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

Tim Procter
Senior Consultant
Indec Consulting

2019

ABSTRACT

Systems engineering, and its systems safety subset, are now deeply embedded in major rail projects in Australia. When dealing with system safety, a systems engineering approach, as set out in such standards as EN 50126, is often used in tandem with assurance case techniques such as Goal Structuring Notation. This combination of systems engineering and safety assurance (SSA) approaches provides a formal, structured, traceable framework to identify and address whole-of-life system safety requirements in highly complex projects.

However, Australian rail projects and operations sit within a wider context, namely the Rail Safety National Law and its regulatory regime, and other work health and safety legislation and legal duties by which railway and rail-adjacent organisations must abide. These duties are often summarised as a requirement to 'ensure safety is managed SFAIRP', and to ensure 'due diligence' is exercised, and are the overriding responsibility in the Australian rail context.

This 'SFAIRP' concept is explicitly included in Australian rail SSA approaches, but often in a manner that indicating a belief that the implementation of SSA discharges all SFAIRP duties. However, although there is considerable overlap, SSA approaches do not align precisely with SFAIRP principles – particularly when attempting to demonstrate diligence in safety-related decisions-making.

This paper explores how SSA techniques goals and methods intersect with and diverge from SFAIRP requirements. It considers the philosophical underpinnings of systems engineering and the drivers for development of assurance cases, the techniques that have arisen as a result, and the advantages they provide. It then discusses the societal and legal basis of 'SFAIRP' and 'due diligence', and the resulting key elements necessary to that demonstrate reasonable pre-event decisions were made in a manner that stands up to post-event legal scrutiny.

The implementation of SSA approaches in a SFAIRP context are then discussed. Implications of this include:

- Compliance with requirements vs. demonstration of due diligence
- Recognised good practice, and its relation to compliance with standards
- Safety culture in projects and organisations
- Pre-event and post-event assurance in a regulated context.

Finally, the paper presents a synthesis of SSA techniques with a decision-making and implementation model addressing SFAIRP requirements. This incorporation of SFAIRP principles in a SSA framework attempts to maintain the significant benefits realised by systems engineering approaches in complex project while ensuring all reasonable steps are taken to ensure system safety.

CONTENTS

1.0 INTRODUCTION

Systems engineering and its systems safety subset are now deeply embedded in major rail projects in Australia. When dealing with system safety a systems engineering approach, as described in such standards as EN 50126 [Ref 7.1], is often used in tandem with assurance case techniques such as Goal Structuring Notation. This combination of Systems (Engineering) and Safety Assurance (known as SSA) approaches provides a formal, structured, traceable framework to identify, address and verify whole-of-life system safety requirements in highly complex projects.

However, Australian rail projects and operations sit within a wider context, namely the Rail Safety National Law [Ref 7.2] and its regulatory regime, and other work health and safety legislation and legal duties by which railway and rail-adjacent organisations must abide. These duties are often summarised as a requirement to exercise 'due diligence' to 'ensure safety is managed SFAIRP', and are the overriding responsibility in the Australian rail context.

This 'SFAIRP' concept is explicitly included in Australian rail SSA approaches, but often in a manner that indicating a belief that the implementation of SSA discharges all SFAIRP duties. However, although there is considerable overlap, SSA approaches do not align precisely with SFAIRP principles – particularly when attempting to demonstrate diligence in safety-related decisions-making.

Examining the goals and methods of SSA approaches and SFAIRP principles and their underlying philosophies can help to show the gaps and overlaps between the two, and hence ensure rail projects meet their Rail Safety National Law duties.

2.0 THE PHILOSOPHY OF SYSTEMS SAFETY AND ASSURANCE

So exactly what is systems safety and assurance? SSA has arises from a combination of **systems engineering** and **assurance case** approaches being implemented in a **safety context**. These three key elements are briefly described in Sections 2.1-2.3, and their synthesis discussed in Section 2.4.

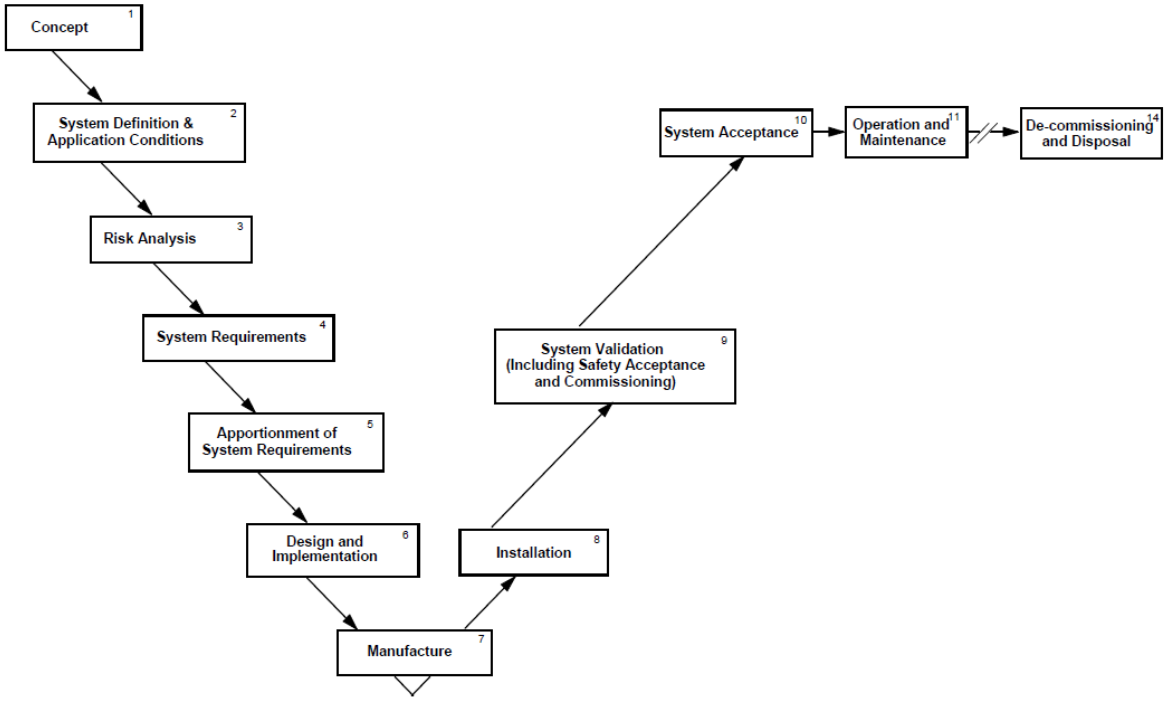
2.1 Systems Engineering

Systems engineering as implemented in the Australian rail industry generally involves, at a high level:

