



Application of SFAIRP and ensuring a sustainable rail future

ROB SCARBRO

Background

- ❖ Royal Navy – Nuclear Submarine, Nuclear Control Systems and Reactor Plant Safety Justification
- ❖ Engineering Safety Practitioner since 2001
- ❖ Development of Safety Cases for Warships, Ordnance and Warships in Harbour, Nuclear Systems and Rail Projects and Rail Operator Engineering / Systems Safety Assurance
- ❖ Rail Examples include:
 - ❖ Waratah Train Project Design Safety
 - ❖ Sydney Metro Northwest Rail Link
 - ❖ RailCorp reform safety assurance
 - ❖ Fire Life Safety for Sydney Trains
 - ❖ Independent Certification of New Generation Rolling Stock QLD
 - ❖ Independent Safety Assessment – Sydney Metro Northwest, Metro Tunnel Project reference Design, SAP EAM implementation Sydney Trains
 - ❖ Director Systems Integration Metro Tunnel Project
 - ❖ Chief Engineer – Rail DoT

Expectations and Experience in Safety Risk

Through past experience, the success of managing safety risks falls to some key elements:

- ❖ Organisations have established approaches to undertaking safety risk assessments and hazard analysis, normally highly structured, Hazard and Operability, Structured What If, HAZID and Day in the Life of Techniques
- ❖ Risk analysis conducted by competent professionals and the inputs are gained with suitably qualified and experienced personnel from a domain and SME perspective (SMEs bring knowledge of known solutions for known problems, which supports the reasonableness)
- ❖ Hazards and risks captured clearly, controls linked causes
- ❖ Compliance to all standards does not equal safety, evidence of using standards must show they mitigate the risks
- ❖ Likelihood and consequences developed based on empirical data, international references where empirical data isn't well captured
- ❖ Controls identified to prevent the hazard eventuating or mitigate the consequences well defined and measurable and verifiable

Other key points to support Safety Arguments:

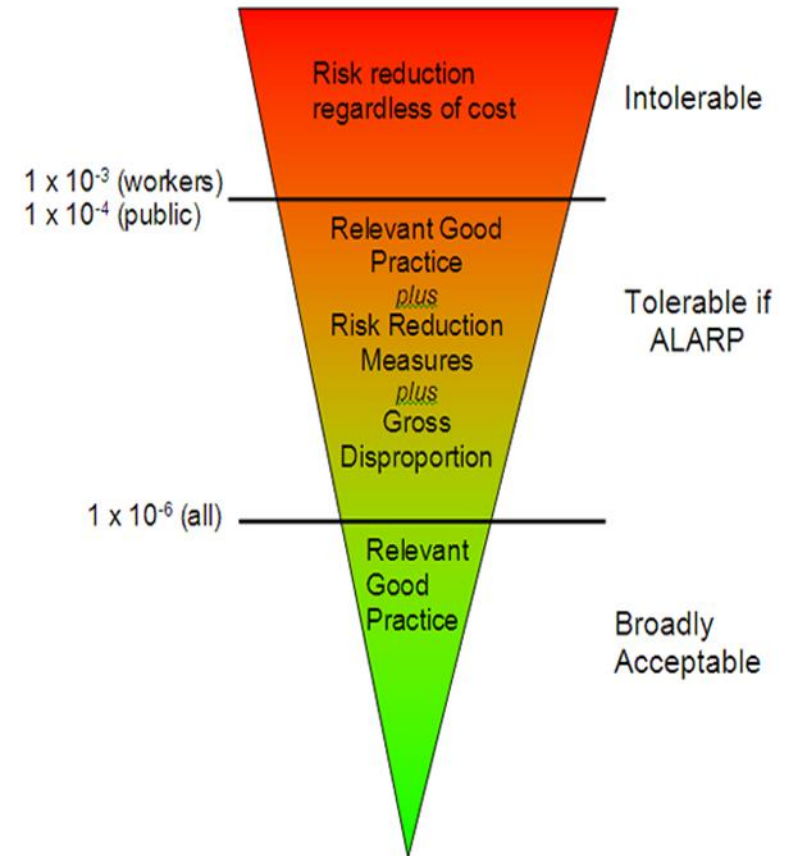
- ❖ Use contemporary good and appropriate standards and understanding how they manage specific hazards
- ❖ Expert Elicitation
- ❖ Benchmarking where appropriate

Are there any key differences between ALARP and SFAIRP?

