

SAFETY-II AS A MANAGEMENT PRINCIPLE

IMPLICATIONS FOR MANAGING AND DEVELOPING AN ORGANIZATION

ERIK HOLLNAGEL, PH.D.
PROFESSOR, JÖNKÖPING ACADEMY (SWEDEN)
VISITING PROFESSORIAL FELLOW, MACQUARIE UNIVERSITY (AUSTRALIA).
E-MAIL: HOLLNAGEL.ERIK@GMAIL.COM

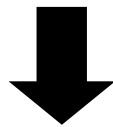
Safety-I: without unwanted outcomes



3. DEFINITIONS

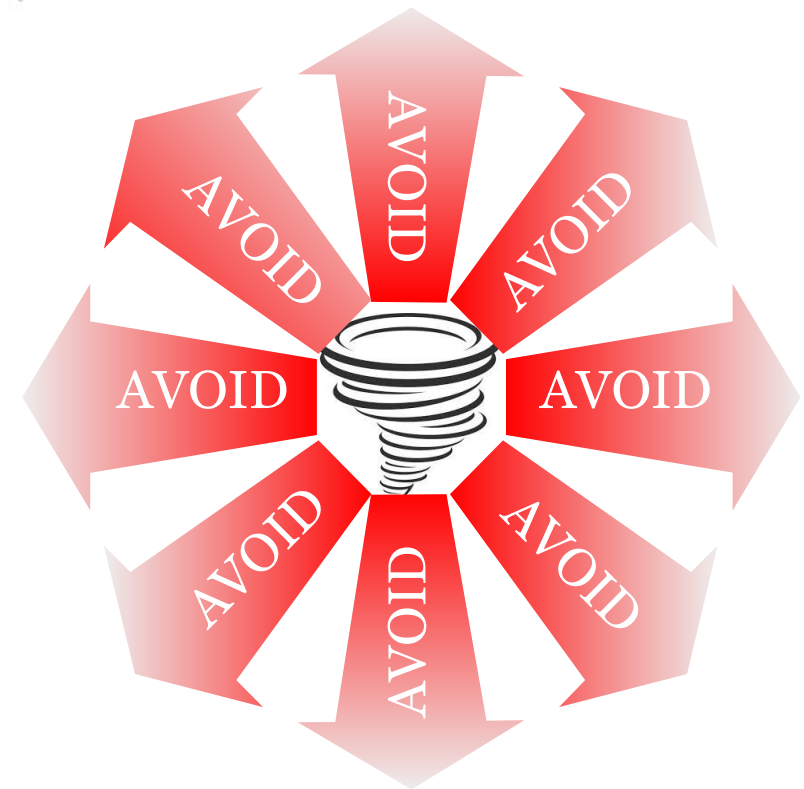
3.20 **Safety.** Freedom from unacceptable risk.

Negative outcomes are caused by failures and malfunctions.



Safety-I:

Analyse accidents and incidents to prevent or eliminate what can go wrong.



(M)any direction(s) will take you away from what you want to avoid

Managing Safety-I

Safety-I is a condition where the number of adverse outcomes (accidents / incidents / near misses) is as low as possible.

The belief in causality (Causality Credo)



- (1) Adverse outcomes happen because something has gone wrong (cause-effect thinking + value congruence between cause and effect).
- (2) Causes can be found and treated (rational deduction).
- (3) All accidents are therefore preventable (zero harm principle).



Prevent, eliminate, constrain.
Safety, quality, etc. are different and require different measures and methods.

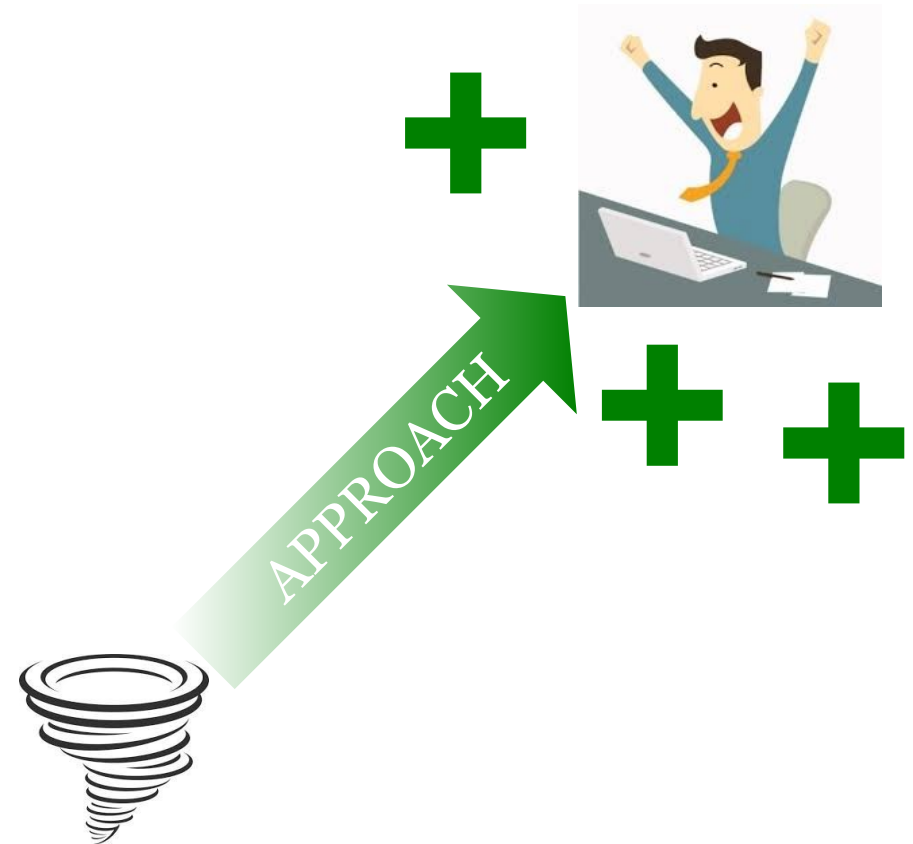
Safety-II: with wanted outcomes

All outcomes (positive and negative)
are the result of performance
variability.



Safety-II:

Support or facilitate what goes well by
studying everyday performance.



... but only one direction will bring you
closer to what you want to attain.

Managing Safety-II

Safety-II is a condition where as much as possible goes well.



Support, augment, facilitate.
Safety, quality, etc. are
inseparable and need matching
measures and methods.

1. Care about what happens all the time rather than what happens rarely. **We always count the number of times something fails, but rarely the number of times it just works.**
2. Look for 'work-as-done' - the habitual adjustments and why they are made. **When something is done, as a part of work, it has usually been done before and gone well before.**
3. Learning should be based on the frequency of events rather than their severity. **Small improvements of everyday performance may be more important than large improvements of rare performance.**

Failures or successes?

When something goes wrong,
e.g., 1 event out of 10.000
($10E-4$), humans are assumed
to be responsible in 80-90% of
the cases.



Who or what are responsible
for the remaining 10-20%?

Investigation of failures is
accepted as important.



When something goes right,
e.g., 9.999 events out of
10.000, are humans also
responsible in 80-90% of
the cases?



Who or what are
responsible for the
remaining 10-20%?

Investigation of successes
is rarely undertaken.

How do we understand what happens?

Design (tools, roles,
environment)



Work-As-Imagined

Work & production planning
("lean" - optimisation)

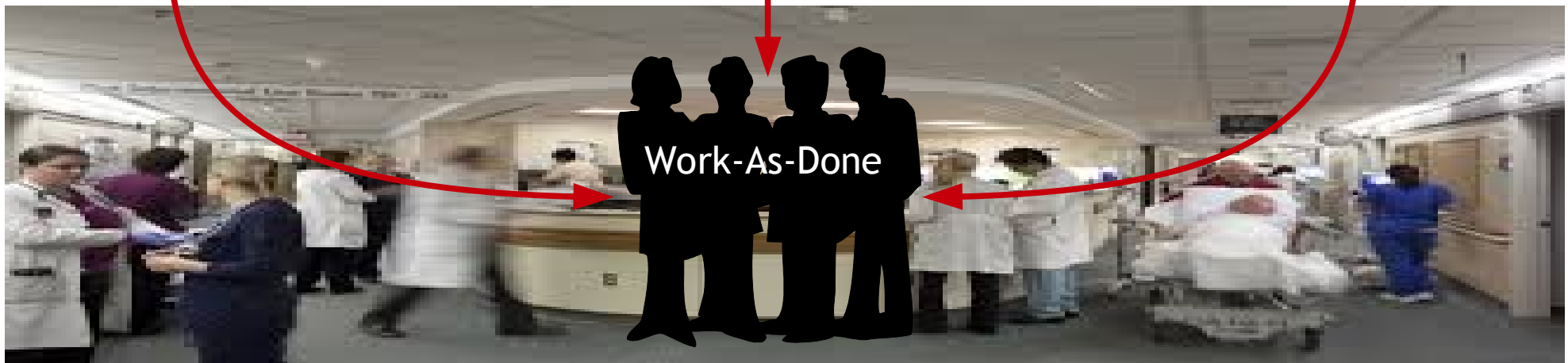


Work-As-Imagined

Safety management,
investigations & auditing

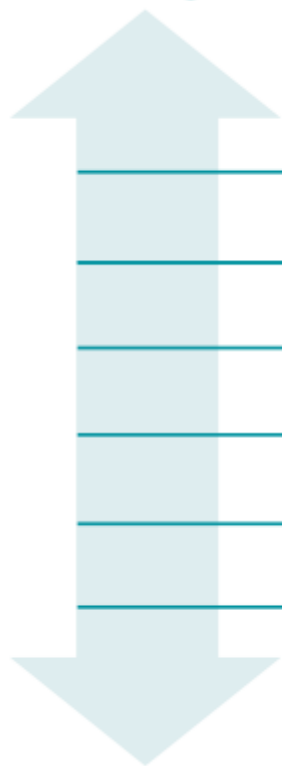


Work-As-Imagined



Efficiency of safety recommendations

Strongest



Remove hazard from system

Forcing functions (force individuals to do things differently)