1. Requirements analysis: The identification and analysis of customer needs and goals (that is, business requirements), and decomposition of these into derived system requirements,
2. Design: Functional analysis to define an architecture, system, subsystems and units, to address the derived requirements,
3. Build: Construction of units,
4. Synthesis: Integration of units into subsystems, and subsystems into a complete system (i.e. a product),
5. Verification that the resultant units, subsystems and system meet the derived requirements, and
6. Validation that the resultant system (i.e. product) meets the customer's overarching needs and goals.

Systems engineering focuses on information sharing and traceability through a product lifecycle, from conception to disposal, between client, constructor, operator and other stakeholders. This is often emphasised by formal gateway-style reviews as projects move from one stage to the next. These are generally conducted at system definition, preliminary design, critical design, testing readiness, and system verification. Care is taken to ensure the status of all requirements is monitored throughout the project.

In a rail context this structure is often shown as a classic V-model:



Source: EN 50126-1:1999 S5.2.10 Figure 10 [Ref 7.1]

Safety is addressed within this structure through series of formal risk assessments. Further requirements identified through these risk assessments are added to those derived in the top-down process for ongoing monitoring and implementation.

Other systems engineering models exist, notably those incorporating iteration of stages with early rollout of product. These approaches (Agile, Scrum etc.) are sometimes adopted in fields such as software development but tend to be unsuitable for rail applications due to the inherent safety issues of operating an incomplete system.

Key systems engineering standards used in the Australian rail context include the EN 50126 suite, EN 50129 etc. [Refs 7.1, 7.3].

2.2 Assurance Cases

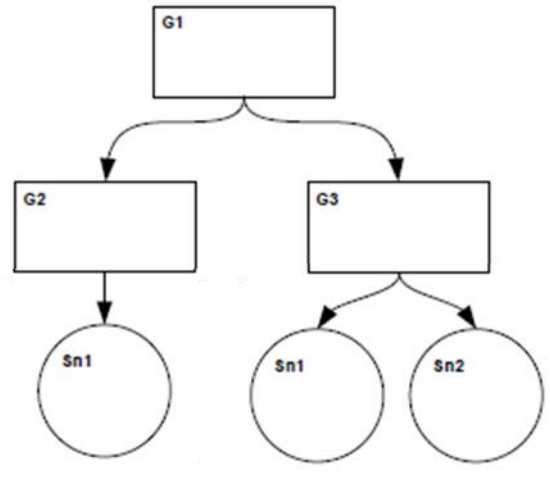
An assurance cases is a formal claim to have achieved an objective (or objectives), supported by evidence. In general, a small number of top-level objectives will be deemed achieved if claims to have achieved a larger number of subordinate supporting objectives are achieved. Evidence 'proving' that an objective has been achieved (i.e. that a specific claim is true) is given in the form of formal documentation.

Assurance cases are used in a range of contexts, including security, safety and dependability. That is, the

A number of schemas exist for documenting assurance cases. These approaches may be graphical or text-based. Graphical approaches include Goal Structuring Notation (GSN) and Adelard Safety Claims Arguments Data (ASCAD).

GSN is the assurance case schema most used in the Australian rail context, often through implementation of the GSN Community Standard [Ref 7.4]. It is essentially a success tree, in which a higher-level 'goal' will be considered achieved if all its subordinate goals are achieved. Lowest level goals are proven (or 'solved') by 'solutions'. Solutions are documented evidence (often described as 'artefacts') – plans, reports, registers, test results etc. Goals, solutions and their relationships may be qualified or further described through 'context' and 'strategy' statements.

Note due to the scale and complexity of rail projects, the evidence provided (the artefacts) often does not formally constitute proof. Rather, it provides assurance to those who rely on it that the claims made are true. For example, assurance that a particular production process has been implemented (the goal) may be provided by an audit report, list of findings and evidence of findings closure (solutions in the form of artefacts).



Goals, sub-goals and solutions in Goal Structuring Notation (adapted from [Ref 7.4])

Two critical aspects of developing assurance cases (including GSN) involve ensuring that:

- Claims (e.g. goals) are completely and explicitly demonstrated by their subordinate goals, and
- Evidence (e.g. solutions) completely and explicitly prove the goals it supports.

Addressing these two key aspects involves detailed critical thinking, often at an early project stages when a lot of uncertainty is present and project objectives are fluid.

2.3 Safety Context

The safety context of the Australian rail industry is the Rail Safety National Law [Ref 7.2] and the duties it places on those who have influence over the safety of rail-related operations. At its highest level, the RSNL states that:

> *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

A person here is meant in the sense of a legal person – e.g. a corporation. Individuals within organisations who work to meet this duty are known as 'officers', and have the following requirement:

> *(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)

So an individual working on a rail project must exercise due diligence to eliminate risks so far as is reasonably practicable [SFAIRP] or, failing that, to minimise risks SFAIRP.

Discharge of this and other duties is overseen the Office of the National Rail Safety Regulator (ONRSR). ONRSR is a statutory body under the RSNL that provides accreditation for rail operations

within Australia. Accredited entities must provide a safety case to ONRSR demonstrating how they have addressed their duties under the RSNL.

