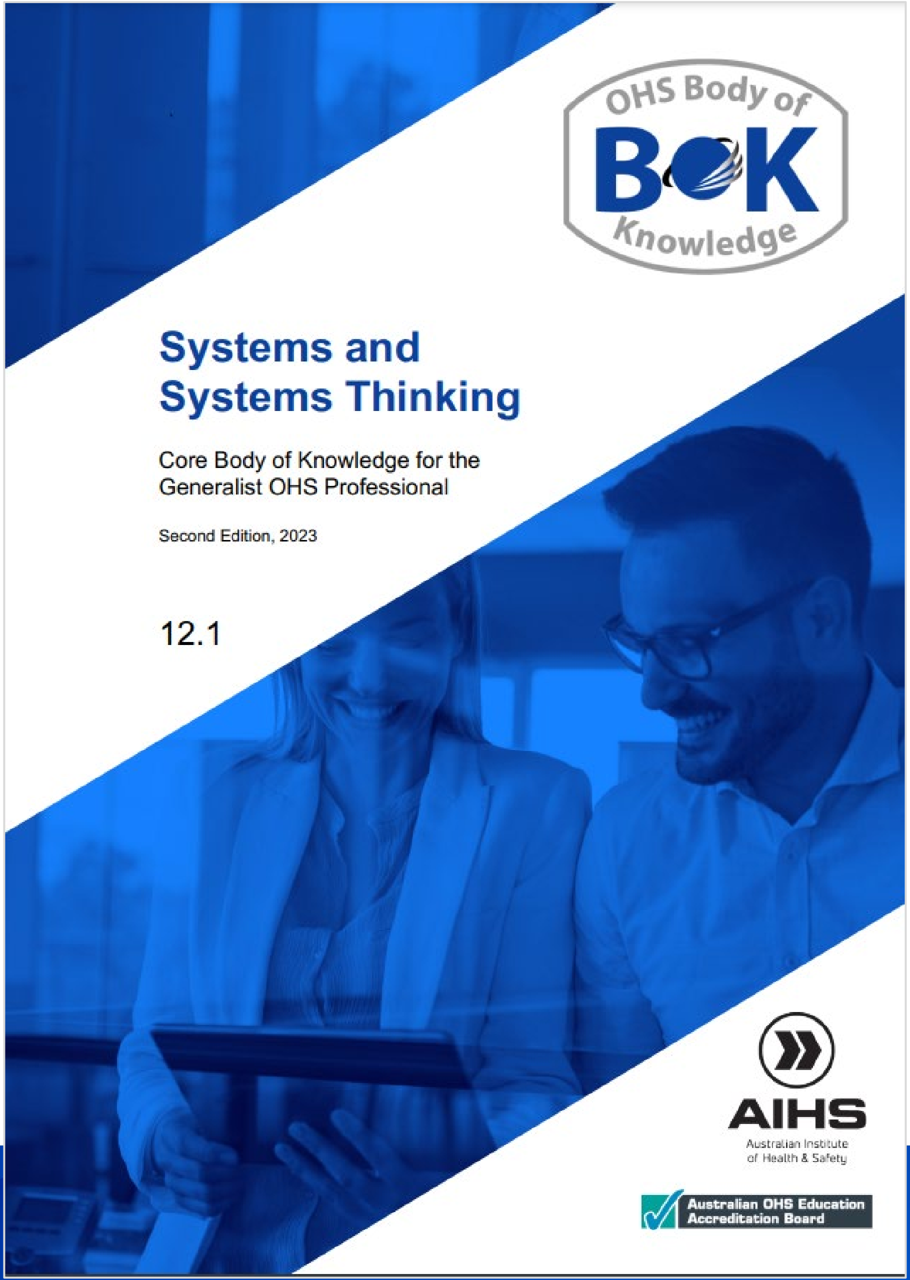
Centre for Human Factors and Sociotechnical Systems

Why do work systems fail? Ten lessons learned about safety and systems failure

Associate Professor Gemma Read

Work Well Conference, Brisbane

17 October 2023


OHS Body of Knowledge
BoK
Systems and
Systems Thinking
Core Body of Knowledge for the
Generalist OHS Professional
Second Edition, 2023
12.1
AIHS
Australian Institute
of Health & Safety
Australian OHS Education
Accreditation Board

What is a system and what is systems thinking?

System:

a set of connected things or devices that operate together (Cambridge)

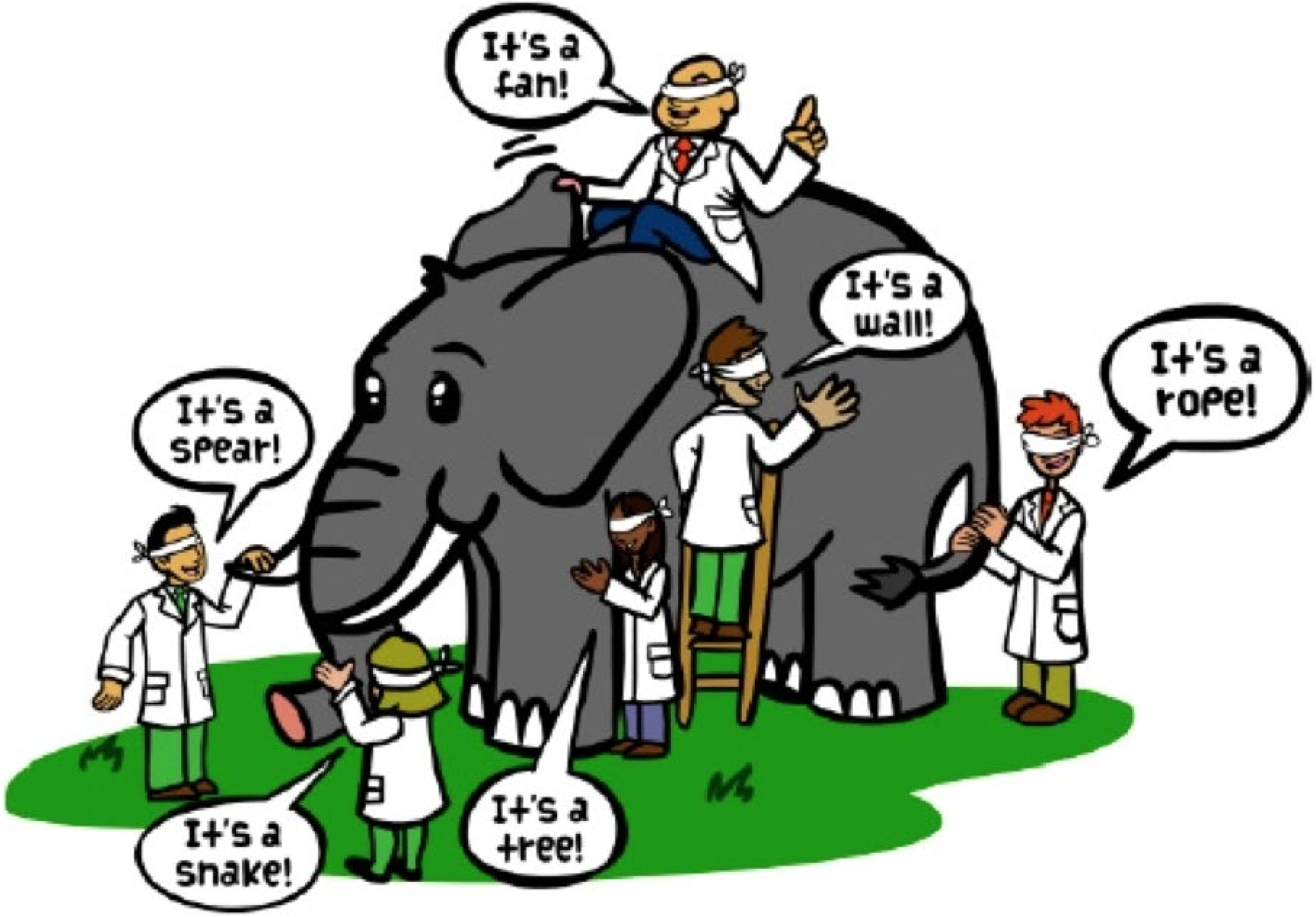
any group of interacting, interrelated, or interdependent parts that form a complex and unified whole that has a specific purpose (Kim, 1999)

an arrangement of parts or elements that together exhibit behavior or meaning that the individual constituents do not (INCOSE)

Systems thinking

"a way of seeing and talking about reality that helps us better understand and work with systems to influence the quality of our lives"

