弾

Resilience Engineering:
Resilient safety management

ERIK HOLLNAGEL

PROFESSOR &
INDUSTRIAL SAFETY CHAIR
MINES PARISTECH
SOPHIA ANTIPOLIS, FRANCE

PROFESSOR II
NTNU
TRONDHEIM, NORGE

E-MAIL: ERIK.HOLLNAGEL@GMAIL.COM

Two views of safety management

A reactive SMS relies on trivial (structural) models (domino model, Swiss cheese model), hence thinks of accidents as cause-effect chains.

- Responses following an adverse event depend on the causes that are found, hence on the "model" that is used
- Responses typically try to "fix" weaknesses to avoid that something happens again, rather than enhancing productivity (predict, plan, produce)

A proactive SMS safety refers to non-trivial (functional) models and sees failures as the flip side of successes.

- Responses focus on functions, on how they can be made more reliable and less variable, and on how to dampen resonance.
- Responses typically try to enhance the organisation's flexibility and capacity to adjust to changes, hence also enhances productivity.

Theory W: Traditional safety perspective

Things go right because:

- Systems are well designed and scrupulously maintained,
- Designers can foresee and anticipate every contingency.
- Procedures are complete and correct
- People behave as they are expected to – as they are taught.

Humans are a liability and performance variability is a threat. The purpose of design is to constrain variability, in order to prevent adverse outcomes.

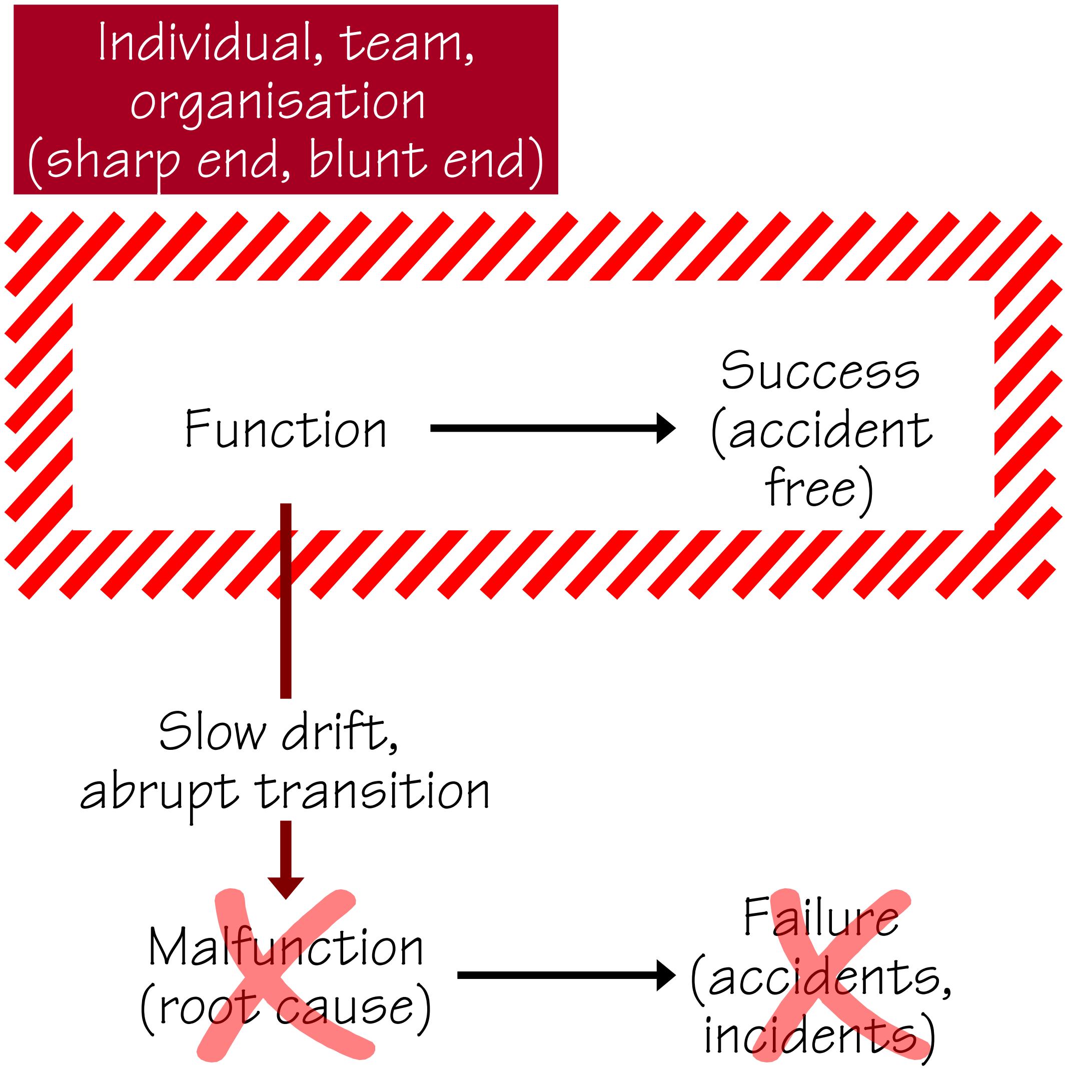
The purpose of risk assessment is to identify in a systematic manner how adverse outcomes (= severe accidents) may be brought about.

