Accident models

MEC-E3004 Safety management in complex sociotechnical systems

Teemu Reiman

MEC-E3004 Safety management in complex sociotechnical systems

- Course consists of:
  - Lectures and course material
  - Learning logs after each lecture
  - Mid-term assignment (accident case)
  - Final paper on a selected topic
- Course lecturer: PhD (Psych.), Teemu Reiman (reimanteemu@gmail.com)
- Course assistant is Douglas Owen (douglas.owen@aalto.fi)

- Course material and all accouncements can be found in MyCourses

MEC-E3004 Safety management in complex sociotechnical systems
Tentative agenda and topics of the lectures

1. 2.3. Introduction and the basic concepts of safety management
2. 9.3 Basic concepts: Human Factors and Safety Management (Douglas Owen)
3. **16.3 Accident models**
4. 23.3 Accident case (BP Texas City refinery explosion in 2005)
   - Mid-term assignment
5. 30.3 Organizational learning

6.4 NO LECTURE

13.4 Returning the mid-term assignment

6. 13.4. Safety culture
7. 20.4. Safety leadership
8. 27.4. The basic principles of safety management
9. 4.5 Safety management systems
10. 11.5. Tools of safety management
11. 17.5 Future challenges and new directions of safety management (TIME!)
12. 25.5 Recap and Q&A
    - Deadline for returning the paper 31.5.2023

Previous lecture: Human factors and safety management – human errors

Human factors and errors

- Information processing – our brains try to make sense of what is happening, join the dots, form patterns
- Performance variability – heuristics, path of least effort, effect of context – human errors are normal, and occur especially when the task demands exceed individual capabilities
- Systems view – humans, technology and organization interacting within another system, the environment

Human performance and errors

James Reason (author of "Human Error"):

"You cannot change the human condition, but you can change the conditions under which people work"

Sidney Dekker:
People do things that make sense to them, given their goals, understanding of the situation and focus of attention at that time

David Woods et al:
"'human error' has evolved from cause, to effect, to mere attribution, that has more to do with those who struggle with a failure in hindsight than with the people caught up in a failing system at the time"

On human errors and organizational factors

In safety management, two opposite views on human error have prevailed (modified from Dekker 2011)

Human error as a competence problem

- Human error is the *cause* of trouble
- Human error can be the conclusion of an investigation
- Human error is itself a useful target for intervention
- Technology and organizations are inherently safe – they just need protection from unreliable humans

Human error as an organizational issue

- Human error is a *symptom* of trouble deeper inside the organization
- Human error is a starting point for deeper investigation
- Meaningful intervention lies in the factors that help produce [both] human expertise and error
- Technology and organizations are not inherently safe – people create safety

In safety management, two opposite views on human error have prevailed (modified from Dekker 2011)

Human error as a competence problem

- Human error is the *cause* of trouble
- Human error can be the conclusion of an investigation
- Human error is itself a useful target for intervention
- Technology and organizations are inherently safe – they just need protection from unreliable humans

THE "OLD" VIEW

THE "NEW" VIEW

Human error as an organizational issue

- Human error is a *symptom* of trouble deeper inside the organization
- Human error is a starting point for deeper investigation
- Meaningful intervention lies in the factors that help produce [both] human expertise and error
- Technology and organizations are not inherently safe – people create safety

The ”new view” on human error sees errors as social attributions rather than individual attributes

- Sources of error are structural (aka system-induced), not personal
  - Local rationality principle
  - Point is not to see where people went wrong, but why what they did made sense to them at the time
- Errors and accidents are only remotely related
  - Accidents are caused by multiple factors
  - The occasional human contribution to failure occurs because complex systems need an overwhelming human contribution for their safety
- Accidents are not the result of a breakdown of otherwise well-functioning processes
  - Accidents are structural by-products of the system’s normal functioning
  - “errors” are needed for system learning

⇒The enemy of safety is complexity, not human error (Dekker 2011)

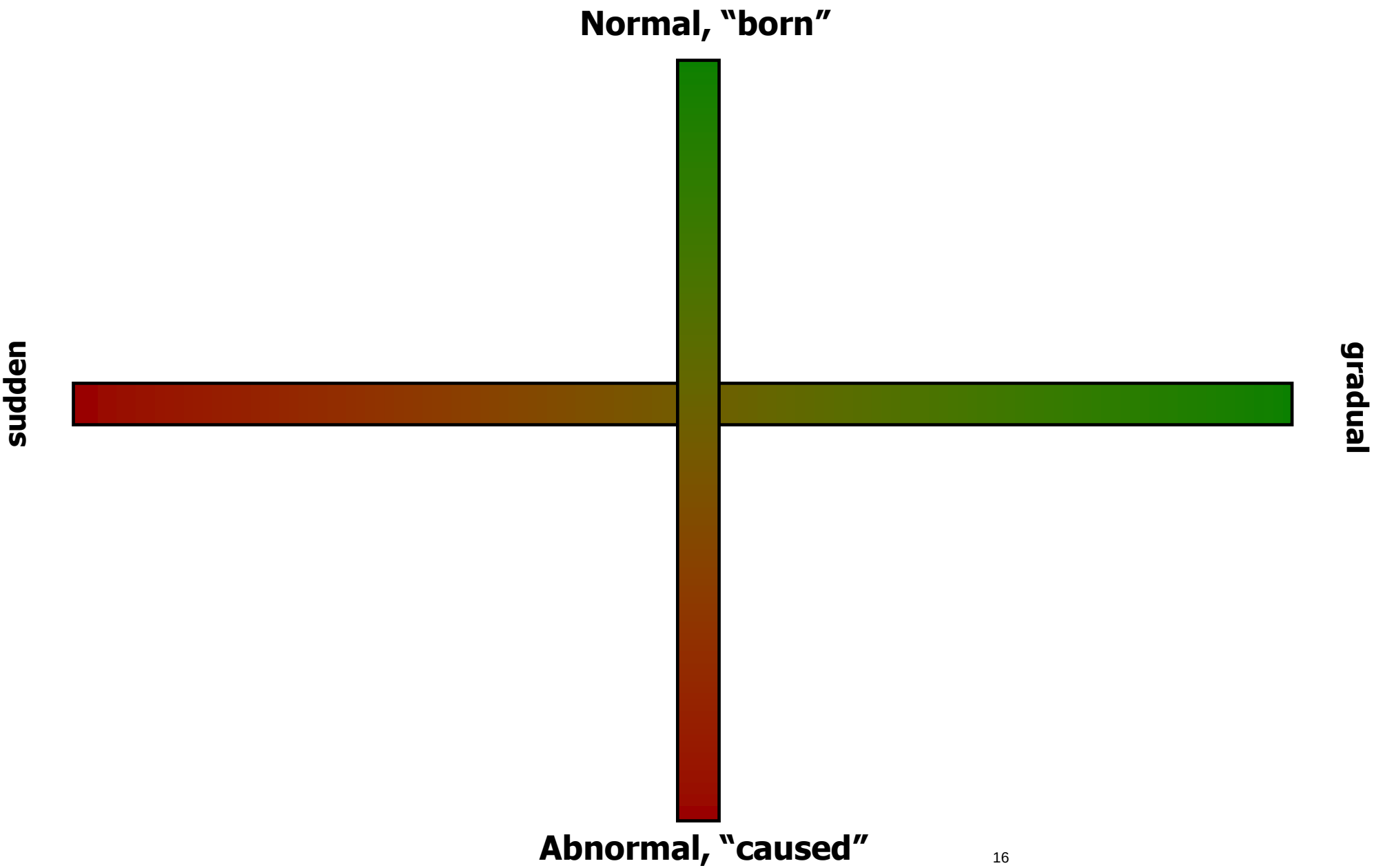
⇒People in complex systems create safety