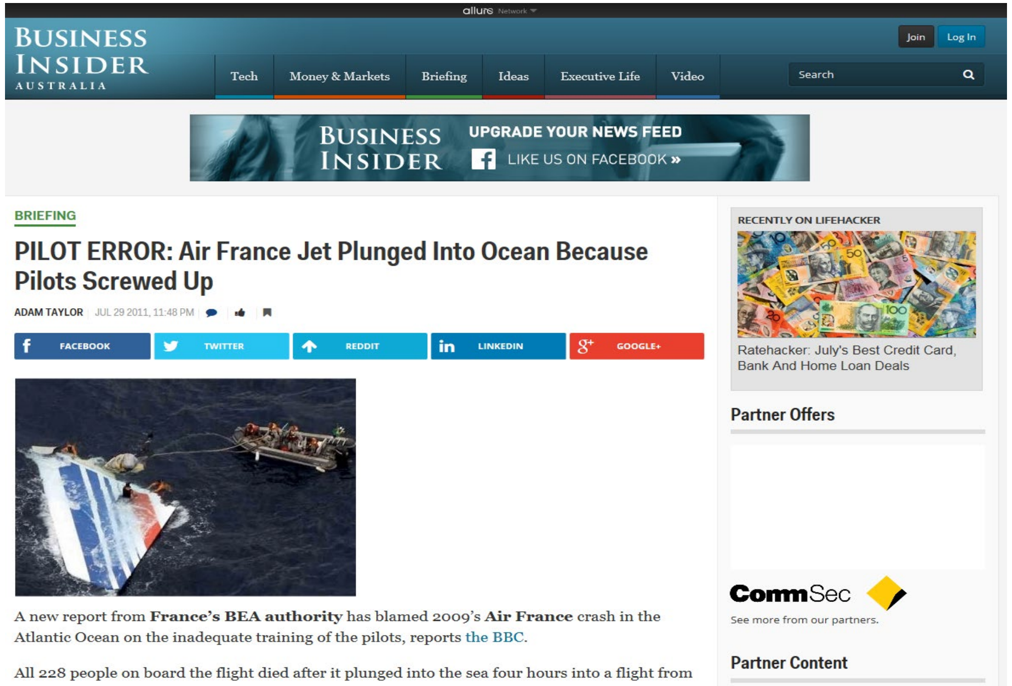
(Kim, 1999)



Work systems are complex systems

- Outcomes emerge from component interactions
- Interactions are non-linear (difficult to predict)
- Systems are influenced by their environment
- Systems are dynamic, constantly changing and evolving
- Systems have a history

Lesson 1. A human error lens is useless (and can be dangerous)



BUSINESS INSIDER AUSTRALIA

Tech | Money & Markets | Briefing | Ideas | Executive Life | Video

BRIEFING

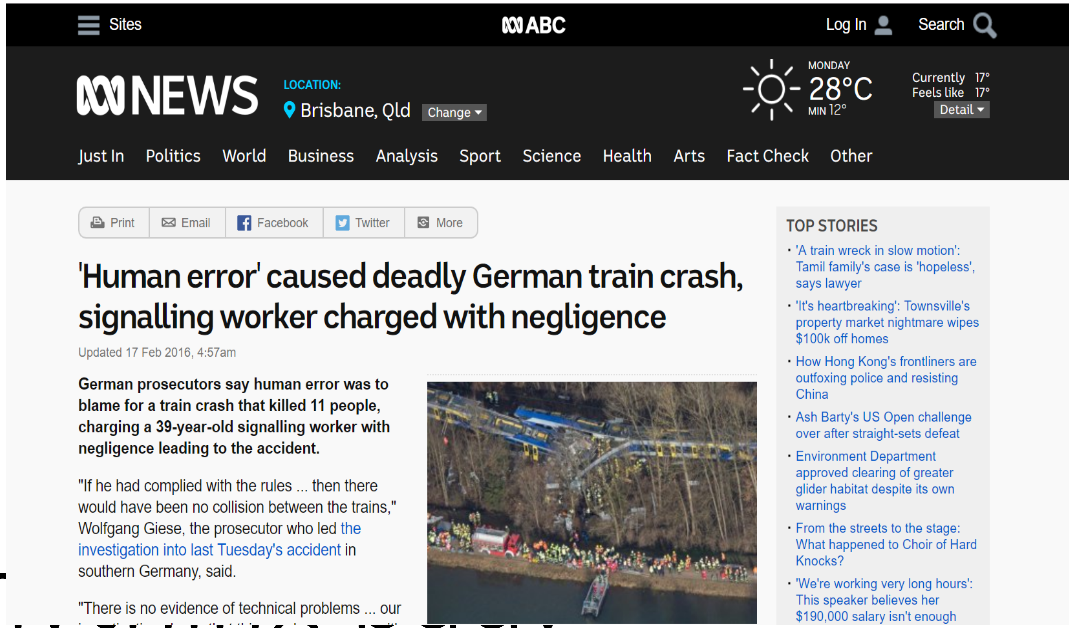
PILOT ERROR: Air France Jet Plunged Into Ocean Because Pilots Screwed Up

ADAM TAYLOR JUL 29 2011, 11:48 PM

FACEBOOK | TWITTER | REDDIT | LINKEDIN | GOOGLE+

A new report from **France's BEA authority** has blamed 2009's **Air France** crash in the Atlantic Ocean on the inadequate training of the pilots, reports the BBC.

All 228 people on board the flight died after it plunged into the sea four hours into a flight from



ABC NEWS

Just In | Politics | World | Business | Analysis | Sport | Science | Health | Arts | Fact Check | Other

'Human error' caused deadly German train crash, signalling worker charged with negligence

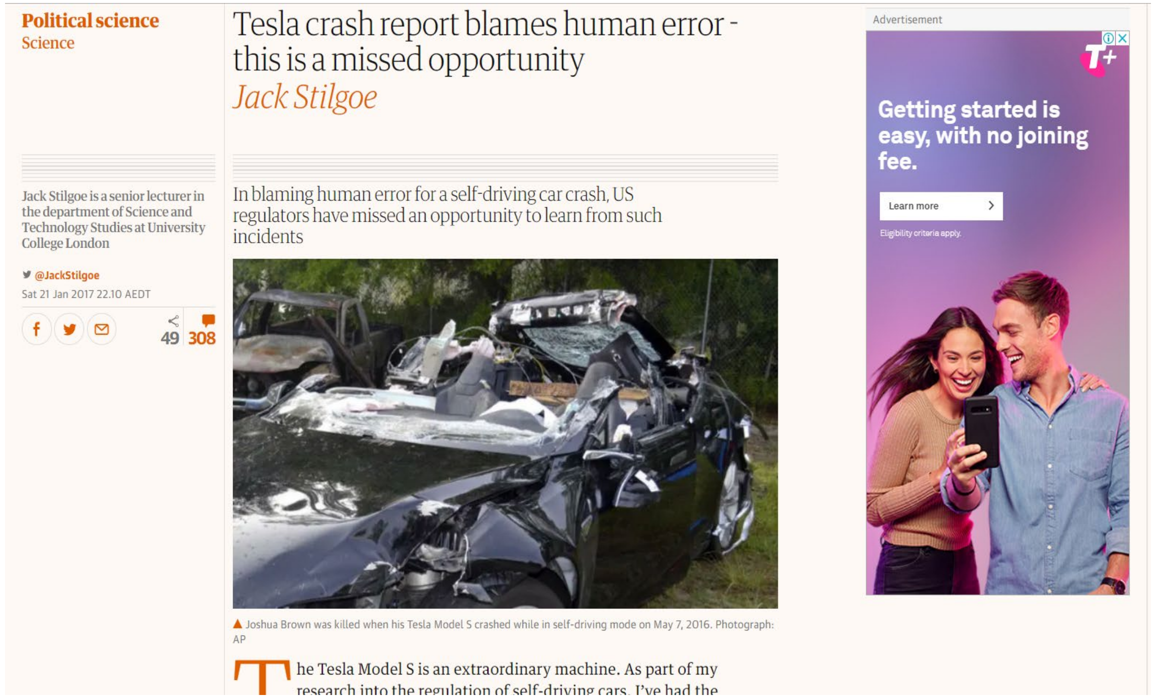
Updated 17 Feb 2016, 4:57am

German prosecutors say human error was to blame for a train crash that killed 11 people, charging a 39-year-old signalling worker with negligence leading to the accident.

"If he had complied with the rules ... then there would have been no collision between the trains," Wolfgang Giese, the prosecutor who led the investigation into last Tuesday's accident in southern Germany, said.