Common assumptions

- Accidents are due to failures or malfunctions of components (“human errors”), equipment malfunctions.
- Risks can be represented by linear combinations or chains of failures or malfunctions. Example: Event tree - fault tree

Theory W: Safety by constraint

Barriers,
regulations,
procedures,
standardization,
elimination



Individual, team, organisation (sharp end, blunt end)

Function

Success (accident free)

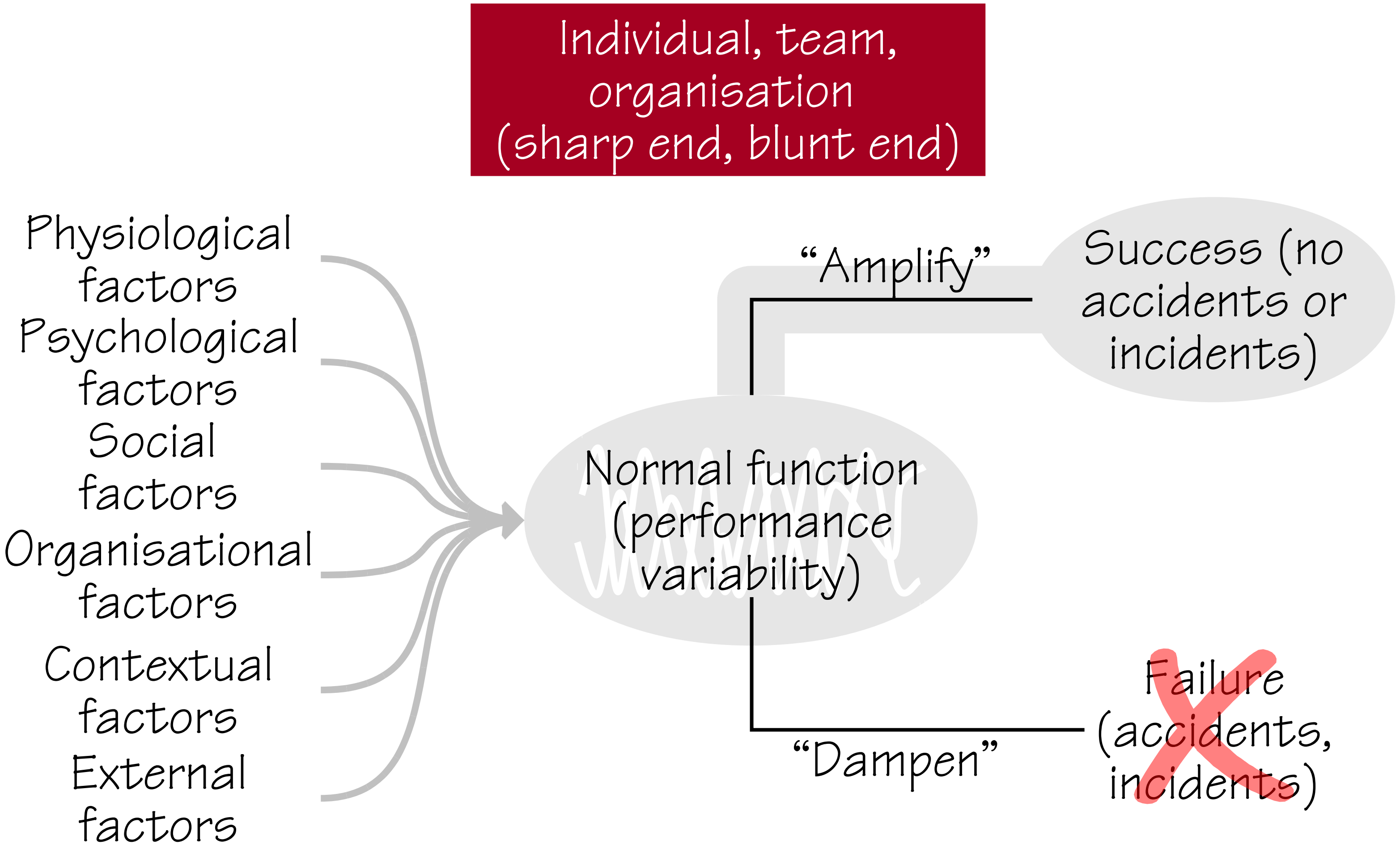
Slow drift, abrupt transition

Malfunction (root cause)

Failure (accidents, incidents)

Safety is achieved by constraining performance

Theory Z: Safety by management


Individual, team, organisation (sharp end, blunt end)
Physiological factors
Psychological factors
Social factors
Organisational factors
Contextual factors
External factors
Normal function (performance variability)
"Amplify"
Success (no accidents or incidents)
"Dampen"
Failure (accidents, incidents)

Performance variability is needed for normal functioning (successes)

Failures cannot be prevented by eliminating performance variability

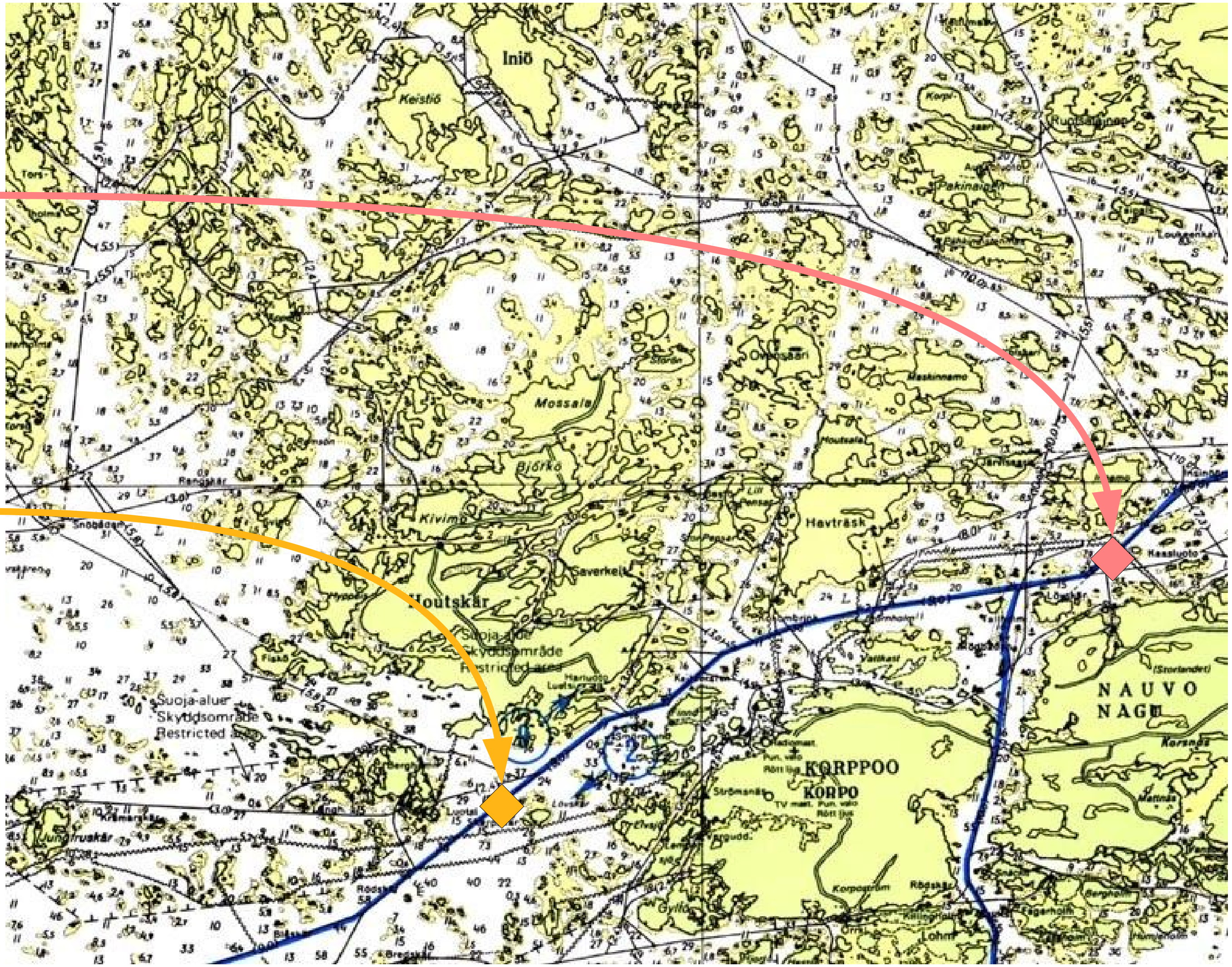
Safety is achieved by managing unwanted combinations of performance variability without adversely affecting successes