Automation and computerization

Standardization and centralization

Simplification

Rules and policies

Reminders/checklists

Inform/educate

Weakest

Types of barrier systems

Physical barrier system

Physically prevents an action from being carried out, or prevents the consequences from spreading

Functional (active or dynamic) barrier system

Hinders the action via **preconditions** (logical, physical, temporal) and **interlocks** (passwords, synchronisation, locks)

Symbolic barrier system (perceptual, conceptual)

Requires an act of **interpretation** to work, i.e. an intelligent and perceiving agent (signs, signals, alarms, warnings)

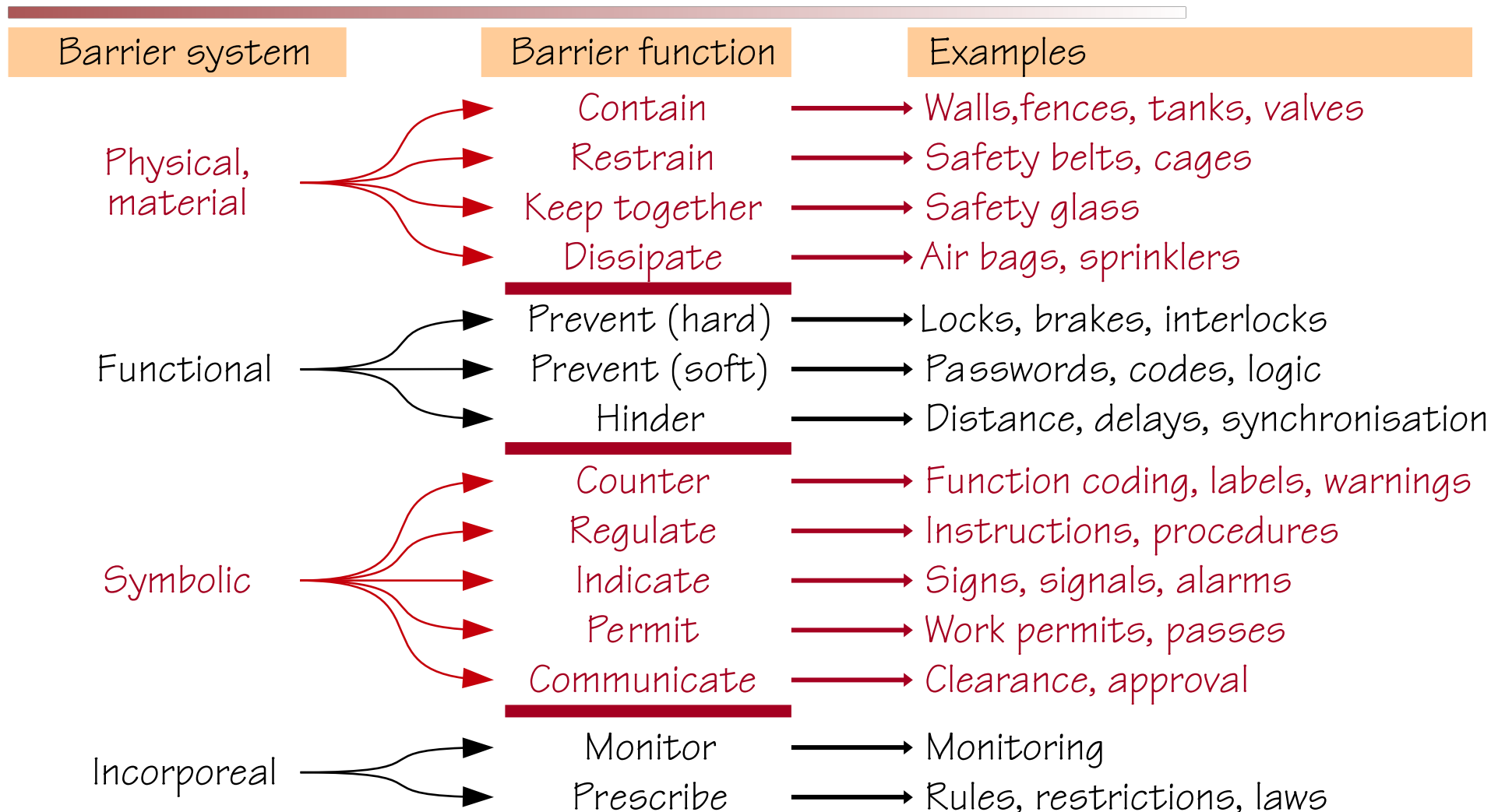
Incorporeal barrier system (non-material barrier)

Not physically present in the situation, rely on **internalised** knowledge (rules, restrictions, laws)

Works in and of itself

Requires someone to respond

Barrier systems / barrier functions



Different ideas about solutions

This will solve
your problems

Macro



Will this solve
our problems?

Meso



This doesn't
solve our
problems

Micro



Why are there different
ideas about what
actually goes on?



And how can they be
reconciled?

Talk to your neighbour



How well do people at the “macro level” (managers, authorities) understand what goes on at the “micro level”?

How can you make sure that a proposed improvement / change will actually work?

Management is like travelling



GOALS or TARGETS:

Where do we want to be?
When should we arrive?



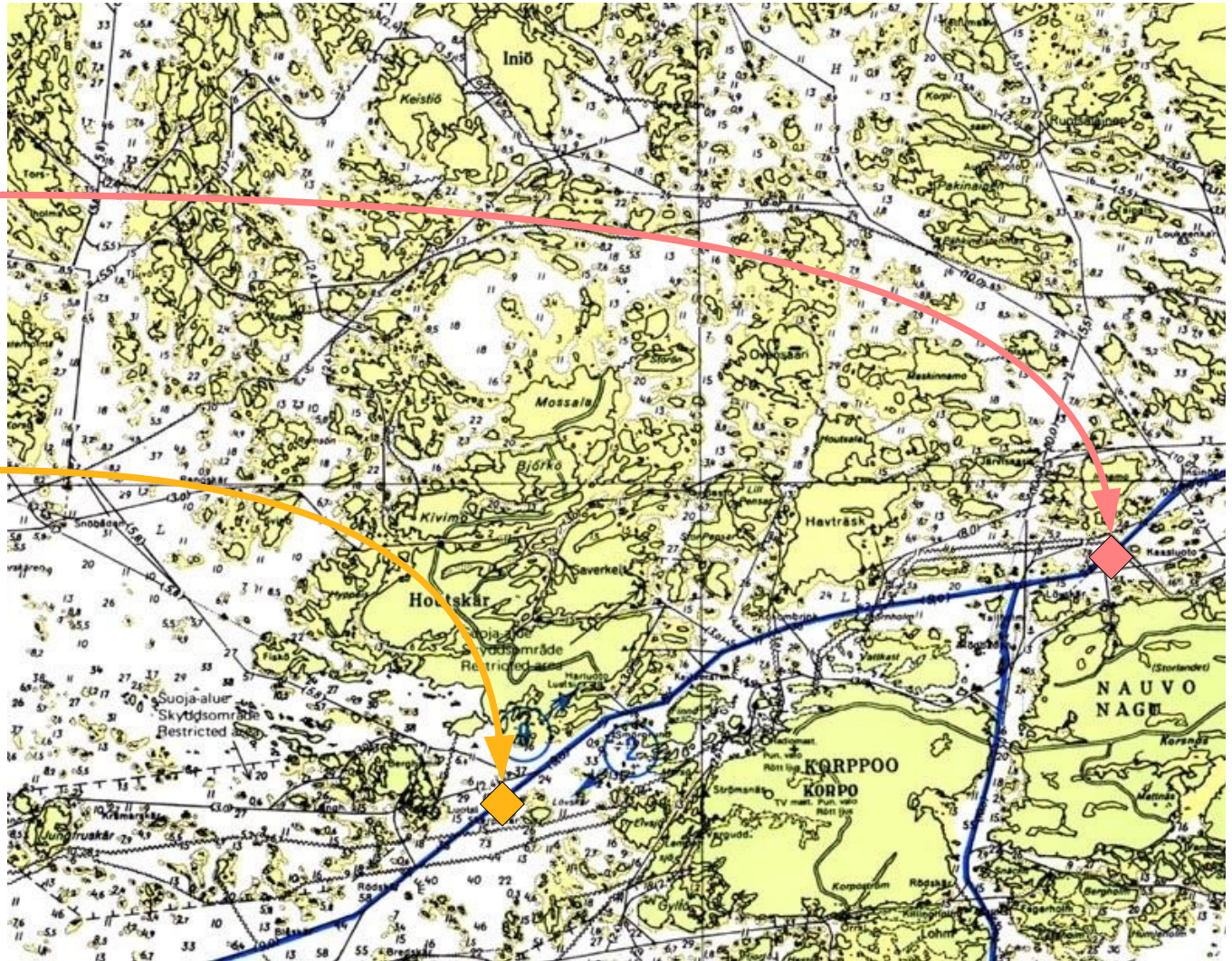
POSITION:

Where are we now?
How well are we doing?



MEANS or PROCESS:

How can we change position (“speed” and “direction”)?



Managing different processes



Goal: Well defined
Position: Known
Means / Process:
Well known, transparent



Goal: Well defined
Position: Known
Means / Process:
Well known, transparent



Goal: well defined
Position: Known
Means / Process:
Well known, transparent

Managing safety



Goal: Defined by
negation
(no accidents)



Position: Vaguely
known or unknown



Means / Process:
Partly unknown, based
on tradition rather
than knowledge.