"There is no evidence of technical problems ... our

of ar



Political science
Science

Tesla crash report blames human error - this is a missed opportunity

Jack Stilgoe

Jack Stilgoe is a senior lecturer in the department of Science and Technology Studies at University College London

@JackStilgoe
Sat 21 Jan 2017 22.10 AEDT

In blaming human error for a self-driving car crash, US regulators have missed an opportunity to learn from such incidents

Joshua Brown was killed when his Tesla Model S crashed while in self-driving mode on May 7, 2016. Photograph: AP

The Tesla Model S is an extraordinary machine. As part of my research into the regulation of self-driving cars, I've had the

Researchers: Medical errors now third leading cause of death in United States

By Ariana Eunjung Cha
May 3, 2016 at 6:30 p.m. EDT

These common medical errors are major killers 1:16

A new study by patient safety researchers shows common medical errors may be the third leading cause of death in the U.S. (Video: Deirdra O'Regan/The Washington Post)

Share

Nightmare stories of nurses giving potent drugs meant for one patient to another and surgeons removing the wrong body parts have dominated

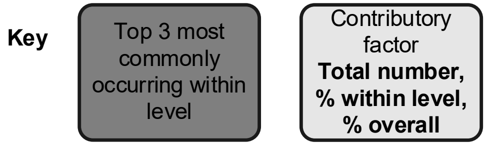
The problem with a human error approach to safety

- It is reductionist
- It is individual and blame focussed
- It overlooks everything we know about the behaviour of complex systems
- It leads to a 'fixing broken components' approach
- It is not aligned with contemporary accident causation models
- It reduces trust and prevents learning

Human error-based safety management

- Training
- Automation
- Procedures
- Reprisals
- Removal

If human error isn't causing accidents, what is?



Incident / accident contributory factors

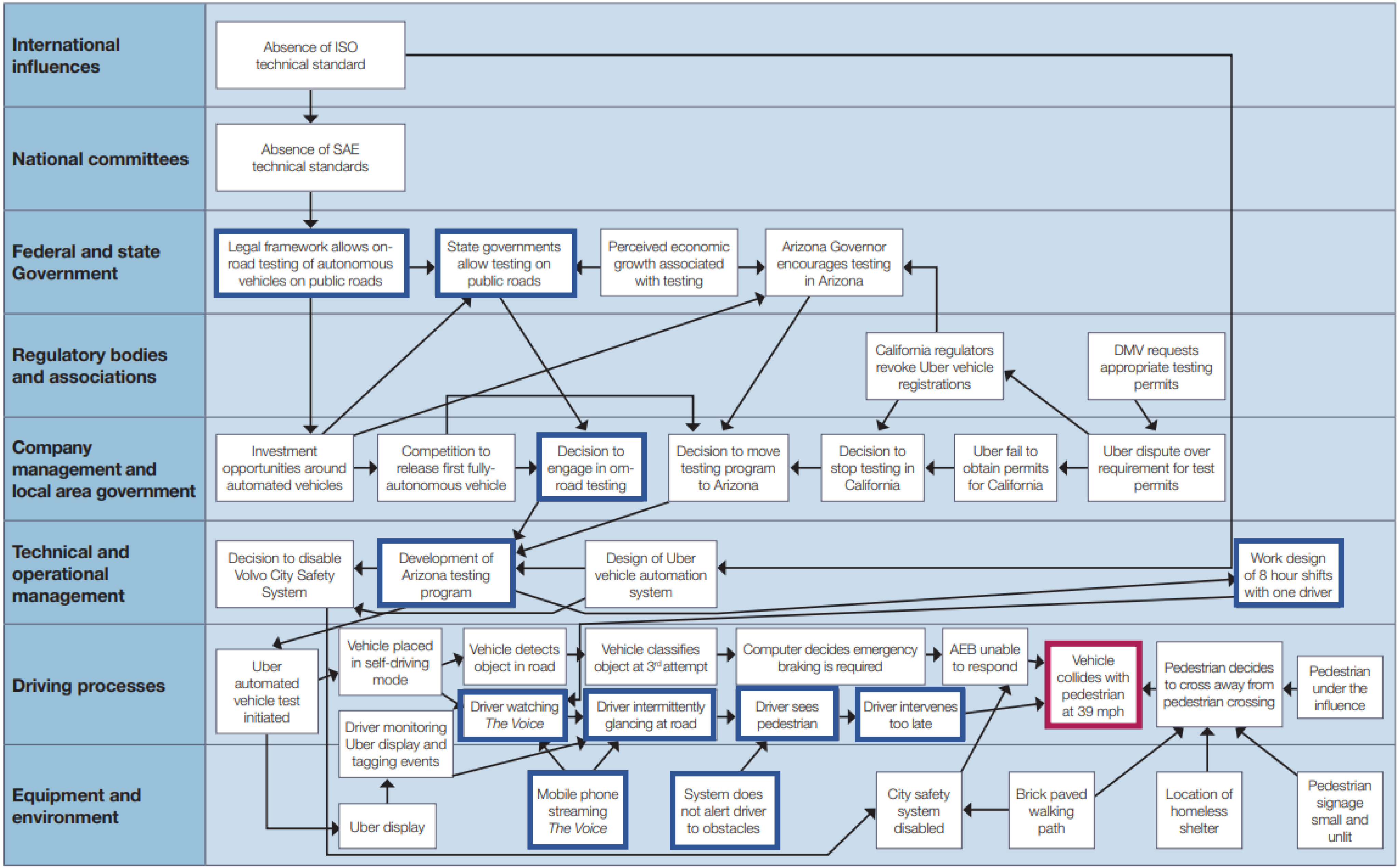
- 23 AcciMaps
- 5,587 contributory factors
- 79 contributory factor types

Salmon, P. M., et al. (2020). The big picture on accident causation: A review, synthesis and meta-analysis of AcciMap studies. *Safety Science*, 126, 1-15.

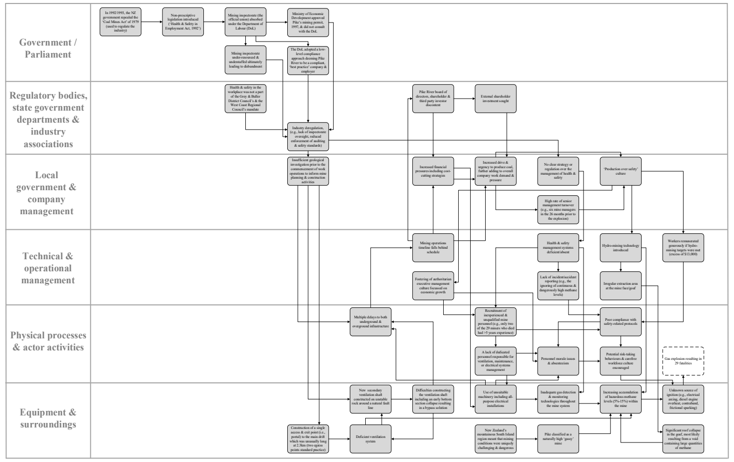
Lesson 2. All incidents are created by multiple interacting contributory factors

Uber-Volvo automated vehicle incident

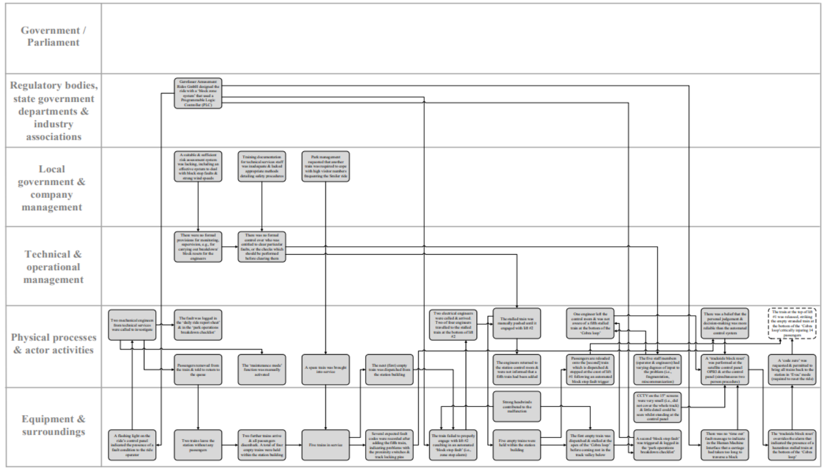
- 18th March 2018
- Uber-Volvo test vehicle hit pedestrian
- Vehicle being tested with human operator in a monitoring role
- Sensors identified the pedestrian, but safety systems had been disabled



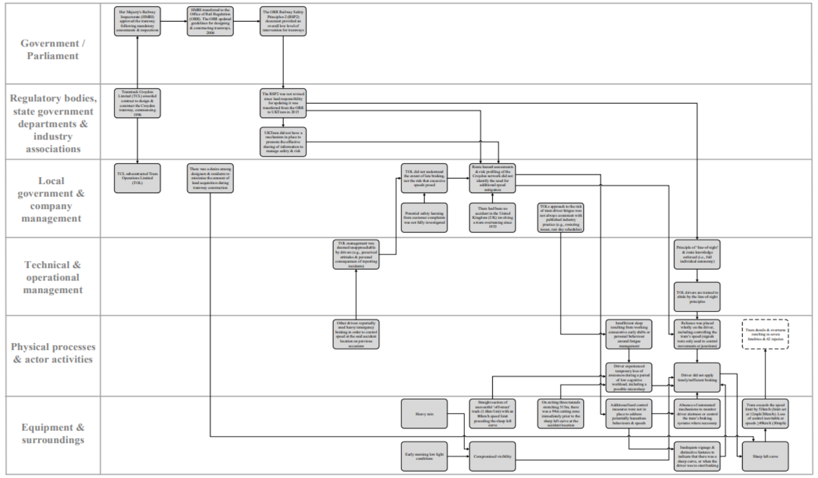
Stanton (2009) Models and methods for collision analysis - https://www.racfoundation.org/wp-content/uploads/Models_and_methods_for_collision_analysis_Stanton_March_2019.pdf



