

# Safety so far as is reasonably practicable What does it mean?

Richard Adams, Manager, Safety & Risk Assurance



# Legislation – the requirement for SFAIRP

Requirement to ensure safety SFAIRP is enshrined in legislation:

- Rail Safety National Law – for railways

*A rail transport operator must ensure, so far as is reasonably practicable, the safety of the operator's railway operations*

*A person who designs, commissions, manufactures, supplies, installs or erects any thing.....must ensure, so far as is reasonably practicable, that the thing is safe if it is used for a purpose for which it was designed, commissioned, manufactured, supplied, installed or erected...*

- Work Health Safety Act 2011

# Legislation – the requirement for SFAIRP

## Work Health Safety Act 2011

*A person conducting a business or undertaking must ensure, so far as is reasonably practicable, the health and safety of;*

- *Workers engaged, or caused to be engaged by the person, and*
- *Workers whose activities in carrying out work are influenced or directed by the person;*

*while the workers are at work in the business or undertaking*

Doesn't just apply to safety of workers:

*A person conducting a business or undertaking must ensure, so far as is reasonably practicable, that the health and safety of other persons is not put at risk from work carried out as part of the conduct of the business or undertaking.*

# SFAIRP Vs ALARP and Risk Tolerability

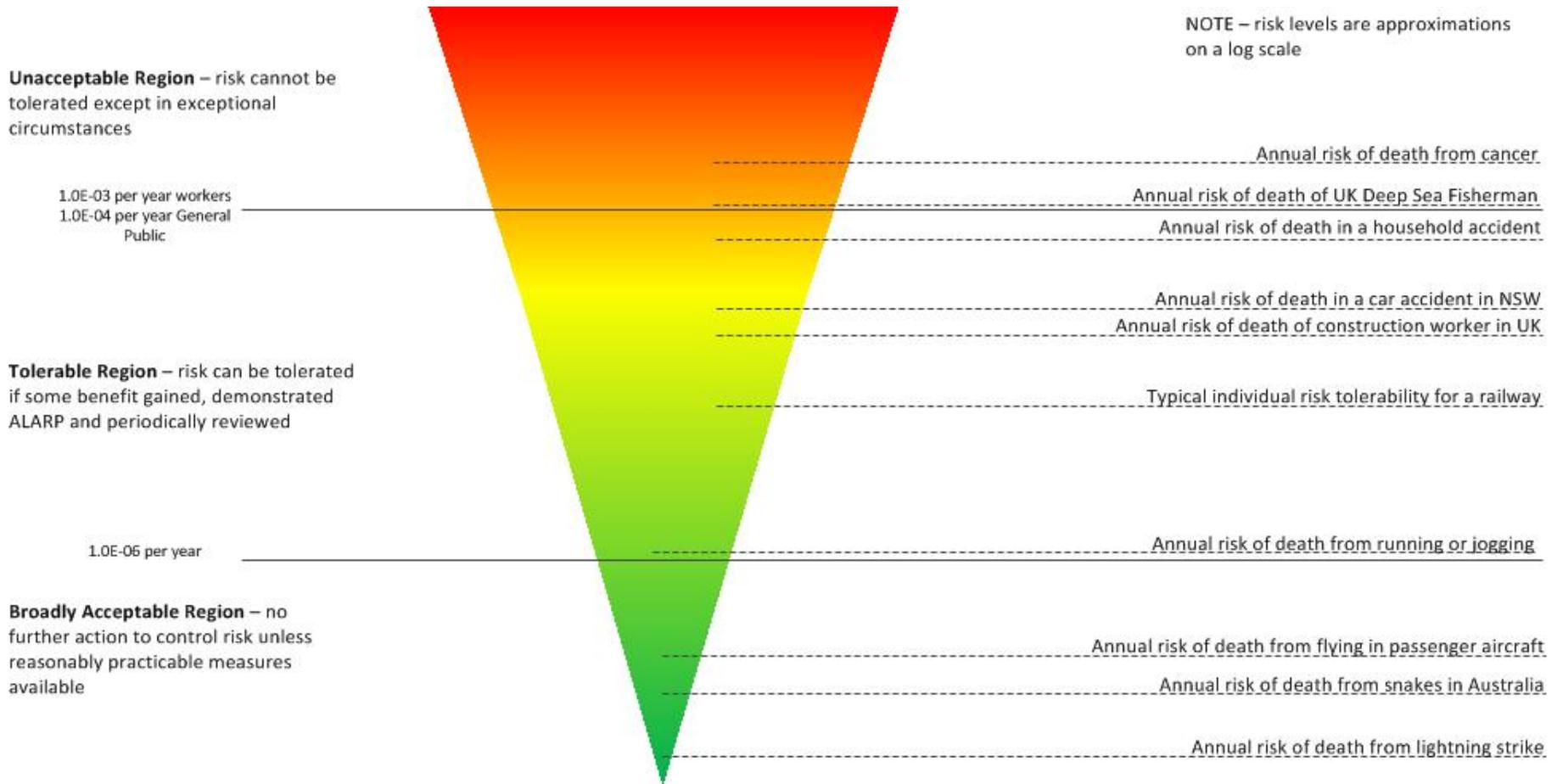
## ORNSR:

*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.*

## UK Health and Safety Executive:

*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. Thus, ALARP describes the level to which we expect to see workplace risks controlled.*

# Risk Tolerability – Typical Risk Levels



# Key concepts

- Reasonable Practicability

*“‘Reasonably practicable’ is a narrower term than ‘physically possible’ ... a computation must be made by the owner in which the quantum of risk is placed on one scale and the sacrifice involved in the measures necessary for averting the risk (whether in money, time or trouble) is placed in the other, and that, if it be shown that there is a gross disproportion between them – the risk being insignificant in relation to the sacrifice – the defendants discharge the onus on them.”*

# Key concepts

Reasonable Practicability continued:

Rail Safety National Law and the WHS Act 2011 define reasonably practicable as:

*..reasonably practicable means that which is, or was at a particular time, reasonably able to be done to ensure safety, taking into account and weighing up all relevant matters including:*

- a) the likelihood of the hazard or the risk concerned occurring; and*
- b) the degree of harm that might result from the hazard or the risk; and*
- c) what the person concerned knows, or ought reasonably to know, about the hazard or risk, and ways of eliminating or minimising the risk; and*
- d) the availability and suitability of ways to eliminate or minimise the risk; and*
- e) after assessing the extent of the risk and the available ways of eliminating or minimising the risk, the cost associated with available ways of eliminating or minimising the risk, including whether the cost is grossly disproportionate to the risk.*

# Key concepts

## Gross Disproportion

- When balancing costs against safety must bias calculation in favour of safety
- No guidance in law or the courts on level – duty holder has to make judgement
- Practice suggests between 2 and 10 dependent on level of risk or consequence
- Also addresses in accuracy in the assessment of risk

## Value of Preventing a Fatality

- To compare costs and safety benefits must convert into currency
- Also known as Value of a Statistical Life (VoSL)
- UK HSE publishes its VpF – not so in Australia