Individuals working on Australian rail projects, then, must exercise due diligence to ensure that the rail systems they build and operate are safe SFAIRP by complying with their duties under the RSNL, and do so in a manner that is communicable to ONRSR.

2.4 Synthesis into Systems and Safety Assurance

In Australia at least, the synthesis of SSA from systems engineering and assurance cases within the RSNL safety context involves the following key aspects:

- 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, and
- Documenting these in a manner that addresses RSNL duties, specifically addressing the 'due diligence' and 'SFAIRP' requirements.

This approach appears driven by a number of major factors:

- The increasing complexity of major rail projects, and the information- and requirements-tracing benefits systems engineering provides,
- The availability of SSA standards which are widely used in other locations such as Europe and the UK – e.g. the EN 50126 suite and the GSN Community Standard,
- A recognition of the importance of formally demonstrating the processes undertaken for safety-related decisions as a means of justifying such decisions after any adverse event, and
- ONRSR's acceptance of SSA methods in rail safety accreditation applications.

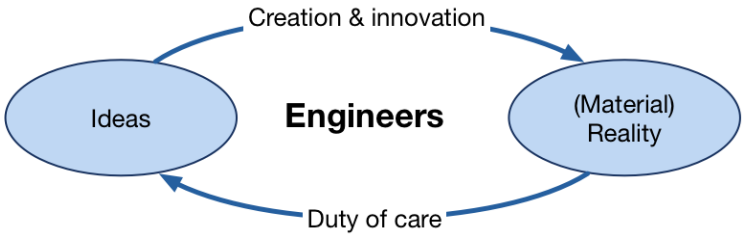
However, compliance with SSA approaches, no matter how strict, does not of itself ensure compliance with the RSNL duties. Section 3 discusses what those duties actually entail.

3.0 RAIL SAFETY IN AUSTRALIA – SFAIRP & DUE DILIGENCE

3.1 Foundations and Duties

The 'due diligence' and 'SFAIRP' duties in the RSNL were adopted from the those in the 2011 Model Work Health and Safety (WHS) Laws [Ref 7.5] adopted in all states except Victoria, which were in turn heavily influenced by Victoria's 2004 Occupational Health and Safety (OHS) Act [Ref 7.6]. The OHS Act adopted the 'SFAIRP' principle after the Maxwell review of Victoria's OHS legislation [Ref 7.7]. This made explicit in Victoria's OHS legislation the notion of 'reasonable practicability', which limits the duty of a person to address a risk to what is 'reasonable' in the circumstances. 'Reasonable practicability' arose from consideration of the more general duty of care under English common law, and how it applied in workplaces and other situations. This duty of care arose in a very real sense from the Golden Rule, or the rule of reciprocity, which states that one should treat others as one would wish to be treated. Or, in a rail safety context, the idea that we should do our best to not damage people through the operation of trains.

When rail projects design and innovate and engineer new rail systems into reality they are simultaneously making real their ideas about how a rail system could work, and making sure the rail system confirms with the idea that we should do our best to not damage people. In other words, the duty to exercise due diligence to eliminate risks SFAIRP or, failing that, to minimise risks SFAIRP. This tension and feedback shown in the figure below between ideas and reality is a fundamental characteristic of engineering.



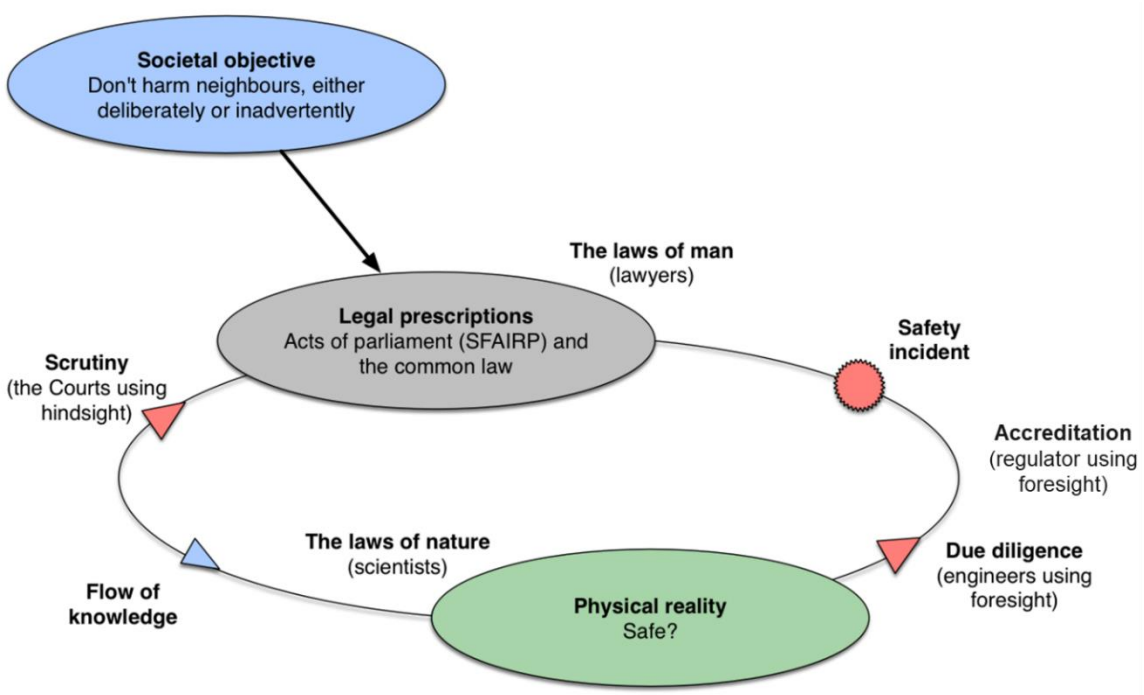
Engineering ideas into reality, and reality into ideas.