Accidents models

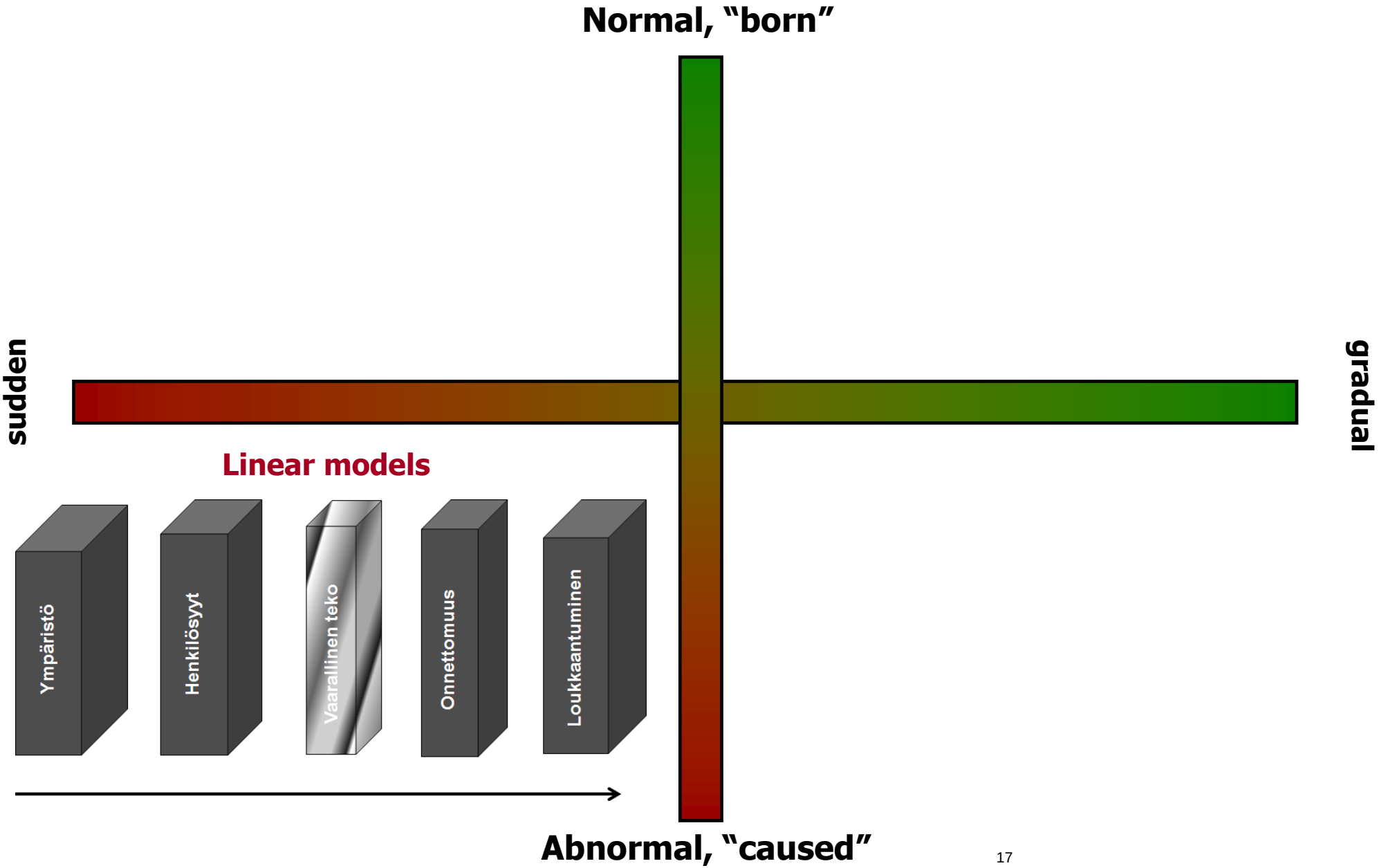
What are accident models

- Accident model is a mental model (an internal belief structure) on
  - Why accidents happen and
  - How a certain accident develops
- Everybody has a more or less explicit and more or less fine-grained accident model
  - Fate and (mis)fortune are still considered as viable ”factors” in accidents (but seldom in safety)
  - People have a need for making sense of events: even a wrong explanation is better than no explanation at all (cf. pattern matching)
- Also the artefacts of the organization (i.e. safety management systems, work practices) have in them embedded some model of accidents
- Accident models affect the way people handle small incidents, how they think about the current safety level, where they devote their attention, and ultimately how the safety culture of the organization develops
- Quite many people still hold accident models where fate, bad luck and individual stupidity play a major part
  - This model can be called the “model of justified accidents”
  - One reason for the prevalence of this model is our tendency to attribute traits to people on the basis of their visible behaviour, and our tendency to believe in a just and orderly world (the fundamental attribution bias)

