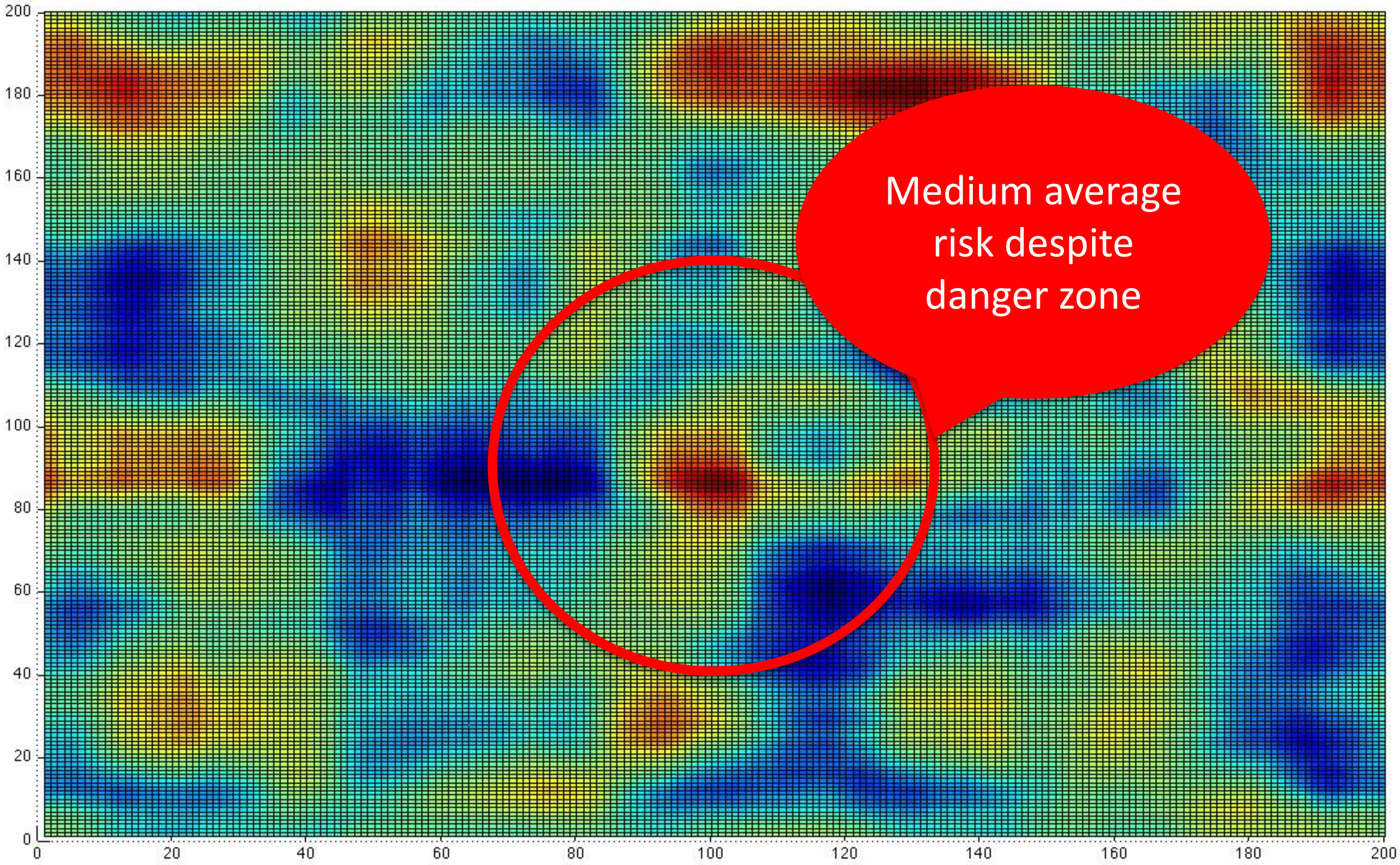


Simple view of combined distribution



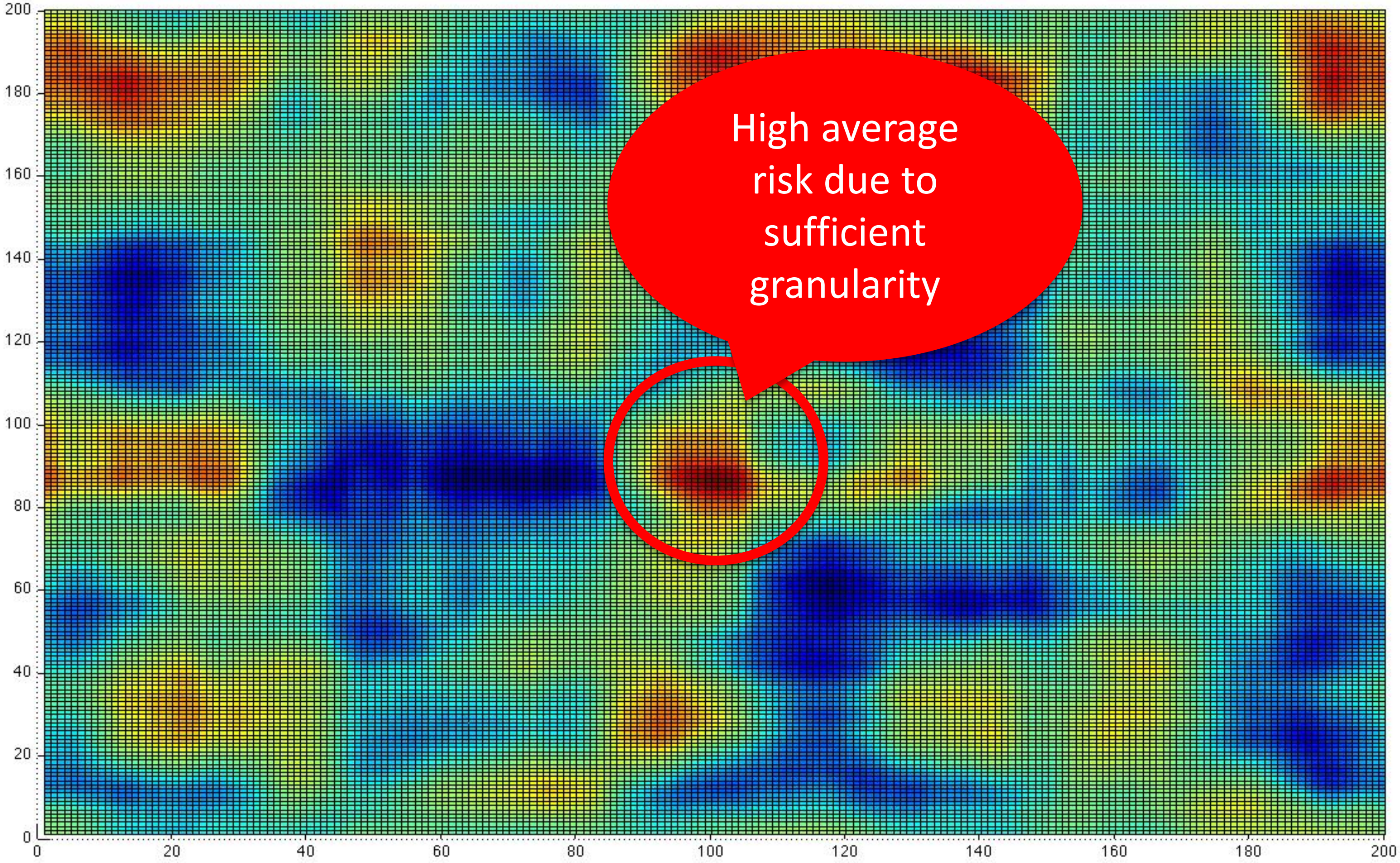
Low average risk despite danger zone

Simple view of combined distribution



Medium average risk despite danger zone

Simple view of combined distribution



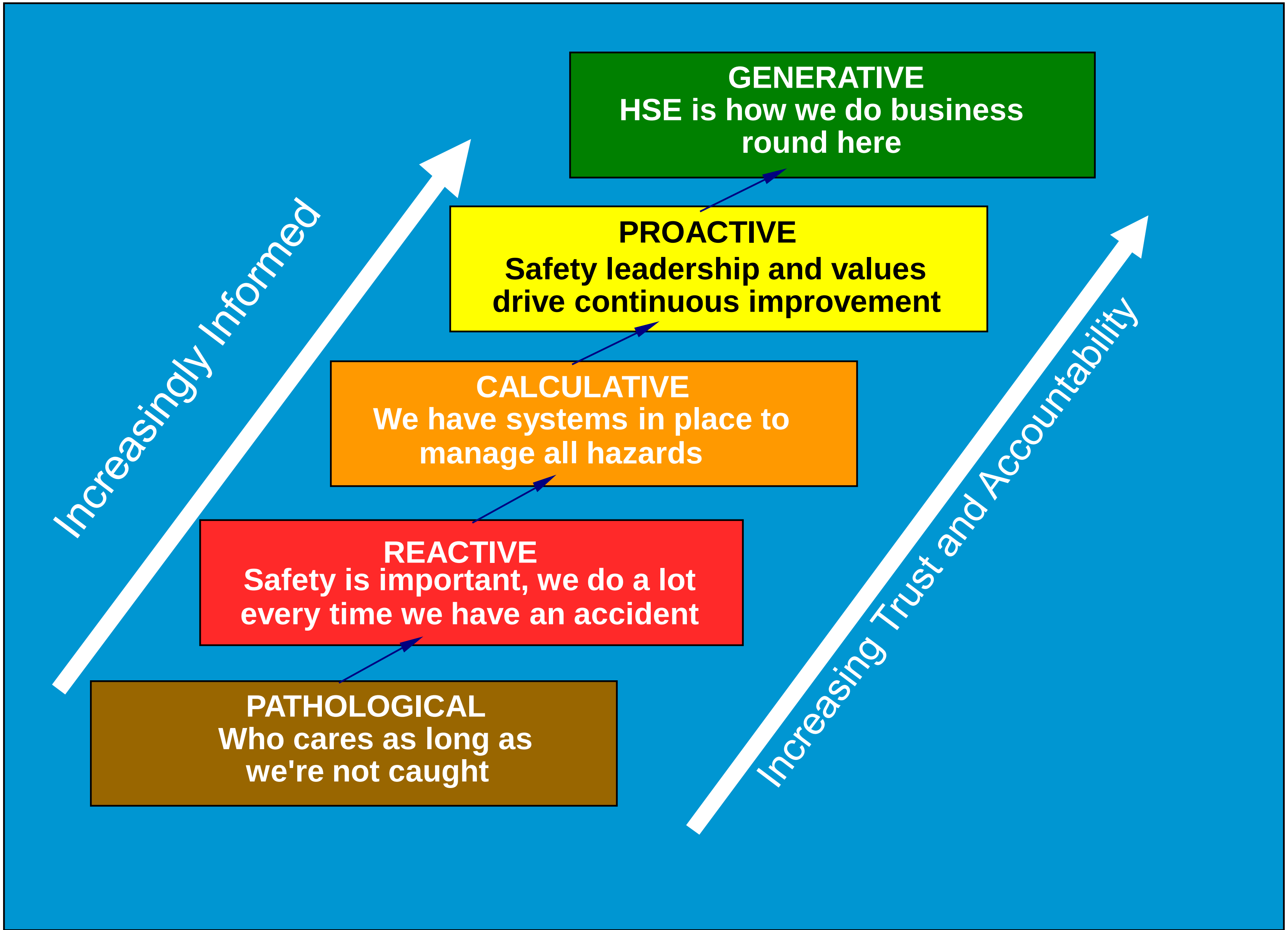
High average risk due to sufficient granularity

Safety
Safety Culture and
Risk Understanding

- Safety is now about how individuals and organisations understand and handle risks

- Different stages on the safety culture ladder may be the result of changes in granularity plus different organizational cultures that can cope with increasing sophistication