# Key concepts

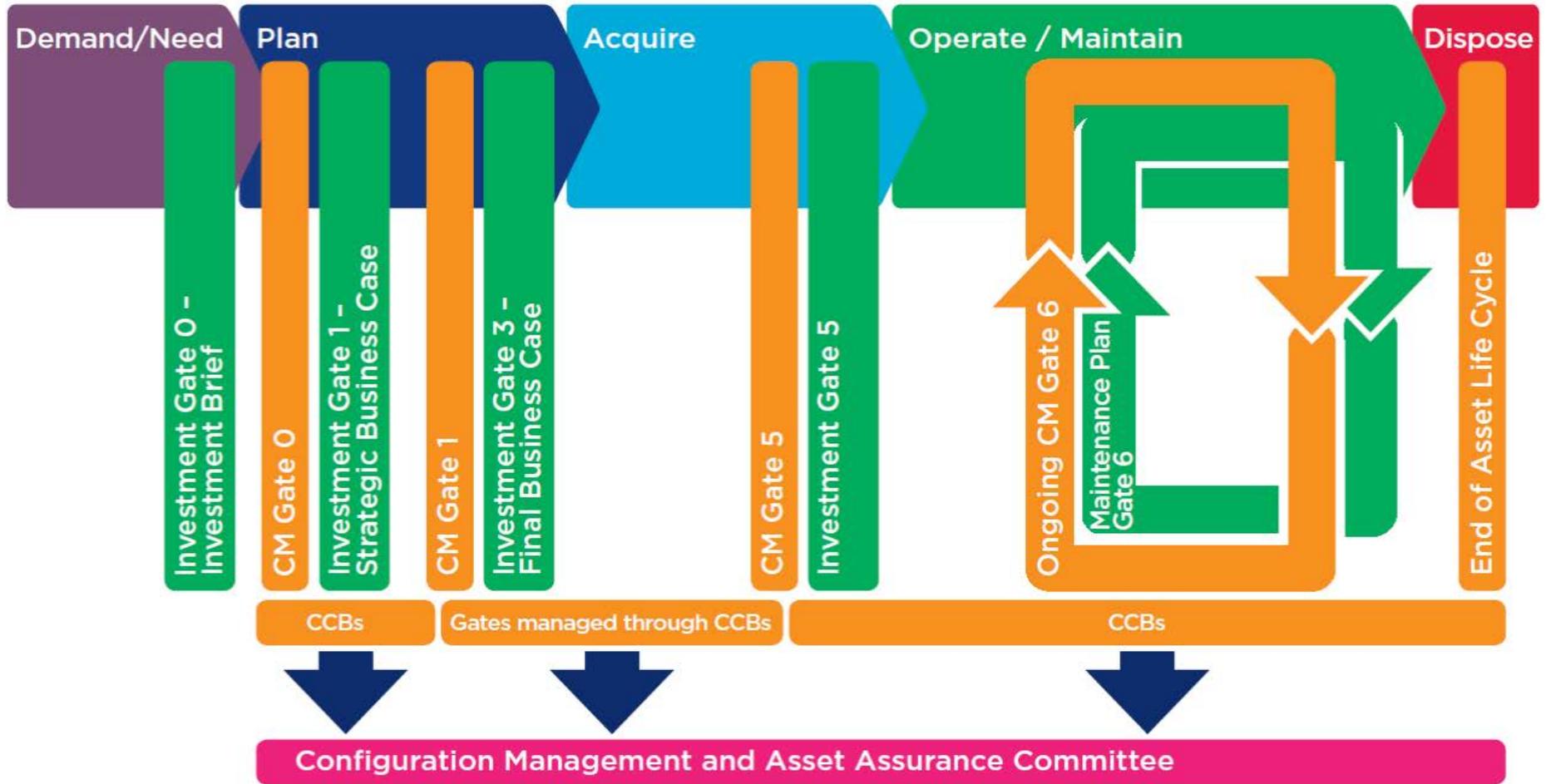
## Equivalent Fatalities / Fatality Weighted Index

- Risk consequences may have various levels – minor injuries, major injuries, fatalities
- To facilitate balance of cost against safety benefit need a measure of consequence
- Equivalent fatality = 1 fatality = 10 major injuries = 200 minor injuries
- Fatality Weighted Injury = 1 fatality = 10 major injuries = 200 minor injuries = 1000 non-reportable minor injuries (under UK RIDDOR)
- Fatality and Serious Injury – used for European Common Safety Targets = 1 fatality = 10 serious injuries

## Ability to pay

- Cannot influence SFAIRP decisions
- Risk exposure cannot be dependent on duty holders financial position

# SFAIRP through the asset lifecycle



# How do we demonstrate SFAIRP?

- Two types of safety decisions:
  - Strategic decisions necessary to meet legal duty or because it makes commercial sense for the business
  - Considering the control of an identified risk
- Good practice arguments
  - Evidence of good practice in similar environment
  - Argument for applicability required
  - Not suitable for novel applications
- Expert judgement
  - Assure the competence of the expert(s)
  - Record the judgement
  - This is not just a workshop activity
- Quantitative analysis
  - Cost benefit analysis

# Planning Phase – Safety Decision Making

- Planning phase is about optioneering and strategic decision making hence making safety related decisions
- Key decisions at this stage have potentially the greatest impact on safety risk
- All decisions need to support a SFAIRP outcome
- Example – extending the life of rolling stock – which is the SFAIRP outcome
  - Extending the life of existing rolling stock with outdated safety controls
  - Re-fitting to provide some improvement in safety functionality – but which?
  - New fleet of rolling stock

# Planning Phase – Safety Decision Making

## Safety Decision Making

- Sound decision making framework
- Scoping of Decisions
- Analysis – understand the risks – legislation, standards, good practice
  - Can be qualitative or quantitative
  - Balancing safety with other risks and opportunities
  - Identifying the optimum risk solution supported by evidence
- Make decision – transparent, rationale and documented
- Review the decision
- Needs to feed into business case and CMAAC submission
- CMAAC Gate1 requirement for specified system to ensure safety SFAIRP