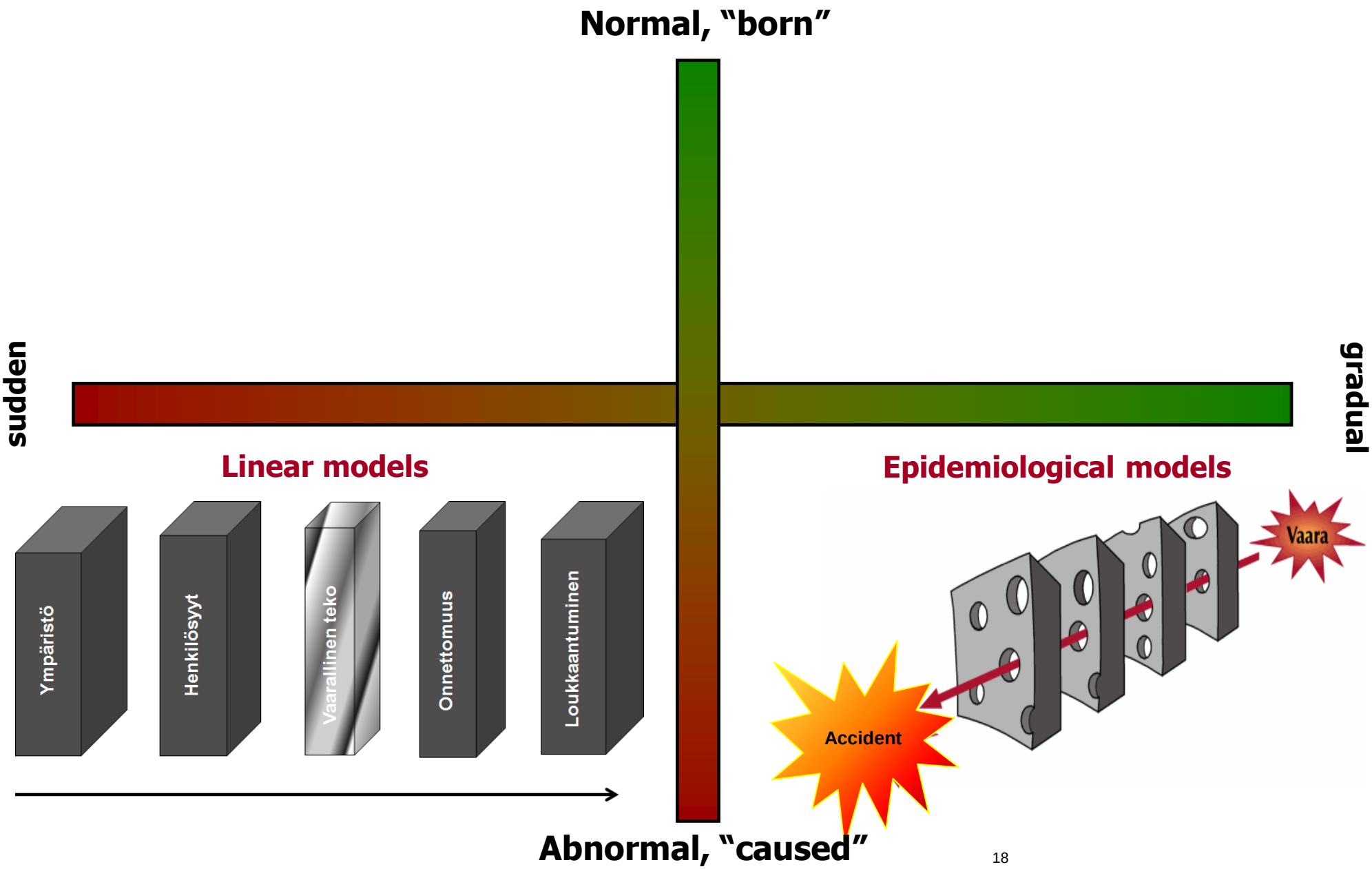
Accident models differ in whether accidents are seen as normal or abnormal phenomena and in how those phenomena happen in time



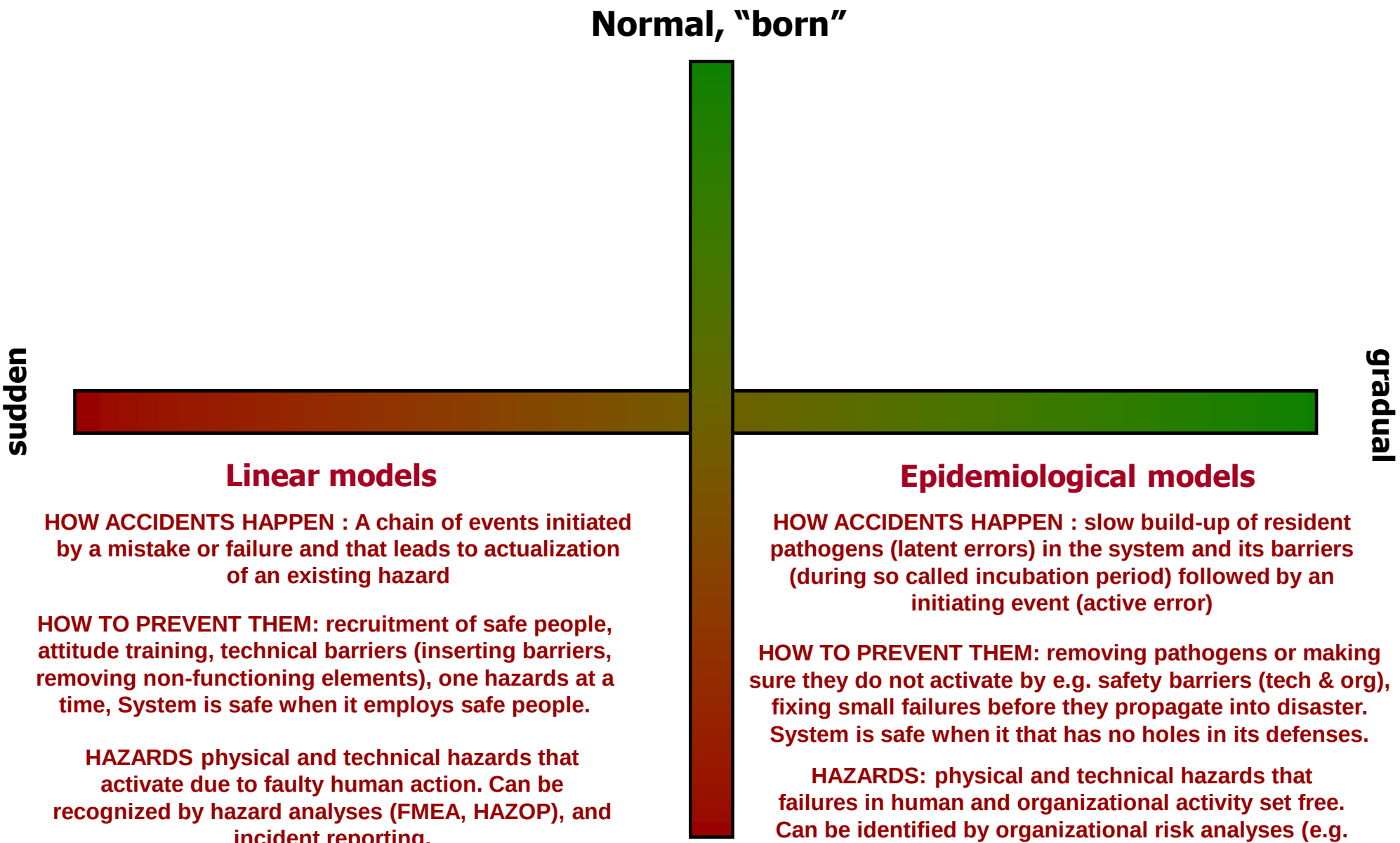
Accident models differ in whether accidents are seen as normal or abnormal phenomena and in how those phenomena happen in time



Accident models differ in whether accidents are seen as normal or abnormal phenomena and in how those phenomena happen in time



Accident models differ in whether accidents are seen as normal or abnormal phenomena and in how those phenomena happen in time



Linear models

HOW ACCIDENTS HAPPEN : A chain of events initiated by a mistake or failure and that leads to actualization of an existing hazard

HOW TO PREVENT THEM: recruitment of safe people, attitude training, technical barriers (inserting barriers, removing non-functioning elements), one hazards at a time, System is safe when it employs safe people.