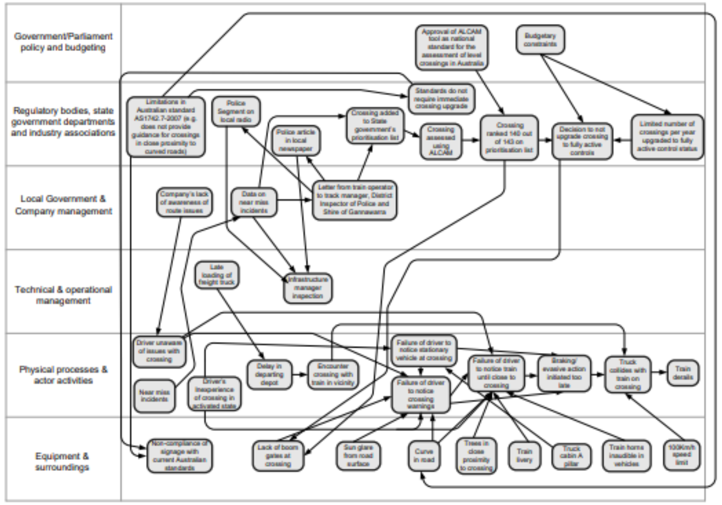
Government / Parliament
Regulatory bodies, state government departments & industry associations
Local government & company management
Technical & operational management
Physical processes & actor activities
Equipment & surroundings



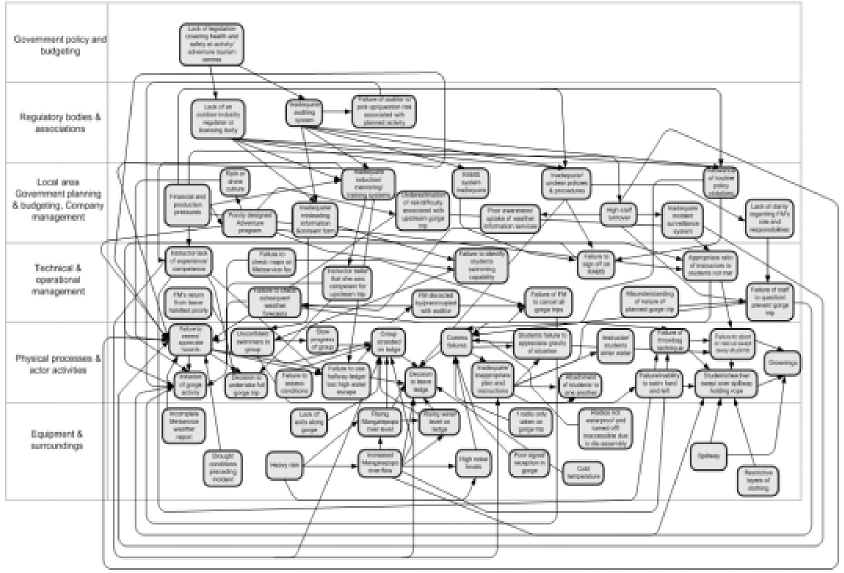
Government / Parliament
Regulatory bodies, state government departments & industry associations
Local government & company management
Technical & operational management
Physical processes & actor activities
Equipment & surroundings



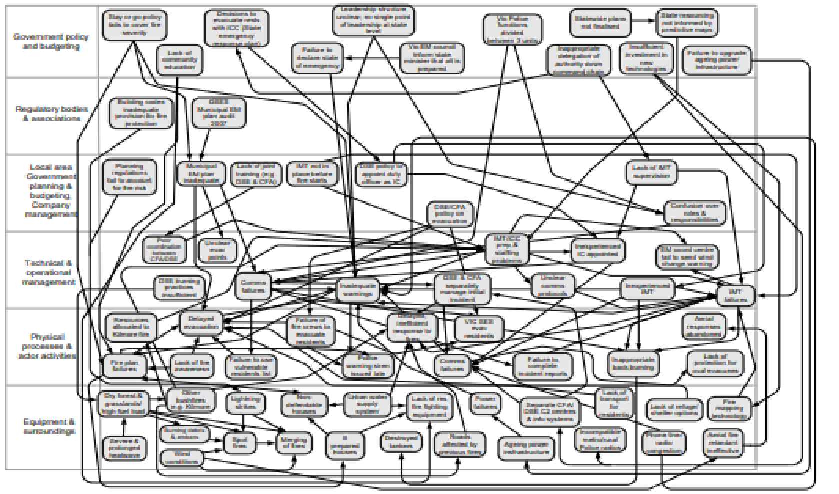
Government / Parliament
Regulatory bodies, state government departments & industry associations
Local government & company management
Technical & operational management
Physical processes & actor activities
Equipment & surroundings



Government/Parliament policy and budgeting
Regulatory bodies, state government departments and industry associations
Local Government & Company management
Technical & operational management
Physical processes & actor activities
Equipment & surroundings



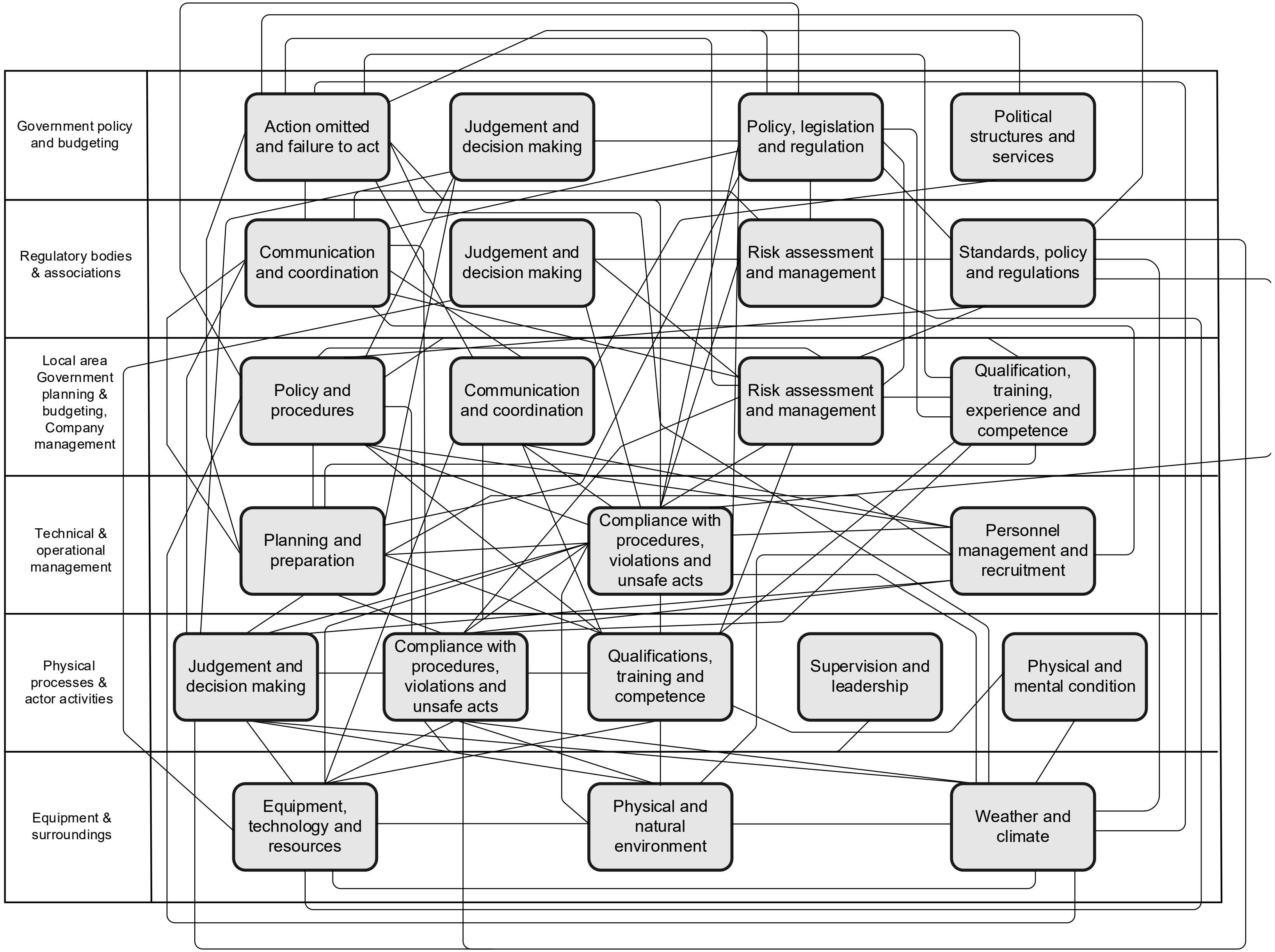
Government policy and budgeting
Regulatory bodies & associations
Local area Government planning & budgeting, Company management
Technical & operational management
Physical processes & actor activities
Equipment & surroundings



