# Compliance vs. Due Diligence: SFAIRP and its Interaction with Systems Safety and Assurance Approaches

**Tim Procter**

International Railway Safety Council Conference
October 2019

INDEC®

# Context – System Safety and Assurance

- System Safety and Assurance (SSA) approaches are used to manage **product safety** in a number of major Australian industries
- Product safety:
  - Related to work health and safety, but generally does not include safety during manufacturing or construction.
  - Aims to ensure a (complex) product – e.g. a train – is sufficiently safe for its intended use.

# Context – SFAIRP and the common law

How safe is safe enough?

- Rail Safety National Law
- Work Health and Safety legislation

→ Eliminate or, failing that, reduce risks so far as is reasonably practicable (SFAIRP)

# The Philosophy of System Safety and Assurance

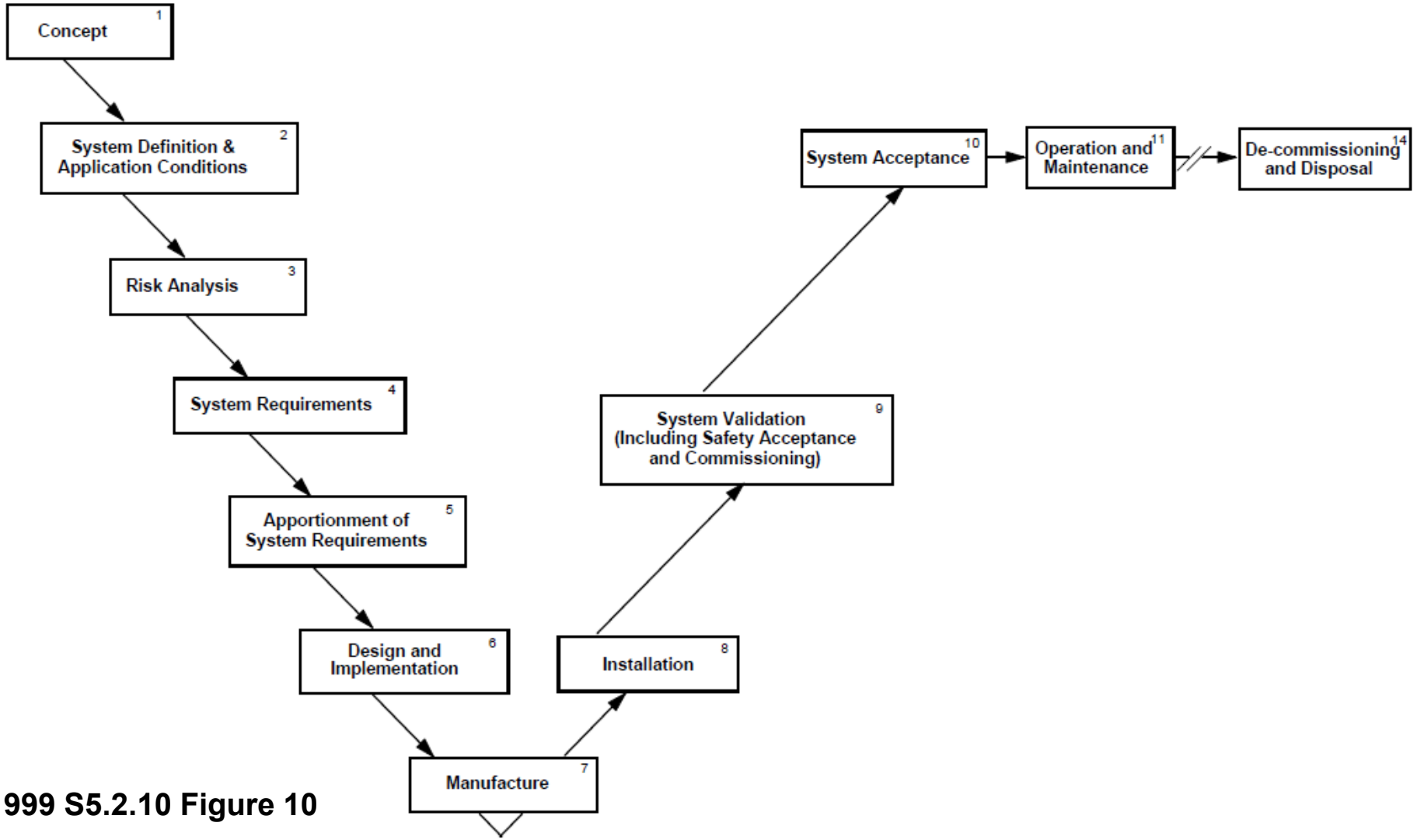
SSA has arisen from:

A combination of **systems engineering** and **assurance case** approaches being implemented in a **safety context.**