- ▶ ONRSR Guideline Meaning of Duty to Ensure **Safety** SFAIRP
[https://www.onrsr.com.au/__data/assets/pdf_file/0009/2412/Guideline-Meaning-of-Duty-to-Ensure-Safety-SFAIRP.pdf]
- ❖ Sometimes the term As Low As Reasonably Practicable (ALARP) is used by the rail industry. Both ALARP and SFAIRP have at their core the concept of '**reasonably practicable**'. The ALARP framework was originally developed to assist those with legal obligations for safety to comply with these obligations. The ONRSR considers that those duties to ensure safety SFAIRP and the ALARP framework generally both call for the same tests to be applied. In legal proceedings, the particular term cited in the relevant legislation will be used. While some legislation in Australia cites the term ALARP, in the case of the RSNL the term cited is SFAIRP.
- ❖ Common Safety Methods and WHS Model Regs – where a risk is well understood and controlled by standards and procedures, explicit risk assessment is not required

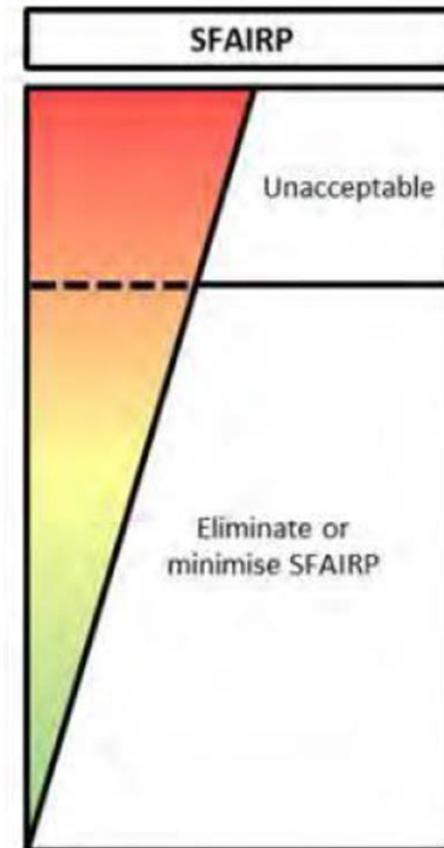
As Low As Reasonably Practicable - ALARP

- The principle that requires risk owners to do whatever is reasonably practicable to reduce risk, even if the risk is deemed tolerable.
- It does not require all risks to be eliminated; but it puts focus on the more significant (higher) risks.
- If risk is in Broadly Acceptable region, further effort to reduce risk not likely to be required.
- However, “*duty holders must reduce risks wherever it is reasonably practicable to do so or where the law so requires it*”.



So Far As Reasonably Practicable - SFAIRP

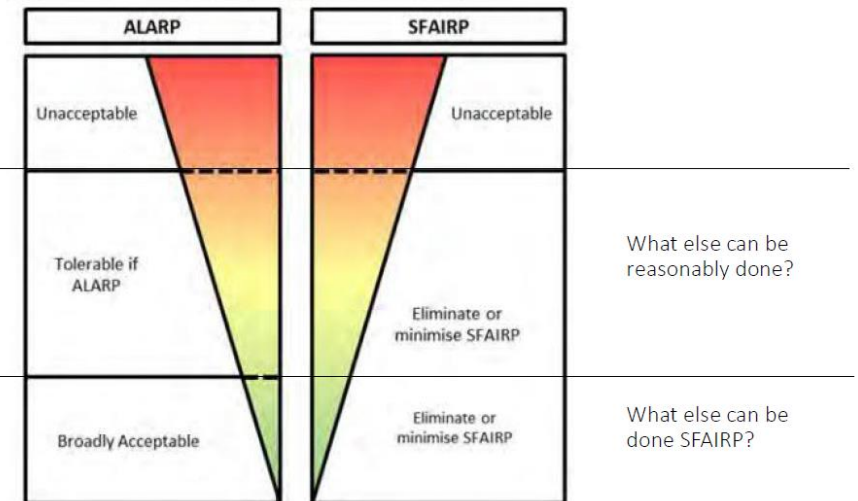
- The duty of a company to ensure health and safety so far as is reasonably practicable ("SFAIRP").
- This requires a company:
 - a) to eliminate risks to safety so far as is reasonably practicable; and
 - b) if it is not reasonably practicable to eliminate risks to safety, to reduce those risks so far as is reasonably practicable.
- SFAIRP does not require everything possible to be done; however it does require everything possible that is practicable to be done, irrespective of the magnitude of the risk.
- The concept of SFAIRP is to achieve the best possible safety outcomes, to the extent that is "reasonably practicable".



Comparison of SFAIRP vs ALARP

- Both HSE and ONRSR consider that: *“duties to ensure health and safety so far as is reasonably practicable (“SFAIRP”) and duties to reduce risks as low as is reasonably practicable (“ALARP”) call for the same set of tests to be applied.”*
- The two terms mean essentially the same thing and at their core is the concept of “reasonably practicable”; this involves weighing a risk against the trouble, time, and money needed to control it.
- Demonstrating that safety risks are ALARP should give confidence that the SFAIRP legal requirement has been (will be) satisfied.
- However, for SFAIRP, it does not matter how low the risk estimate is, if more can be done for very little effort (control must be reasonably practicable), then the failure to do so would be considered negligent in the event of an incident.