The Safety Culture Ladder



GENERATIVE
HSE is how we do business round here

PROACTIVE
Safety leadership and values drive continuous improvement

CALCULATIVE
We have systems in place to manage all hazards

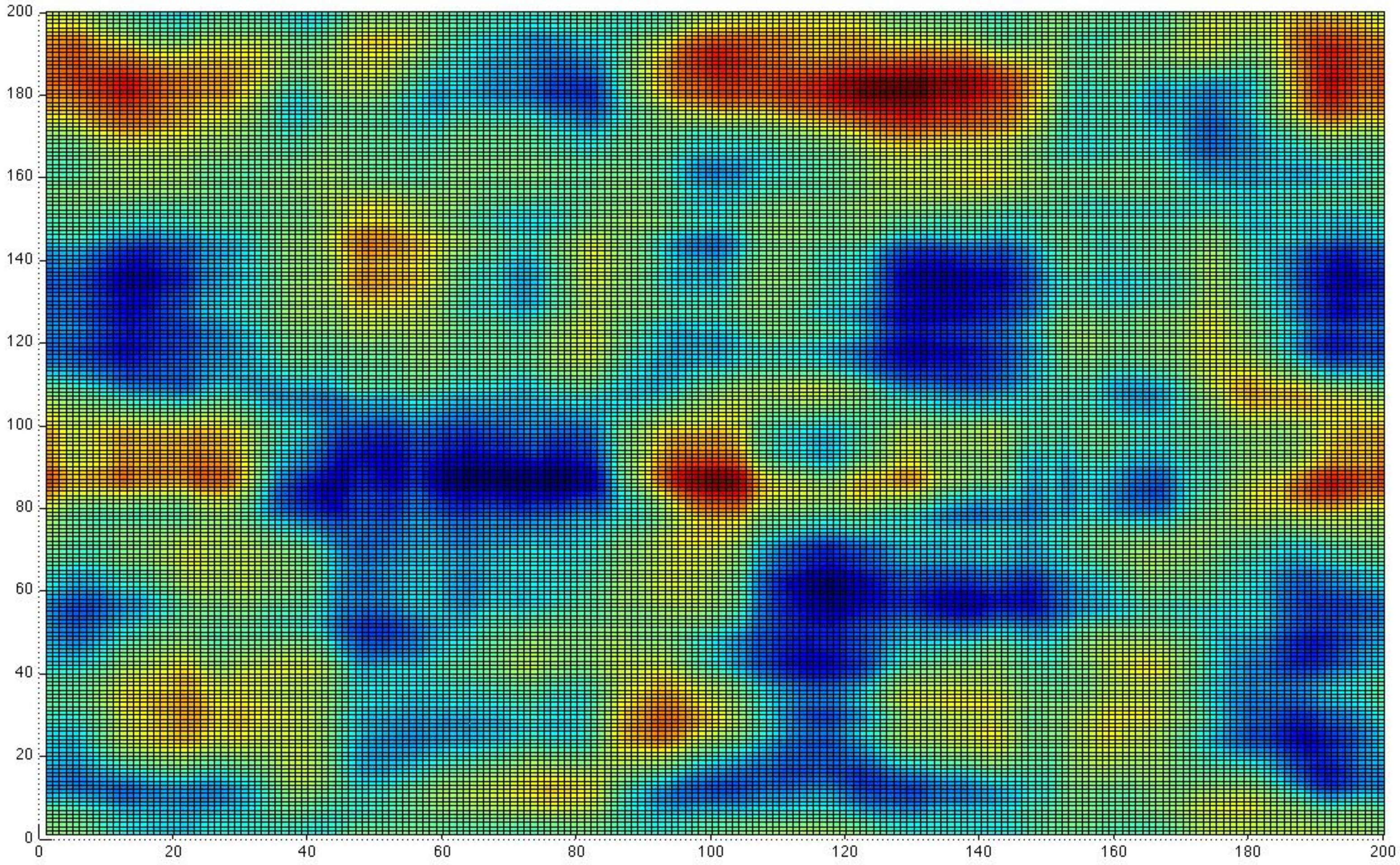
REACTIVE
Safety is important, we do a lot every time we have an accident

PATHOLOGICAL
Who cares as long as we're not caught

Risk understanding

- In the pathological, risks and the management of them are seen as external responsibilities.
  - This means that there are no internal structures for dealing with it.