Safety: What is the goal?

Global Aviation Safety Roadmap

Goals and Objectives:

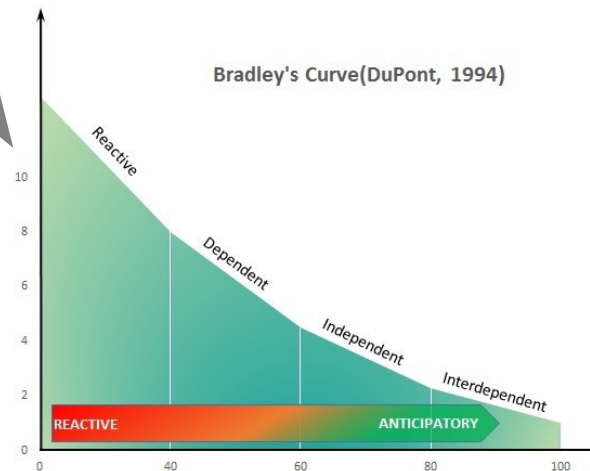
- Provide a common frame of reference for all stakeholders
- Coordinate and guide safety policies and initiatives worldwide to reduce the accident risk
- Avoid duplication of effort and uncoordinated strategies
- Encourage close industry and government cooperation on common safety objectives

6

**Safety Is Our #1 Goal
Each and Every Day!**

Safety goals are rarely described explicitly

**ONE TEAM,
ONE GOAL
ZERO
ACCIDENTS**



Goal: The “zero accident” approach

OUR PURPOSE

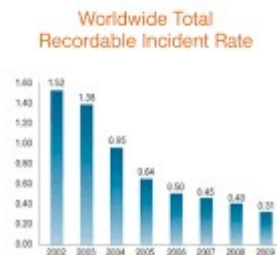
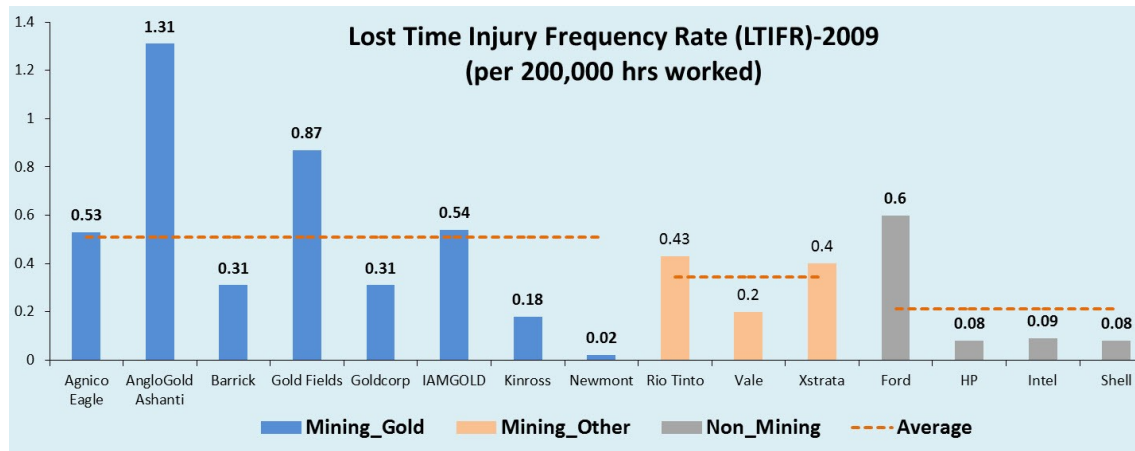
To produce [X] safely, securely and profitably - without harm to people or the environment.

OUR BELIEFS and GUIDING PRINCIPLES

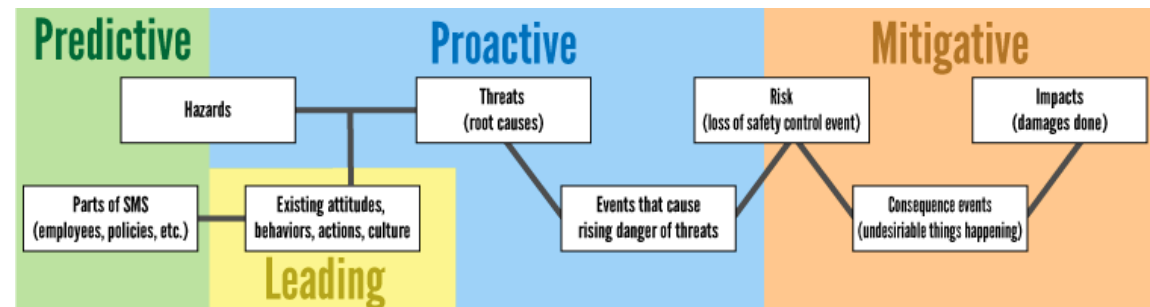


1. Safe production is our most important goal.
2. **All injuries and environmental incidents are preventable.**
3. Any task that can't be done safely without harm to the environment will not be done.
4. **Each person is accountable for his or her own safety, the safety of their coworkers and protecting the environment.**
5. Each person is expected to identify hazards and manage risks to people and the environment.
6. **Each person must have the necessary skills to work safely and protect the environment.**
7. Working safely with respect for people and the environment is a condition of employment.

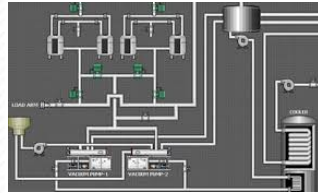
Safety: What is the position?



Most, if not all, safety measures refer to negative outcomes (accidents, etc.)

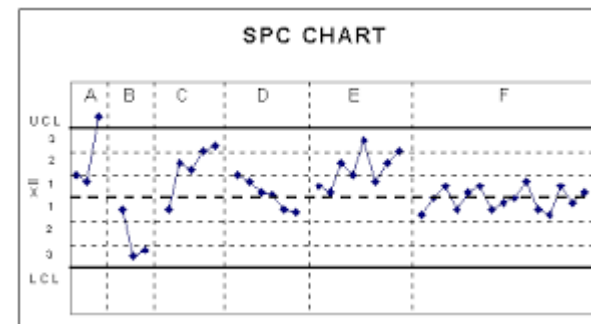
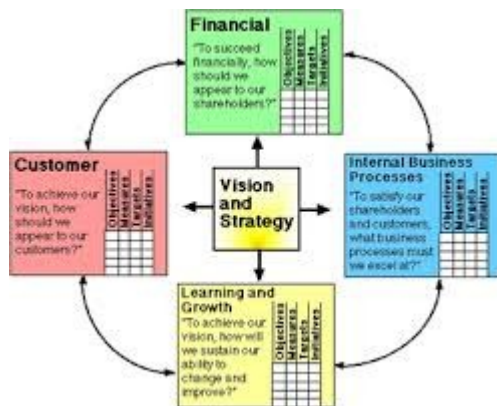
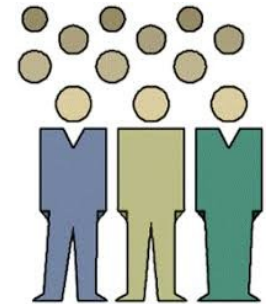


How do we know where we are?



Technological systems are designed and built.
We know what the “components” are, how they should work and can therefore define meaningful measurements.

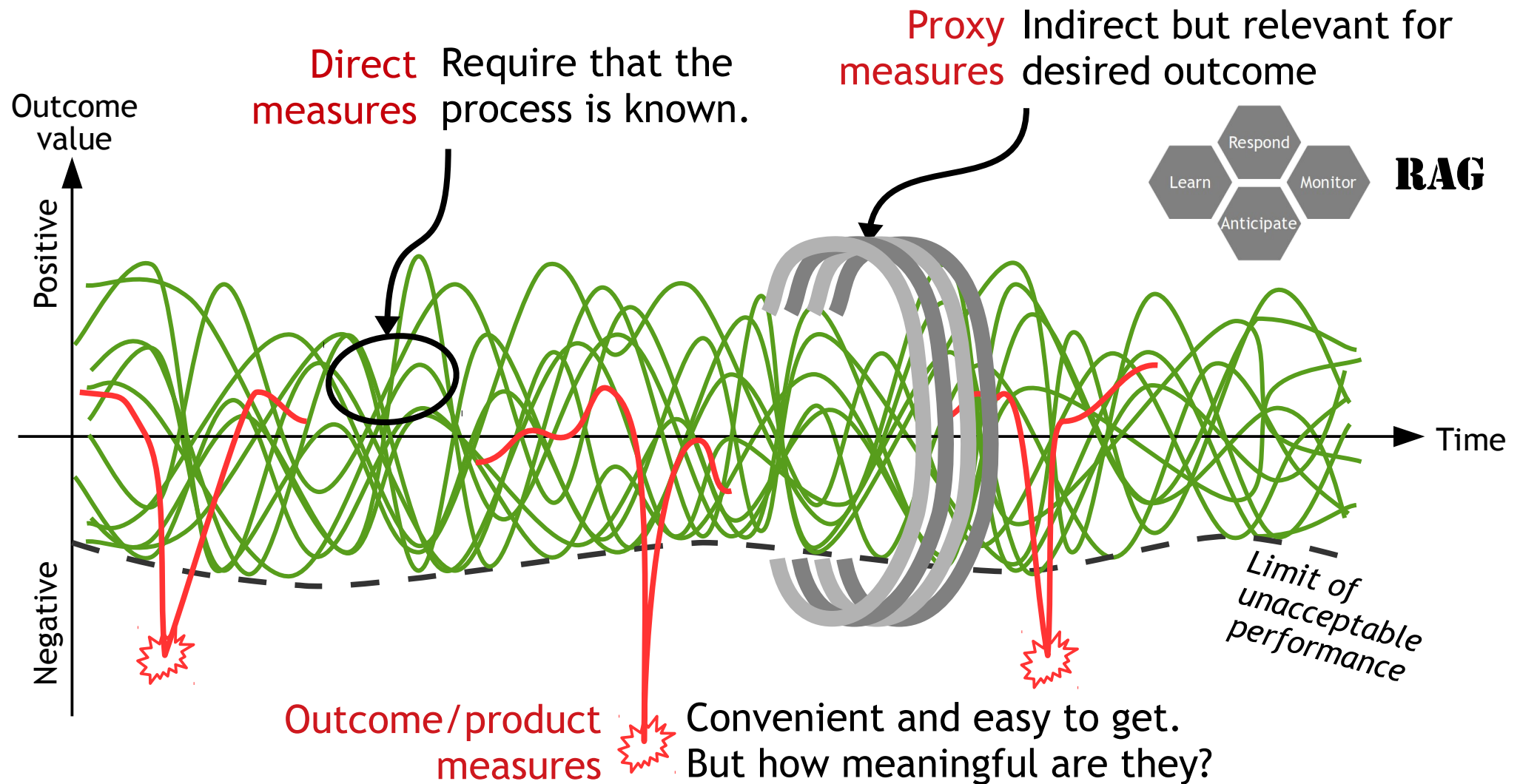
Organisations “grow” but are not built.
We know little of how they actually work and it is therefore difficult to define meaningful measurements.