ONSRSR – “We would not normally expect lengthy studies, CBA etc for risks in the ‘broadly acceptable’ region”



SFAIRP application at the working level

► **Regular examples encountered:**

- “You shouldn’t use likelihood to consider implementing these controls, it wouldn’t be SFAIRP”
- You’re not SFAIRP unless this is implemented (Without any anchoring to the safety risk and risk reduction an activity assertedly manages)
- If it is technically possible, then it must be done
- If you can do it you MUST or it isn’t SFAIRP
- Precautionary Principle used to argue erring on side of safety, irrespective of risk, in railways, we have good knowledge of the consequences
- Gross disproportion isn’t an acceptable justification alone not to do something
- You must do it because SFAIRP requires you to apply “What you ought reasonably know” (without the other aspects to this statement about the risk, likelihood, consequence and identified safety controls to manage the risk)
- SFAIRP is different to ALARP and if you can do it you MUST
- If you touch an asset (regardless of the scope of a project / or change) you inherit the uplift to a “SFAIRP standard” regardless of if the risks are not changed by the project and are already accepted
- ALARP is all about QRA/CBA and justifying not implementing controls

Emerging effects of these statements

► What's wrong with the Statements:

- The statements are rarely anchored on the discussion of risk, the link that the RSNL and other safety legislation is about managing **Safety Risk** So Far As is Reasonably Practicable appears lost
- Rejection of solutions on grounds individuals have deemed it isn't SFAIRP moves from a well established defensible process of established risk assessment processes, with experienced people, gaining consensus of controls and effectiveness and the level of residual risk, along with determining what else is reasonably practicable for the **level of remaining risk and further elimination or reduction**
- In past experience, engagement about engineering safety focuses on the safety risk, the use of SFAIRP in the absence of safety risk, loses the meaningful discussion and understanding of the safety risks, to ensure reasonable and appropriate controls are implemented to effectively manage safety
- Industry focuses so much on Safety in Design Workshops and SFAIRP, it has lacked maturity in risk management, as required by ONRSR and other safety regulators as the key to managing safety risk effectively
- Nobody intending to drive a poor outcome, but see their role of guardian of SFAIRP and there is an overall risk aversion, rather than inputting into effective risk management process

Summary

- ▶ In summary
- We need to advocate and ensure the discipline of managing **Safety Risk – So Far as is reasonably practicable** is better understood
- We should ensure we are meeting the SFAIRP test of implementing reasonable controls, but noting that there is a finite amount of tax payers money and we need to ensure the optimal safety risks are managed while maintaining a sustainable transport solution
- Solutions need to fit in funding envelopes, with solutions built on good practice and management of novel risks, or identified industry improvements
- Direction of disproportionate costs to lower order risks, or the costs of over-analysing to achieve no change increases the costs of sustaining railways and costs to taxpayers and/or passengers, potentially reducing funding for future projects that would deliver material safety benefits, such as reducing level crossing removals.
- There is an apparent fear of making risk based decision, which moves to an apparent need for individuals to form views of SFAIRPness rather than relying on the established processes and consensus through the process.
- Writing of standards where the authors do not incur the costs, can further drive costs, with the lack of clear risk analysis of stated risk improvement, versus the costs incurred.

Summary

- ONRSR's guidelines and other referenced material provides a clear well articulated overview of SFAIRP; but
- At a working level there appears to be a lack of understanding and a fear of SFAIRP in relation to managing safety risk, and/or fear of not doing everything in case something happens in the future regardless of risk;
- Focus on Safety in Design, Compliance and SFAIRP but lacking mature management of risk and clear paths to communicating managed risk, residual risks and rejected controls to inform "Decision Makers" ultimate risk acceptance authorities
- As captured in ONRSR guidelines "There are no guarantees that a court will agree with a duty holder's determination of what is or was 'reasonably practicable' in a given situation, however, it is far more probable the court will agree with the duty holder's determination of what is or was 'reasonably practicable' **if a process of justified decision making is adhered to.**"
- By spending significant money on either controls that are disproportionate for the safety benefit, we drive ongoing increases into both new rail projects and operating expenditure, which can raise question about future projects and sustainability of the railways. At the broader level, if focusing on low level risks to an unsustainable level, we may prevent or minimise future rail projects and lose the safety benefit of removing cars off roads, where we have much higher safety incidents.
- Based on the above, it is incumbent on us as an industry to ensure managing safety risk SFAIRP is understood, that we equip our people to understand their part in contributing to safety risk and maintaining a sustainable industry