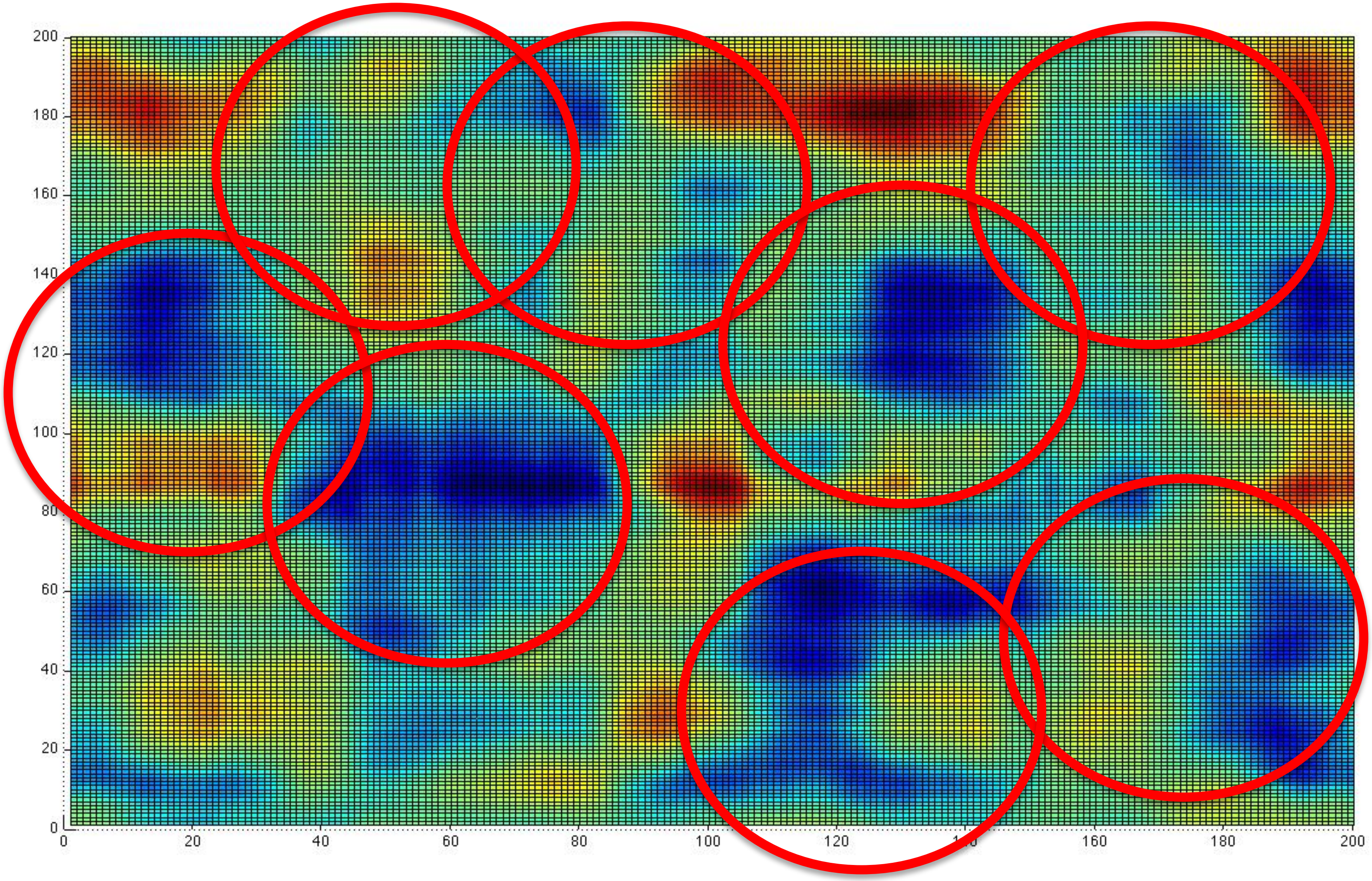
Simple view of combined distribution



Risk understanding

- The reactive organisation gains understanding from the risks it has suffered.
  - The willingness to learn from these means that there is organisational understanding of those risks, but not the risks that haven’t happened yet.
  - The risk understanding flows to the core of the organisation in a haphazard manner

Reactive behavior within N-dimensional risk space

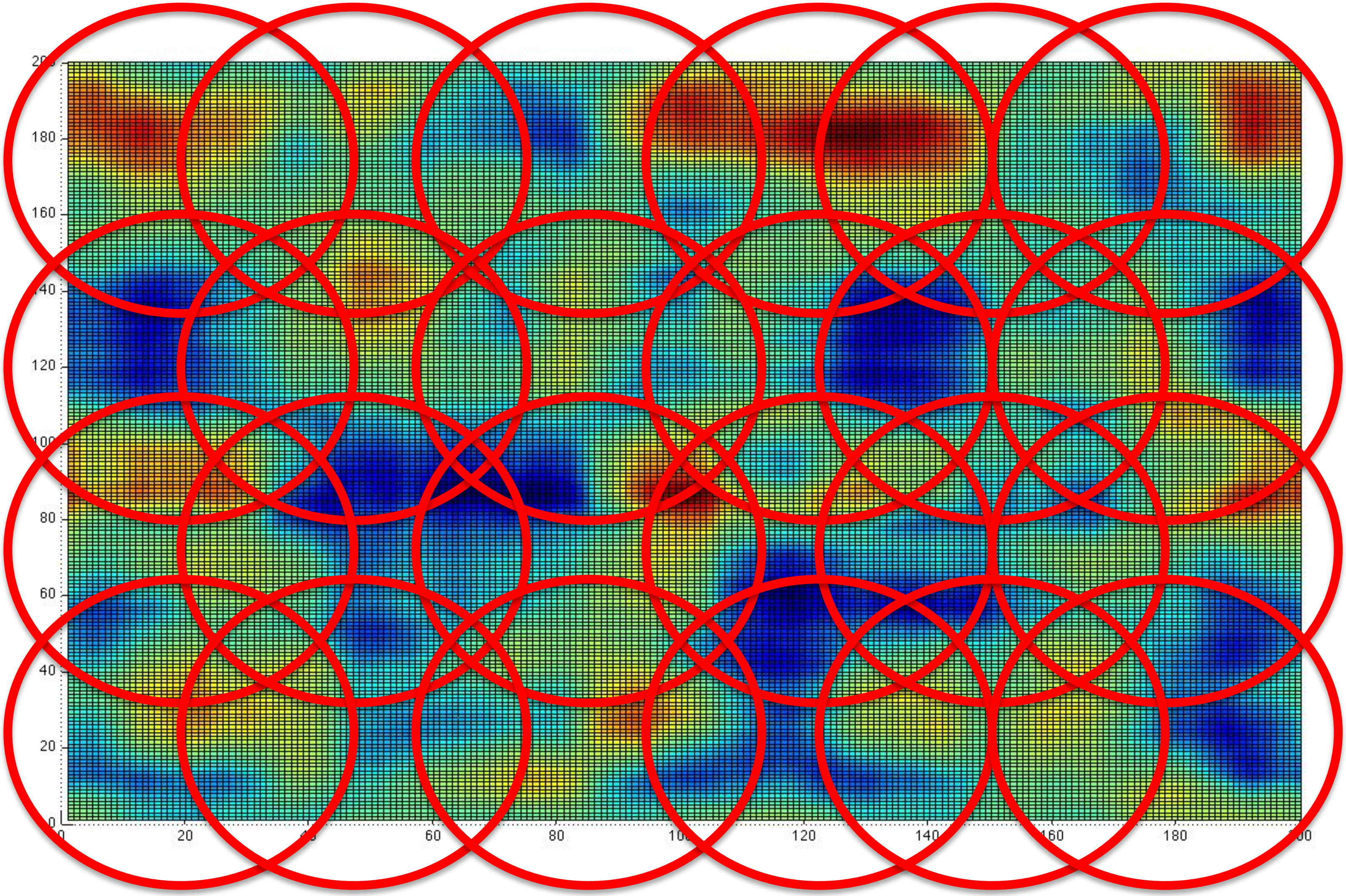


Risk understanding

- The Calculative organisation realises that their exposure also includes incidents that haven’t occurred yet.
- There is a formal process for exploring the risk space.