Managing resilience is like steering

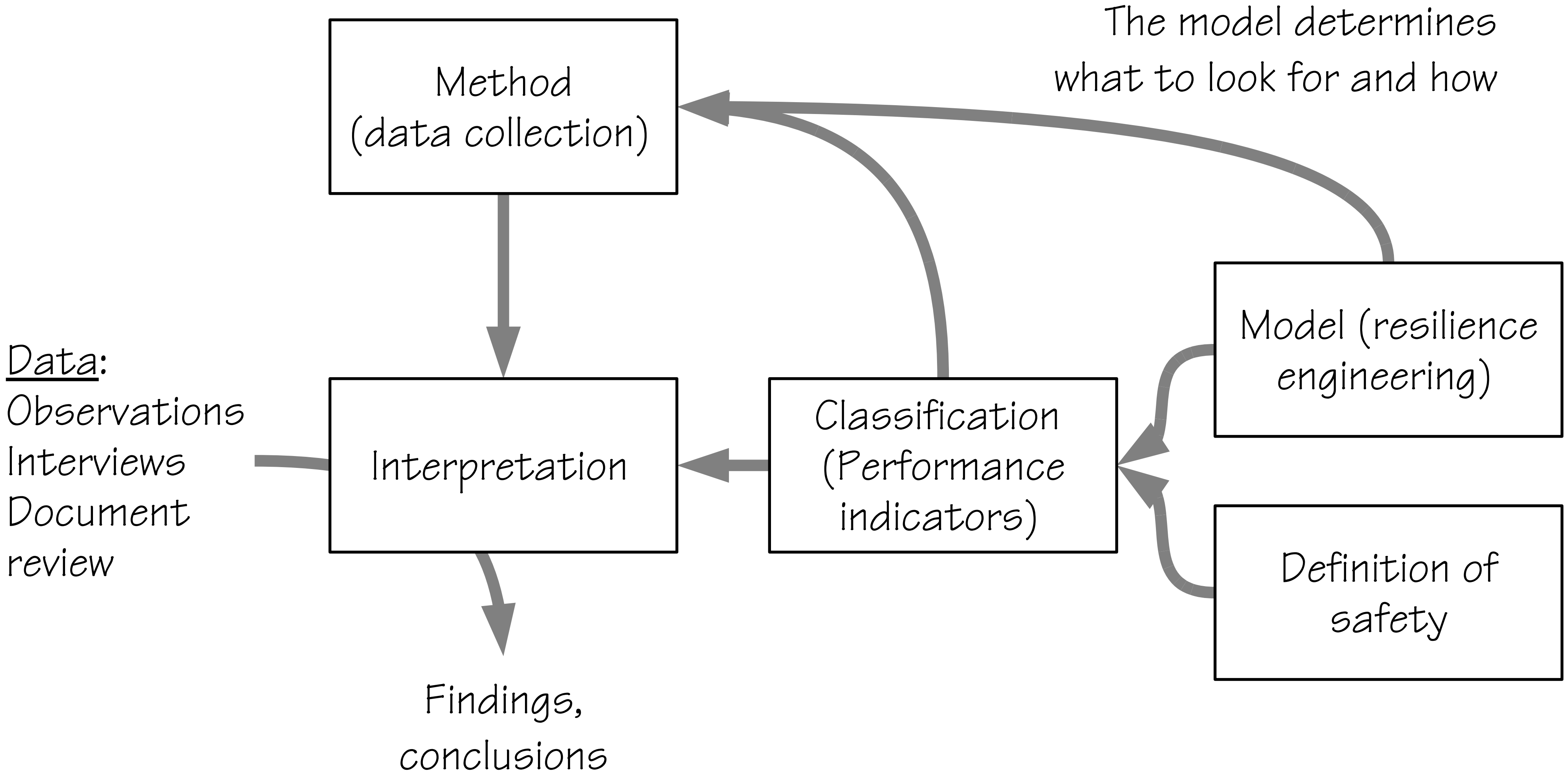
PROCESS:
Where are we (the current 'position')?
How well are we doing?

GOALS:
Where do we want to be (goal or target) and when?

CONTROLS:
How can we get there (effective means)?
What should we look out for on the way?