3.2 Post-event Scrutiny

But what does the SFAIRP duty actually require? How is it decided if a risk was minimised SFAIRP? How should individuals demonstrate due diligence in this regard?

Given the source of these requirements the answer is perhaps not surprising; the Courts determine this post-event on a case by case basis, with the benefit of hindsight. Engineers, on the other hand, must act to address their SFAIRP duty through due diligence using foresight, a more difficult task. Regulators (such as ONRSR) likewise give accreditation to entities conducting regulated activities (e.g. rail operations) based on pre-event knowledge.

Below is an expanded version of the figure above, showing where engineers, regulators and the Courts fit in this process.



The flow of pre- and post-event knowledge

Understanding how, following a specific event, the Courts go about determining if a SFAIRP duty was discharged throws light on how pre-event 'due diligence' and SSA activities may address the SFAIRP duty.

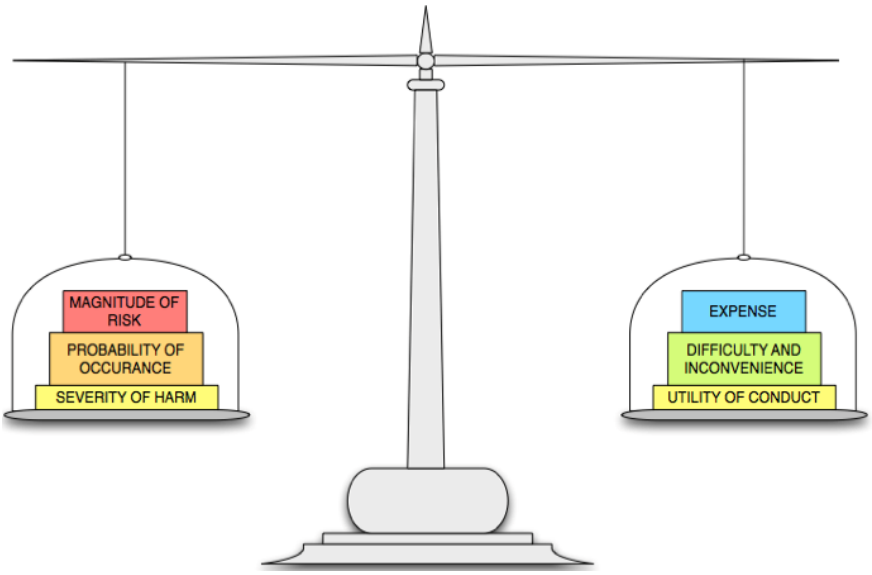
In making this decision the Courts consider two basic questions:

- 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?

When considering reasonableness of measures that could have been in place the Courts will generally take recognised good practice as a starting point. Recognised good practice is a standard to which all engineers are held. It encompasses measures which are demonstrably reasonable due to their implementation in other similar situations.

Good practice is encapsulated in many places, including standards and guidelines for design, operation, asset management and so on. It is also present in regulations, which may contain good practice that is so well recognised that the governments agree that it must be mandated. If good practice is not implemented for a known risk it is unlikely that the SFAIRP duty would be considered met.

The Courts then consider for reasonableness any further options that could have been implemented. This involves a balance of the factors in the diagram below.



The Shirt Calculus (Robinson, Francis & Procter, 2018 [Ref 7.8], adapted from Sappideen and Stillman (1995) [Ref 7.9]

This is based on the Mason J's decision in the High Court in Wyong Shire Council v. Shirt (1980) [Ref 7.10], known as 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.*

Note that nowhere in this process do the Courts use the notion of a 'tolerable' or 'acceptable' level of risk. In fact, they do not consider them appropriate, as stated by Gibbs CJ in Turner v. South Australia (1982) [Ref 7.11]:

> *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.*

Taking into account all of these concepts, the Court determines if, in the case of the event it is examining, individuals exercised due diligence and persons discharged their SFAIRP duty.

3.3 Pre-event Due Diligence

There are essentially infinite ways in which people may be damaged in any particular context, and, correspondingly, infinite actions that may be taken to prevent this. A problem engineers face in rail projects is that in their foresight-based safety-related decisions they must (attempt to) consider all potential people-damaging events, rather than the single events the Courts examine with hindsight. Further, to meet the 'due diligence' and 'SFAIRP' requirements described above, engineers must make these decisions in a way that satisfactorily addresses the Courts' two questions.

A key to solving this problem is realising that 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.

Given this, and taking into account the Courts' approach as described in Section 3.2, engineers should provide compelling answers to the following 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?

Steps necessary to satisfactorily address these questions have been discussed in various places and contexts (see e.g. [Ref 7.8], [Ref 7.12], [Ref 7.13], [Ref 7.15]). These steps are summarised below for application in a rail context.

3.3.1 That there is a formal argument as to why all credible, critical hazards have been identified.

Identification of hazards should comprise a functional completeness check, comparing identified hazards with critical exposed groups (i.e. drivers, maintenance workers, operations personnel, patrons, members of the public, road users etc.) and other critical exposed elements (i.e. property and the environment). This should include all relevant phases (e.g. design, construction, commissioning, operations and decommissioning), as well as degraded operations and emergency situations.

This should be supplemented by a zonal or geographic completeness check, based on hazards that may arise at or from specific assets in particular locations (bridges, turnouts, stations, junctions etc.)

The logic of these hazard identification completeness checks should be scrutinised through an ongoing review of historical rail network safety hazards and incidents. Incident databases such as those maintained by RISSB can be useful for this.

This process should be supported and informed by an ongoing dialogue with the Australian rail industry to understand emerging safety issues and themes. This should include generative interviews with staff and workers, discussion with regulators and feedback from patrons.