# Systems Engineering

- Identification of required high level and overarching functions and characteristics of a system
- Decomposition of these into specific detailed requirements for ‘sub-systems’ – e.g. different engineering design disciplines
- Formal tracking of incorporation of these requirements into the design and construction of the system
- Testing of constructed subsystems and the systems as a whole to verify and validate that requirements are met

# Systems Engineering V-Model

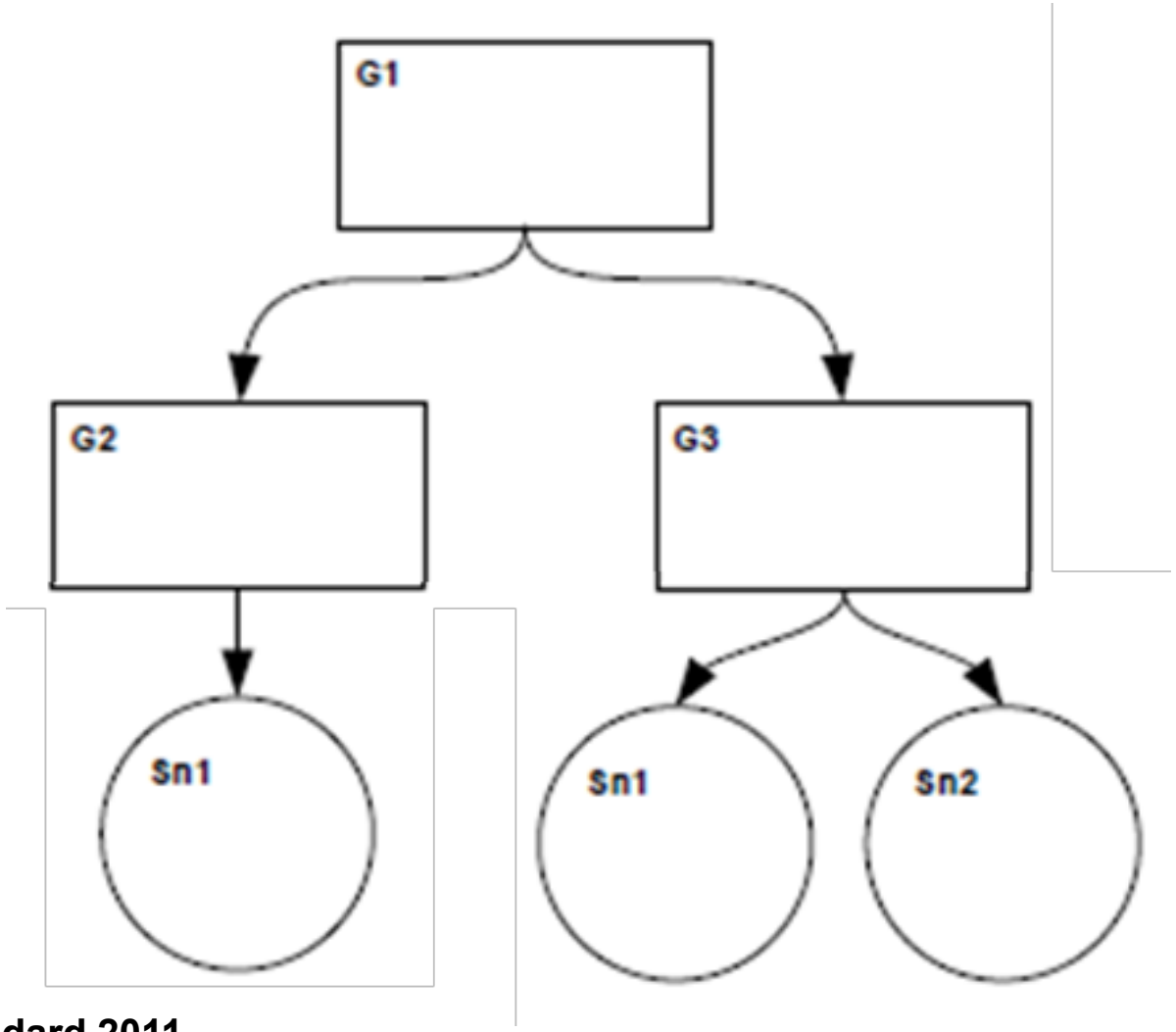



**Source: EN 50126-1:1999 S5.2.10 Figure 10**

# Assurance Cases

- A formal claim to have achieved an objective (or objectives), supported by evidence.
  - Top-level objectives deemed achieved if subordinate supporting objectives are achieved.
  - Evidence ‘proving’ that an objective has been achieved given in the form of formal documentation.

