# Towards Risk Acceptance - The City Rail Link Project

**Russell McMullan**

29 Feb 2018 v2

CityRailLink

cityraillink.co.nz

cityraillink

Presentation developed for the Construction Clients' Group Safety in Design practice forum

# Introduction


Russell McMullan
Systems Assurance Manager City Rail Link Limited
GCertSafLead, AdvDipAeroEng, NZCE, MRAeS, IMNZ

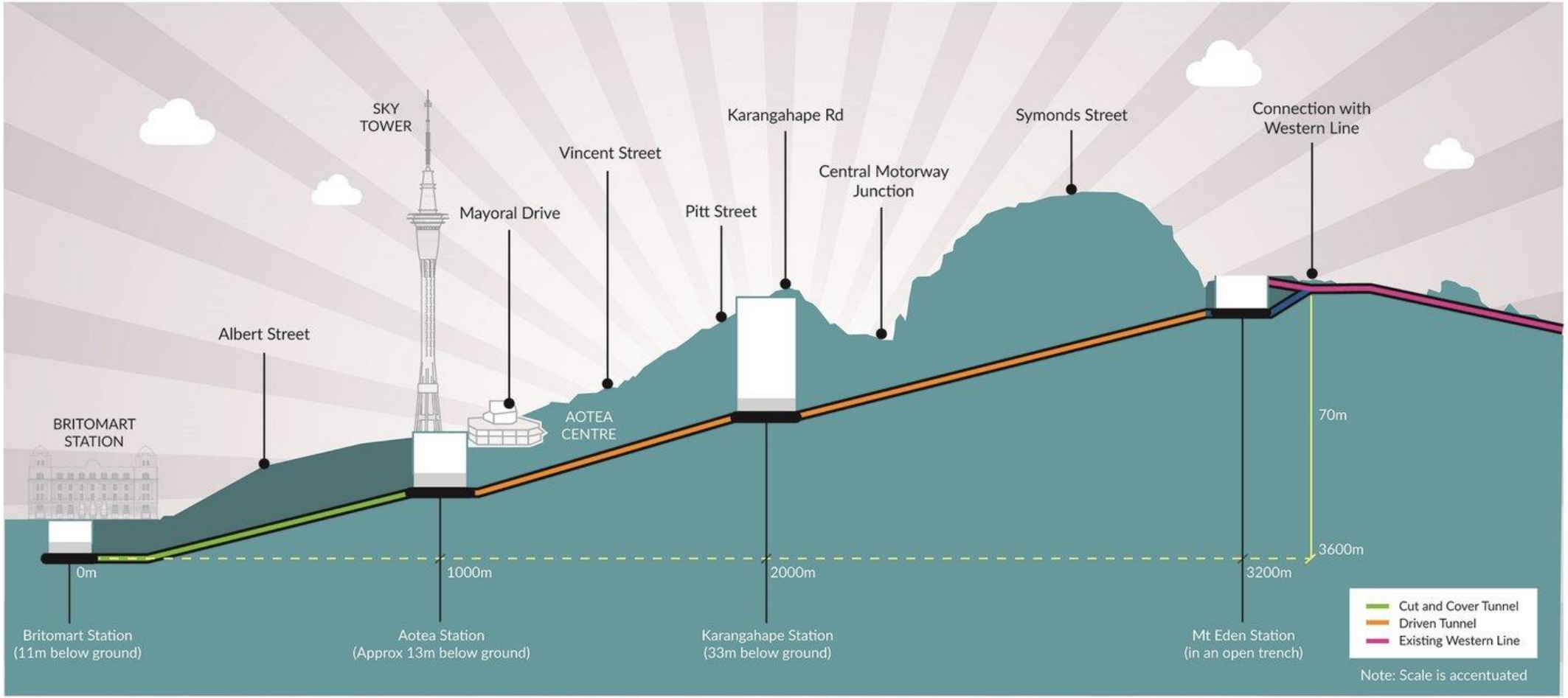
Background:
+ 2 years City Rail Link
+ 5 years consulting high risk industries (incl. rail)
+ 18 years military aerospace engineering

Things:
+ systems safety
+ systems engineering
+ safety assurance / safety risk management
+ safety critical software certification (aviation)
+ organisational resilience
+ operational safety
+ systems integration
+ technology strategy
+ information security
+ safety critical project delivery

# Presentation

- Introduction to the City Rail Link Project
- A quick exercise
- Approaches to risk acceptance
- Application to CRL
- Safety benchmarking for CRL
- Implementing the benchmark
- Applying to other infrastructure or activities
- .... one more thing...