The logic of indicators



The model determines what to look for and how

Method (data collection)

Data: Observations Interviews Document review

Interpretation

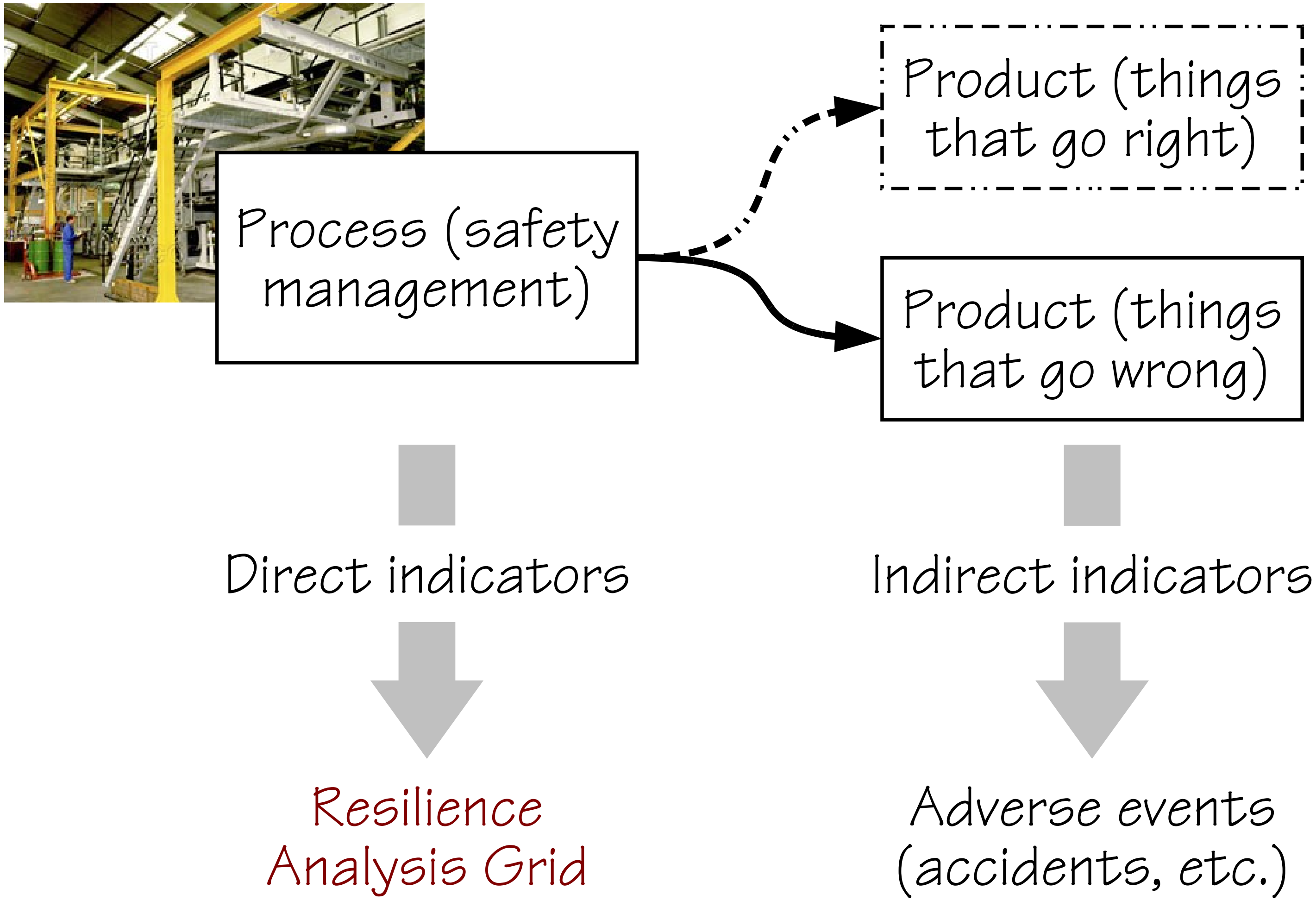
Classification (Performance indicators)

Model (resilience engineering)

Definition of safety

Findings, conclusions

Measures of products vs. processes



Process (safety management)

Product (things that go right)

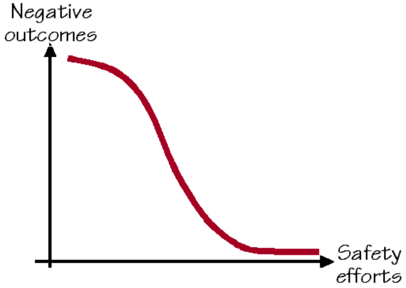
Product (things that go wrong)

Direct indicators

Indirect indicators

Resilience Analysis Grid

Adverse events (accidents, etc.)



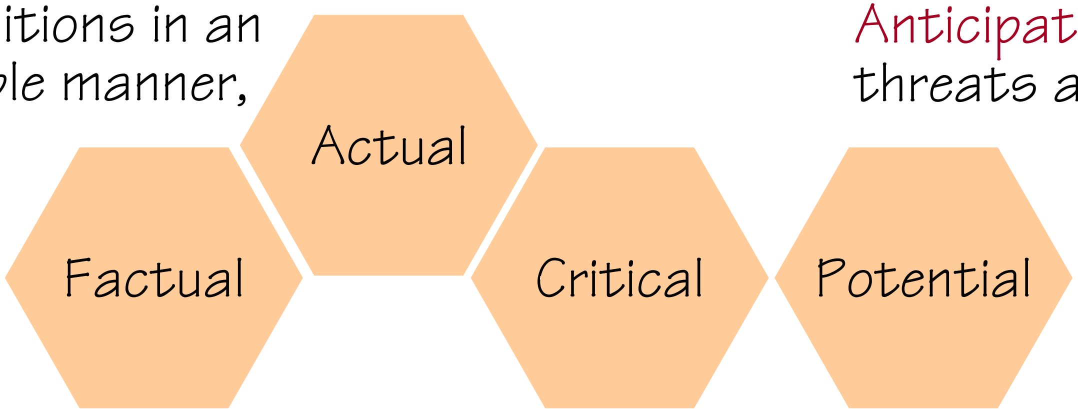
The resilient organisation

Resilience is the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions.