  – The formal movement of risk understanding to the organisational core allows for the creation of more powerful risk management tools

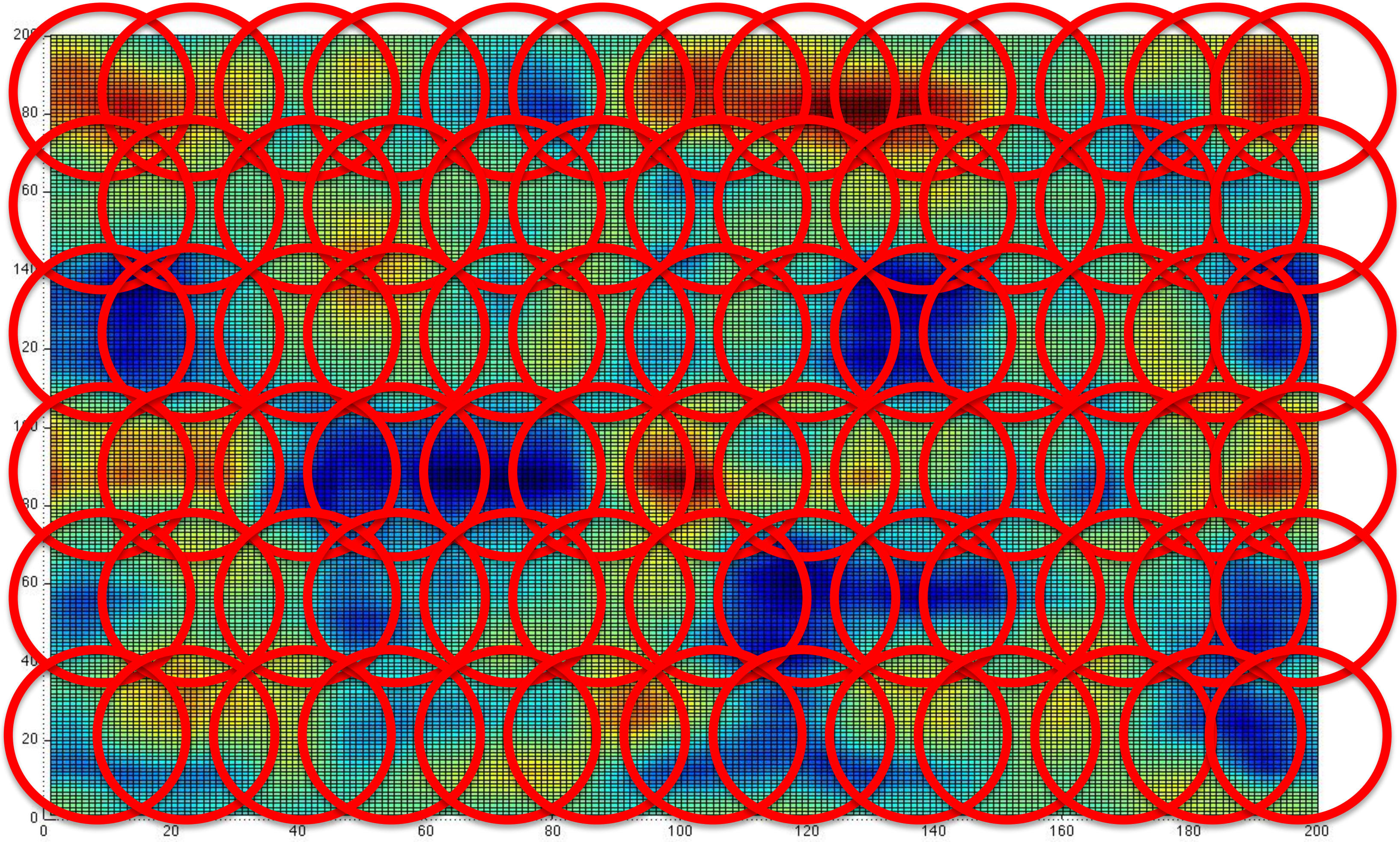
Systematic (calculative) behavior within N-dimensional risk space



Risk understanding

- The proactive organisation realises that the tools built in the calculative are more effective if placed in the hands of those actually dealing with the risks.
- This means that while there is still formal exploration of the risk space this is conducted by those on the front lines. This allows for a much finer understanding of the risks space.
- The flow of risks understanding is now in two directions, with the knowledge and understanding gained in the calculative step being effectively combined with local conditions.

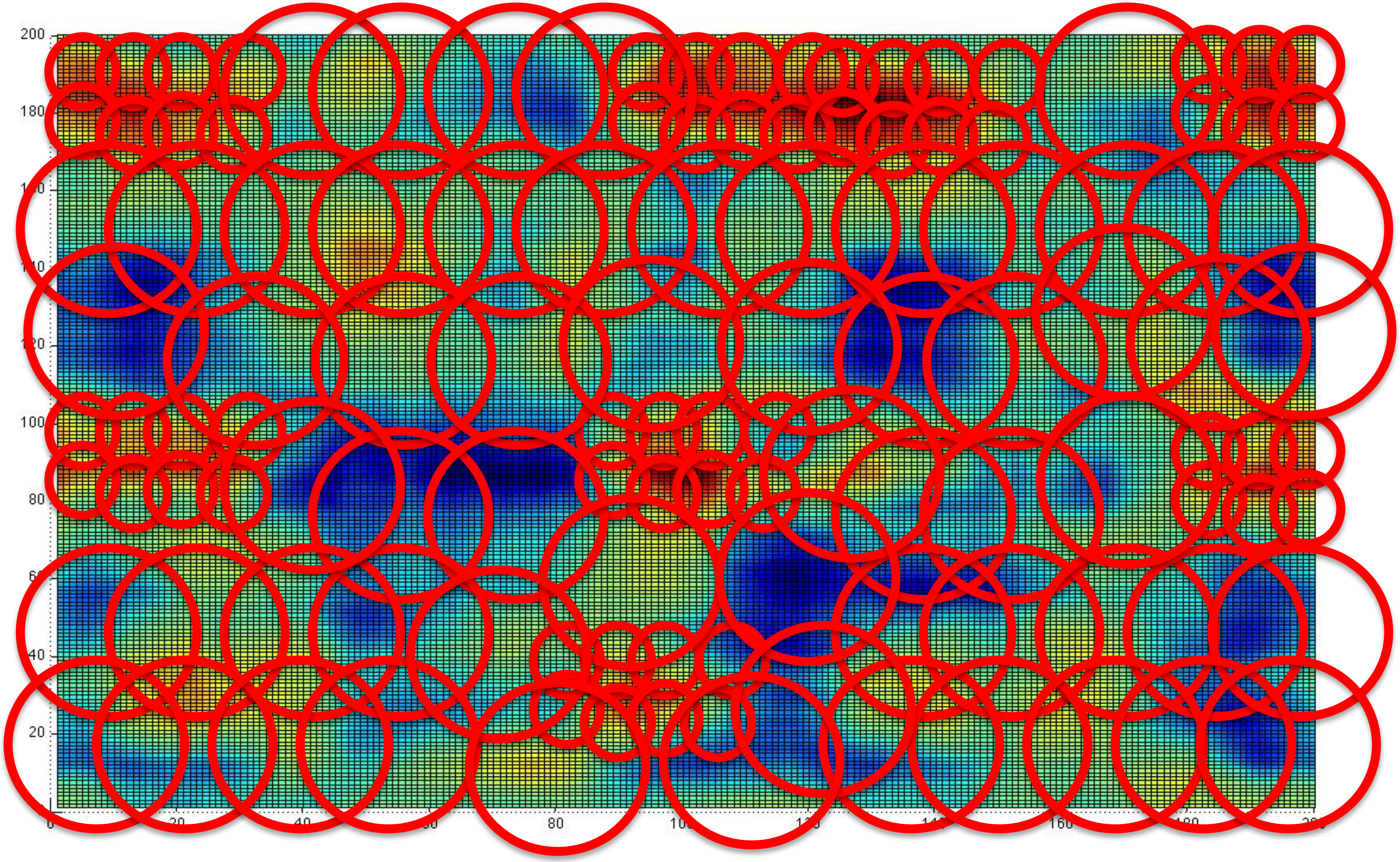
Systematic behavior within N-dimensional risk space with risk understanding pushed down to workforce level (Proactive)



Risk understanding

- The Generative organisation lives and breathes risk understanding.
- The flow of understanding is multi-dimensional. Due to the strength of relationships there no longer is a formal structure powering the flow. (This is one of the pitfalls of the Generative).
- The flexibility to move around the risk space afforded by the comprehensive understanding of the risks means marginal propositions can still be profitable due to the reduction in exposure.