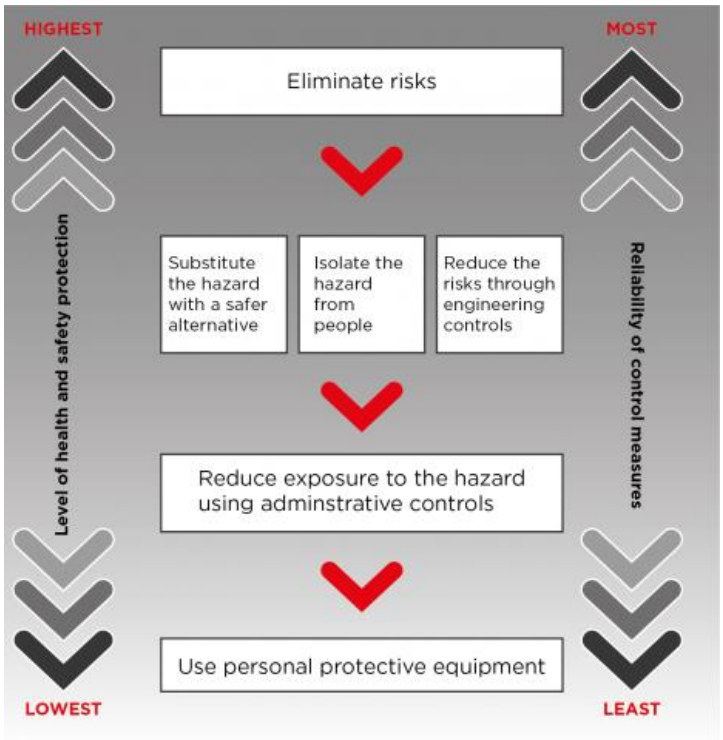
3.3.2 That for each significant hazard all recognised good practice controls are in place, and if not, have been tested for reasonableness, and in the particular circumstances demonstrated as being unreasonable.

Recognised good practice is accepted as the baseline suite of precautions for generic industries. This is codified in international and Australian standards, industry codes and guidelines, and informal but accepted means of addressing common issues.

Persons must provide evidence demonstrating that for each significant hazard all recognised good practice precautions are in place. Where recognised good practice is not considered appropriate reasoning must be provided as to why, showing how the hazard is being managed to a similar standard by different means.

If recognised good practice is not implemented without justification for the critical hazards that it addresses, and no other control is put forward in its place, it is likely the operation in question would be considered prohibitively dangerous.

3.3.3 That 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 as shown in the diagram below.



Hierarchy of control measures, Safe Work Australia [Ref 7.15]

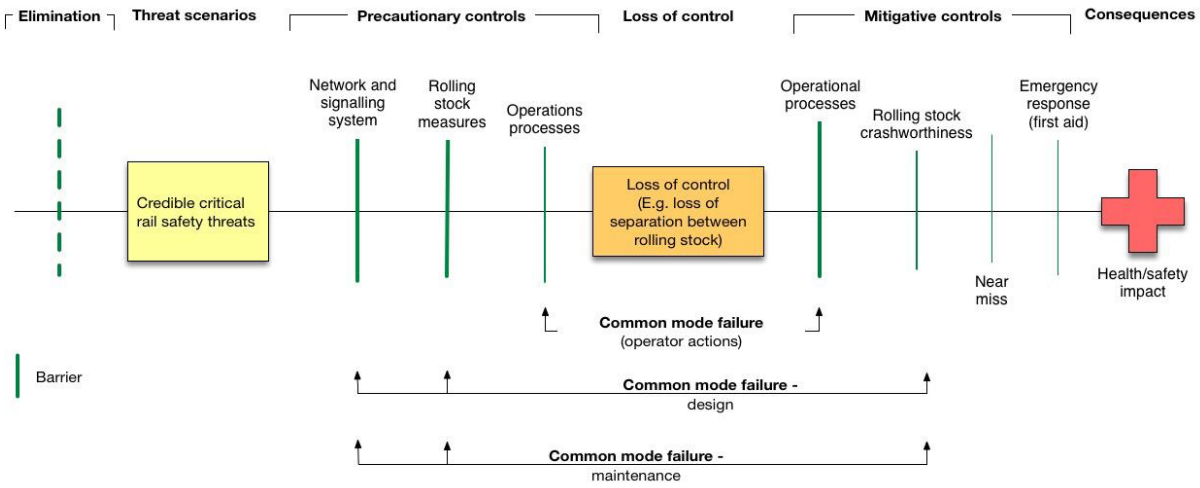
The hierarchy of controls should be applied when considering further controls for a hazard. In Ref 7.14 ONRSR notes that "While the hierarchy of controls is not a feature of the RSNL, the ONRSR still expects duty holders to prioritise more effective and reliable controls ahead of less effective ones."

This must be done regardless of the level of risk as estimated in the ALARP approach. That is, a precaution that moves the estimated risk to a 'tolerable' or 'acceptable' zone must not be adopted at the expense of another control higher up the hierarchy of controls if the latter is justified on the balance of the significance of the risk versus the effort required to reduce it (i.e. the Shirt Calculus).

Similarly, a potential control justified on this balance must not be rejected based on a 'tolerable' risk level. While European SSA standards (e.g. [Ref 7.1]) may require a 'risk tolerability' approach, ONRSR specifically addresses the mismatch between this and SFAIRP requirements, noting that "ONRSR will still expect the duty holder to eliminate or minimise risks assessed as being in this region SFAIRP", in line with the Gibbs CJ judgement quoted in Section 3.2 above.

It should be noted that this process does not necessarily require detailed quantitative or qualitative assessment of risk, especially when dealing with low-probability – high-consequence events where estimations of likelihood are inherently unreliable. Often a better approach is to develop an understanding of the credible worst case of the hazard in question, and the mechanisms through which it may manifest. Using this one can develop, in order of the hierarchy of controls, a timeline of

the controls in place to address it (if any). The potential control can then be assessed based on the incremental benefit it will provide at the point in this timeline that it would act, and the time, difficulty and expense of implementing and maintaining it. This approach is shown in the threat-barrier diagram below.