# Goal Structuring Notation




**Adapted from GSN Community Standard 2011**

# Safety Context – Legal Duties

*A duty imposed on a person under this Law to ensure, so far as is reasonably practicable, safety requires the person—*
*(a) to eliminate risks to safety so far as is reasonably practicable; and*
*(b) if it is not reasonably practicable to eliminate risks to safety, to minimise those risks so far as is reasonably practicable.*

**RSNL Section 46—Management of risks**

*(1) If a person has a duty or obligation under this Law, an officer of the person must exercise due diligence to ensure that the person complies with that duty or obligation.*

**RSNL Section 55—Duty of officers to exercise due diligence § (1)**

## Overseen by the Office of the National Rail Safety Regulator (ONRSR)

# Synthesis into Systems and Safety Assurance

- Inclusion of a project objective of developing and implementing a safe system as a high-level goal in a GSN assurance case
- Adopting a systems engineering approach to identifying safety requirements, through safety assessments conducted throughout the V-model process
- Documenting these in a manner that addresses RSNL duties, specifically addressing the ‘due diligence’ and ‘SFAIRP’ requirements.

# Rail Safety in Australia – Foundations and Duties

**Rail Safety National Law** (2012) → rail context

↑

**2011 Model Work Health and Safety Laws** (2011) → ‘due diligence’

↑

**Victorian Occupational Health and Safety Act** (2004) → ‘SFAIRP’

↑

**Maxwell Review** (2004) → ‘reasonable practicability’

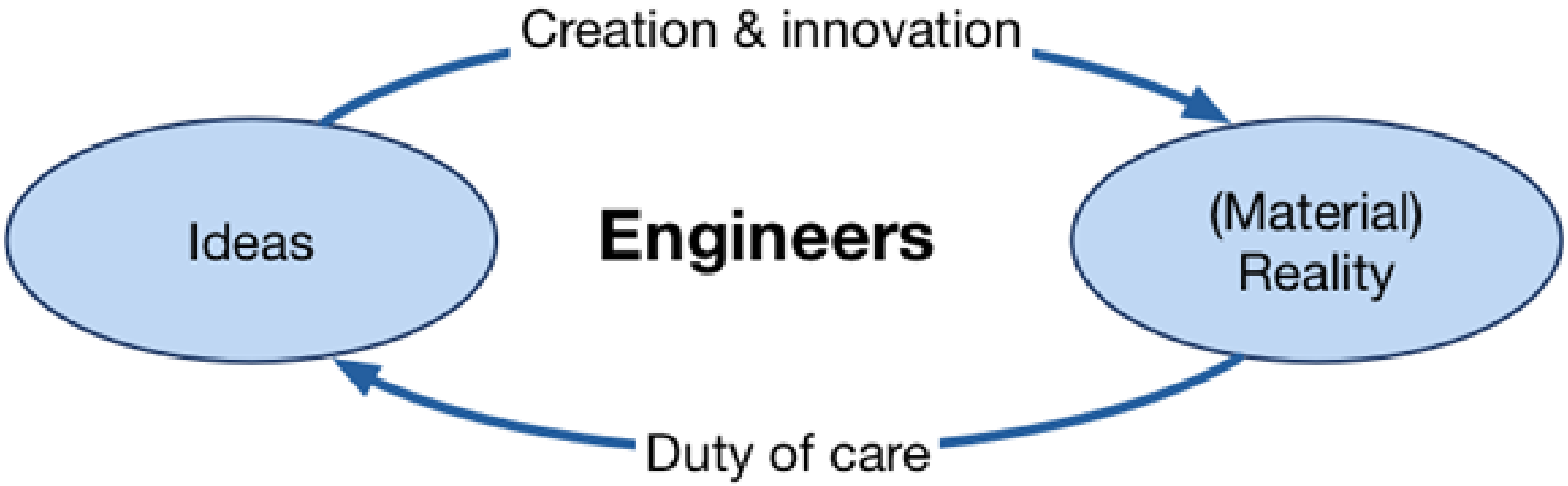
↑

**Australian / English common law** → ‘duty of care’

↑

**Golden Rule** / rule of reciprocity

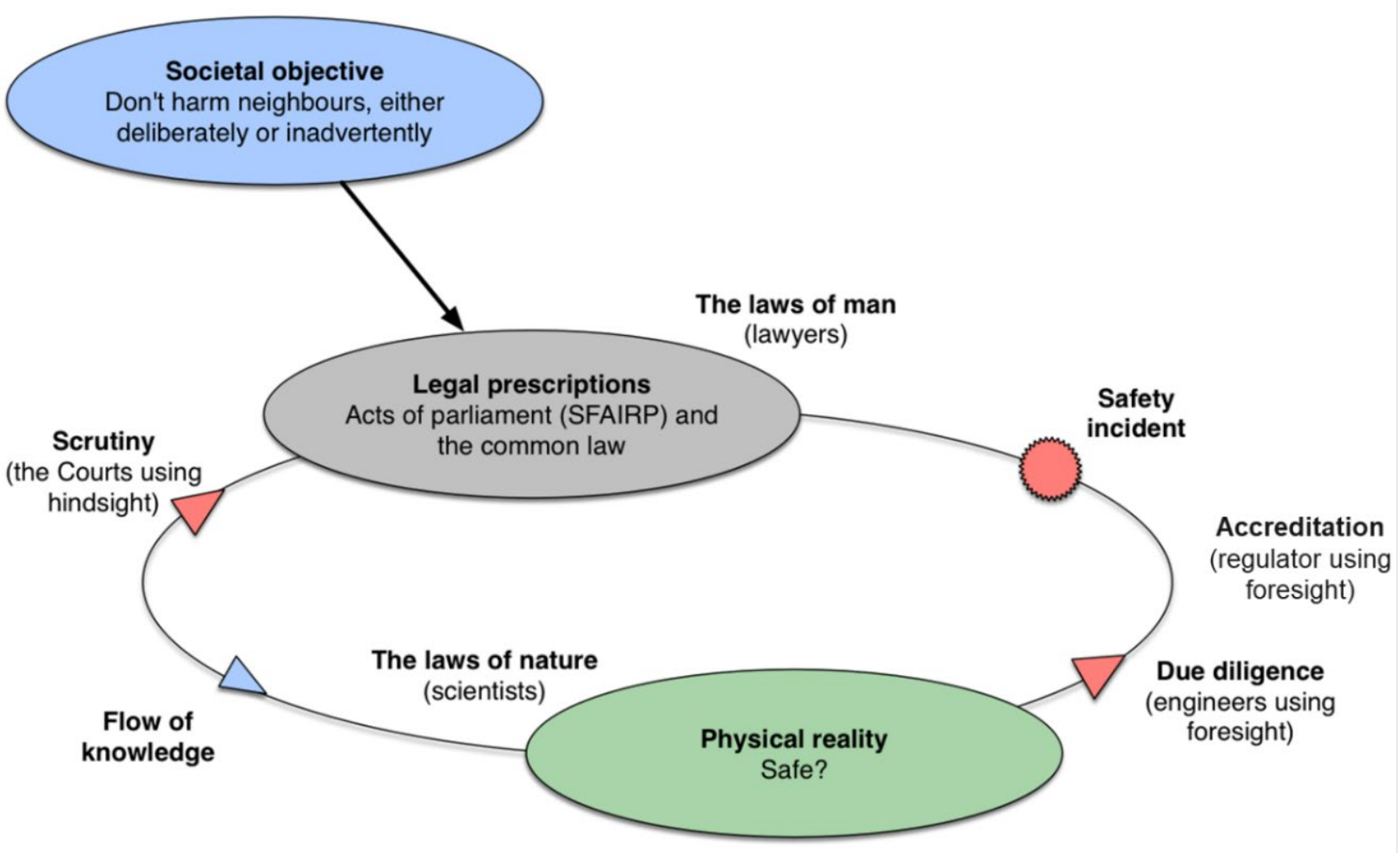
# Ideas into Reality, Reality into Ideas



# Post-event Scrutiny

- **Courts** determine if SFAIRP outcome achieved on a post-event, case-by-case basis, using hindsight.
- **Engineers** must act to address their SFAIRP duty through due diligence using foresight → more difficult task.
- **Regulators** (such as ONRSR) give accreditation to entities conducting regulated activities (e.g. rail operations) based on pre-event knowledge.

# The flow of pre- and post-event knowledge



# The Courts' Two Questions

The Courts consider two basic questions:

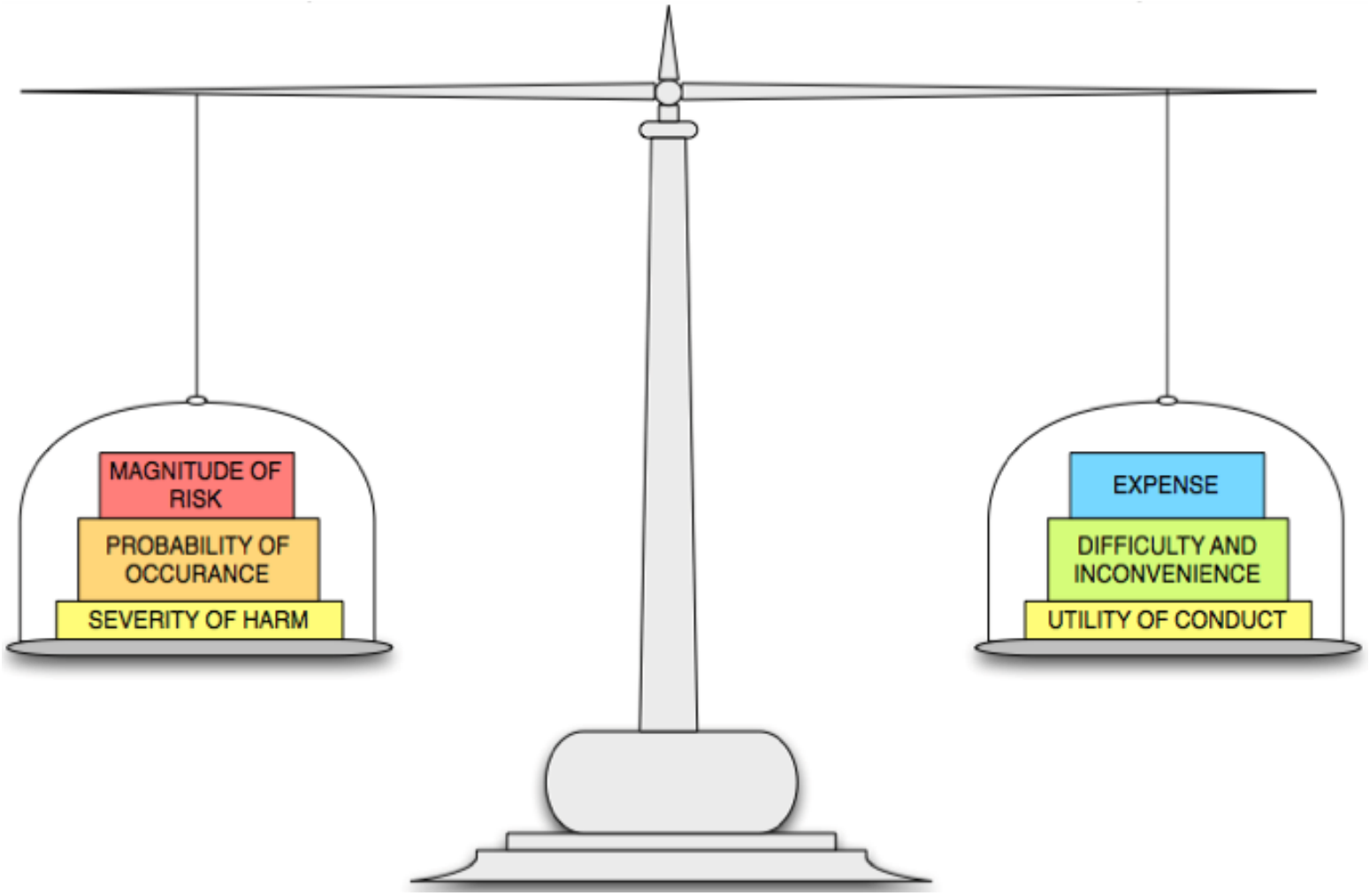
- Was it reasonable, prior to the event, to think that this could occur? If not, why not?
- Was there anything else which ought to have been in place which, if it had been in place, would have stopped this from happening?

# The Shirt Calculus

*The perception of the reasonable man's response calls for a consideration of the magnitude of the risk and the degree of probability of its occurrence, along with the expense, difficulty and inconvenience of taking alleviating action and any other conflicting responsibilities which the defendant may have.*

**Mason J in Wyong Shire Council v. Shirt (1980)**

# The Shirt Calculus




Robinson, Francis & Procter, 2018, adapted from Sappideen and Stillman (1995)

# No Tolerable Level of Risk

*Where it is possible to guard against a foreseeable risk, which, though perhaps not great, nevertheless cannot be called remote or fanciful, by adopting a means, which involves little difficulty or expense, the failure to adopt such means will in general be negligent.*

**Gibbs CJ in Turner v. South Australia (1982)**

# Pre-event Due Diligence

- Infinite ways people may be damaged
- Infinite actions available to prevent this
- Engineers (must attempt) to consider all these using foresight, rather that look at one event with hindsight as the Courts do
- Must also explain decisions in a manner that addresses the Courts' two questions

# Pre-event Due Diligence

Exercising due diligence doesn’t necessarily mean being correct.

That is, engineers are allowed to be wrong in a decision they make, so long as the decision was reasonable.

# The Engineer's Four Questions

1. What are the threats? How bad could they credibly be? Why is there confidence no critical threats have been overlooked?
2. What are the options to address the identified threats? Firstly, what is recognised good practice? Secondly, are there further practicable measures available?
3. Of the available options, which are reasonable? ( i.e. considering the factors listed in the Shirt Calculus.)
4. What quality assurance is in place to ensure the selected options will be implemented and remain effective?