$$CPI = \frac{\sum_{i=1}^n CPI_i \times weight_i}{\sum_{i=1}^n weight_i}$$

Consumer Price Index

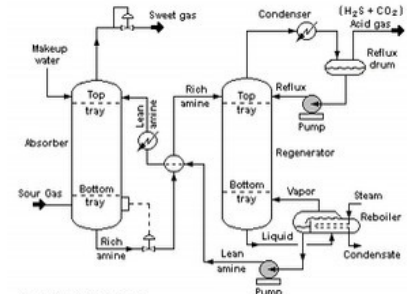
Management requires measurements



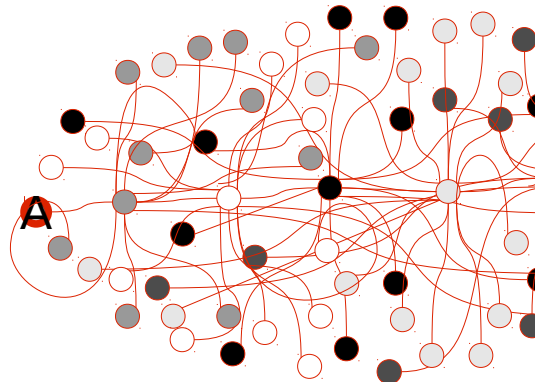
Means: Understanding systems



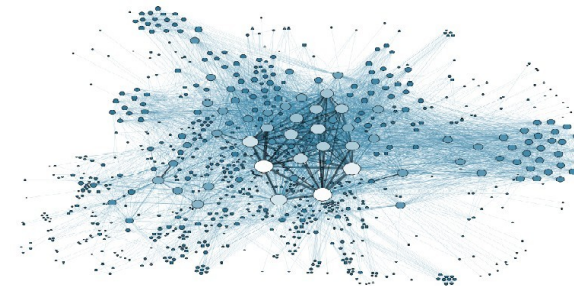
Simple system
(technical)



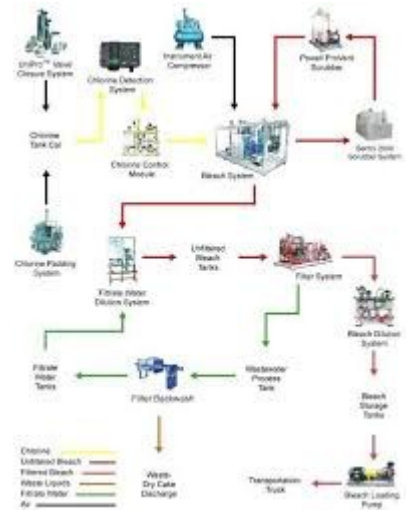
Complicated system
(socio-technical)



Complex system
(intractable)



SafetySynthesis

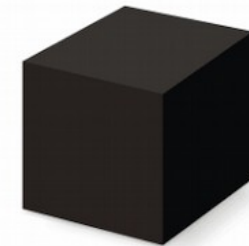
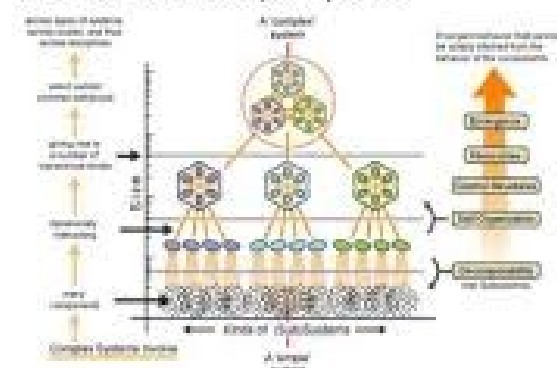


The diagram illustrates a comprehensive model of organizational performance. It features a central cluster of interconnected boxes representing internal organizational factors, surrounded by external and individual/organizational performance components. The components and their relationships are as follows:

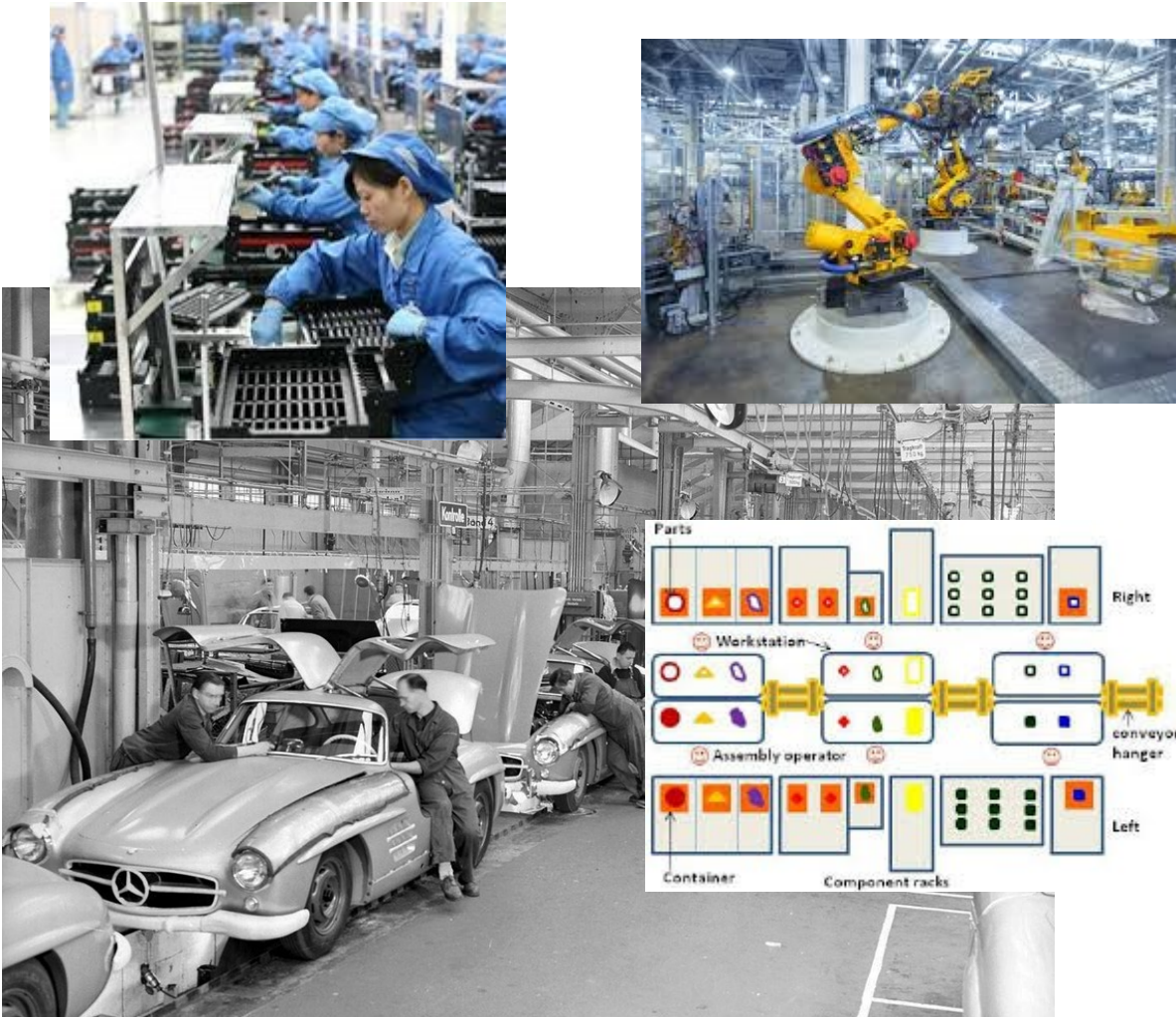
- External environment** (grey box) at the top, connected to Mission & strategy, Leadership, and Organisational culture.
- Mission & strategy**, **Leadership**, and **Organisational culture** form the top layer of internal factors.
- Structure**, **Management practices**, and **System (policies/procedures)** form the middle layer.
- Task & individual skills**, **Work unit climate**, and **Individual needs & characteristics** form the bottom layer of internal factors.
- Motivation** is positioned below Work unit climate.
- Individual and organisational performance** (grey box) at the bottom, receiving input from Motivation and the entire internal system.