HAZARDS physical and technical hazards that activate due to faulty human action. Can be recognized by hazard analyses (FMEA, HAZOP), and incident reporting.

Epidemiological models

HOW ACCIDENTS HAPPEN : slow build-up of resident pathogens (latent errors) in the system and its barriers (during so called incubation period) followed by an initiating event (active error)

HOW TO PREVENT THEM: removing pathogens or making sure they do not activate by e.g. safety barriers (tech & org), fixing small failures before they propagate into disaster. System is safe when it that has no holes in its defenses.

HAZARDS: physical and technical hazards that failures in human and organizational activity set free. Can be identified by organizational risk analyses (e.g. MORT, fault trees), and operating experience systems.

Latent versus active failures – key concepts in epidemiological model of James Reason

- Latent conditions (sometimes also called latent failures) are such features of the system that make it more prone to fail
  - These conditions can be related to technology, personnel, organization, or to their interaction
  - The conditions can weaken the system's defenses, hide some hazards, create gaps and increase opacity & hide information
  - These conditions make active failures more probable and severe in consequences, and can also promote violations (e.g. time pressure, conflicting or poor procedures)
- Active failures are human errors or violations that can have an immediate or quite immediate effect on hazards or the system defenses
  - typically not a sign of incompetence, but rather a combination of contextual, task and person related factors
- Instead of putting too much focus on preventing active failures, focus should be put on identifying and correcting latent conditions
  - Changing negative conditions into positive capabilities

Typical latent conditions and root causes as identified in event investigations

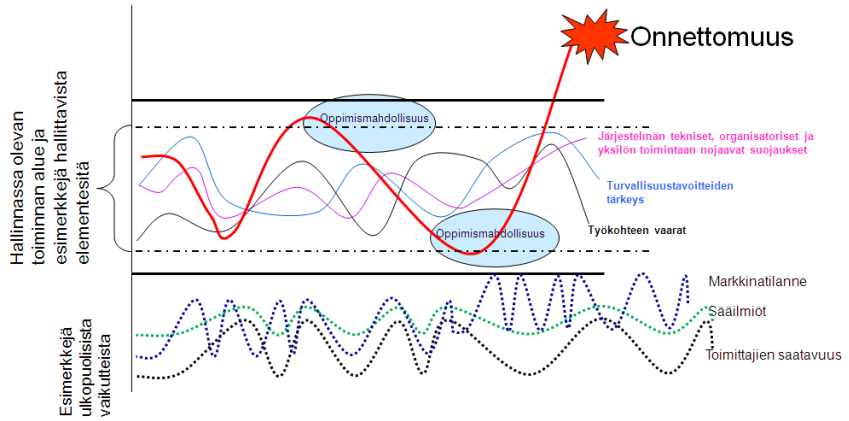
- Deficiencies in planning and organizing of work
- Lack of competence and training
- Workload and stress
- Inadequate rules or procedures
- Deviation from rules or procedures
- Inadequate interface design
- Inadequate tools or equipment
- Poor communication
- Poor team work
- Ineffective leadership and management

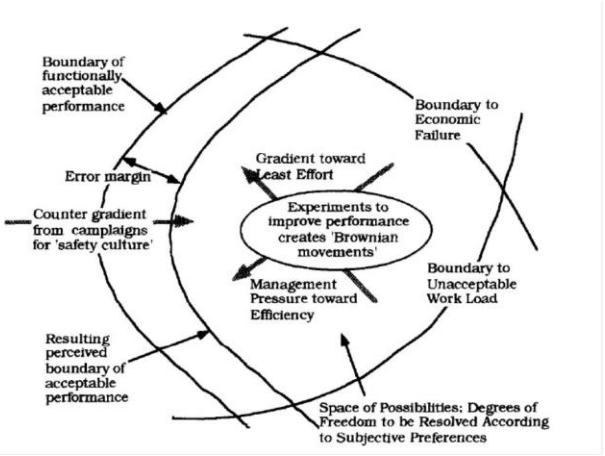
Accident models differ in whether accidents are seen as normal or abnormal phenomena and in how those phenomena happen in time

Open system models

Normal, "born"

Organizational models

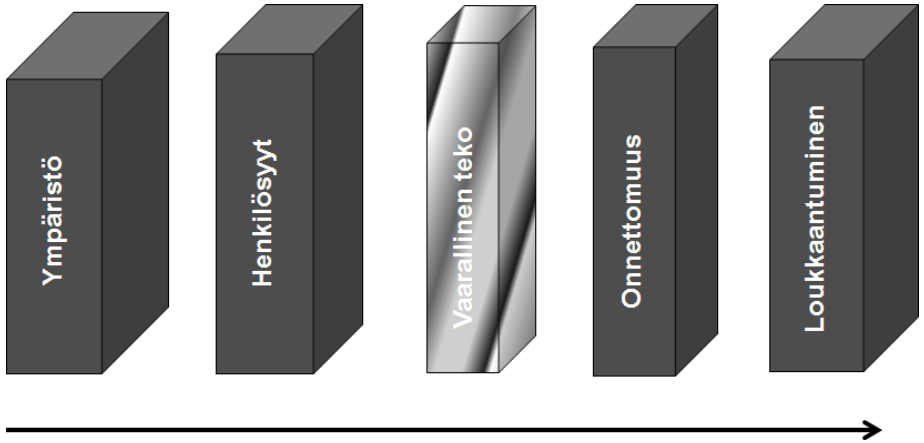




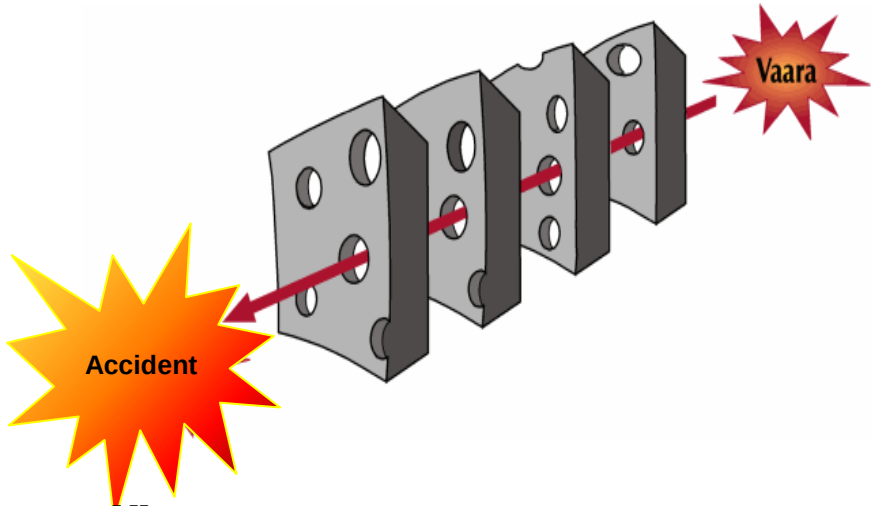
sudden

gradual

Linear models



Epidemiological models



Abnormal, "caused"