Systematic behavior within N-dimensional risk space with risk understanding pushed down to workforce level with improved focus on high risk areas (generative)

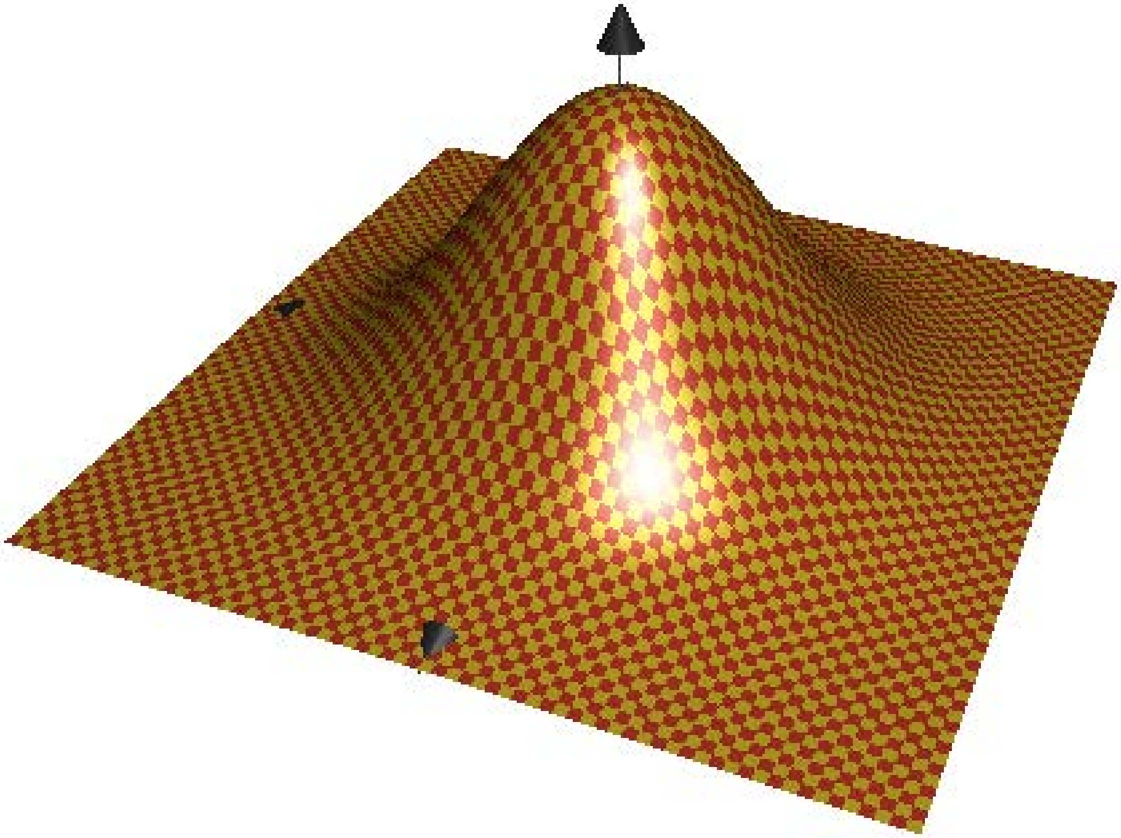


Possibility Space

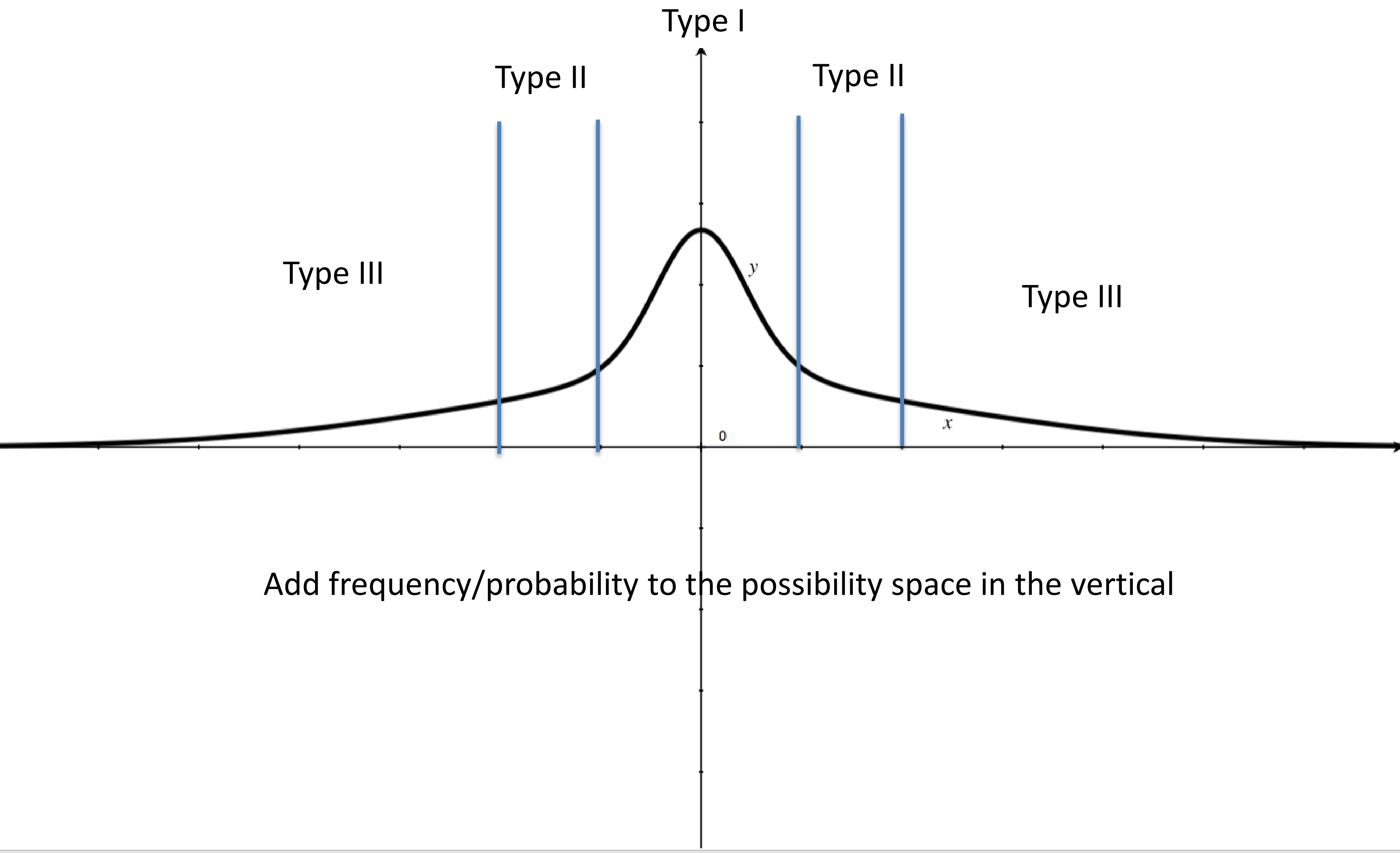
- An aggregated representation of the frequency of possibilities for an outcome level
- Adds in specific consequences to initial risk space
- These are the possible consequences of specific scenarios

- “How often would this scenario occur if there was no risk management?”
- Then we can ask what risk management adds
  - In this example it is only high consequence outcomes
  - but they generalize over outcomes