Arrows indicate the direction of influence and feedback loops between these components. A dashed line encircles the central internal factors, and a red box labeled "Manager" is shown on the left, suggesting a managerial role in the process.

Characteristics of Complex Systems



Tractable systems



Simple descriptions
with few details
(technology, people)

Principles of
functioning are
known

System does **not**
change while being
described

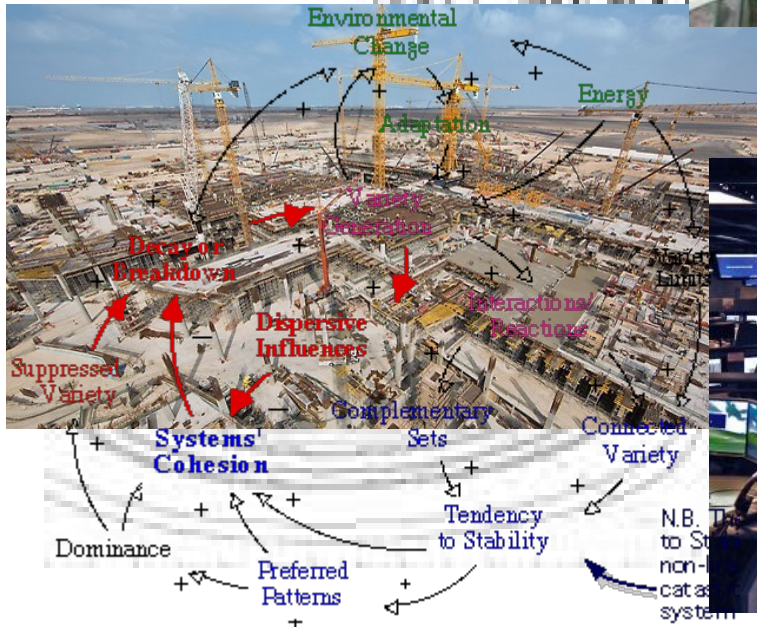
Intractable systems



Elaborate descriptions with many details

Principles of functioning are partly unknown

System changes before description can be completed



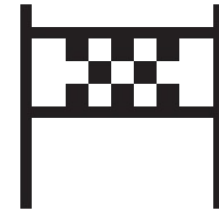
Goals, position and means



Legacy
Industry practice
Current trends



Indirect, lagging
“measures”



Tradition
Standards
Requirements

Control inputs
(management
interventions)



Outcomes
(products)

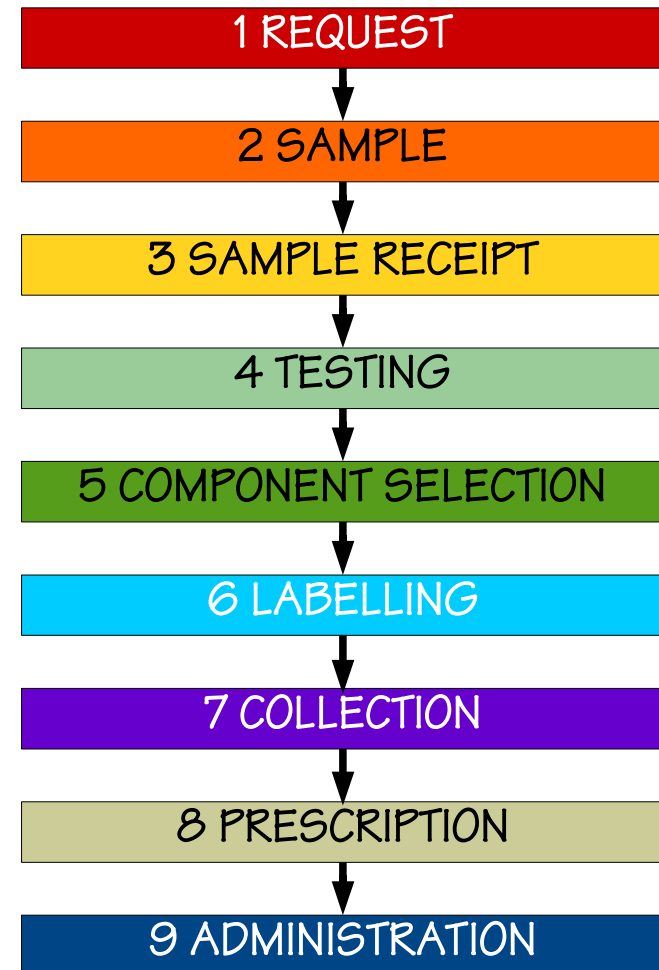
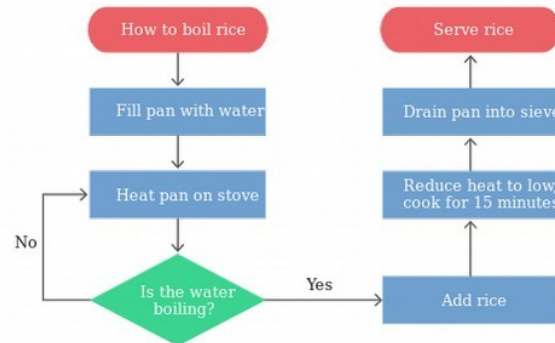
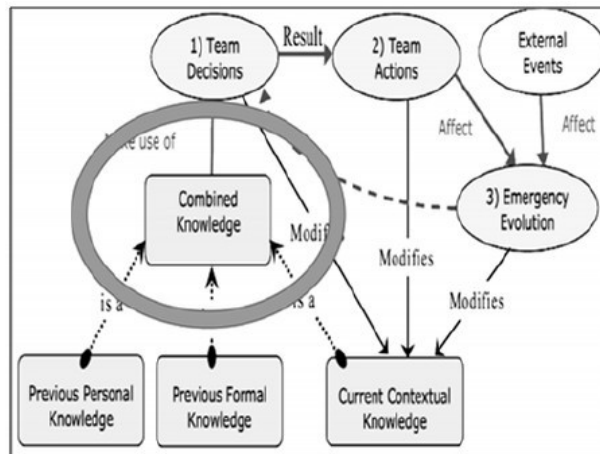
Change management
Safety culture
QA / QM - Lean

Work-as-Done,
everyday practices.
(mostly unknown)

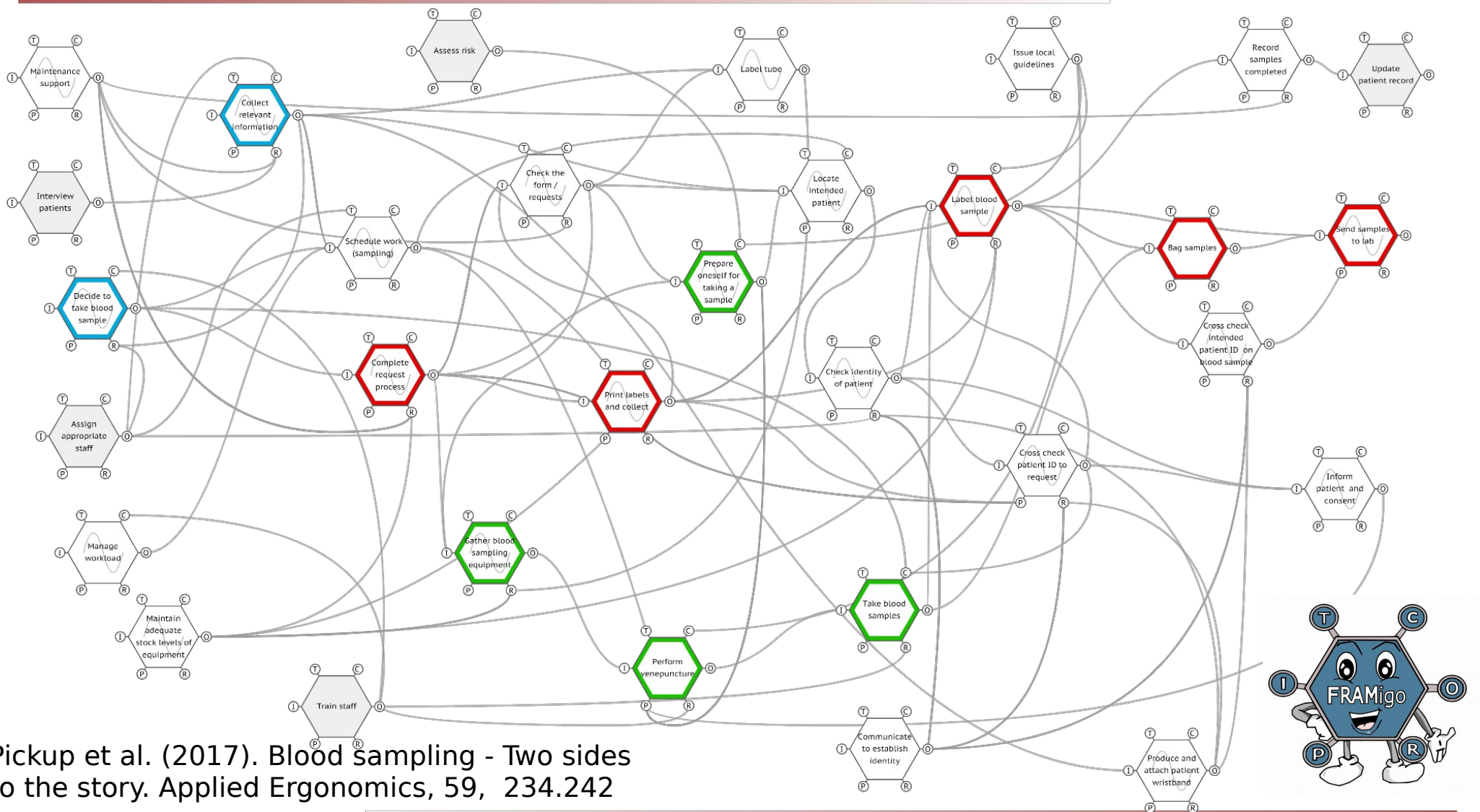
Accidents, losses
Performance indicators
Balanced Scorecards

SafetySynthesis

There are many tools/methods to describe Work-as-Imagined.