Threat-barrier diagram for generic rail safety hazards

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

Persons must provide evidence demonstrating that implemented precautions are inspected and maintained to ensure they remain effective. This should be done through formal quality assurance (QA) processes for physical and procedural precautions.

QA for physical precautions would be expected to include evidence of inspections, scheduled maintenance, repairs and so on. QA for procedural precautions would be expected to include evidence of initial and refresher training for staff, scheduled reviews of procedures, formal change management processes and so on.

Depending on the type of rail project this would be provided from a variety of sources, including from the project itself, from the ultimate client (e.g. a state government), the manufacturer, the operator, ONRSR, and so on.

4.0 SSA IN A SFAIRP CONTEXT

Noting the various elements of SSA, and the steps required to meet RSNL and WHS legislation SFAIRP requirements, how do SSA and SFAIRP goals and methods overlap? How do they diverge?

System safety approaches can indirectly follow processes addressing the due diligence requirements of the RSNL and WHS legislation, but can also end up focusing on maintaining detailed records and following standards at the expense of considering what actually constitutes good safety decisions in the specific project context.

SFAIRP approaches, on the other hand, can result in multiple disconnected assessments made within a project with insufficient consideration of overarching project goals and requirements.

The table below identifies specific related aspects of the SSA and SFAIRP approaches on large projects, and determines if the SSA and SFAIRP approaches are aligned, complementary, or misaligned.

SSA approach	SFAIRP approach	Comparison
Context and structure of approach		
Overarching focus on project delivery and achieving safety aspects of gateway reviews.	Overarching focus on post-event decision explanation and justification of safety-related decisions.	**Complementary** – SSA approach help ensure safety-related decisions are made within an overall project context with consideration of project critical success factors.
(Project teams, and hence) documentation structured in subsystems and delivery phases to facilitate project management and delivery.	Documentation structured in manner best explicable for post-event scrutiny. May not provide an efficient structure for project management and delivery.	**Potential misalignment** – clear planning and communication is necessary to ensure documentation is structured in a manner appropriate for post-event scrutiny but without requiring inefficient project structures. Matrix project organisational structures with discipline and package leads can help with this.
Silos and division between safety engineers and design/manufacturing engineers.	Integration of team members and knowledge into a single decision-making process for safety-related matters.	**Complementary** – SFAIRP approach helps break down silos between safety specialists and others.
Formally integrated within project delivery processes.	Is sometimes run in parallel to project delivery processes.	**Complementary** – SSA approach ensures safety decision-making is a formal part of project processes process
Focus on implementation of safety risk management process.	Focus on the unique context and content of the safety risk assessment.	**Complementary** – SFAIRP approach ensures appropriate context and content used within SSA's consistent decision-making process.
Risk identification approach		

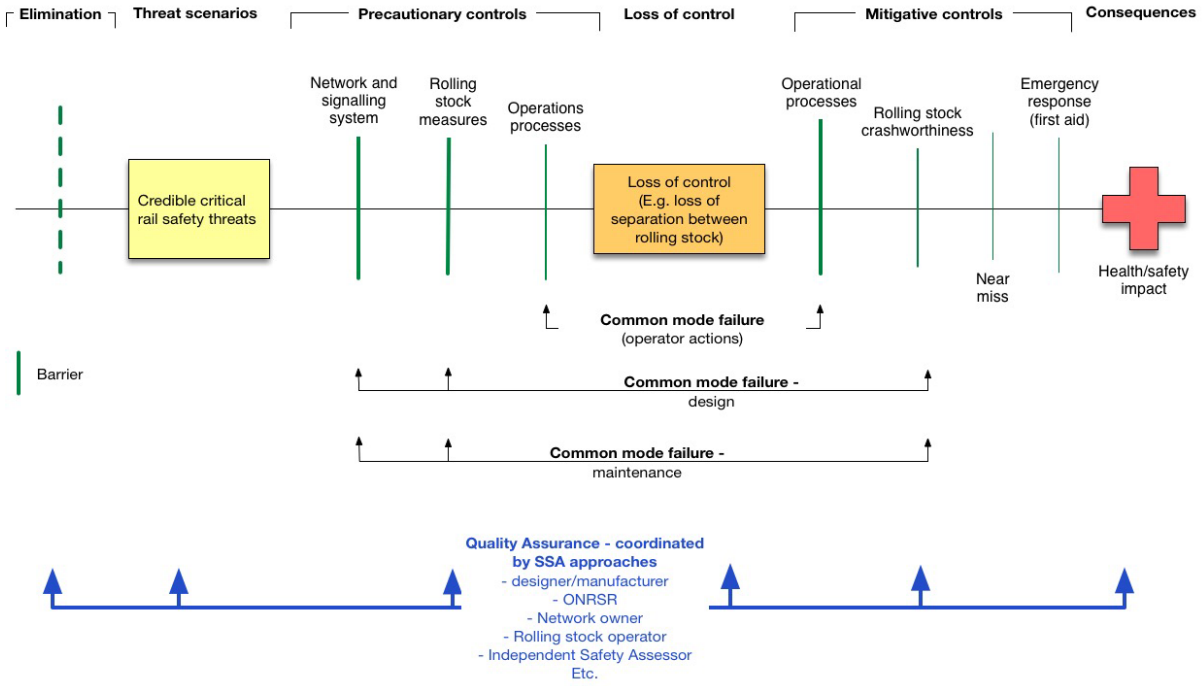
SSA approach	SFAIRP approach	Comparison
May include use of hazard logs, GSN, etc. from previous projects as basis for new projects.	Generates new list of hazards for each assessment, using previous work as a check for gaps rather than a foundation to build on.	**Misaligned** – history is not always a good predictor of the future. Use of existing documentation as the basis for new projects may reproduce any flaws in previous assessments, and may not adequately consider the particular context of the new project. However, understanding of prior thinking and events is essential to a satisfactory SFAIRP approach.
Exhaustive detail may be taken as evidence of completeness in hazard identification.	Formal completeness check required for threat identification.	**Complementary** – SFAIRP formal high-level completeness check indicates where more detailed analysis will (and will not) be beneficial, and ensures detail is within the appropriate context. However identifying many risks will not of itself provide a formal completeness check.
Presence of subject matter experts (SMEs) may be taken as evidence of completeness in hazard identification.	Formal completeness check required for threat identification.	**Complementary** – SFAIRP formal high-level completeness check are best developed in consultation with the best available knowledge of the situation in question. However SMEs in isolation will not provide formal completeness check.
Deliberate excision of 'human factors' from safety assessments can lead to a focus on safety-related usability, ergonomics etc. and an assumption that other persons exposed to hazards are passive.	Deliberate integration of human interaction within the assessment context, and a focus on critical exposed groups at different locations and phases of the project.	**Potential misalignment** – care must be taken to formally consider all critical exposed groups within safety assessments. Formal consideration of all critical exposed groups in all project phases can help with this during safety assessments. Human factors, usability, ergonomics etc. are necessarily part of this.
May identify failed controls as hazards – e.g. non-compliance with standard is a failed control, not a hazard in itself.	Formally differentiates between controls and threats through use of threat timelines.	**Potential misalignment** – care must be taken to understand what the hazard in question is and from where it arises. The 'damaging energy' model is useful in this regard.