A practice of Resilience Engineering / Proactive Safety Management requires that all levels of the organisation are able to:

Respond to regular and irregular conditions in an effective, flexible manner,

Anticipate long-term threats and opportunities



Learn from past events, understand correctly what happened and why

Monitor short-term developments and threats; revise risk models

The Resilience Analysis Grid (RAG)

A resilient system must be able to respond, monitor, anticipate, and learn. It is not resilient if it lacks any of these abilities, even if it excels on some of the others.

The proper balance between the four abilities depends on what the system does. For instance, it is very important for a fire brigade to be able to respond. But it may be more important for a business to be able to anticipate.

The Resilience Analysis Grid provides a measure or profile of how well a system does on each of the four abilities. This can be used as the basis for proposing specific ways of either improving an ability or re-establishing the proper balance.

The RAG is a process measure rather than a product measure, since it shows the current level of resilience and of how well the system does on each of the four main capabilities. It must therefore be made regularly.

Resilience Analysis Grid (RAG)

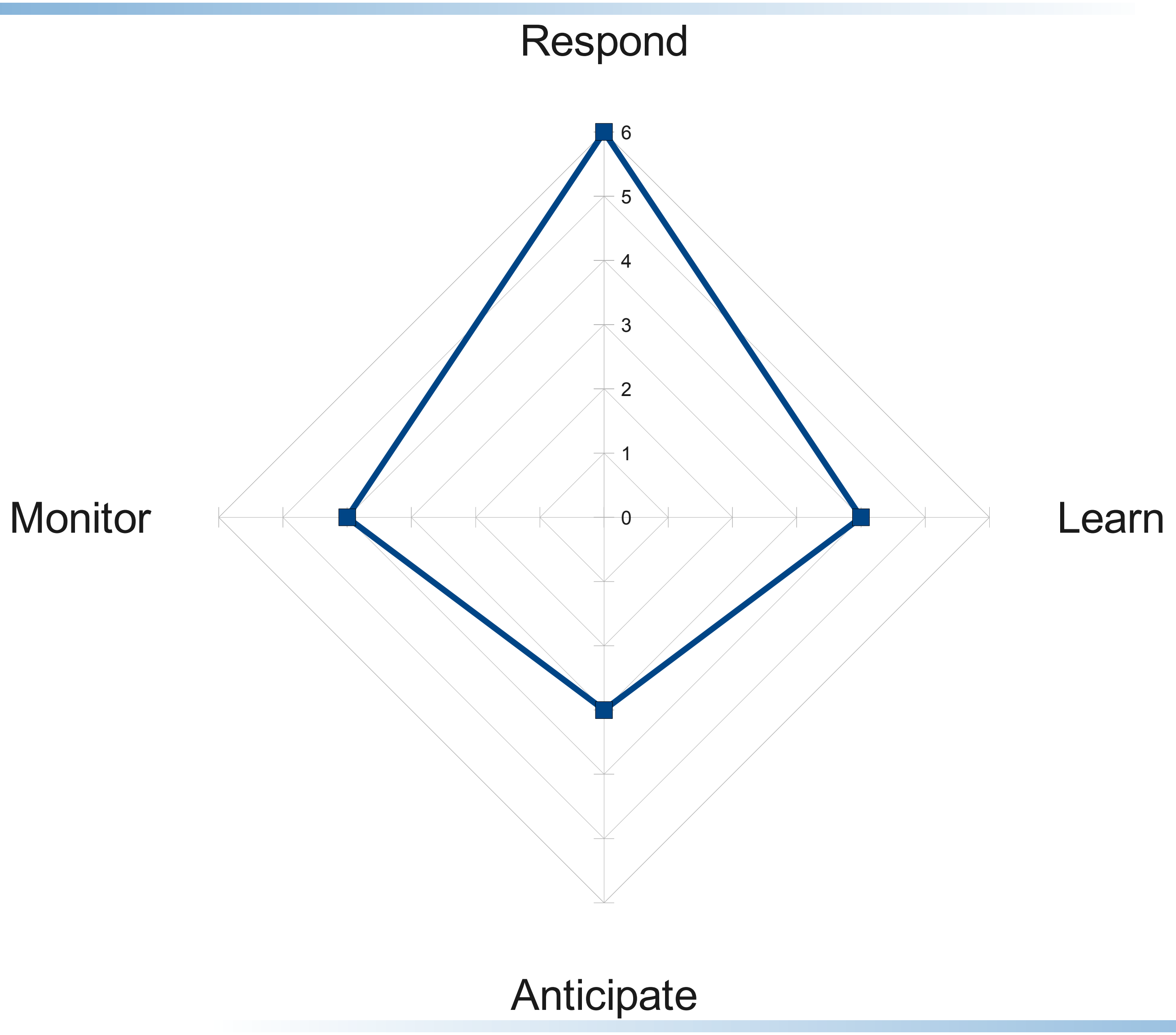
<table>
<tr><td colspan="6">The ability to respond: How ready is the organisation to respond and how able (quickly and efficiently) is it to respond when something unexpected happens?</td></tr>
<tr><td>Excellent</td><td>Satisfactory</td><td>Acceptable</td><td>Unacceptable</td><td>Deficient</td><td>Missing</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

<table>
<tr><td colspan="6">The ability to monitor: How well is the organisation able to detect changes to work conditions that may affect the its ability to carry out current or intended operations?</td></tr>
<tr><td>Excellent</td><td>Satisfactory</td><td>Acceptable</td><td>Unacceptable</td><td>Deficient</td><td>Missing</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

<table>
<tr><td colspan="6">The ability to anticipate: How large an effort does the organisation put into what may happen in the near future? Is anticipation a strategic concern?</td></tr>
<tr><td>Excellent</td><td>Satisfactory</td><td>Acceptable</td><td>Unacceptable</td><td>Deficient</td><td>Missing</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

<table>
<tr><td colspan="6">The ability to learn: How well does the organisation make use of formal and informal opportunities to learn from what happened in the past?</td></tr>
<tr><td>Excellent</td><td>Satisfactory</td><td>Acceptable</td><td>Unacceptable</td><td>Deficient</td><td>Missing</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Hypothetical resilience profile (overall)



Measuring ‘How to Respond’

Analysis item (ability to respond)	Score or evaluation
Event list: What are the events for which the system has a prepared response?	
Background: How were these events selected (experience, expertise, risk assessment, etc.?	
Relevance: When was the list created? How often is it revised? On which basis is it revised?	
Threshold: When is a response activated? What is the triggering criterion or threshold? Is the criterion absolute or does it depend on internal / external factors?	
Response list: How was the specific type of response decided? How is it ascertained that it is adequate? (Empirically, or based on analyses or models?)	
Speed: How fast is full response capability available?	
Duration: For how long can a 100% effective response be sustained?	
Stop rule: What is the criterion for returning to a “normal” state?	
Response capability: How many resources are allocated to the response readiness (people, materials)? How many are exclusive for the response potential?	
Verification: How is the readiness to respond maintained? How is the readiness to respond verified?	