... but few to describe Work-as-Done

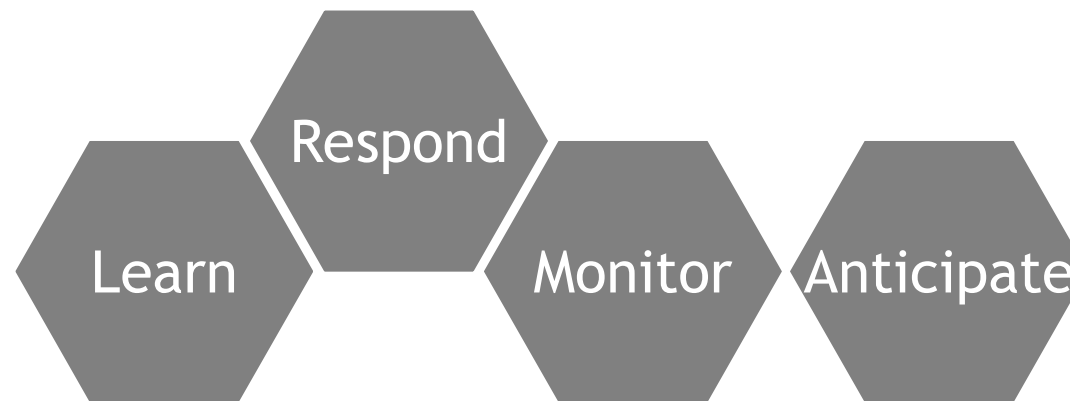


Pickup et al. (2017). Blood sampling - Two sides to the story. *Applied Ergonomics*, 59, 234-242

Potentials for resilient performance

The four potentials for resilient performance can be used as proxy measures of the “position” of an organisation, i.e., how well it functions.

An organisation’s performance is resilient if it can function as required under expected and unexpected conditions alike (changes / disturbances / opportunities).

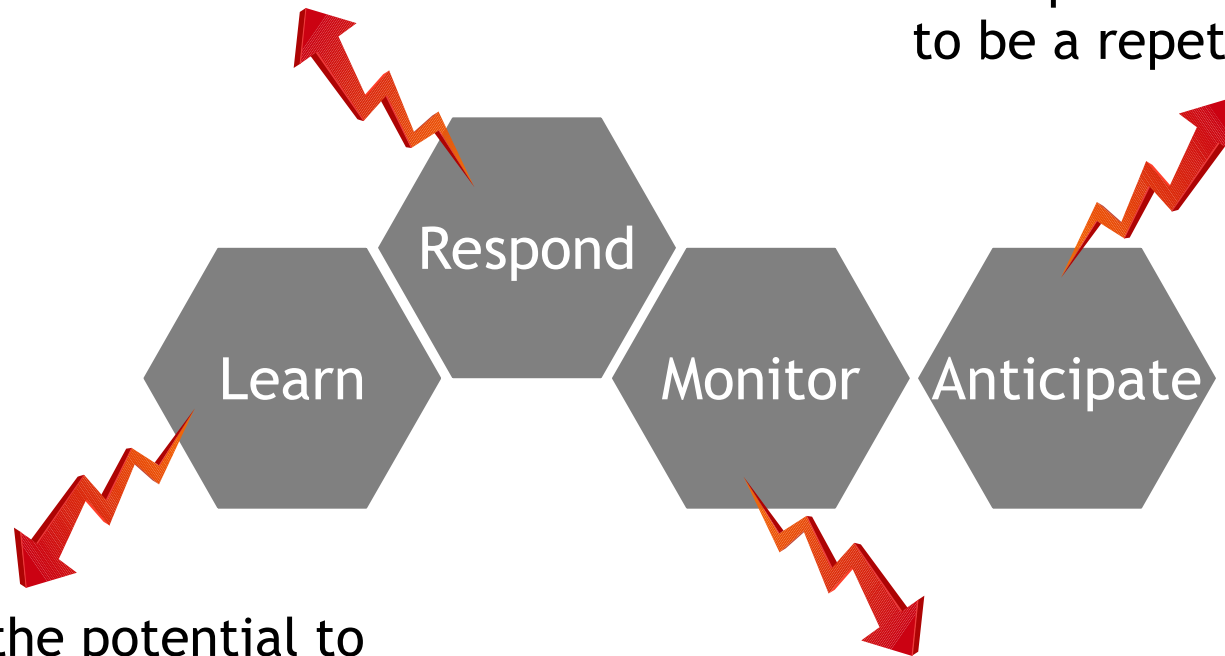


Resilient performance requires that an organisation has the potentials to **respond**, **monitor**, **learn**, and **anticipate**.

Why the four potentials are needed

Without the potential to respond, threats and opportunities will go unanswered.

Without the potential to anticipate the future is assumed to be a repetition of the past.



Without the potential to Learn, the system will always respond in the same way and rely on the same indicators.

Without the potential to monitor, everything that happens will be a surprise

As high as reasonably practicable



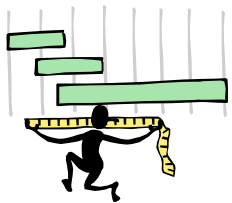
Respond

For which events is there a response ready?

What is the threshold of response?

How many resources are allocated to response readiness?

...



Monitor

How have the indicators been defined?

How many indicators are leading and how many are lagging?

What is the delay between measurement and interpretation?

....



Learn

What is the learning based on (successes – failures)?

Is learning continuous or event-driven?

How are the effects of learning verified and maintained?

...



Anticipate

What is the implicit/explicit “model” of the future?

How far does the organisation look ahead (“horizon”)?

What risks are the organisation willing to take?

...

The Resilience Assessment Grid (RAG) SafetySynthesis



		Target*	Status
Event list	Is there a prepared list of possible and potential events or conditions for which the system should be ready to respond?		
Relevance of event list	Has the list been verified and/or is it revised on a regular basis?		
Response set	Have responses been planned and prepared for every event in the list? Do people know what to do when one of these events occur?		
Relevance of response set	Does the system check that the responses are adequate? How, and how often, is this done?		
Response start and stop	Are the triggering criteria or threshold well defined? Are there clear criteria for when to return to a "normal" state?		
Activation & duration	Can an effective response be activated fast enough? Can it be sustained as long as needed?		
Response capability	Are there sufficient support and resources to ensure response readiness (people, equipment, materials)?		
Verification	Is the readiness to respond (response capability) adequately maintained? Is the readiness to respond verified regularly?		
		Target	Status
Indicator list	Does the organisation have a list of regularly used performance indicators?		
Relevance	Is the list verified and/or revised on a regular basis?		
Validity	Has the validity of indicators been established?		
Delay	Is the delay in sampling indicators acceptable?		
Sensitivity	Are the indicators sufficiently sensitive? Can they detect changes and developments early enough?		
Frequency	Are the indicators measured or sampled with sufficient frequency? (Continuously, regularly, every now and then?)		
Interpretability	Are the indicators / measurements directly meaningful or do they require some kind of analysis?		
Organisational support	Is there a regular inspection scheme or schedule? Is it properly resourced? Are the results communicated and put to use?		
		Target	Status
Selection criteria	Does the organisation have a clear plan for which events to learn from (frequency, severity, value, etc.)?		
Learning basis	Does the organisation try to learn from things that go well or does it only learn from failures?		
Learning style	Is learning event driven (reactive) or continuous (scheduled)?		
Categorisation	Are there any formal procedures for data collection, classification, and analysis?		
Responsibility	Is it clear who is responsible for learning? (Is it a common responsibility or assigned to specialists?)		
Delay	Does learning function smoothly or are there significant delays in the learning process?		
Resources	Does the organisation provide adequate support for effective learning?		
Implementation	How are 'lessons learned' implemented? (Regulations, procedures, training, instructions, redesign, reorganisation, etc.)		
		Target	Status
Corporate culture	Does the corporate culture encourage thinking about the future?		
Acceptability of uncertainty	Is there a policy for when risks / opportunities are considered acceptable or unacceptable?		
Time horizon	Is the time horizon of the organisation appropriate for the kind of activity it does?		
Frequency	How often are future threat and opportunities assessed?		
Model	Does the organisation have a recognisable and articulated model of the future?		
Strategy	Does the organisation have a clear strategic vision? Is it shared?		
Expertise	What kind of expertise is used to look into the future? (In-house, outsourced?)		
Communication	Are the expectations about the future known throughout the organisation?		

Comprises four sets of questions, one for each potential. The questions are:

SPECIFIC – address issues that are important for a concrete organisation.

DIAGNOSTIC – point to details of a potential that are meaningful to assess.

FORMATIVE – answers can be used to make decisions about how to improve potentials.