SSA approach	SFAIRP approach	Comparison
Controls identification approach		
Focus on compliance with standards.	Focus on understanding the good practice contained in standards, and how it may apply to the situation being considered.	**Misaligned** – mere compliance with standards does not guarantee due diligence has been exercised, nor that something is safe.
May not emphasise recognised good practice as a starting point for controls identification.	Requirement to formally consider recognised good practice.	**Potential misalignment** – recognised good practice must be considered as a starting point for controls identification.
Requirements may arise from decomposition of high-level requirements, or from controls identified in risk assessments. Requirements derived in the overarching context of the project (i.e. high-level project requirements, not just safety).	Identification of controls done within context of assessment, but non-safety-related project goals (i.e. critical success factors) may not be explicitly defined or clearly understood during assessment – may lead to optimal safety outcome at the unnecessary expense of other project goals.	**Complementary –** Explicit understanding and statement of overarching project goals through high level requirements helps ensure
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.	Potential for controls to be stated in a manner that is unclear or not verifiable.	**Complementary –** the combination of a) developing controls and stating them in the manner in which they are to be implemented, and b) translating controls into formal verifiable requirements, helps ensure appropriate controls are linked to clear requirements. Care must be taken to avoid unclear controls being linked to incomplete or generic requirements, and that links are not omitted.
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.	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.	
Approach to determination of reasonableness of controls		
May not include formal consideration of hierarchy of controls when determining which controls to accept and reject. May lead to adoption of simple controls that act lower in the hierarchy at the expense of more complex controls that act higher in the hierarchy.	Requires consideration of hierarchy of controls when determining reasonableness of potential controls.	**Potential misalignment** – hierarchy of controls must be considered in testing potential controls for reasonableness

SSA approach	SFAIRP approach	Comparison
May attempt to demonstrate reasonableness/SFAIRP on a line-by-line basis in a hazard log even if a potential control will apply to more than line (i.e. more than one hazard).	Must consider all benefits provided by a potential control when determining if it is reasonable for implementation.	**Potential misalignment** – SFAIRP decision-making should be done in the wider context of each option considered for reasonableness, not in isolation. That is, all benefits must be considered, not just the risk initially considered.
Inclusion of '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.	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.	**Misaligned** – SSA decision-making processes must align with RSNL and WHS legislation SFAIRP requirements. Decision-making processes involving 'tolerable' and 'acceptable' risk levels do not do this.
Requirement for formal statement that safety risk has been reduced SFAIRP.	No requirement for formal 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.	**Misaligned** – although the requirement for a formal SFAIRP statement ensures the requirement to reduce safety risks SFAIRP is kept as an explicit goal, it can give the incorrect impression that it can be determined before an event that the SFAIRP duty has been discharged.
Approach to control implementation and quality assurance		
Focus on positive demonstration of claims through provision of evidence (assurance case approach).	Requirement for positive demonstration of discharge of duties through provision of evidence (due diligence requirement).	**Aligned**.
Focus on evidence-based proof that requirements have been implemented in design and manufacturing.	Requirement that implemented controls be maintained and not eroded over time, but may assume that an organisation's existing quality assurance system is sufficient to do this.	**Complementary** – SSA's formal traceability and proof of control implementation (including ongoing maintenance) is essential.
May confuse controls and quality assurance measures – for example a safe work procedure is a control, but training is quality assurance to ensure the procedure is followed correctly (i.e. that the control is effective).	Formally differentiates between controls and quality assurance.	**Potential misalignment** – care must be taken to understand the measure that directly addresses the risk in question (i.e. the control) and to not simply rely on quality assurance (e.g. training) with the assumption that the control (e.g. the procedure) is correct.

5.0 SYNTHESIS OF SSA AND SFAIRP REQUIREMENTS

Section 4 shows a great potential for synergy between SSA and SFAIRP approaches, albeit with some misalignments. In essence, this comes from the melding of good decision making – using SFAIRP requirements – with formal process implementation – using SSA approaches.



However, to achieve a successful synthesis of SSA and SFAIRP it is critical to remember that SSA is a tool used to achieve a goal, not a goal in itself. The goal here is safety, and in the Australian/NZ context that is eliminating or (failing that) reducing risk SFAIRP. SSA gives us an approach to help achieve that, but, but will not achieve it by simple implementation, no matter how strict.

Particular care should be taken with respect to the following items.

- **Context and structure of approach**
  Projects must ensure that project documentation is structured and written in a manner that clearly describes safety-related decision processes and outcomes, and not simply provide outputs of project teams organised by discipline. Matrix project organisational structures with discipline and package leads can help with this.