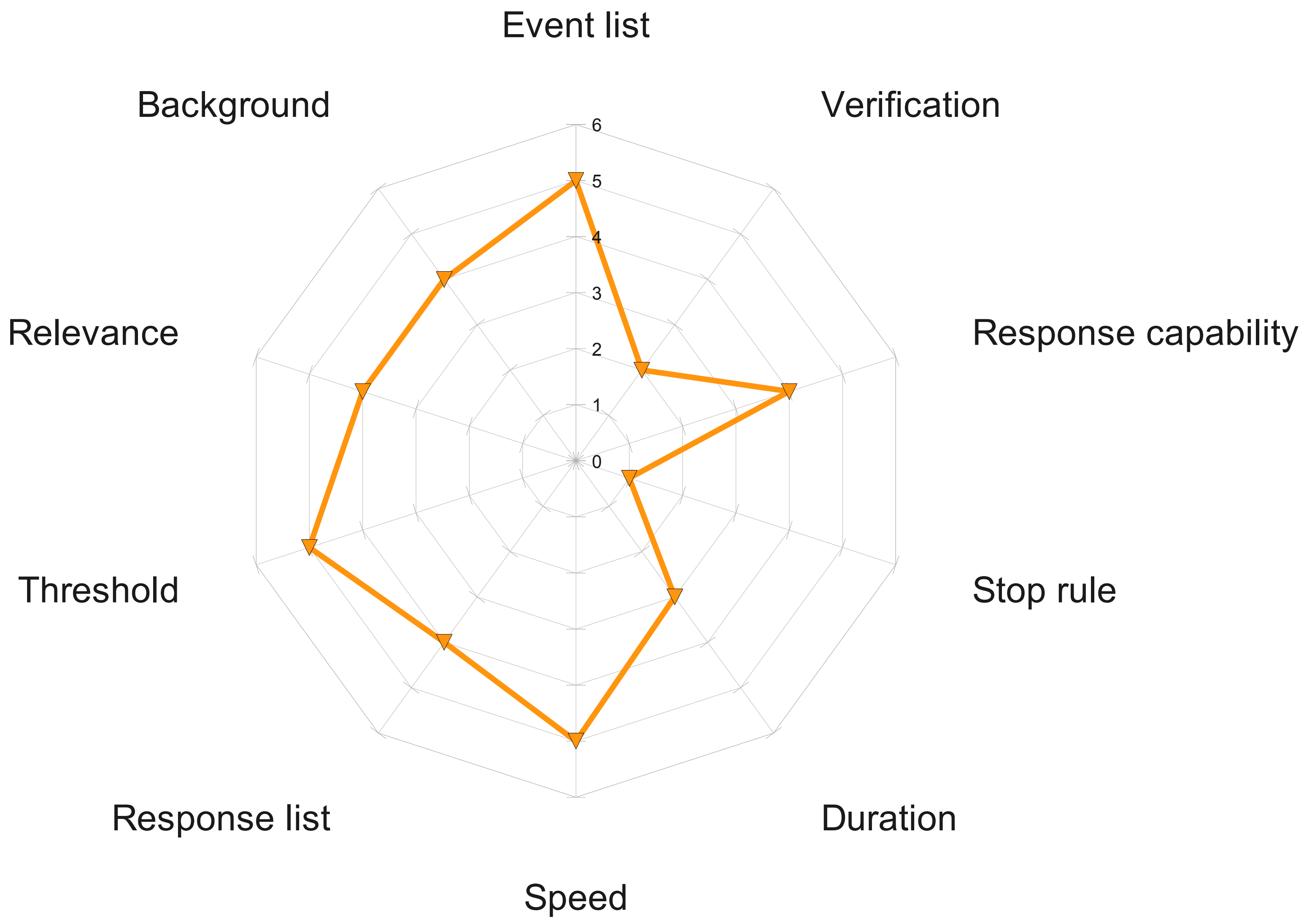
Excellent	The system on the whole exceeds the criteria addressed by the specific item.
Satisfactory	The system fully meets all reasonable criteria addressed by the specific item.
Acceptable	The system meets the nominal criteria addressed by the specific item.
Unacceptable	The system does not meet the nominal criteria addressed by the specific item.
Deficient	There is insufficient capability to meet the criteria addressed by the specific item.
Missing	There is no capability whatsoever to address the specific item.