Defining the four models (Reiman 2015)

Normal, 'born'

Open system models

HOW ACCIDENTS HAPPEN: normal variability in some parts or elements of the system resonate with variability with other parts causing a stochastic event. Unexpected combinations create hazards.

HOW TO PREVENT THEM: understanding how people and organizations normally function, supporting daily trade-offs, recognizing sources of variability and potential combinations that create hazards

HAZARDS: combination of existing hazards and new emergent situation specific hazards

Organizational models

HOW ACCIDENTS HAPPEN: Organizations gradually drift and develop routines, normalize and simplify their environment until some previously recognized or completely new hazard actualizes.

HOW TO PREVENT THEM: understanding how the organization functions, and the gap between formal and informal organization, making the boundaries of safe activity visible, monitoring the changes in the boundary

HAZARDS: combination of existing latent hazards and new slowly emerging system hazards

sudden

gradual

Linear models

HOW ACCIDENTS HAPPEN : A chain of events initiated by a mistake or failure and that leads to actualization of an existing hazard

HOW TO PREVENT THEM: recruitment of safe people, attitude training, technical barriers (inserting barriers, removing non-functioning elements), one hazards at a time, System is safe when it employs safe people.

HAZARDS physical and technical hazards that activate due to faulty human action. Can be recognized by hazard analyses (FMEA, HAZOP), and incident reporting.

Epidemiological (closed systems) models

HOW ACCIDENTS HAPPEN: slow build-up of resident pathogens (latent errors) in the system and its barriers (during so called incubation period) followed by an initiating event (active error)

HOW TO PREVENT THEM: removing pathogens or making sure they do not activate by e.g. safety barriers (tech & org), fixing small failures before they propagate into disaster. System is safe when it that has no holes in its defenses.

HAZARDS: physical and technical hazards that failures in human and organizational activity set free. Can be identified by organizational risk analyses (e.g. MORT, fault trees), and operating experience systems.

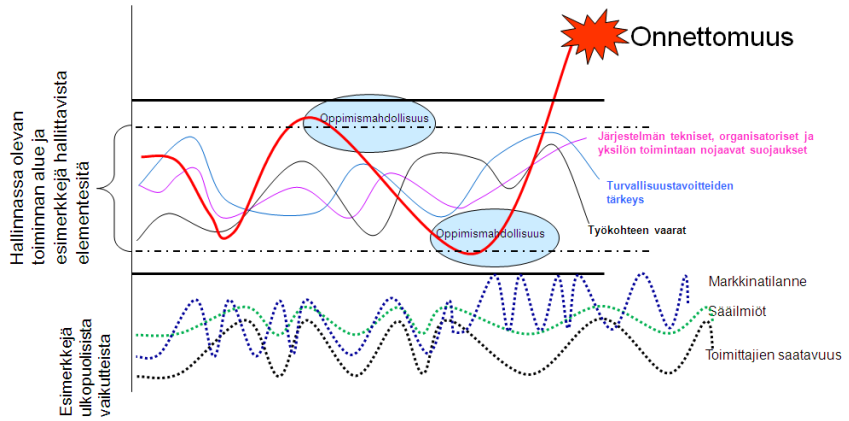
Abnormal, 'caused'

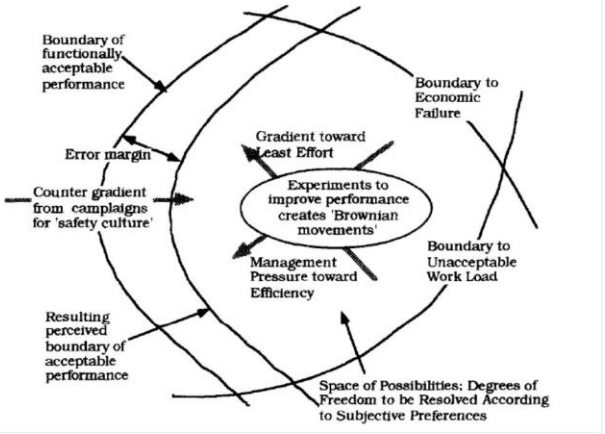
Accident models differ in whether accidents are seen as normal or abnormal phenomena and in how those phenomena happen in time

System models

Normal, "born"