# 1. Completeness Check

A formal argument as to why all credible, critical hazards have been identified:

- Functional completeness check, comparing
  - Identified hazards
  - Critical exposed groups and critical elements
  - All relevant phases
- Zonal or geographic completeness check
- Check against incident databases

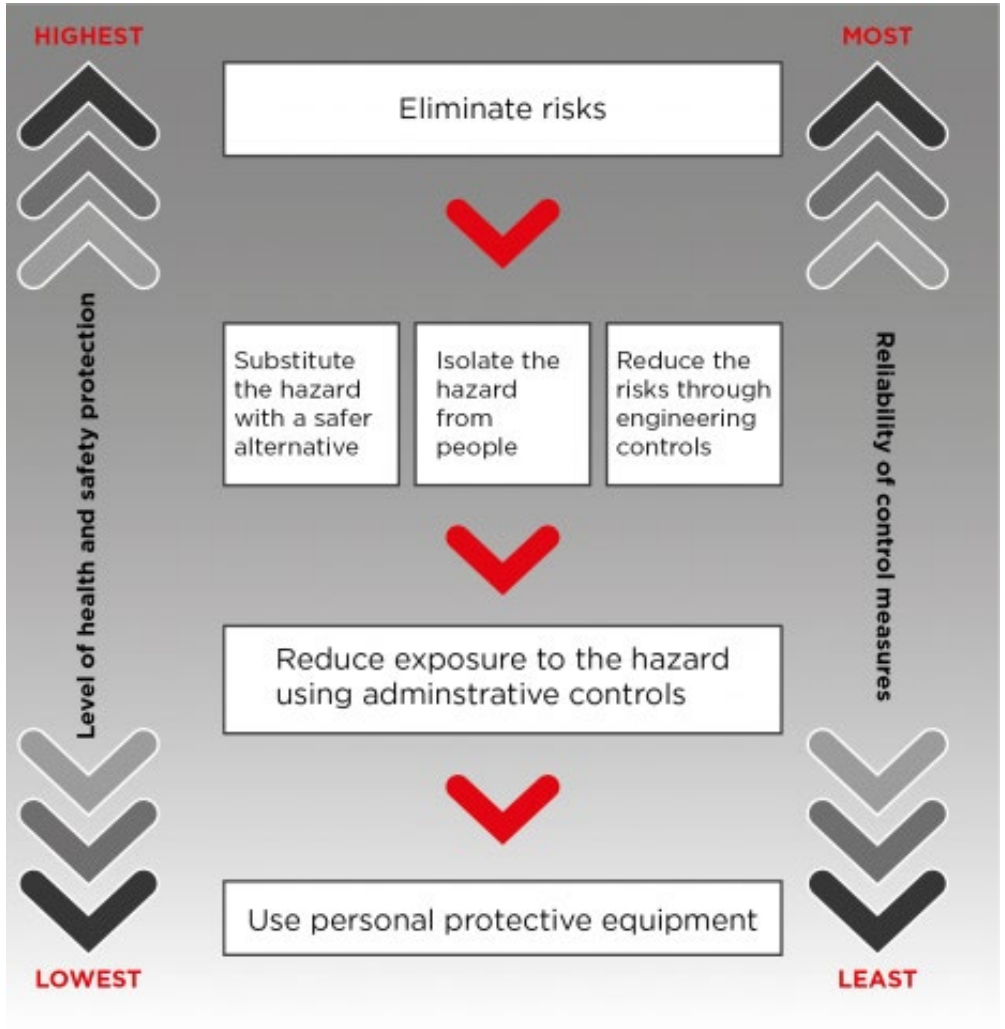
# 2. Good practice controls

For each significant hazard, all recognised good practice controls are in place, and if not, have been tested for reasonableness, and in the particular circumstances demonstrated as being unreasonable.

# 3. Further Options

Further possible practicable controls are considered (even if the risk is considered to be reduced to a ‘tolerable’ level), and that when considering further precautions, the hierarchy of controls is applied.