# City Rail Link Project

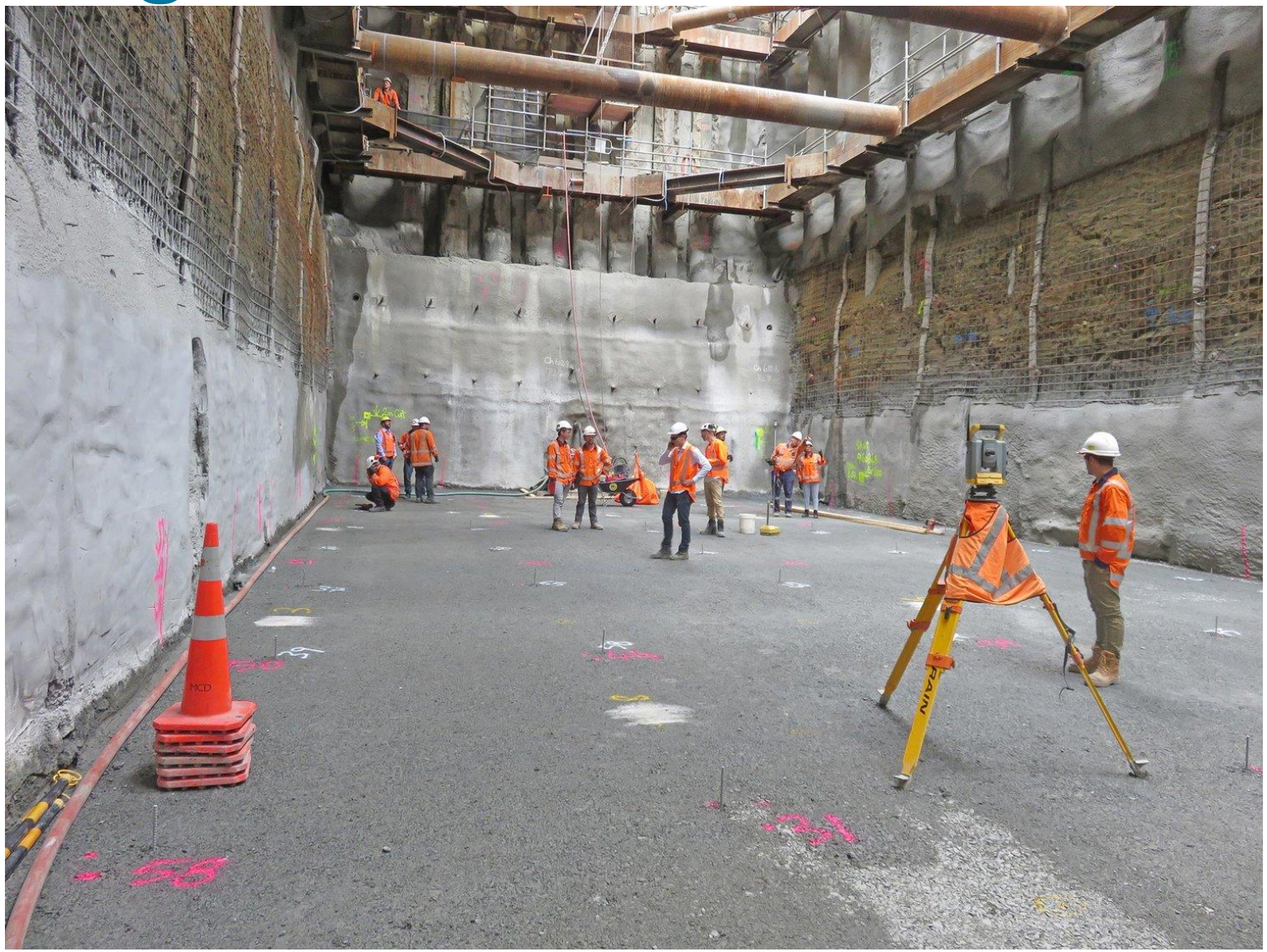



www.cityraillink.co.nz

# Benefits of CRL

- Double the number of trains on the network
- Double the capacity of the rail network
- Capacity of over 30,000 people per hour
- Doubles the number of people living within 30 minutes travel of the city.

# Project Progress



# Project Progress

# Assumptions

- The audience has an understanding of risk concepts
- ‘SiD’ is using ‘register’ to quantify and record

TRANSPORT AGENCY

MacKays to Peka Peka

**Safety in Design Risk Assessment Register**

Project Name: MacKay's to Peka Peka Alliance

Sector: Sector 330-350: Leinster Ave to Wharemauku

Author (Role): Nathanael Sterling, SiD Facilitator, and Doug Stirrat (Zone Design Manager)

Approved By:

Revision: 2

Job No: 3320901

Date: 16 October 2014

Stage of Design / Project: Concept Confirmation

| RISKS ASSOCIATED WITH DESIGN ELEMENTS | | | | | | | PROPOSED MITIGATION MEASURES | | | | | | RESIDUAL RISK | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Discipline | Ref | Cause & Outcome | Existing controls (current design or current environment) | Likelihood | Consequence | Risk Rating | Control Hierarchy: 1) Elimination 2) Substitution 3) Engineering 4) Administrative 5) Personal Protective Equipment | Likelihood | Consequence | Risk Rating | Status | Action Owner (Discipline Lead) | Residual Risk | Client / Asset Owner Acceptance / Comment |
| 1 Construction Phase - Process of Building the Asset | | | | | | | | | | | | | | |
| Stormwater | 1.01 | Deep excavations, risk of fatality in excavation through engulfment of water or soft soil due to high water table and weak soils (Services and Stormwater) | Confined space procedures. Trenching and deep excavation guidelines | Unlikely | Permanent Injury | Extreme | Remove need to access deep trenches through design and/or construction methods. | Rare | Permanent Injury | | Live | Construction Team | Constructors. Deep trench at wastewater pipe south of Wharemauku Stream could not be removed. Residual construction risk. Detailed construction methodology to be developed. | |