Organizational models

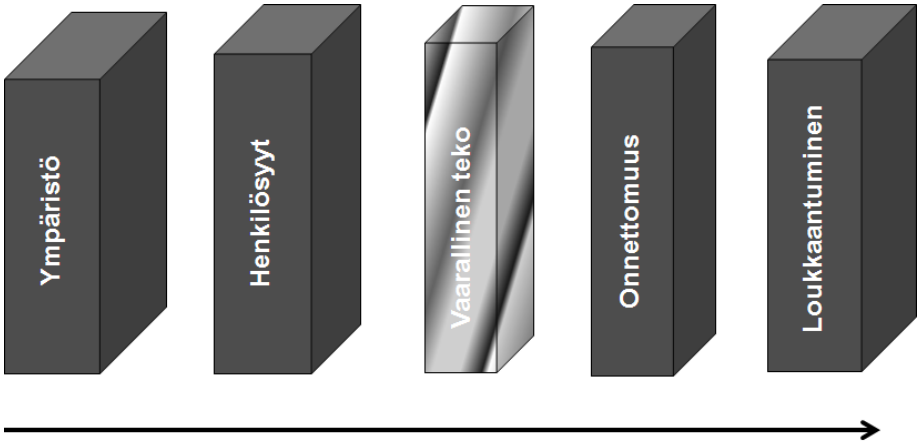




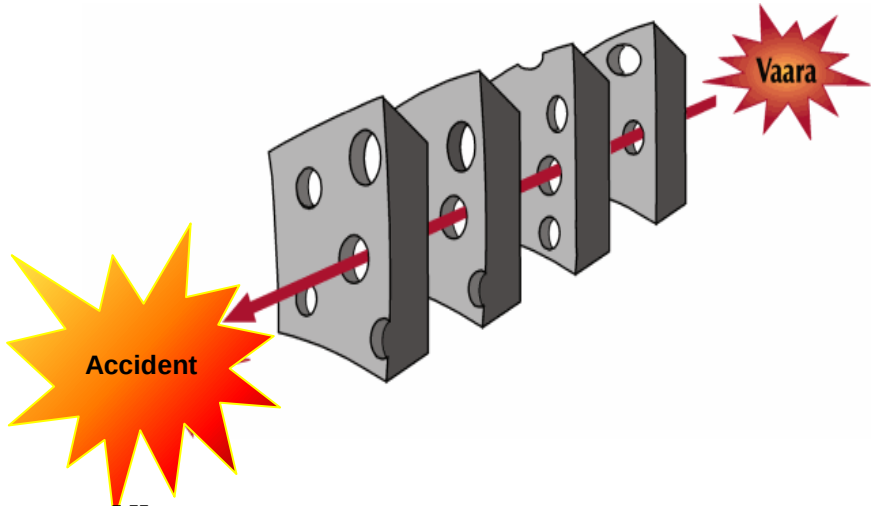
sudden

gradual

Linear models



Epidemiological models

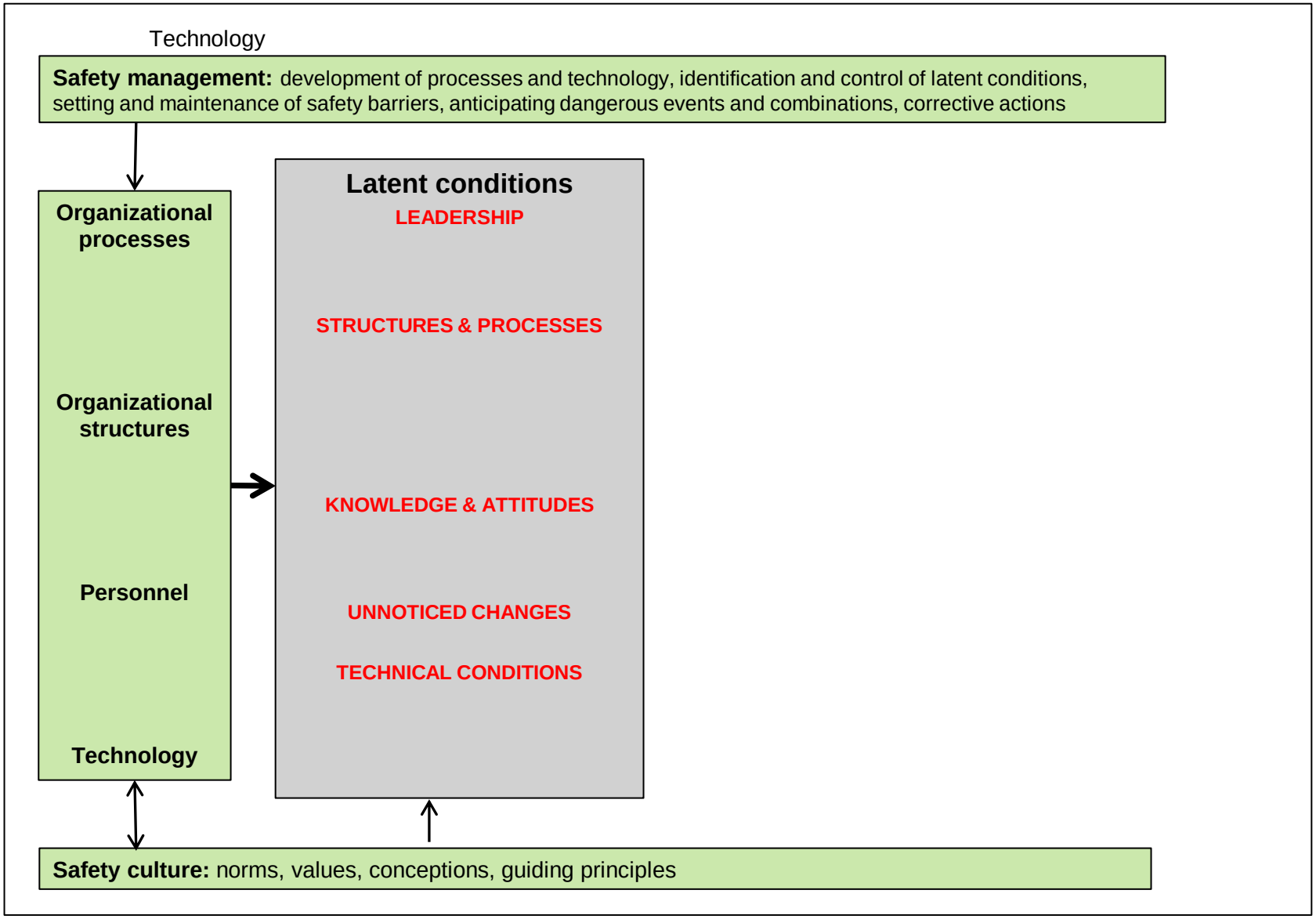


Abnormal, "caused"