Government policy and budgeting
Regulatory bodies & associations
Local area Government planning & budgeting, Company management
Technical & operational management
Physical processes & actor activities
Equipment & surroundings

Lesson 3. There is a generic causal network that frequently appears in incidents

A generic causal network

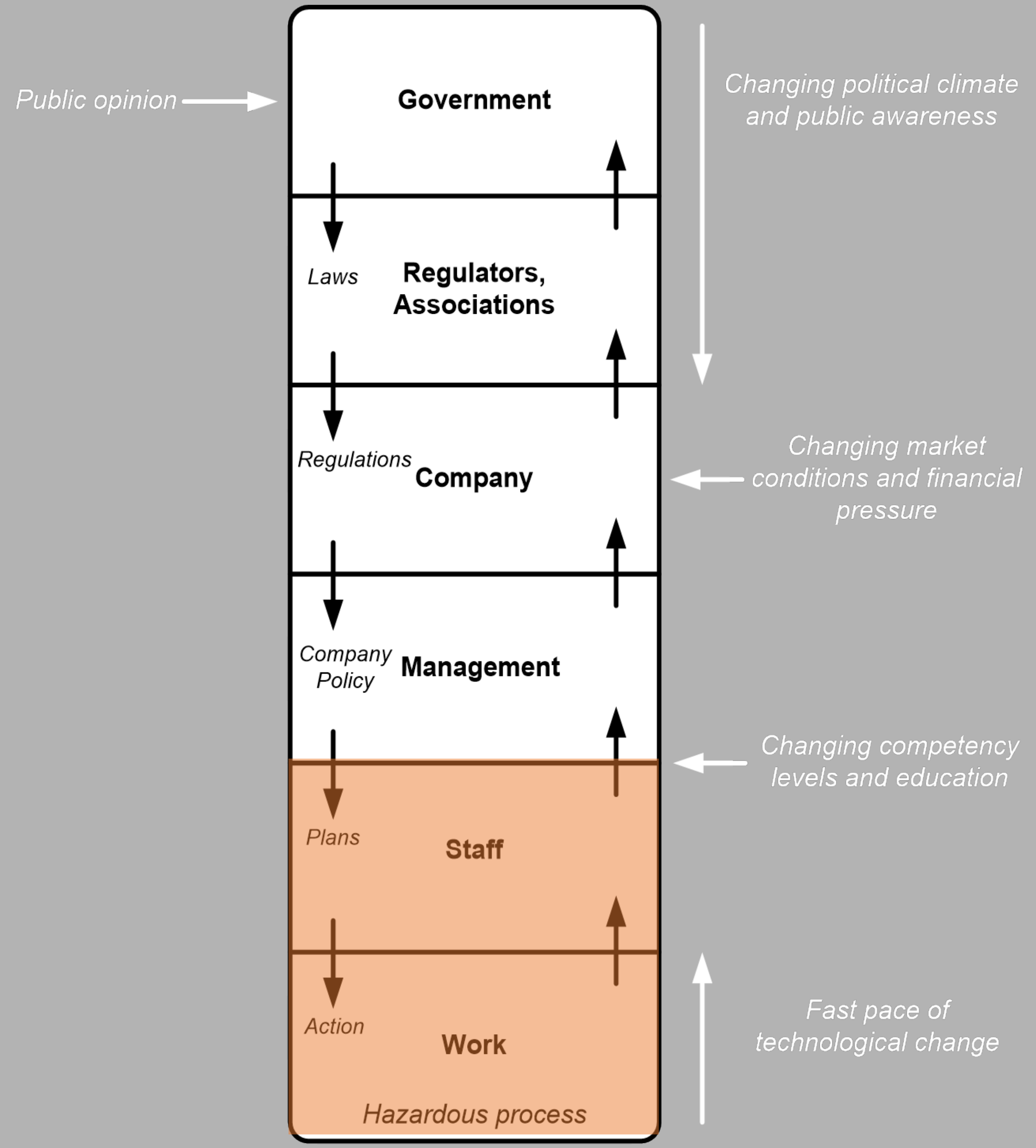


Salmon, P. M., et al. (2020). The big picture on accident causation: A review, synthesis and meta-analysis of AcciMap studies. *Safety Science*, 126, 1-15.

Lesson 4. Most risk and safety management methods are out of date

The problem with methods

- They do not consider the broader work and societal system
- They do not look at interactions (e.g. between risks, between contributory factors)
- They do not consider emergent risks
- They are failure (and human error) based
- They are not aligned with contemporary models of safety and accident causation



Safety Science xxx (2017) xxx–xxx

Contents lists available at ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/ssci

Risky systems versus risky people: To what extent do risk assessment methods consider the systems approach to accident causation? A review of the literature

Clare Dallat *, Paul M. Salmon, Natassia Goode

Centre for Human Factors and Sociotechnical Systems, University of the Sunshine Coast, Faculty of Arts and Business, Locked Bag 4, Maroochydore DC, QLD 4558, Australia

ARTICLE INFO

Article history:
Received 16 April 2016
Received in revised form 15 March 2017
Accepted 19 March 2017
Available online xxxx

Keywords:
Risk
Risk assessment
Risk assessment methods
Systems thinking

ABSTRACT

Accidents are now widely acknowledged to be a systems phenomenon. As part of a proactive approach to safety management, organisations use risk assessment methods to identify the hazards and associated risks that may lead to accidents. Although there is an extensive body of literature on the need for a systems thinking approach in accident analysis, little has been said regarding the theoretical underpinnings of risk assessment methods. The aim of this paper was to systematically review the risk assessment methods presented in the literature and evaluate the extent to which they are underpinned by a systems thinking approach. A total of 342 methods spanning a range of safety-critical domains were evaluated using Rasmussen's tenets of accident causation. A key finding is that the majority of existing risk assessment methods are not consistent with Rasmussen's model of accident causation (arguably the most popular model in safety science circles). Instead, the majority of risk assessment methods focus on risks at the so called sharp-end and largely view accidents as emerging from a linear, or chain-of-events process. This overlooks emergent risks at other levels of the system, including supervisory, managerial, regulatory and government levels. The findings therefore suggest that the majority of existing risk assessment methods may be inadequate for identifying hazards and analysing risks within complex sociotechnical systems. The implications for risk assessment practice are discussed.

1. Introduction

Within the field of safety science, a number of models have been developed to explain accident causation in safety-critical domains (e.g. Heinrich, 1931; Leveson, 2004, 2011; Perrow, 1984; Rasmussen, 1997; Reason, 1990). They represent an evolution of the beliefs surrounding the aetiology of accidents over the past century (Salmon et al., 2011). In the 1930s, accidents were largely understood to be the result of failures in hardware or equipment. In the 1970s, a new understanding prevailed: accidents were the result of failures resulting from unsafe acts or 'human error', involving the front line operator at the so-called 'sharp end' (Woods et al., 1994). Reason's (1990) seminal work and the introduction of the "Swiss Cheese Model", shifted the emphasis onto the latent failures residing throughout organisational work systems. This view of accident causation still dominates in many organisations (Underwood and Waterson, 2013). However, the work of Rasmussen (1997) caused a seminal shift in the way that safety science views accident causation. Accidents are now widely acknowledged to be a systems phenomena (Hollnagel and Goteman, 2004; Dekker, 2011). This position currently prevails within accident analysis research (Underwood & Waterson, 2013).

This shift in thinking surrounding accident causation did not occur in a vacuum and was precipitated by several significant, large scale disasters such as the Challenger Space Shuttle Disaster (Leveson, 2004), Three Mile Island explosion (Reason, 1990), and the Herald of Free Enterprise sinking (Reason, 1990). These disasters prompted a substantial rethink in how accidents occur, and subsequently led to a shift and evolution into how we study them. The approach referred to hereafter as 'Systems Thinking' subsequently emerged to assist in the explanation of such 'systems failures', as opposed to a limited description of human errors (Rasmussen, 1997; Leveson, 2004; Hollnagel and Goteman, 2004).

Although this approach has proved highly useful, when used for safety management the primary limitation of accident analysis methods is that they are reactive, examining events that have already happened. This reactive approach has been criticised for a number of reasons, not least because it relies on rare large scale

* Corresponding author.
E-mail address: clare.dallat@research.usc.edu.au (C. Dallat).

Systems thinking approaches to risk assessment?