Resilience Assessment Grid (RAG)

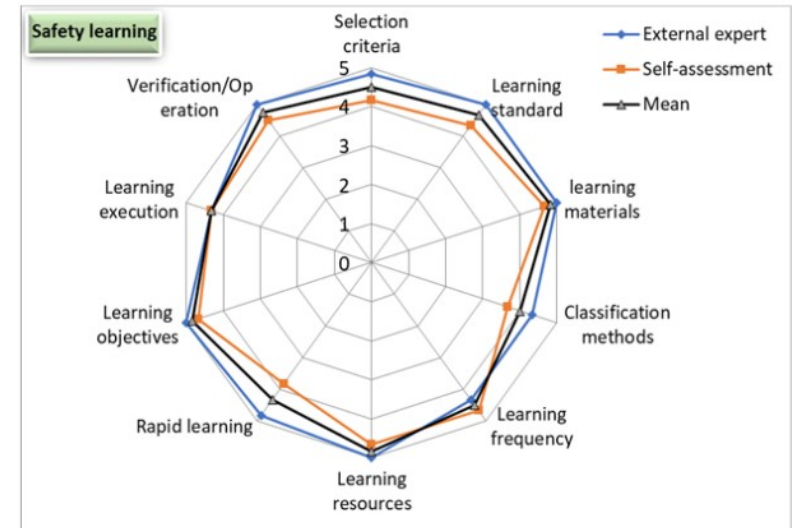
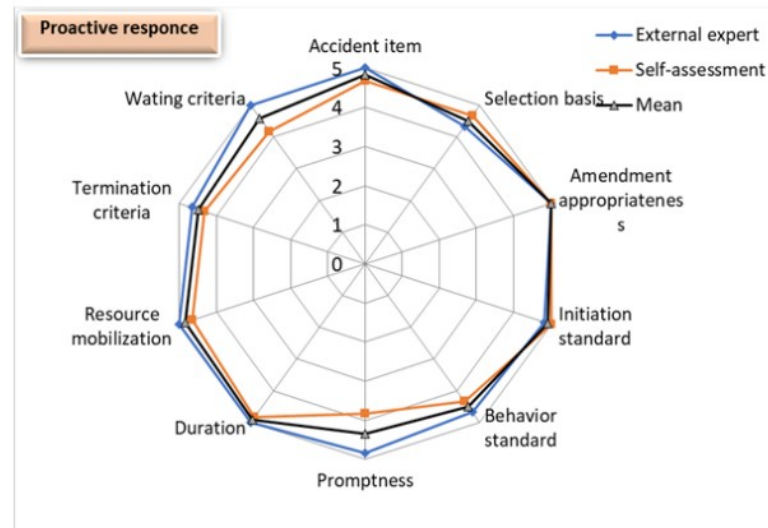
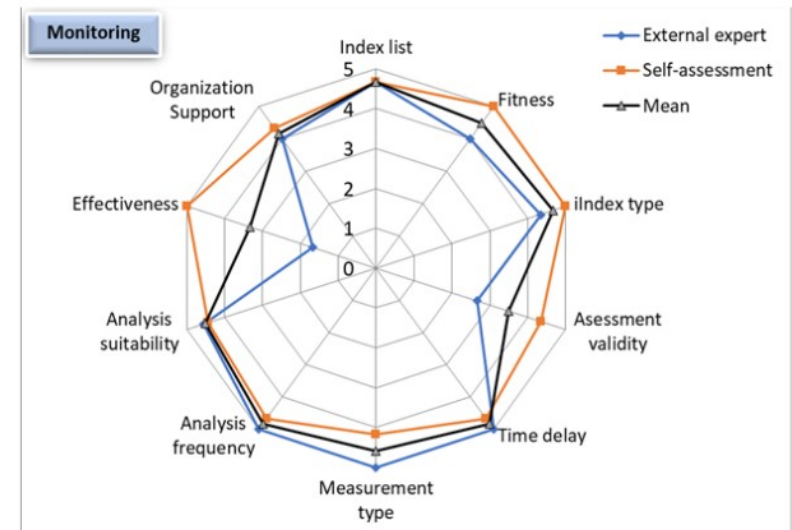
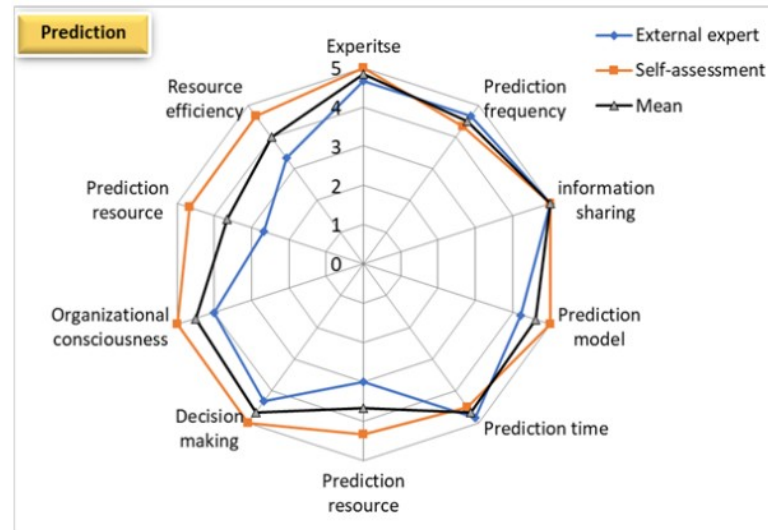


RAG profile for the ability to respond (constructed example)

Resilience Assessment Grid

RAG: Resilience Assessment Grid

How well is an organisation able to Respond, Monitor, Learn and Anticipate?



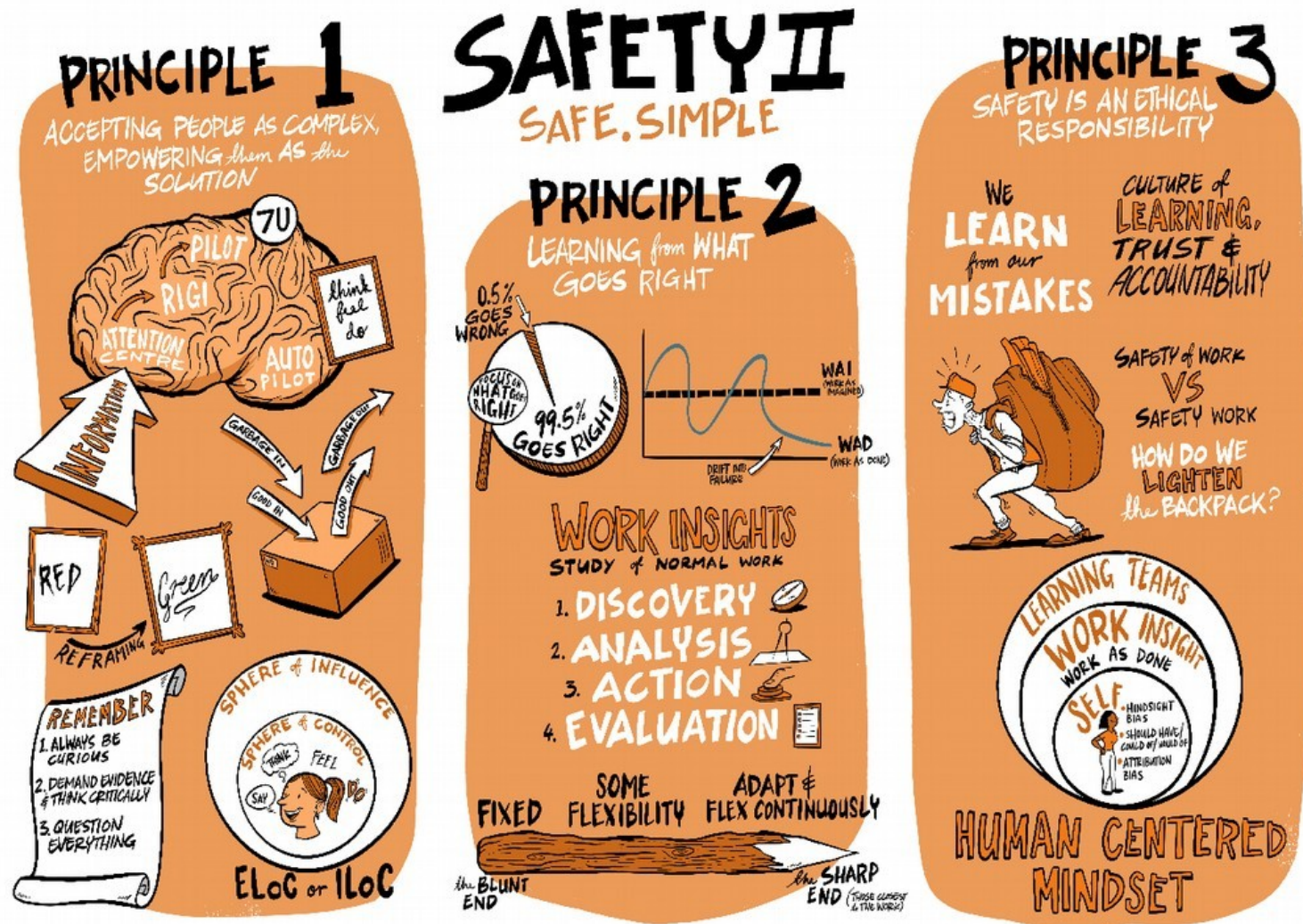
Talk to your neighbour



How do you define how safe you need to be? What is the goal?

How can you determine if developments go in the right direction and with the right speed?