Common characteristics of major accidents in modern sociotechnical systems

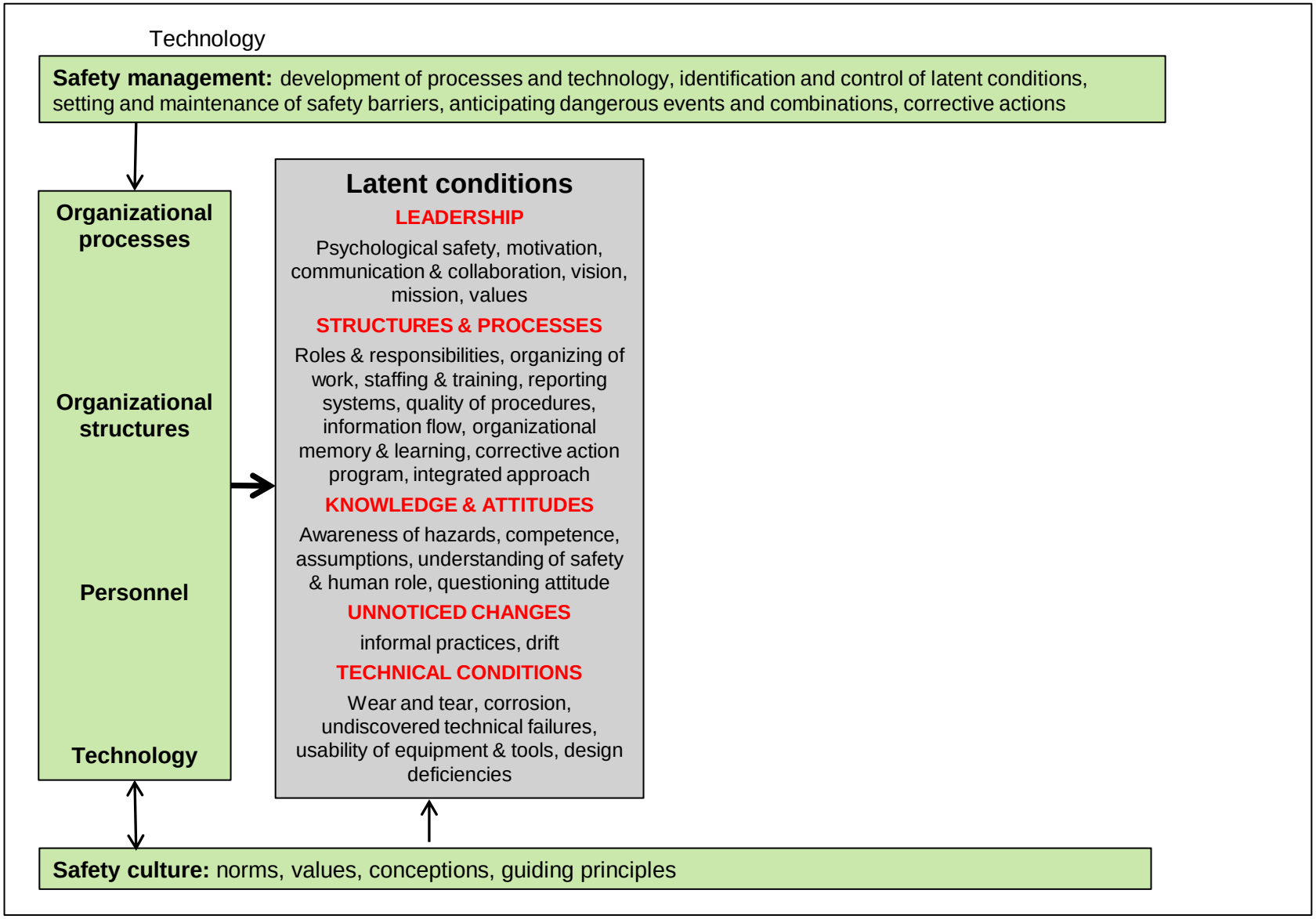
- They rarely have a single cause, a single clear mishap or malfunction as a source
  - On the other hand, ordinary mistakes can do extraordinary damage in complex technological systems
  - Typically adverse conditions develop over time, during so called incubation period
  - During this period there are weak signals that if spotted and investigated could prevent the accident
  - Typically these weak signals are neglected due to either normalizing them, or considering them in isolation as non-significant
  - Thus, *most accidents are unexpected but not sudden*
- Accidents are rarely caused by a single exceptional event but rather they are a consequence of an *unexpected combination of several ordinary events*
- Key terms:
  - Latent conditions / latent mistakes / system weaknesses
  - Performance variability / errors
  - Combinations / interactions / resonance

A simplified accident model illustrating how incidents are born out of a combination of latent conditions, active variability and errors and various concurrent events.



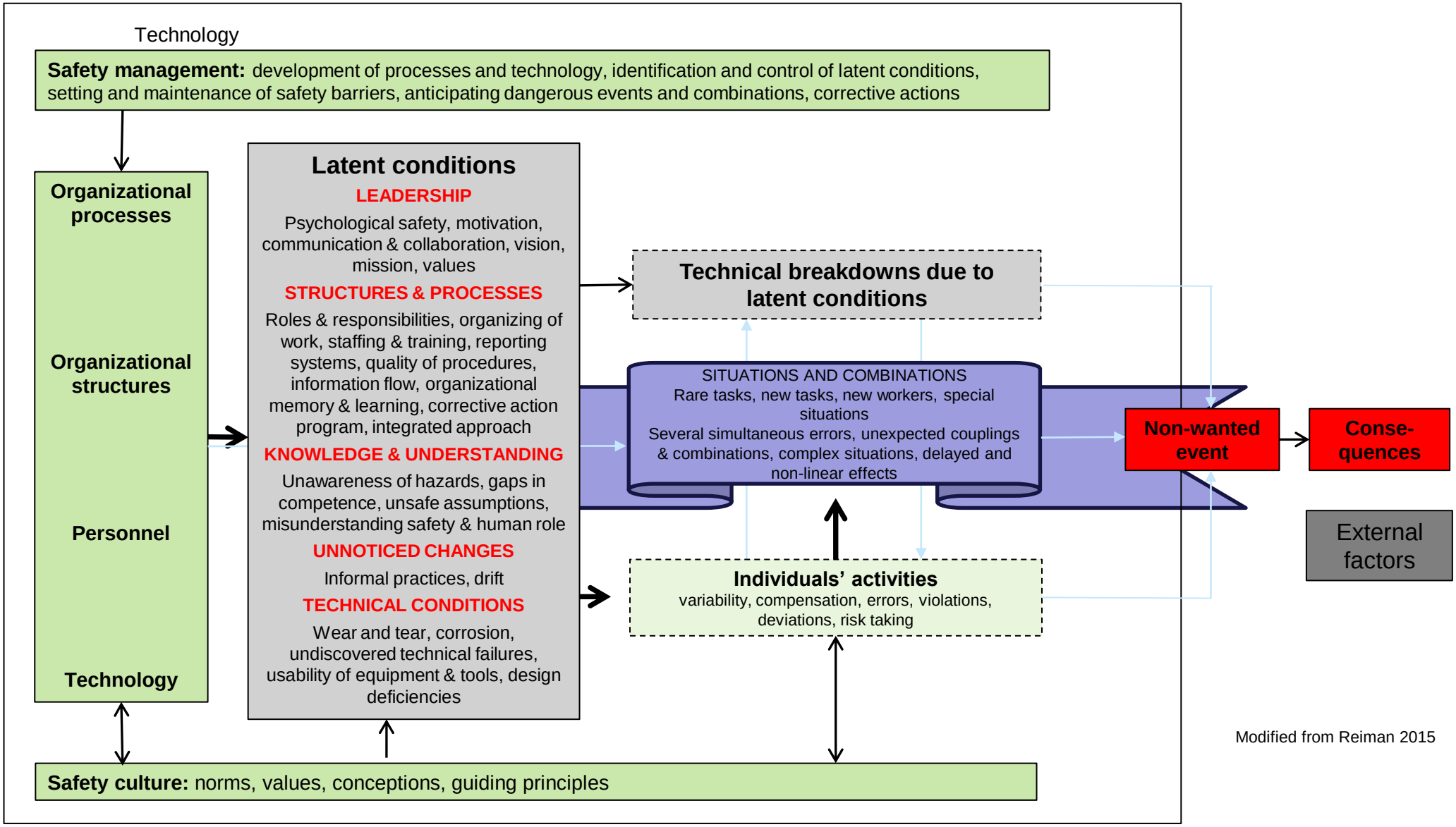
Modified from Reiman 2015

A simplified accident model illustrating how incidents are born out of a combination of latent conditions, active variability and errors and various concurrent events.