# Hierarchy of control measures

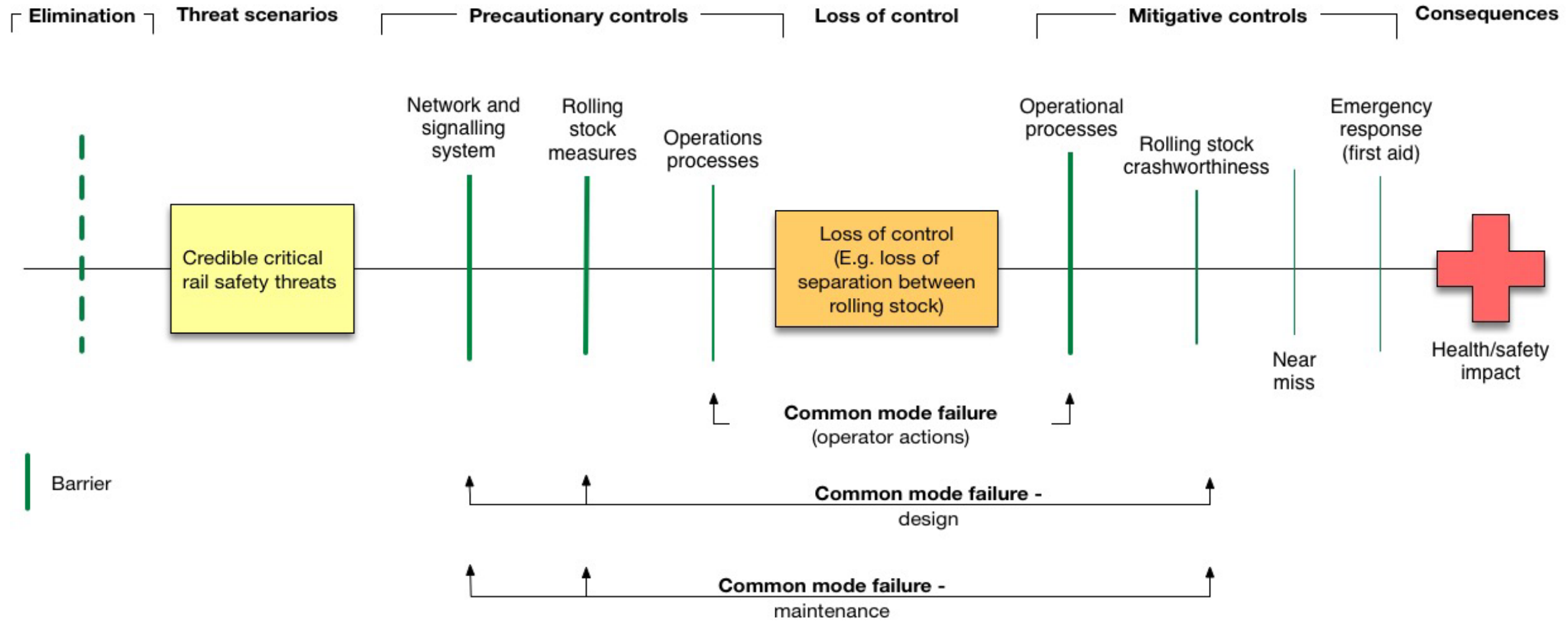



**Safe Work Australia (2018), *Model Code of Practice: How to manage work health and safety risks***

# 4. Implementation and maintenance of controls

That a quality assurance system is in place to ensure all reasonably practicable controls are implemented and remain effective.

# Threat-barrier Diagram for Generic Rail Safety Hazards



# SSA in a SFAIRP Context

- Great potential for synergy between SSA and SFAIRP approaches.
- Melding of good decision making – using SFAIRP requirements – with formal process implementation – using SSA approaches.
- But – potential for misalignment…

# SSA in a SFAIRP Context

SSA approaches may:

- Indirectly follow processes addressing the due diligence requirements – not easily explained to others
- Focus on maintaining detailed records and following standards at the expense of considering what actually constitutes good and explicable safety decisions in the specific project context.

# SSA in a SFAIRP Context

SFAIRP approach may result in:

- Multiple disconnected assessments made within a project
- Insufficient consideration of overarching project goals and requirements

→ especially true for major projects with inherent organisational knowledge limits

# Critical Misalignments

SSA may include use of hazard logs, GSN, etc. from previous projects as basis for new projects.

---

SFAIRP generates new list of hazards for each assessment, using previous work as a check for gaps rather than a foundation to build on.

# Critical Misalignments

SSA may focus on compliance with standards.

---

SFAIRP requires focus on understanding the good practice contained in standards, and how it may apply to the situation being considered.

# Critical Misalignments

SSA may include ‘tolerable’ and ‘acceptable’ risk levels in decision-making processes due to adoption of European standards. Includes ‘tolerable hazard rates’ inasmuch as they feed into SIL allocations.

---

SFAIRP approach incorporates duty of care, SFAIRP and due diligence requirements, including: recognised good practice as a starting point, the Shirt Calculus for further potential options, and no acceptable lower level of risk.

# Critical Misalignments

SSA Requirement for formal statement that safety risk has been reduced SFAIRP.

---

SFAIRP has no requirement for a formal SFAIRP statement – whether or not safety risk has been reduced SFAIRP is only ever determined by the Courts post-event – but is demonstrated through decision-making process.

# Potential Misalignment

SSA Identification of many clearly defined safety requirements (based on identified controls and decomposition of high-level requirements) for implementation and formal monitoring throughout a project.