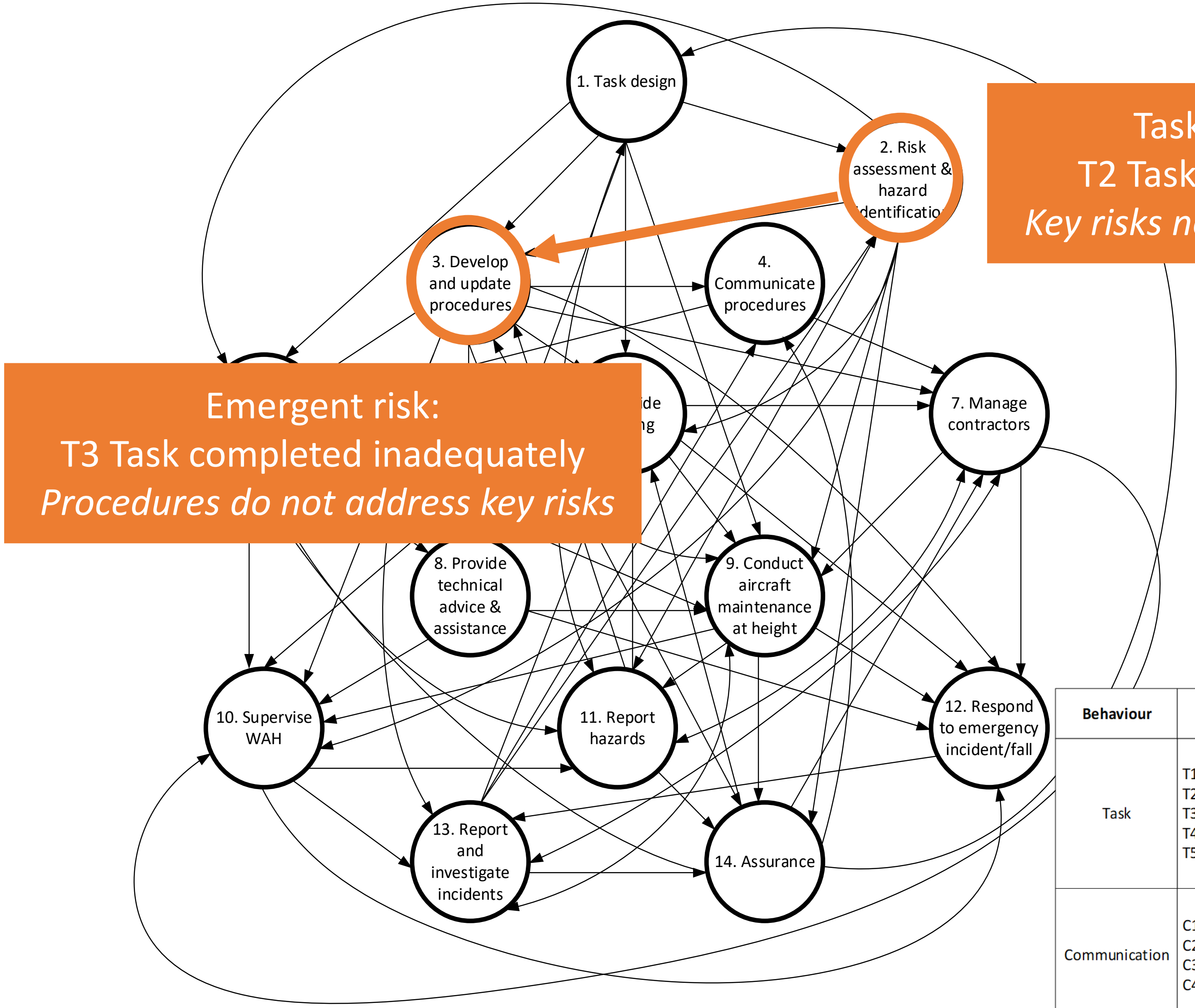
- Understanding of **work system**
- Assessment of risks **across the system**
- Mitigation strategies for overall system
- Current methods:
  - Net-HARMS - Networked Hazard Analysis and Risk Management Systems (Dallat et al., 2018)
  - EAST Broken Links (Stanton & Harvey, 2017)
  - STPA - Systems Theoretic Process Analysis (Leveson, 2011)
  - FRAM - Functional Resonance Analysis Method (Hollnagel, 2012)

Lesson 5. ‘Emergent’ risks are the ones that will catch you out

Emergence

- Outcomes that result from interactions between elements in the system that cannot be fully explained or reliably predicted in advance by examining the elements in isolation
- Emergent risks are those that emerge when other risks across the system interact with one another
- Net-HARMS method (Dallat et al., 2018) developed to pro-actively identify emergent risks

Working at heights aircraft maintenance



Task risk:
T2 Task omitted
Key risks not identified

Behaviour	Risk Modes
Task	T1 – Task mistimed T2 – Task omitted T3 – Task completed inadequately T4 – Inadequate task object T5 – Inappropriate task
Communication	C1 – Information not communicated C2 – Wrong information communicated C3 – Inadequate information communicated C4 – Communication mistimed
Environmental	E1 – Adverse environmental conditions

Lesson 6. Accidents are not always caused by failures

Normal performance and the Boeing 737 MCAS crashes

Lion Air Flight 610, 198 deaths

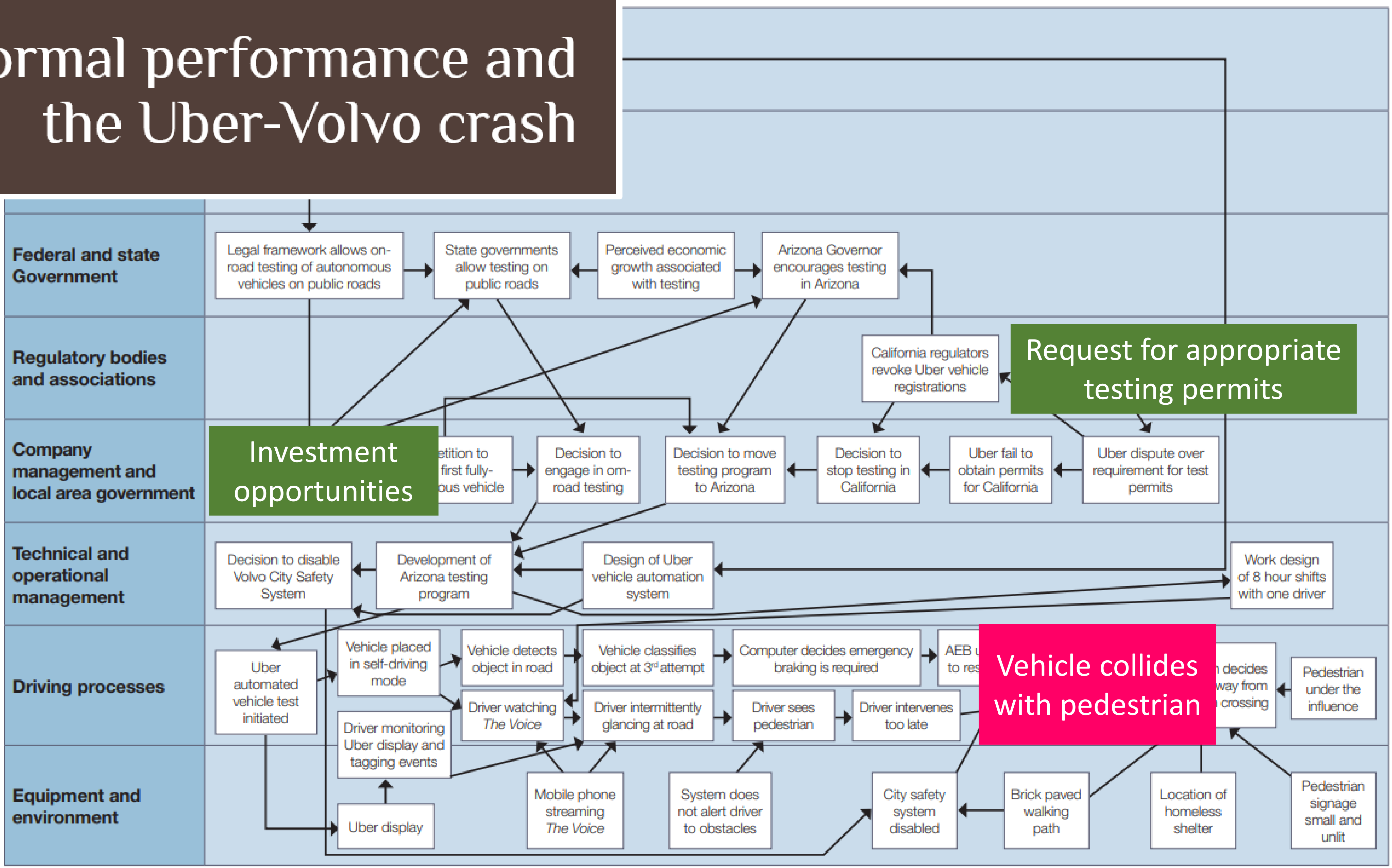
Ethiopian Airlines Flight 302, 157 deaths

“They were far too close to the ground, and needed to gain altitude. Yet when Capt Yared Getachew tried to guide the nose of the Boeing 737 upwards, an electronic system forced it down again”

“They had no idea what was going on. Each time they tried to bring the nose up, their actions would be reversed a few seconds later as automatic systems forced it down again.”