- **Risk identification approach**
  Projects must ensure a formal high-level completeness check is undertaken for hazard identification, supported by SSA approaches. This means that:
  - Incident databases and previous work must be used as a checklist, not a foundation,
  - The presence of all relevant SMEs is a starting point, not a sign-off for completeness,
  - All critical exposed groups should be formally considered in all project phases, with human factors, usability, ergonomics etc. informing hazard and control identification.

  Projects should describe identified hazards in terms of the safety impact that may eventuate (e.g. in terms of the damaging energy), as opposed to in terms of a failed control (e.g. non-

compliance with a standard). This allows clearer explanation of the reasonableness of other potential controls considered.

- **Controls identification approach**
  Projects should ensure that recognised good practice is considered as a starting point for controls identification, not as a sign-off that all reasonable controls are in place. In particular, projects should note that compliance with standards does not guarantee due diligence has been exercised, nor that something is safe. The ideas contained in the standards are the good practice, not the standards themselves. This distinction is especially critical when multiple standards can be chosen to address the same risk (see e.g. [Ref 7.16]).

  Projects should also ensure that identified controls are all linked to requirements, and that the requirements cover the whole of the controls in sufficient detail that the intent of the control is met during requirements implementation.

- **Approach to determination of reasonableness of controls**
  Projects must ensure that SSA decision-making processes align with the SFAIRP requirements of the RSNL and WHS legislation. In particular:
  - The hierarchy of controls must be considered in testing potential controls for reasonableness,
  - Testing for the reasonableness of a specific potential control should consider the benefit it brings to all hazards it works upon, not only the line in the hazard log being looked at.

  Projects should note that decision-making processes involving 'tolerable' and 'acceptable' risk levels do not satisfy SFAIRP requirements. Projects should note that the decision-making processes in some European standards (and those influenced by European standards, e.g. the AS4292 suite [Ref 7.17]) are framed in terms of 'tolerable' or 'acceptable' levels of risk and the ALARP framework. This feeds into functional safety requirements and Safety Integrity Level (SIL) ratings (see e.g. AS61508 [Ref 7.18] and [Ref 7.3]) and mixes quite thoroughly the ideas of tolerable risk and recognised good practice. While benchmarking of risk levels is appropriate and can help identify outliers requiring closer review it does not form a sign-off in and of itself.

  Projects should exercise caution when justifying rejection of potential controls using quantified risk levels, gross disproportionality factors and measures such as the value of statistical life, as these may represent a measure of risk 'tolerability' that may be misused through adjustment of a gross disproportionality factor or the value of statistical life.

  Projects should also note that providing a statement that all risks are reduced SFAIRP does not make this so, and may discourage consideration of further potential controls.

- **Approach to control implementation and quality assurance**
  Projects should embed the SFAIRP decision-making process with the typically robust SSA quality assurance procedures to ensure reasonable controls are implemented and maintained. However, projects should ensure that quality assurance is not identified as a control in and of itself. Rather, it should be described as the activities that support controls to ensure they remain effective.

In summary, SSA approaches can provide an efficient and effective framework within which robust safety-related decisions can be made using SFAIRP requirements.

6.0 CONCLUSION

System Safety and Assurance and SFAIRP requirements are each of significant value to the rail industry, and hence to society as a whole. However often, depending on the scope, scale and industry, an attempt is made to shoehorn one into the other, often informally. This is manifestly inadequate; more often than we realise we are saved by good project managers, good engineers and the low probabilities of adverse safety outcomes that together they ensure. This never works forever.

Complex rail projects need a SFAIRP-based approach to system safety (or a system safety-based approach to SFAIRP). This paper has examined where SSA and SFAIRP complement each other, and presented the concept of a synthesis that could be expanded and implemented. The author hopes it informs future Australian rail projects.

7.0 REFERENCES

7.1 EN 50126:1999 – *Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)*, *Part 1: Basic requirements and generic process* and *Part 2: Guide to the application of EN 50126-1 for safety*.

7.2 State Government of South Australia (2012), *Rail Safety National Law (South Australia) Act*.

7.3 EN 50129:2003 – *Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling*.

7.4 Origin Consulting (York) Limited (2011), *GSN Community Standard Version 1*.

7.5 Safe Work Australia (2011), *Model Work Health and Safety Laws*.

7.6 State Government of Victoria (2004), *Occupational Health and Safety Act*.

7.7 Maxwell, C. (2004), *Occupational Health and Safety Act Review*, Department of Treasury and Finance, State Government of Victoria.

7.8 Robinson, R., Francis, G., & Procter, T., (2018), *Engineering Due Diligence (10th Ed)*.

7.9 Sappideen, C, & Stillman, R. H., (1995), *Liability for Electrical Accidents: Risk, Negligence and Tort*. Engineers Australia Pty Ltd, Sydney.

7.10 High Court of Australia, *Wyong Shire Council v. Shirt* (1980) 146 CLR 40.

7.11 High Court of Australia, *Turner v. South Australia* (1982) 42 ALR 669.

7.12 R2A Pty Ltd, (2016), *Electricity Network Safety Management System Formal Safety Assessment Audit Guidance*. Prepared for New South Wales Independent Pricing and Regulatory Tribunal. Available on IPART website.

7.13 Office of the National Rail Safety Regulator (2016), *Guideline: Meaning of duty to ensure safety so far as is reasonably practicable – SFAIRP*.

7.14 Engineers Australia (2014), *Engineers Australia Safety Case Guideline 3rd Edition*.

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

7.16 Procter, T., & Henderson, L. (2016), *Rail Tunnel Fire Safety System Design in a SFAIRP Context*. Presented at Conference of Railway Excellence, Melbourne, 2016.

7.17 Australian Standard 4292:2006 – *Railway safety management Part 1: General requirements* and *Part 3: Rolling stock*.

7.18 Australian Standard 61508:1999 – *Functional safety of electrical/electronic/programmable electronic safety-related systems*.