Phrasing of questions

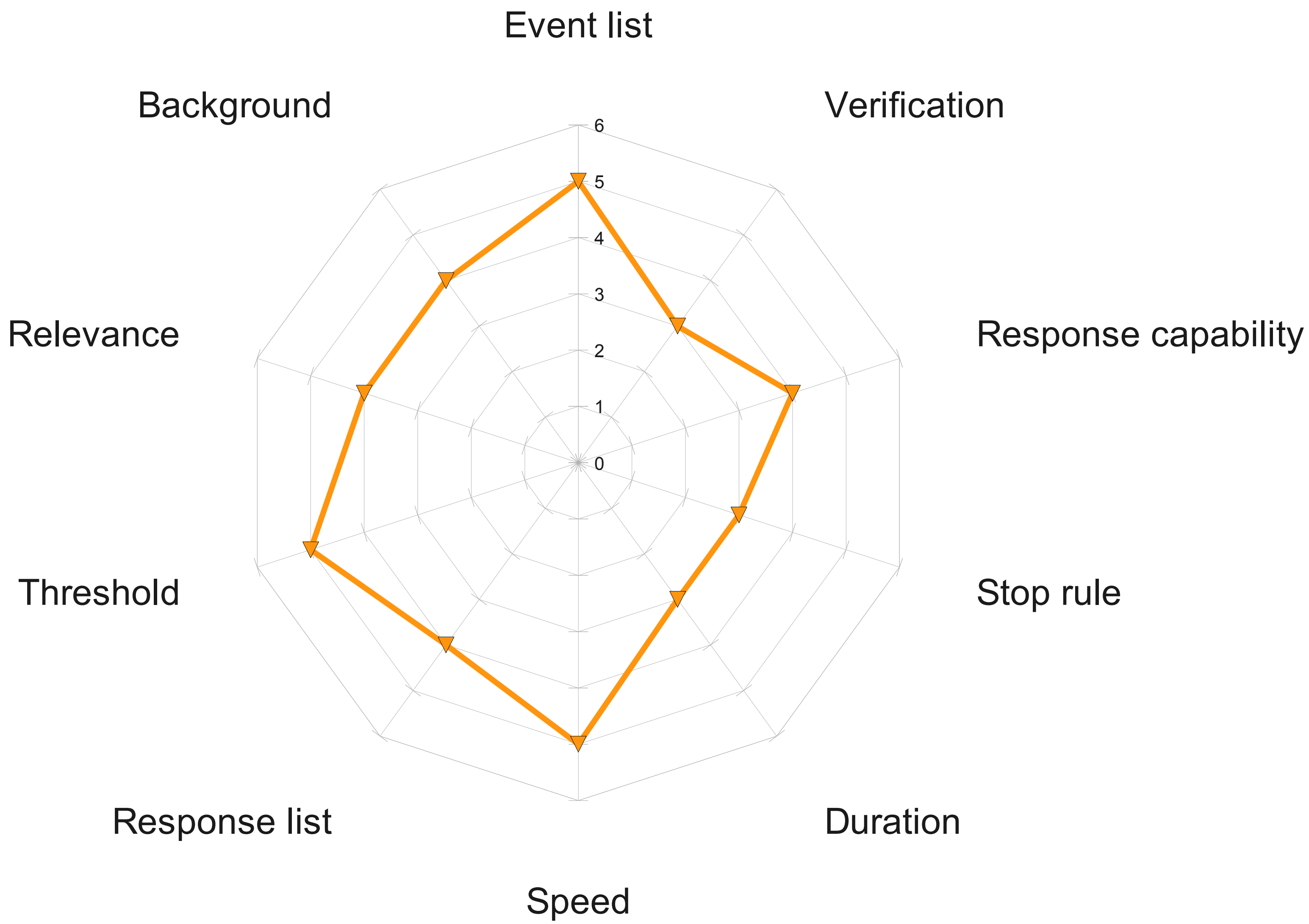
How do you rate the company's strategies for updating the response list of abnormal situations?					
Excellent	Satisfactory	Acceptable	Unacceptable	Deficient	Missing

The strategies for updating the response list of abnormal situations are adequate.				
Strongly agree	Agree	Not sure	Disagree	Strongly disagree

Hypothetical resilience profile (respond)



Hypothetical resilience profile (respond)



Example of subcategories for the RAG

Responding	Monitoring	Anticipating	Learning
Response selection	Coherence (of indicators)	Culture	Selection criteria
Experience	Revision	Expertise	Investigations
Validity	Leading indicators	Approach	Resources
Competence	Lagging indicators	Definition (of changes)	Use of experience
Activation criteria	Validity	Frequency	Organisation
Stop rule	Frequency	Time horizon	

Integrated planning (offshore)

		E	S	A	U	D	M
Respond	The integrated plan is continuously updated to reflect the varying needs of the installation.						
	Active short-term plans are rescheduled when a certain threshold for risk on the activities are reached.						
	If there are problems in execution of activities, the activities can be reprioritized and/or replaced.						
	Our planners are experienced and understand the problems that may occur in the execution of activities.						
Learn	There is a well-functioning two-way communication between the offshore- and onshore organization during planning						
	There is a well-functioning performance measurement system for how the integrated planning process works.						
	We emphasize experience-and knowledge transfer among the people working in the company's integrated planning						
	The integrated planning is being continuously improved.						

Three steps to resilience

What is the resilience profile of your organisation?

Apply the Resilience Analysis Grid. Take time to consider and debate the results.
NB: This should be done on a regular basis rather than as a single snapshot.
Look for strengths and weaknesses in how the organisation responds, monitors, anticipates, and learns.

What can you do to ensure a resilient organisation in your site?

Look at what goes right as well as what goes wrong – on all levels.
Find the main trade-offs (ETTOs) that are the basis for safety and productivity.
Understand why they happen and how they can either be strengthened or dampened.

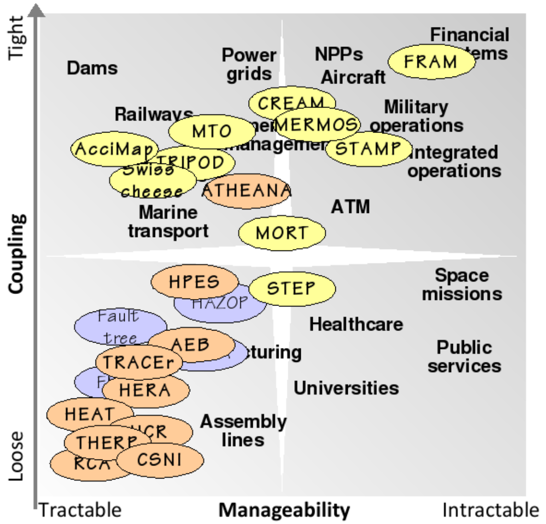
What can you do from tomorrow on to improve the resilience of your organization?

Study the detailed resilience profiles (for each ability).
See what needs to be improved, and decide how best to do it.
Consider costs and benefits – both short-term and long-term.
Think of when you can reasonably expect to see results of improvements.