What went wrong inside Boeing’s cockpit? BBC News, 2019

Normal performance and the Uber-Volvo crash



Stanton (2009) Models and methods for collision analysis - https://www.racfoundation.org/wp-content/uploads/Models_and_methods_for_collision_analysis_Stanton_March_2019.pdf

Lesson 7. Automation is not a silver bullet!

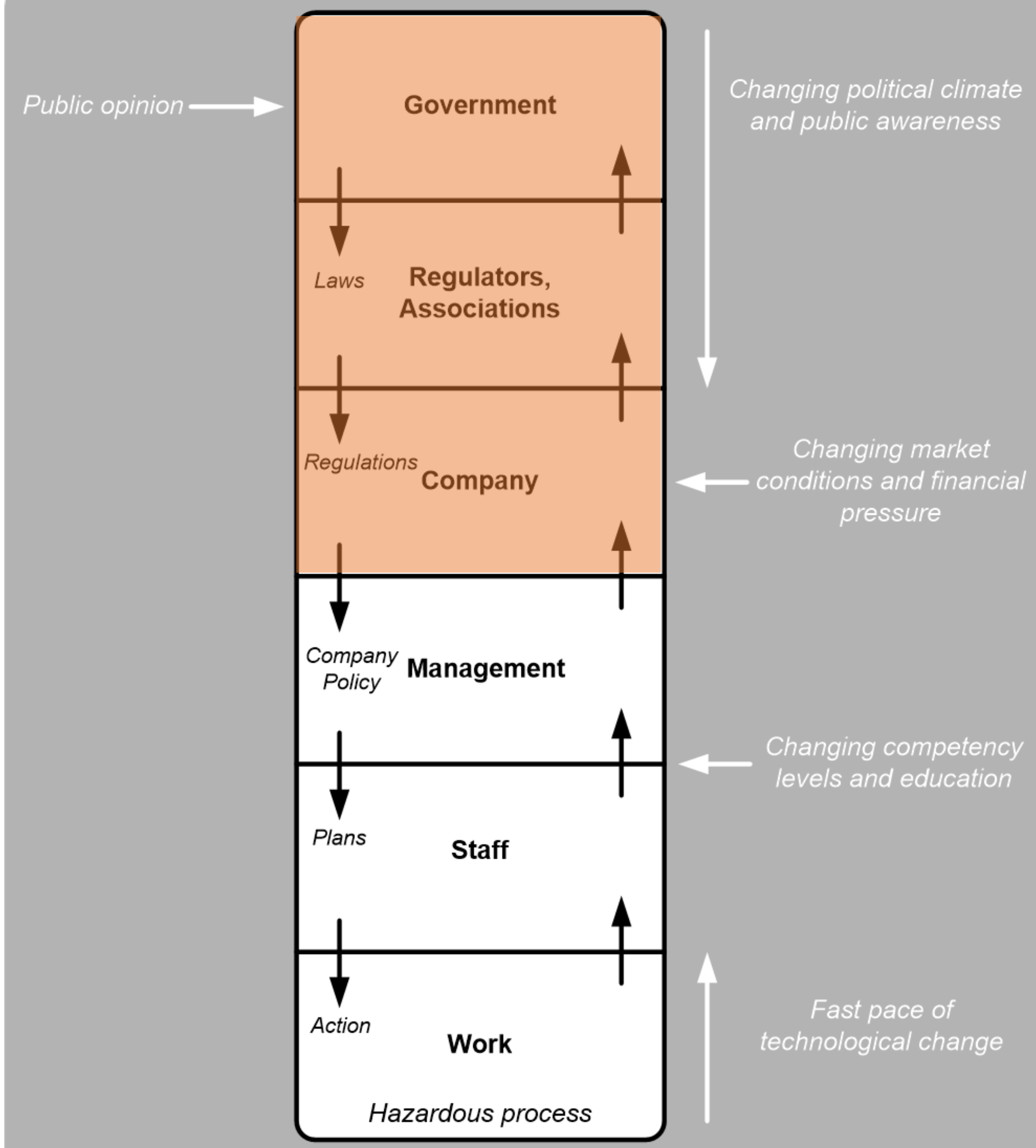
Ironies of Automation (Bainbridge, 1983)

- The more advanced, the more critical humans become
- Design flaws are a major source of operating problems
- Humans are left to do the tasks that cannot be automated
- Skill degradation
- Highly skilled operators are required when automation fails
- Humans are no good at monitoring (“The impossible task”)

“For automation to fulfil its promise, designers must not focus on the design of the automation, but on the design of joint human-automation system”

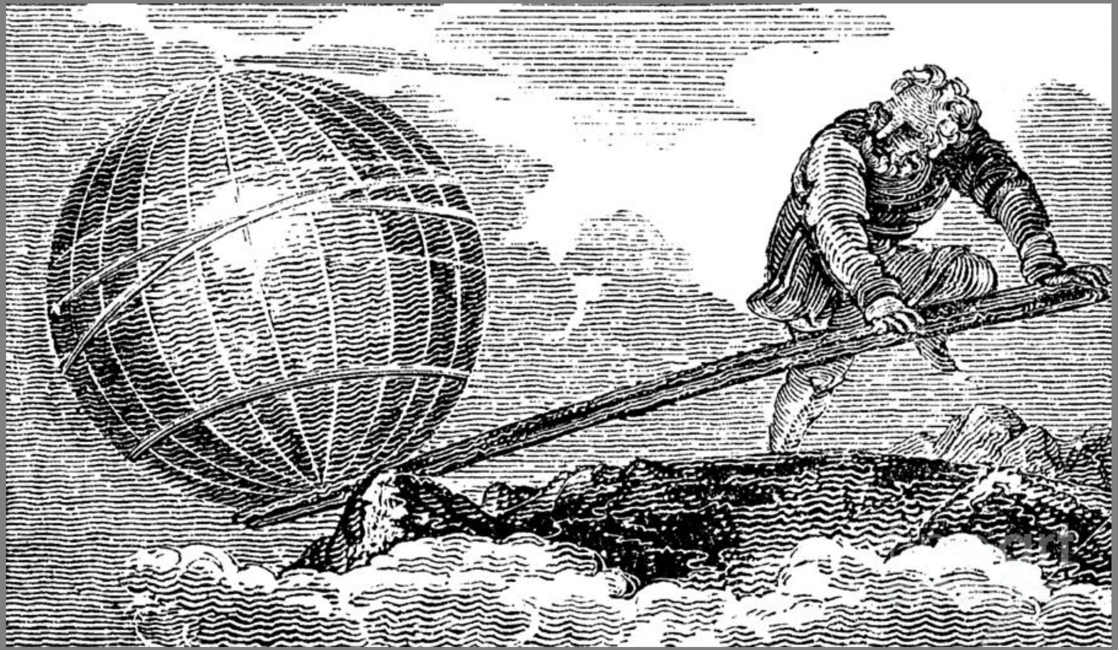
(Lee & Seppelt, 2009)