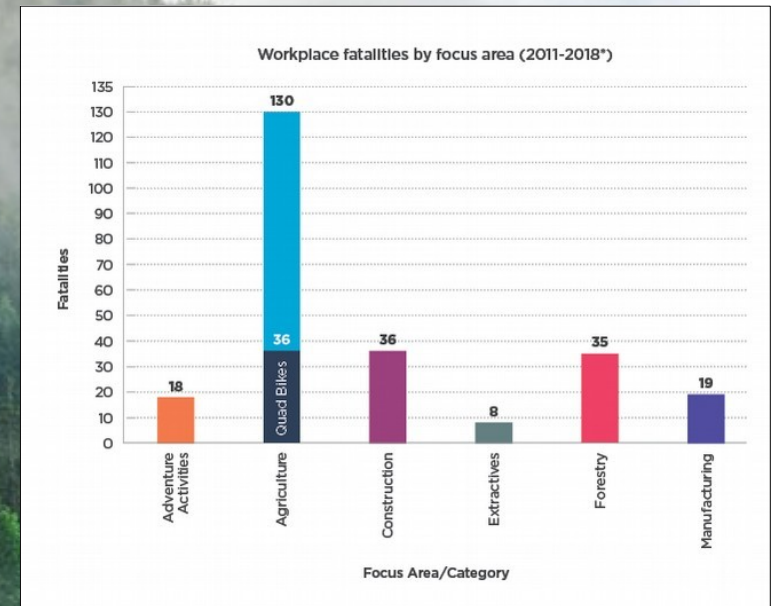
Queensland Urban Utilities



Learning from Work-as-Done in NZ logging *Safety Synthesis*

Response To Fatalities: Fix the failures

- Independent Forestry Review
- Increase mechanisation
- Increase regulation
- Increase certification
- Improve access to information: SafeTree



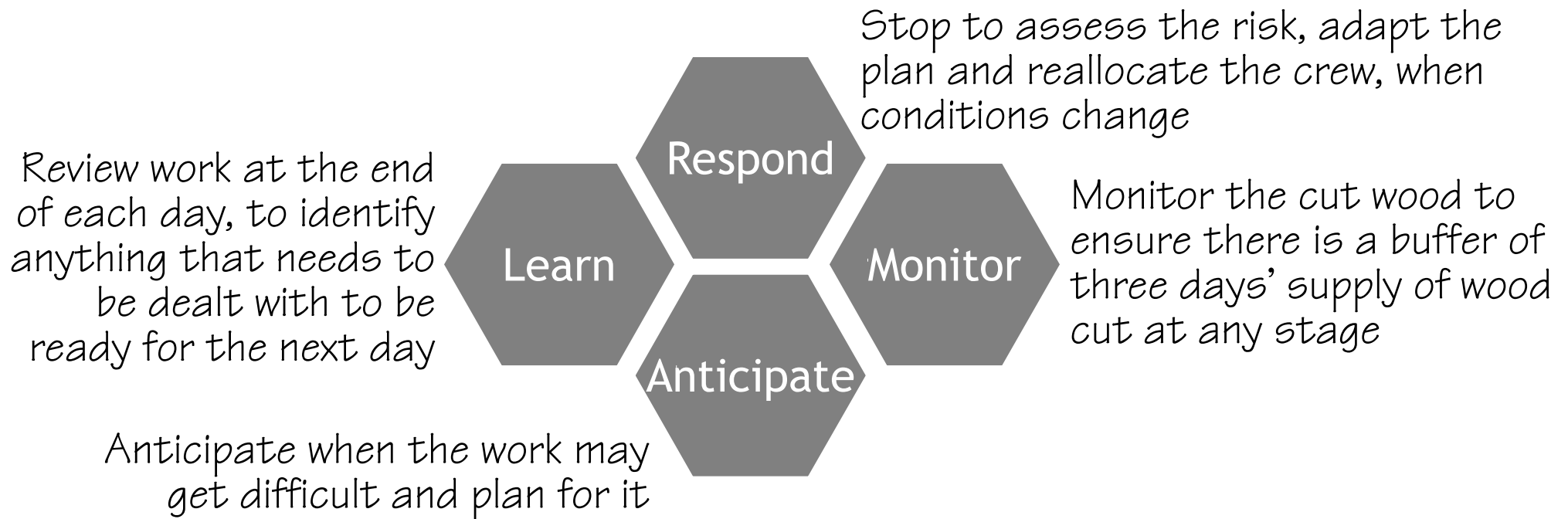
Dr. Hillary Bennett



Lessons from the Learning Teams

Emerging Themes

Inclusive, visible and approachable leadership
Trust, respect and confidence
Teamwork, common goal and collaboration
Cross functional knowledge and skills
Work practices



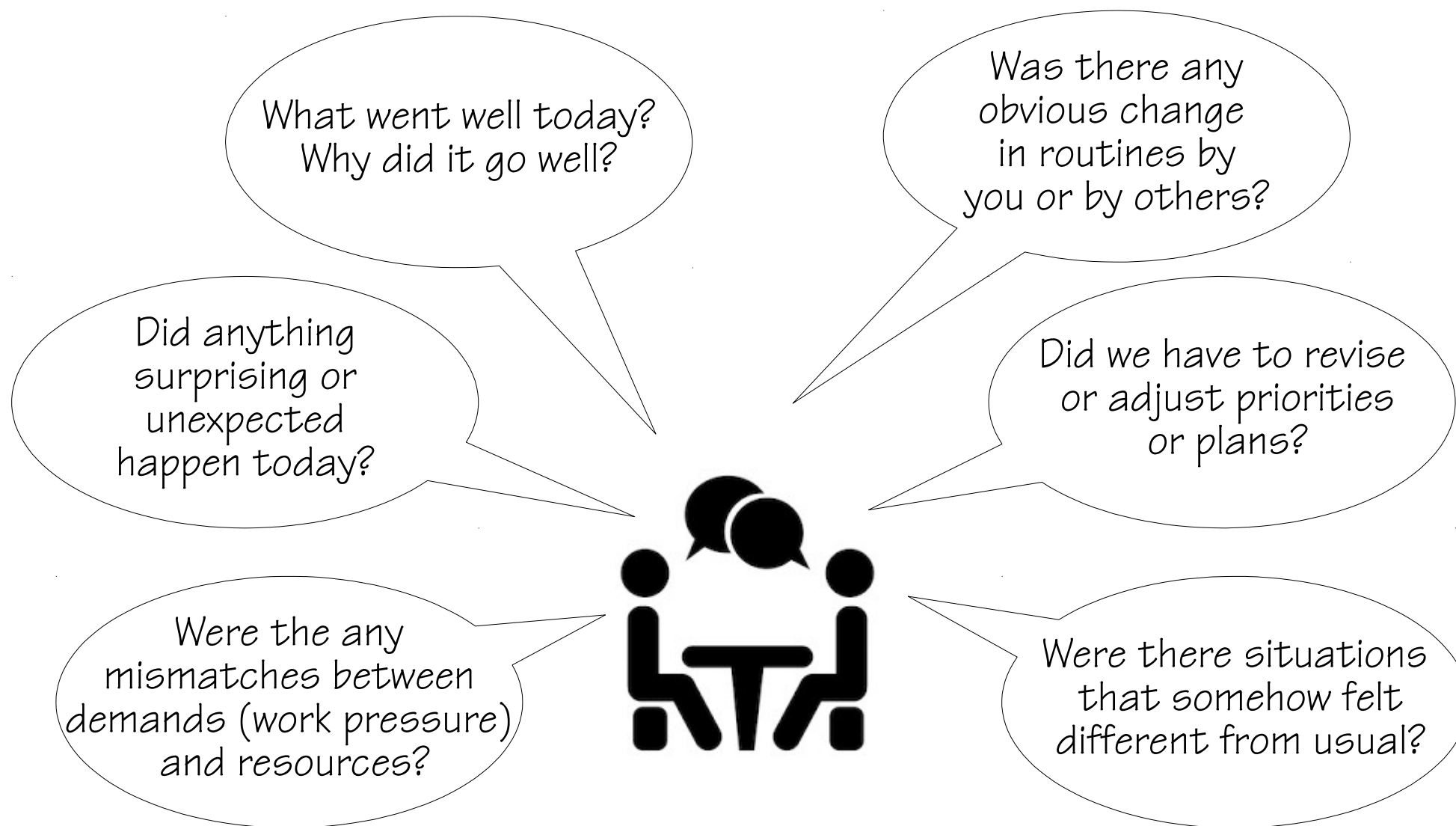
Resilient Performance Enhancement Toolkit *Synthesis*

The purpose of the RPET is to facilitate learning from work that goes well and use the experience to do even better. The RPET aims to ensure that:

- ▶ Learning takes place when work takes place and preferably as a natural part of work, e.g., at the end of each day.
- ▶ Learning takes place where work takes place – from the “coalface” to the boardroom. Learning should be immersed in the work environment and not happen off-site.
- ▶ Learning is by and for the people who do the work. Learning should be based on what they know and remember from the work situation, not what they discover when others ask about it.



RPET guidance questions



RPET data support

12

< Feb >

< 2019 >

Mon	Tue	Wed	Thu	Fri	Sat	Sun
01/28	01/29	01/30	01/31	02/01	02/02	02/03
02/04	02/05	02/06	02/07	02/08	02/09	02/10
02/11	02/12	02/13	02/14	02/15	02/16	02/17
02/18	02/19	02/20	02/21	02/22	02/23	02/24
02/25	02/26	02/27	02/28	03/01	03/02	03/03
03/04	03/05	03/06	03/07	03/08	03/09	03/10

(please select)

Save

Name

Link

Add

Legend

-  A day gone, but not yet discussed
-  A red safety related event
-  An amber safety related event
-  A yellow safety related event
-  A day discussed
-  A lesson learnt
-  A lesson learnt
-  A lesson learnt
-  A day in the future

Conclusions

The consequence of adopting a Safety-II perspective is not that safety should be managed differently.

The consequence is rather that something other than safety should be managed.

The focus should be an organisation's potentials to function as required under expected and unexpected conditions alike (changes / disturbances / opportunities).

The goal is to establish, grow, and maintain the potentials.

The position is the current assessment of the potentials (resilience profile).

The means are to define and implement or sustain changes to the potentials on a functional rather than a structural basis.

It is the dilemma of safety management is that we inadvertently create the complexity of **tomorrow** by trying to solve the problems of **today** with the mindset of **yesterday**.