Conclusions

Industrial safety has gone through several developments (ages), reflecting the changes in socio-technical systems.

Age of technology (industrial revolution to 1979)
Age of human factors (1979 to end of 20th Century)
Age of safety management (mid-1980s – ???)



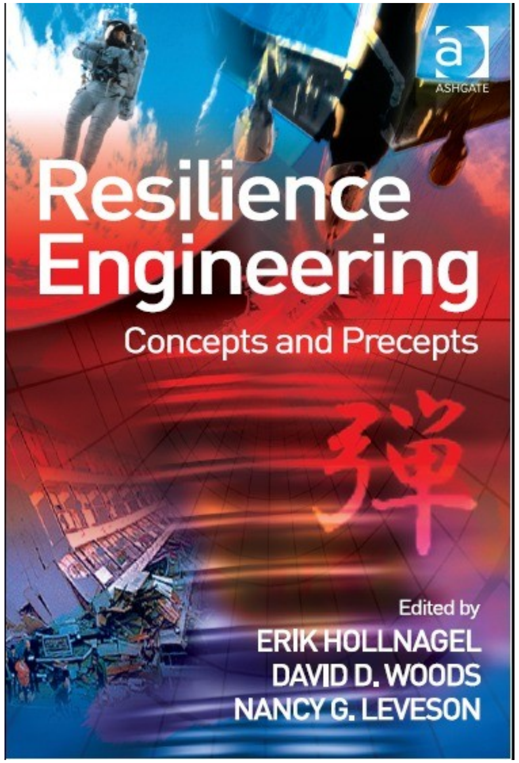
Safety methods are always developed to solve the problems at the time, and in the near future.

But socio-technical developments mean that things can go wrong in ways that challenge existing methods.

It is therefore necessary every now and then to supplement the existing approaches to safety management with new tools and techniques.

Tempora mutantur, et nos mutamur in illis

Books about Resilience Engineering



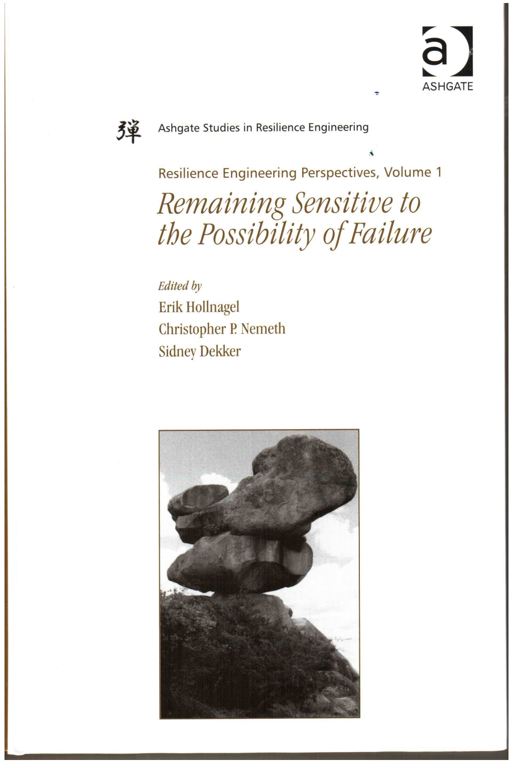
ASHGATE

Resilience Engineering

Concepts and Precepts

Edited by
ERIK HOLLNAGEL
DAVID D. WOODS
NANCY G. LEVESON

Resilience Engineering (2006)
Spanish translation (2010)



ASHGATE

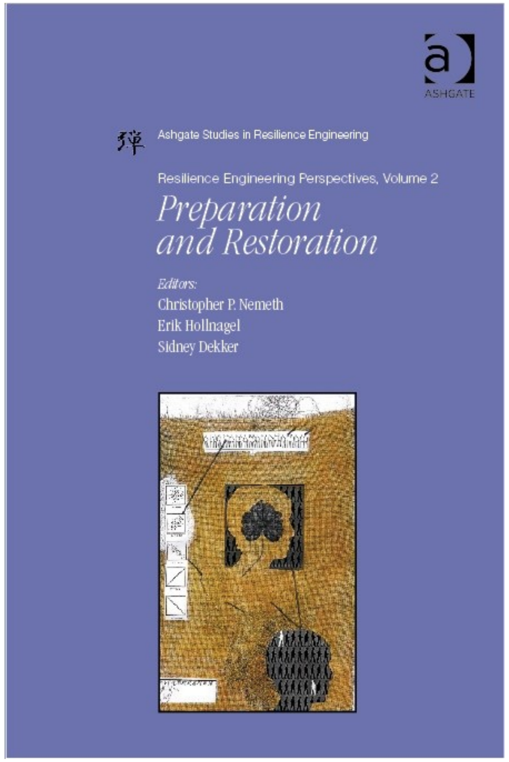
Ashgate Studies in Resilience Engineering

Resilience Engineering Perspectives, Volume 1

Remaining Sensitive to the Possibility of Failure

Edited by
Erik Hollnagel
Christopher P. Nemeth
Sidney Dekker

Remaining sensitive to the possibility of failure (2008)



ASHGATE

Ashgate Studies in Resilience Engineering

Resilience Engineering Perspectives, Volume 2

Preparation and Restoration

Editors:
Christopher P. Nemeth
Erik Hollnagel
Sidney Dekker

Preparation and restoration (2009)

RESILIENCE ENGINEERING IN PRACTICE:
A GUIDEBOOK

Preparation and restoration (2011)

Resilience Engineering Association

The goal of the Association Is to provide a forum for coordination and exchange of experiences, by bringing together researchers and professionals working in the RE domain and organisations applying or willing to apply RE principles in their operations. Research and practice in RE Engineering aims to establish a new way of thinking about safety and organizational capabilities to sustain performance over time in the face of contingencies.

If you are interested, send a mail to
rea@resilience-engineering.org

The first General Assembly of the REA will be held in connection with the
Fourth Resilience Engineering Symposium
Sophia Antipolis, France, June 8-10, 2011
www.resilience-engineering.org