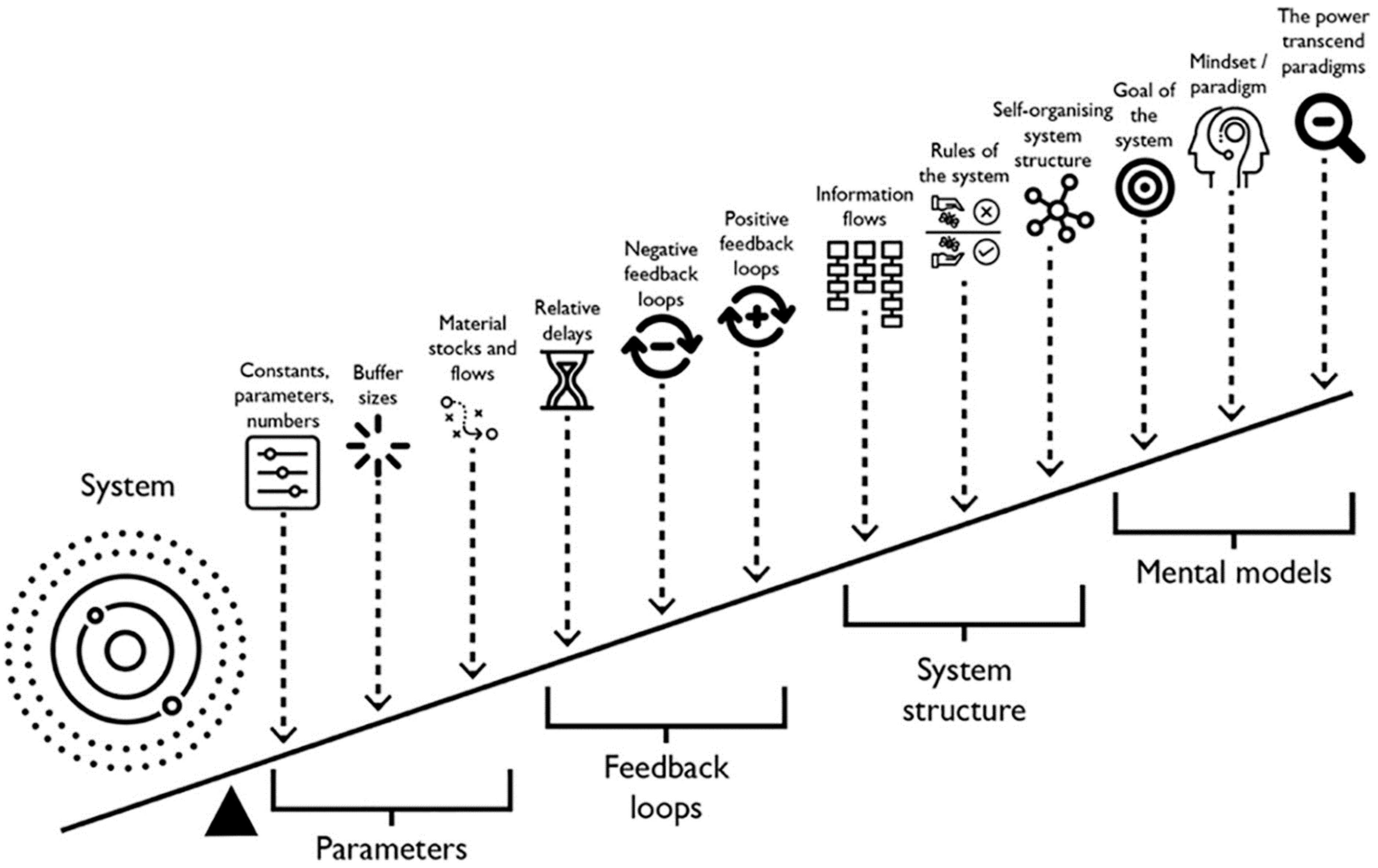
Lesson 8. Fixing ‘broken components’ won’t solve anything



Search for leverage points

"places within a complex system where a small shift in one thing can produce big changes in everything" (*Meadows*)





https://www.behaviourworksaustralia.org/blog/how-systems-thinking-compliments-behavioural-approaches-in-solving-complex-problems

Lesson 9. There will be unintended consequences


POLICIES
PROCEDURES

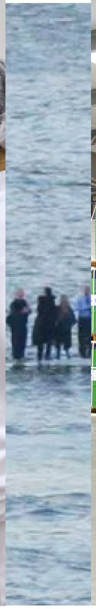
Lesson 10. Humans are the glue that hold badly designed systems together

VATCH

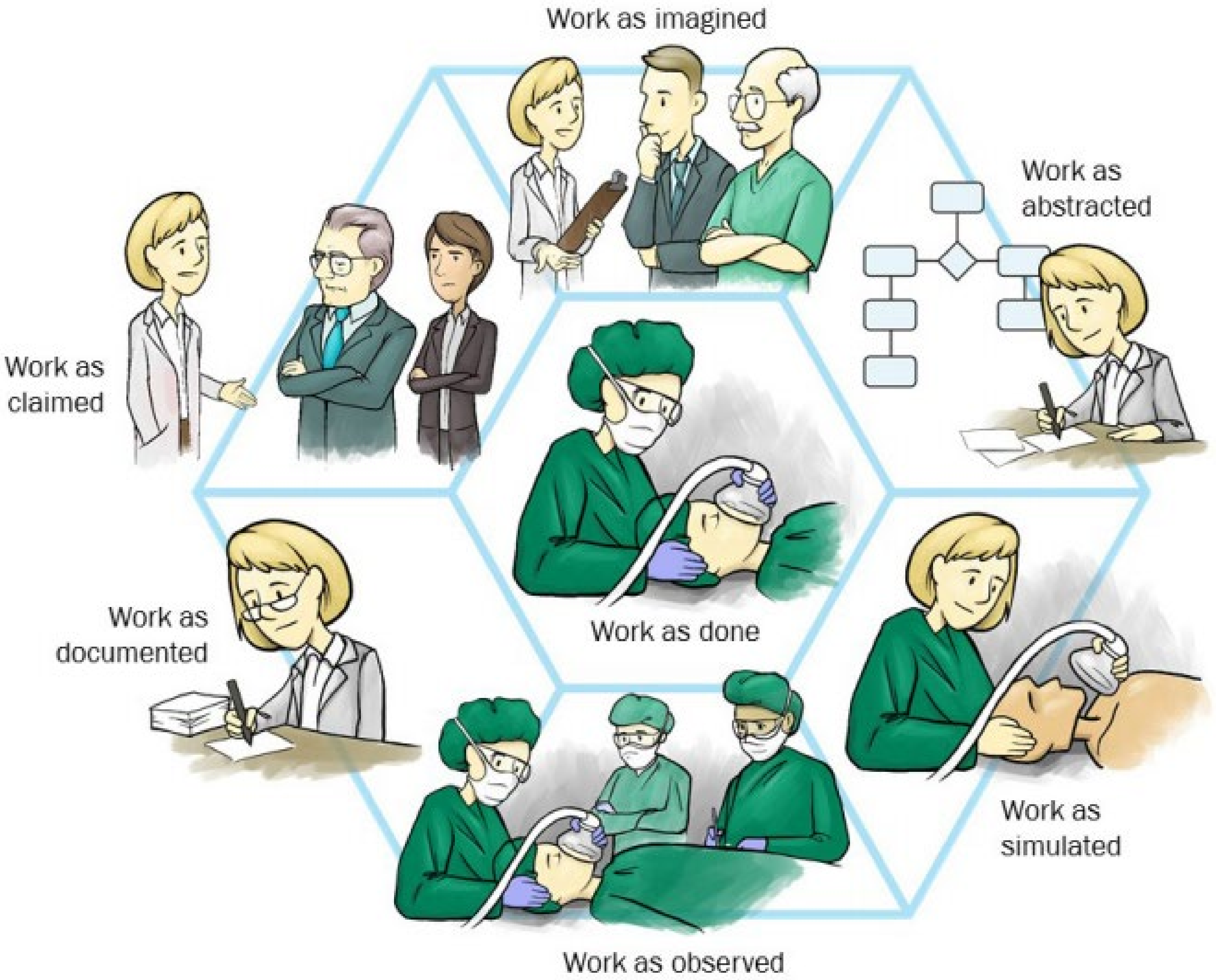
isse
n'

ger tells

By Diane Herbst | Published on January 13, 2023 12:29PM EST



The plane and passengers in the Hudson River on Jan. 15, 2009. PHOTO: BEBETO MATTHEWS/AP/SHUTTERSTOCK



Deutsch (2017)

“everyday performance variability provides the adaptations that are needed to respond to varying conditions, and hence is the reason why things go right” (Hollnagel et al, 2015)

A challenge to the safety community

- Embrace complexity & systems thinking
- Reject 'human error' as a cause
- Treat incidents as learning opportunities
- Use systems thinking methods when assessing risk / investigating incidents / developing interventions
- Manage emergence & unintended consequences
- Identify and use leverage points to enact change
- Challenge automation
- Acknowledge the role that workers play in keeping the system safe – treat them as heroes and seek to understand how they do it

Thank you!

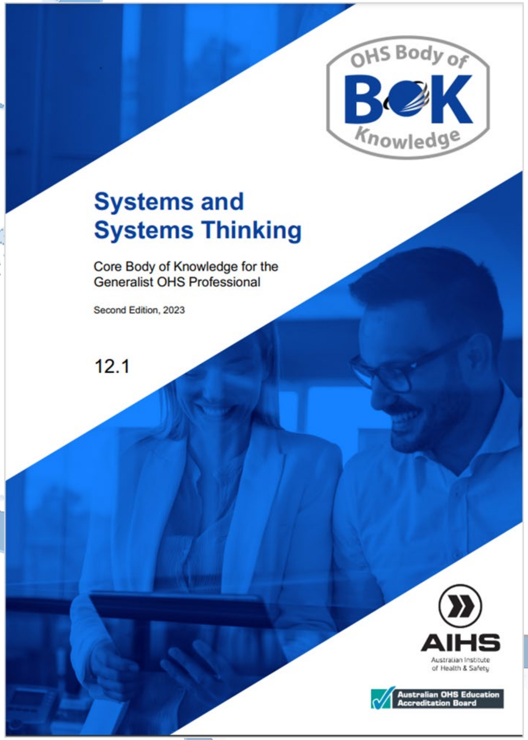
https://www.usc.edu.au/research/centre-for-human-factors-and-sociotechnical-systems

gread@usc.edu.au

gemma-read

@gemma_read

@hfandsts



UniSC Australia

Centre for Human Factors and Sociotechnical Systems