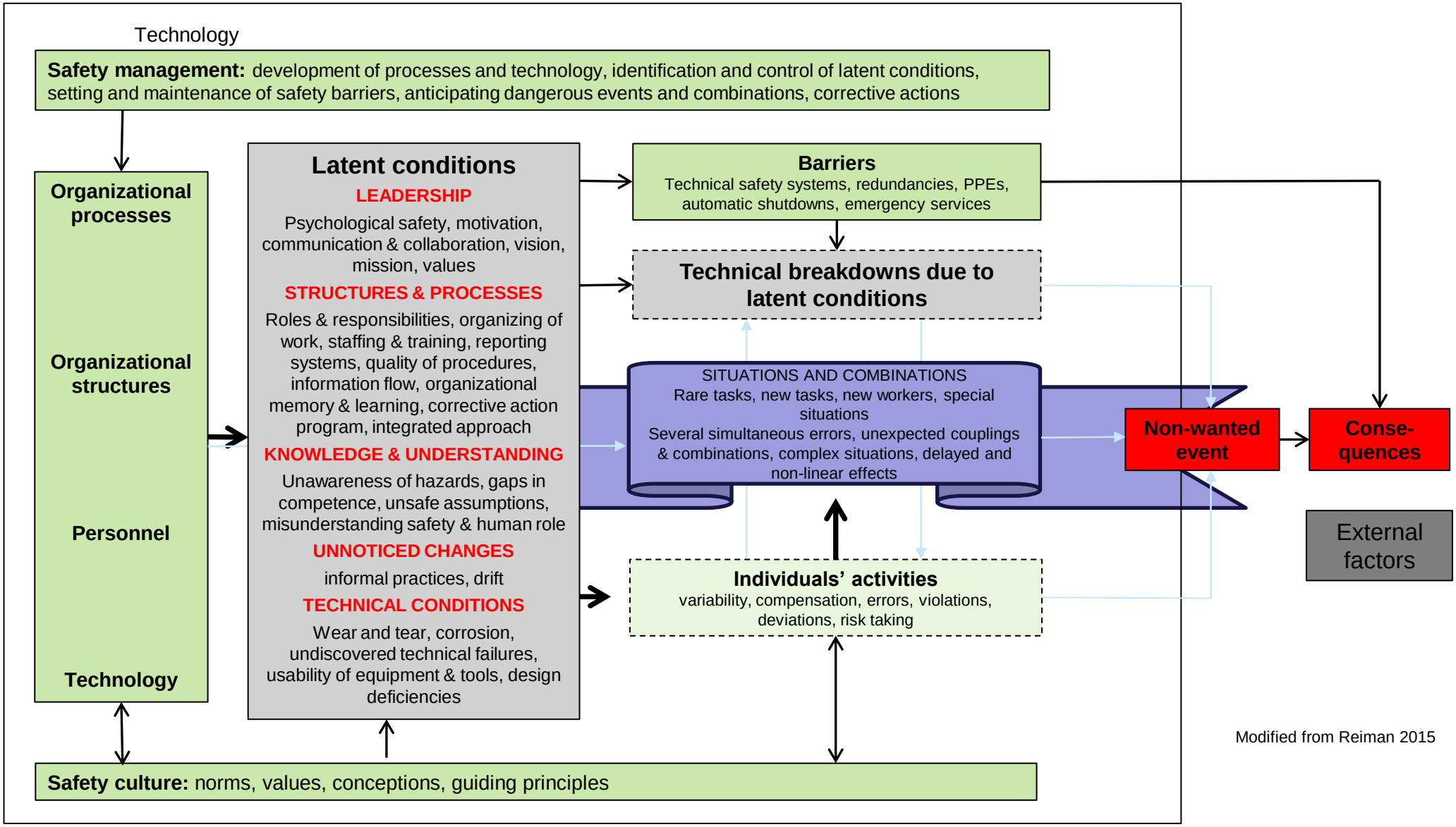
Modified from Reiman 2015

A simplified accident model illustrating how incidents are born out of a combination of latent conditions, active variability and errors and various concurrent events.



Modified from Reiman 2015

A simplified accident model illustrating how incidents are born out of a combination of latent conditions, active variability and errors and various concurrent events.



Modified from Reiman 2015

Most often accidents are caused by the things the organization ignores or does not consider important

"organizations are defined by what they ignore – ignorance that is embodied in assumptions – and by the extent to which people in them neglect the same kinds of considerations" (Weick, 1998, p. 74).

Next lecture

- BP Texas City case example
- Read description from the MyCourses webpage BEFORE the lecture
- No need to remember (or understand) everything in the description – we will go through the case during the next lecture

References

- Dekker S. (2011). Drift into failure. From hunting broken components to understanding complex systems. Farnham: Ashgate.
- HaSPA (Health and Safety Professionals Alliance).(2012). The Core Body of Knowledge for Generalist OHS Professionals. Tullamarine, VIC. Safety Institute of Australia
- Hollnagel, E. (2004). Barriers and Accident Prevention. Hampshire, Ashgate.
- Reason, J. (1997). Managing the risks of organizational accidents. Aldershot: Ashgate.
- Reason, J. (2016). Organizational Accidents Revisited. Farnham, Ashgate.
- Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. Safety Science, 27, 183-213.
- Reiman, T. (2015). Turvallisuusasiantuntijoiden roolit, toimintatavat ja tarvittavat kyvyt ja taidot. VTT Technology 198. Espoo, VTT. Available from: www.vtt.fi/inf/pdf/technology/2014/T198.pdf
- Vaughan D. (1996). The Challenger launch decision. Chicago: University of Chicago Press.
- Weick. K.E. (1998). Foresights of failure: an appreciation of Barry Turner. Journal of Contingencies and Crisis Management, 6, 72-75.
- Woods, D.D., Dekker, S., Cook, R., Johannesen, L., Sarter, N. (2010). Behind Human Error. Second Edition. Ashgate.
- Underwood, P. & Waterson, P. (2013). Accident Analysis Models and Methods: Guidance for Safety Professionals. Loughborough University.
- Underwood, P. & Waterson, P. (2013). Systemic accident analysis: Examining the gap between research and practice. Accident Analysis & Prevention 55, 154-164.
- Sklet, S. (2004). Comparison of some selected methods for accident investigation. Journal of Hazardous Materials 111, 29-37.
- Fu, G., Xie, X., Jia, Q. (2020). The development history of accident causation models in the past 100 years. Process Safety and Environmental Protection 134, 47-82.