---

SFAIRP Potential for controls to be stated in a manner that is unclear or not verifiable.

# Potential Misalignment

SSA: Large amount of detail and potential for human error in translation form control to requirement/s and in data entry means some controls may not be fully implemented by linked requirements, may be linked to generic rather than specific requirements, or may not be linked to requirements at all.

---

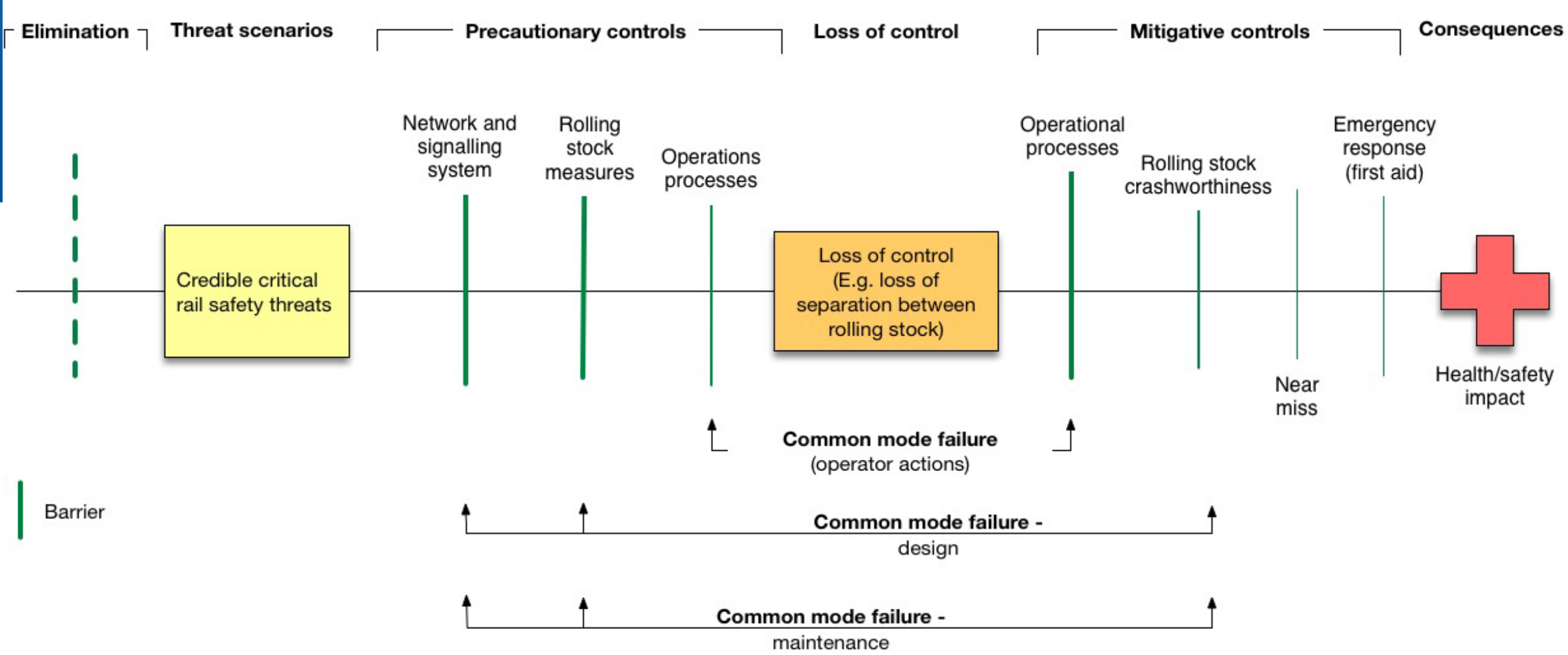
SFAIRP: Controls identified in a SFAIRP assessment are stated in the manner in which they are to be implemented in the specific project context without further translation required.

# Synthesis

- Remember SSA is a tool used to achieve a goal, not a goal in itself
- The goal is safety – in this context, demonstrating due diligence and eliminating or, failing that, reducing risk SFAIRP

# Synthesis – Key Elements

- Context and structure of approach
- Risk identification approach
- Controls identification approach
- Approach to determination of reasonableness of controls
- Approach to control implementation and quality assurance




**Quality Assurance - coordinated by SSA approaches**

- designer/manufacturer
- ONRSR
- Network owner
- Rolling stock operator
- Independent Safety Assessor

Etc.

# Conclusion

System Safety and Assurance and SFAIRP requirements are each of significant value to the rail industry, and hence to society as a whole

Integration of the two is often informal or ad hoc – this is insufficient.

→ Complex rail projects need a SFAIRP-based approach to system safety, or a system safety-based approach to SFAIRP.