# SFAIRP in Design

- SFAIRP to be considered in all phases of design
  - SFAIRP demonstration is always required
- Key is integration of system safety activities into design process
  - Hazard Log is key – links safety risks and design requirements
  - Designer's awareness of safety risks and hazard log content
- Each design decision is potentially a safety decision and should be recorded
- Record of discarded options is at least as important as those included
- Consider the holistic risk of design when considering design options
  - Reducing one risk may increase or introduce other types of risk
- Must assure than all reasonably foreseeable risks identified
- Must apply the hierarchy of controls

## Hierarchy of Controls

**Elimination**

**Substitution**

**Isolation**

**Engineering Controls**

**Administrative Controls**

**Personal Protective Equipment**

# Elements of a Design SFAIRP Demonstration

- Compliance with standards – they generally represent good practice
- All safety risks are identified and controlled
  - For each risk controls are identified and reasonable practicability considered – rejected controls must be recorded
  - Hierarchy of controls applied and evidenced
  - Holistic view of risk considered
  - Is the design the 'SFAIRP' design not just are all the identified risks managed to SFAIRP
- All design decisions are documented including rejected options
- Use of expert opinion where necessary – this can be the designers
- Engagement with relevant stakeholders in the future risk – operator / maintainer and asset owner
- Cost Benefit Analysis / QRA where beneficial
- Assurance evidence:
  - Fully managed hazard log
  - Technical safety justification for the asset (significant changes)

# The role of standards in SFAIRP

- Standards generally represent good practice
- The standards development process needs to consider SFAIRP
- A SFAIRP / Safety Argument cannot generally rely entirely on standards
- ASA has a standards assurance process:
  - Risk register justifying that standard provides all reasonably practicable risk controls
  - Assurance documents for significant or novel standards that provides SFAIRP argument

# SFAIRP – existing Vs new or altered assets

- SFAIRP in the operational phase is a challenge
- Many existing assets do not have a SFAIRP justification
- New or altered assets should have – safety argument must consider risks at network level
- Challenge is where to spend available resources to maintain network safety and to address areas that may not be SFAIRP i.e. reasonably practicable to upgrade / replace – despite ability to pay not supporting SFAIRP judgements
- We can't do everything at once
- Asset Management Framework and CMAAC Gate 6 try to address this
- Must understand the risks on the network and prioritise
- Some tools in place to support this:
  - ALCAN model
  - Level crossings model

# Cost Benefit Analysis

- Detailed quantified analysis of costs against benefits
- Must be part of a decision making framework - cannot provide the only justification for a SFAIRP decision
- Cannot undermine standards or good practice

## Benefits

- Generally for a SFAIRP justification looks at safety benefit – converted to currency by VpF

## Losses

- Capital costs
- Through life costs
- Safety losses
- Costs of asset repair

# Cost Benefit Analysis

- Gross disproportion must be considered i.e. decision must be biased in the favour of safety
- Must consider options, benefits and costs as if they are a concept – it is NEVER EVER acceptable to say we are too far through the change – it is now too late and expensive to put it right – THAT IS NOT SFAIRP

## Limitations

- Complex and expensive – in many cases a common sense qualitative analysis or scoping calculation can reach the correct outcome
- Requires adequate data
- Must be supported by a comprehensive risk identification activity – all relevant risks must be understood
- In accurate due to complex modeling and data

# Removing controls

- Sometimes called reverse SFAIRP / ALARP
- Possible to attempt to argue that an increase in risk is merited due to cost reductions and /or operational benefits
- Would have to consider that good practice is maintained and previous experience is considered generally unlikely to be successful
- Removing controls
- Demonstrate change in circumstances
- Current position clearly exceeds the SFAIRP position
- Risk is low and control measures conservative
- Obsolescence issues but must consider replacement controls

# What does SFAIRP mean to the ASA?

Impacts almost everything we do:

- Standards – support SFAIRP and must be justified as SFAIRP
- Concessions – must ensure safety SFAIRP
- Non-conformances – must ensure safety SFAIRP
- Type approval – must assure product ensures safety SFAIRP
- Configuration management and CMAAC – checks for SFAIRP justification
- Asset Management – supports ongoing SFAIRP mature of network
- AEO Authorisation – assures organisations have the capability to design, deliver and assure assets that ensure safety SFAIRP

# Summary

- The duty to ensure safety SFAIRP relates to almost every activity we do
- We need to balance safety with other risks and opportunities but must always be able to demonstrate we have ensured safety SFAIRP
- Absence of evidence of risk is NOT evidence of absence of risk