Scenarios in 3 dimensions

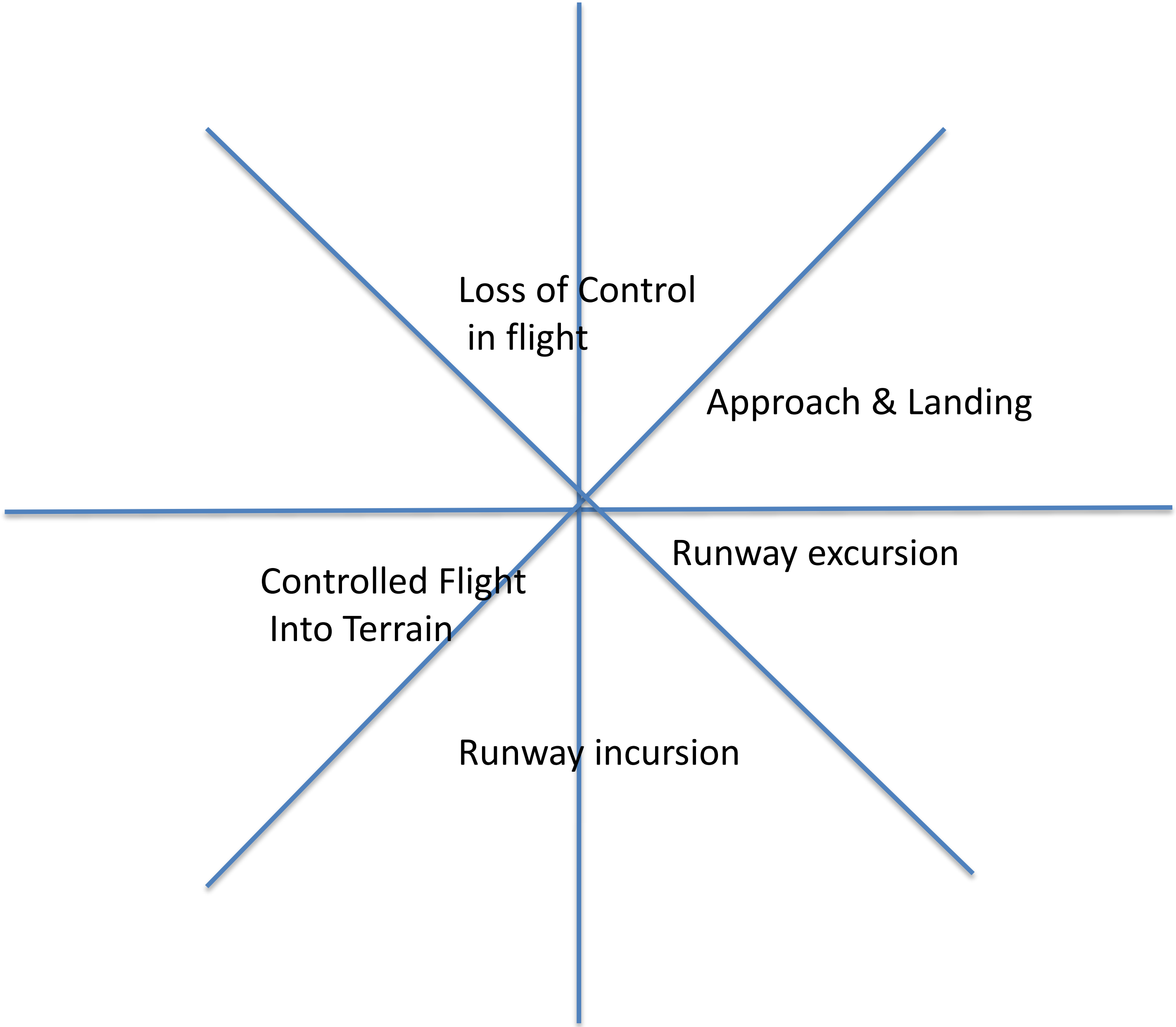


Each tile represents a possible scenario



Add frequency/probability to the possibility space in the vertical

Possibility space for aviation



Loss of Control in flight

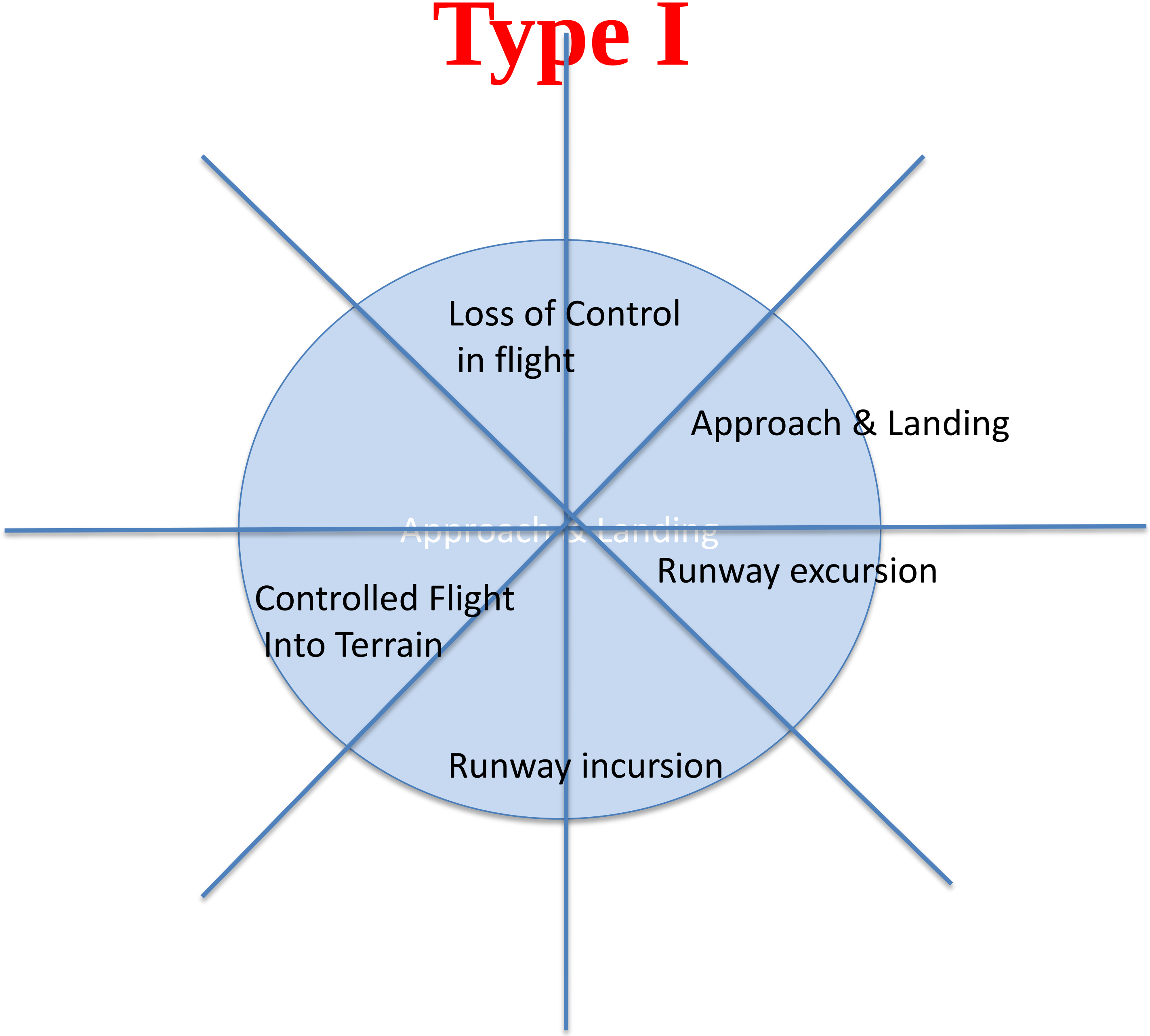
Approach & Landing

Runway excursion

Controlled Flight Into Terrain

Runway incursion

Type I



Loss of Control in flight

Approach & Landing

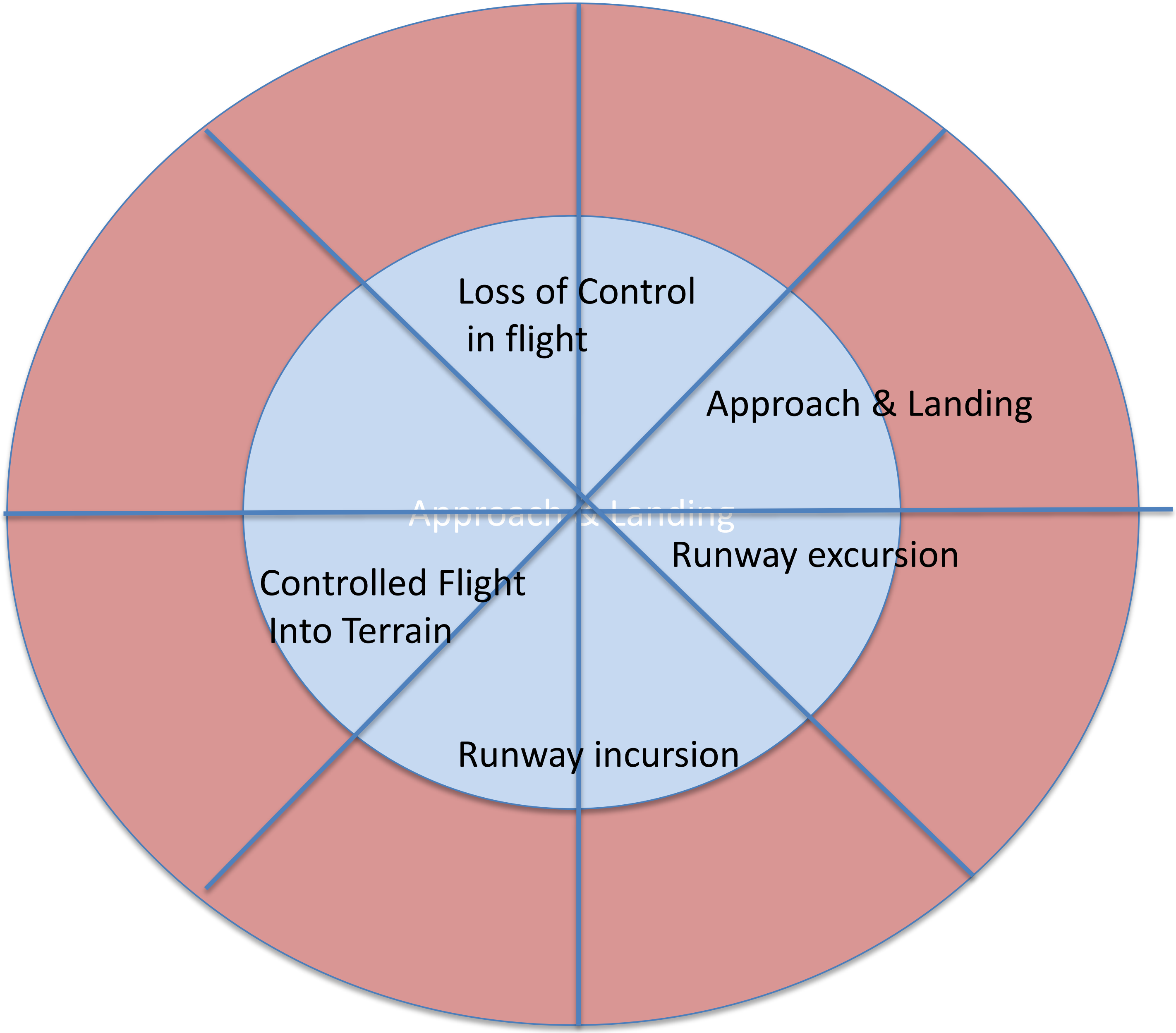
Approach & Landing

Runway excursion

Controlled Flight Into Terrain

Runway incursion

Type II



Loss of Control in flight

Approach & Landing

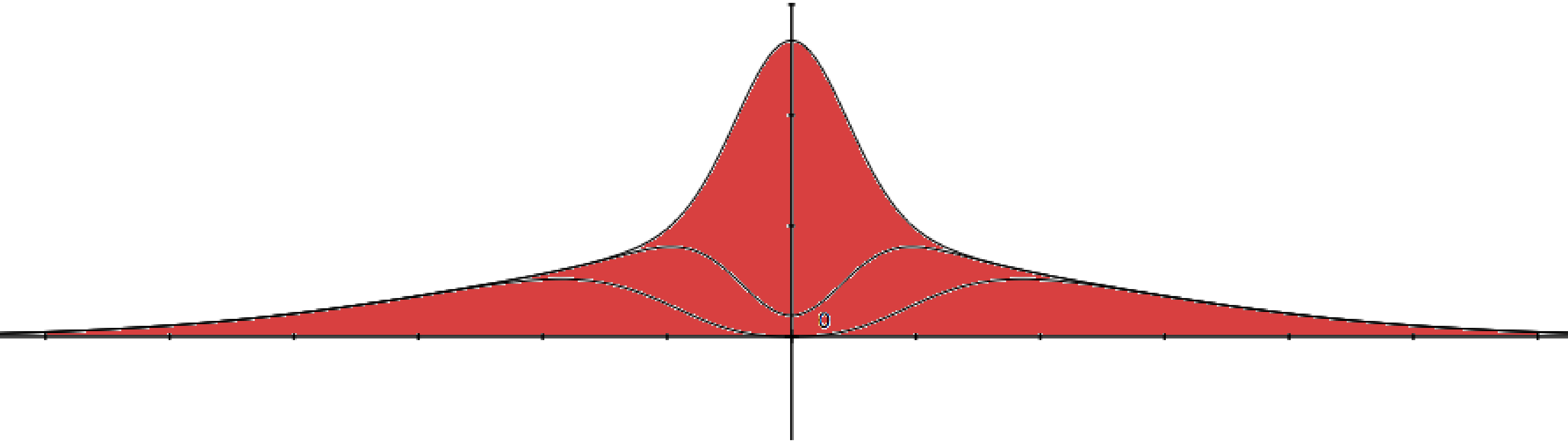
Approach & Landing

Runway excursion

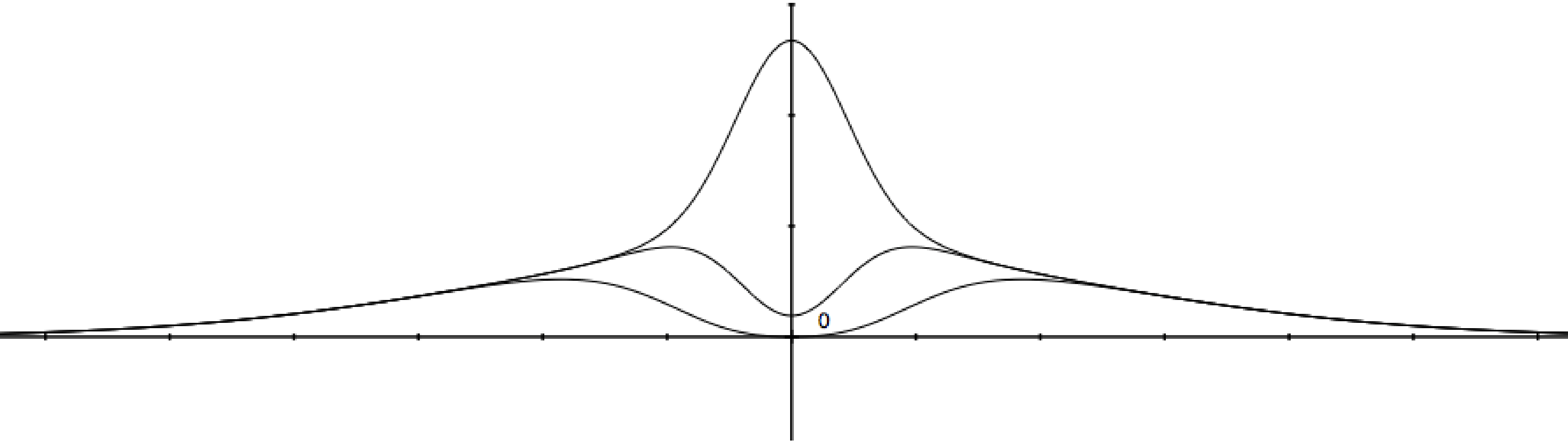
Controlled Flight Into Terrain

Runway incursion

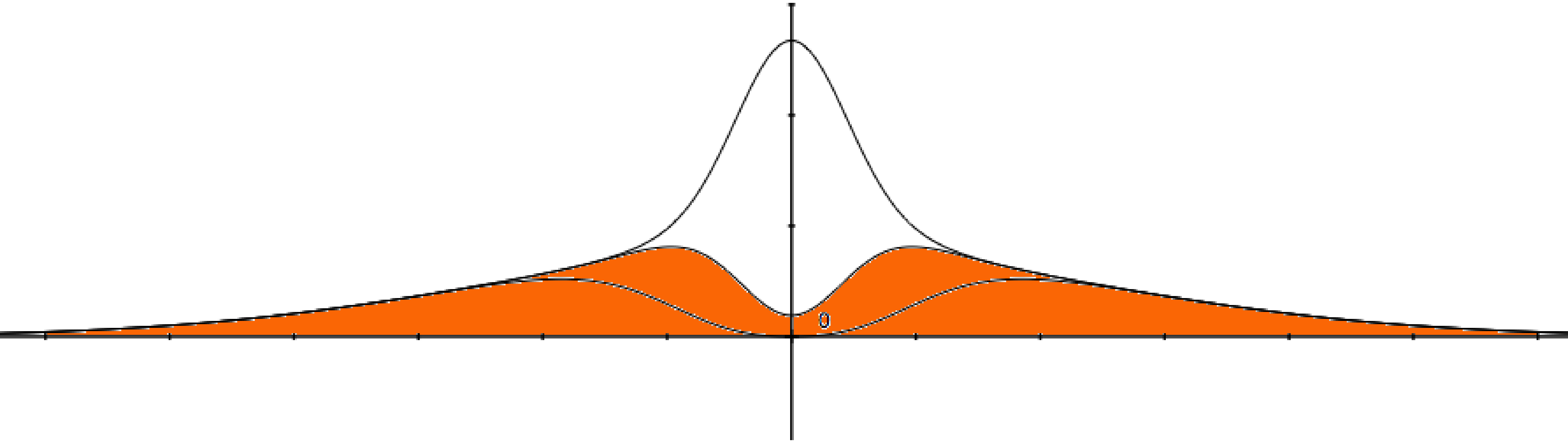
Possibility Space
Unmanaged



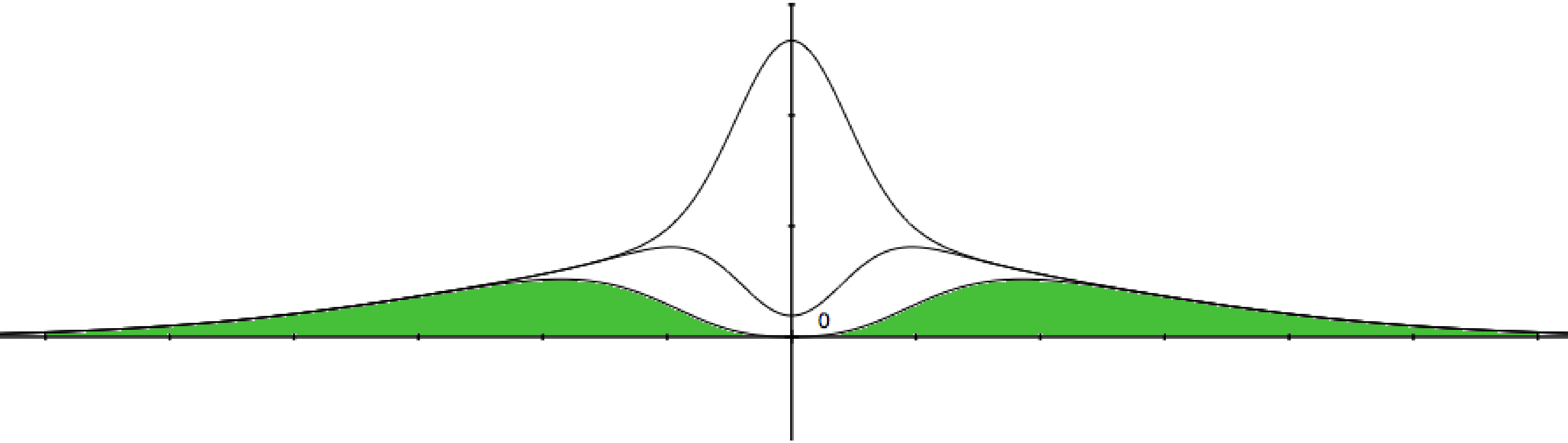
Possibility Space Managed



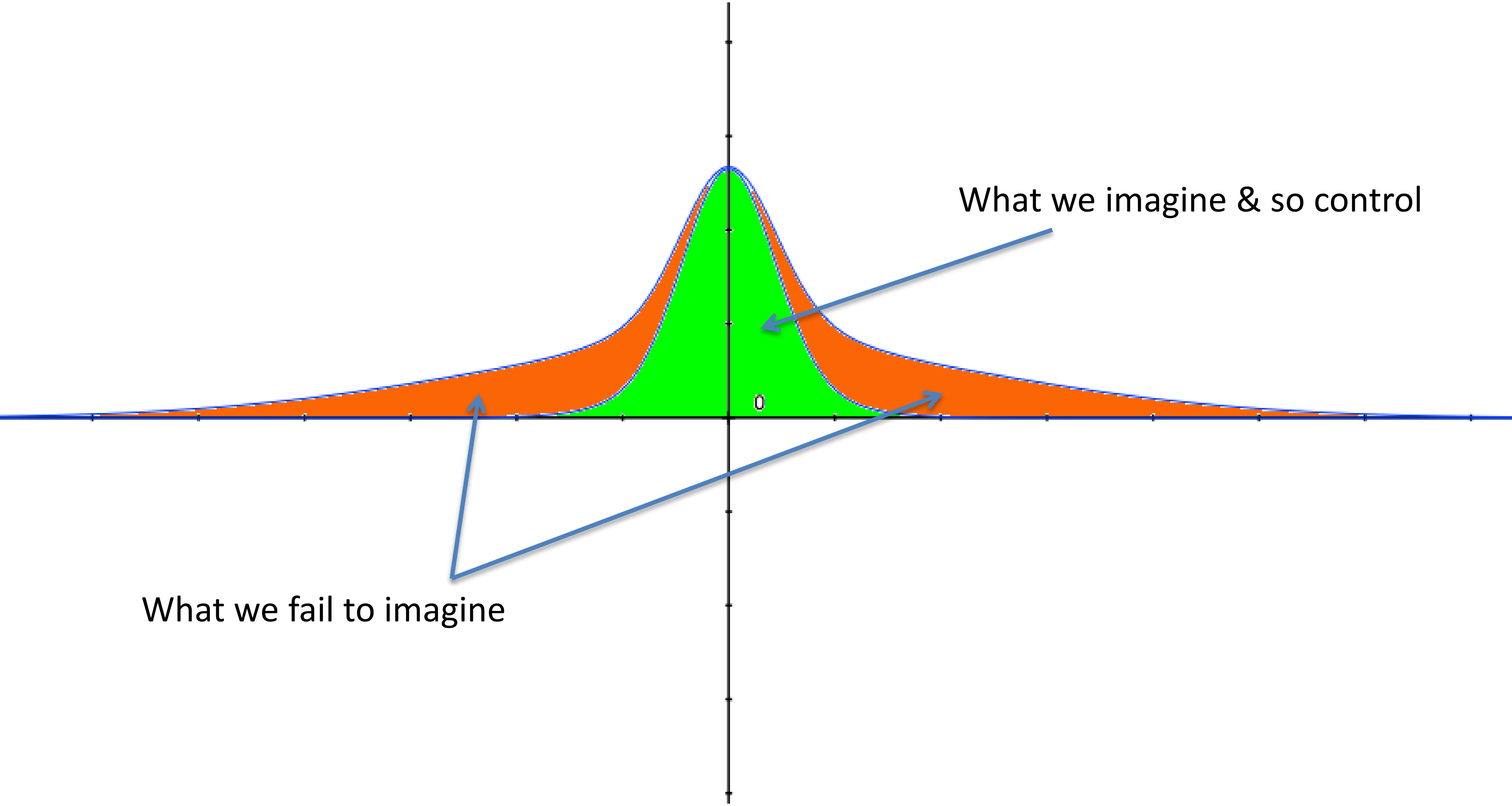
Possibility Space
Type I only managed



Possibility Space
Types I and II managed



The imagination gap



What we imagine & so control

What we fail to imagine

Who has control over the types of accident?

- Type I is direct and places responsibility on the individual’s span of control
  - Individuals control what is directly in their line of fire
- Type II requires the organisation – line management – to ensure conditions are safely managed because they can control them
  - Management controls the conditions under which we work
  - Management has less control over individuals
- Type III involves weird combinations that are only within the span of control of top management
  - Senior management sets the goals and standards for work
  - What work we do and how it gets done

Conclusion

- The three types can be related to those who can influence them
  - Type I - individuals
  - Type II – line management
  - Type III – senior management
- All possible incidents are type III, the rest are approximations
- The most obvious type I are well understood
- Imagination-limited incidents require more proactive approaches to prevention

Conclusion II

- Safety is a multi-dimensional concept that reflects resilience to triggers – perturbations
- More advanced safety cultures have more sophisticated understanding of their risk space
- The size of possibility space means we cannot prepare for all eventualities in detail