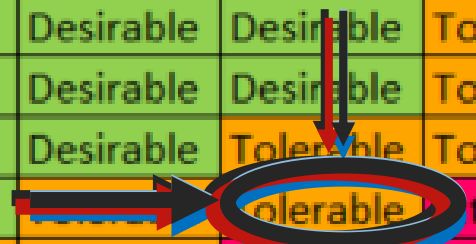
# Quick Exercise

- Which is the hazard?
  - Working at heights
  - Slip / trip fall
  - Injury from a fall
  - Fall from heights
  - Gravity
  - Fatigue
  - Human error
  - Lack of training

# Quick Exercise

- Consider ‘Person struck by train at a platform’
- Other events: fall on escalator, fall on track, etc, etc.

| | | | Consequence Level | | | | |
|---|---|---|---|---|---|---|---|
| | | | No Effect | Minor | Major | Critical | Catastrophic |
| | | | 0 | 0.005 | 0.1 | 1 | 10 |
| Frequency Level (per year) | Incredible | 0.0001 | Desirable | Desirable | Desirable | Tolerable | Tolerable |
| | Rare | 0.01 | Desirable | Desirable | Desirable | Tolerable | Tolerable |
| | Remote | 0.1 | Desirable | Desirable | Tolerable | Tolerable | Intolerable |
| | Occasional | 1 | Desirable | Tolerable | Tolerable | Intolerable | Intolerable |
| | Frequent | 10 | Tolerable | Tolerable | Intolerable | Intolerable | Intolerable |



0.1 EqF/ year

0.1 EqF/ year

0.1 EqF/ year

0.1 EqF/ year

0.1 EqF/ year

0.1 EqF/ year

0.1 EqF/ year

0.1 EqF/ year

0.1 EqF/ year

0.1 EqF/ year

**Sum = 1 EqF/ year**

# Question

- Is the potential for 10 ‘major’ harm events in one year acceptable?

# CRL Safety Benchmarking Study

- CRL is a portion of the network


*Figure 2 - CRL hazard risk as a fraction of national hazard risk.*

# 6 approaches to risk acceptance

1. Absolute:
   - Maximum acceptable risk: some maximum quantifiable value of risk / harm
2. Comparative
   - Not worse that what is currently being done: follow existing best practice
3. Relative
   - ‘Safer than other systems’: society is comfortable with what has been achieved
4. So Far As Is Reasonably Practicable (SFAIRP)
   - Cost of mitigating further is grossly disproportionate to the benefit of the mitigation (i.e. follow a process, not tied to absolute risk).
5. Implied acceptability
   - ‘Normal’ set of mitigations are applied: ‘someone’ deems the mitigations are ok
6. *Fiat*
   - Latin: ‘let it be done’ -> because I said so -> someone authorised accepts the risk

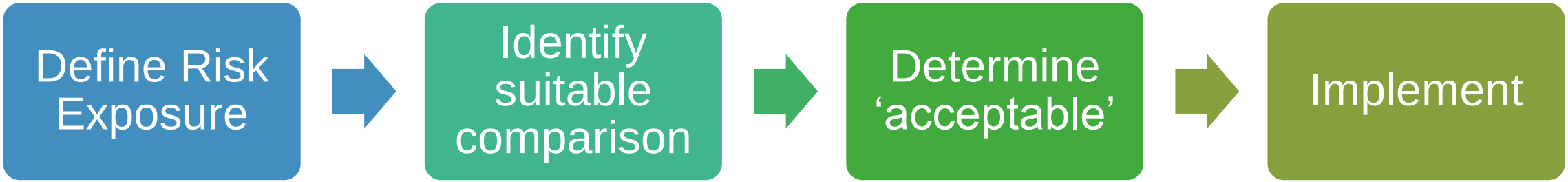
# CRL risk acceptance challenges

# CRL Risk Acceptance Assumptions

- Absolute
  - What is an acceptable limit?
- Comparative
  - Not worse than current NZ?
  - ‘As safe as an internationally safe railway’?
  - NZ best practice or International best practice?
- Relative
  - Safer than other modes (car / bus / cycle)!
- SFAIRP
  - HSWA (2015) / Railways Act (2005) require SFAIRP
- Implied acceptability
  - What are the ‘features’ that imply acceptability?
- *Fiat*
  - Do all the approval authorities agree on the acceptance process?

CityRailLink

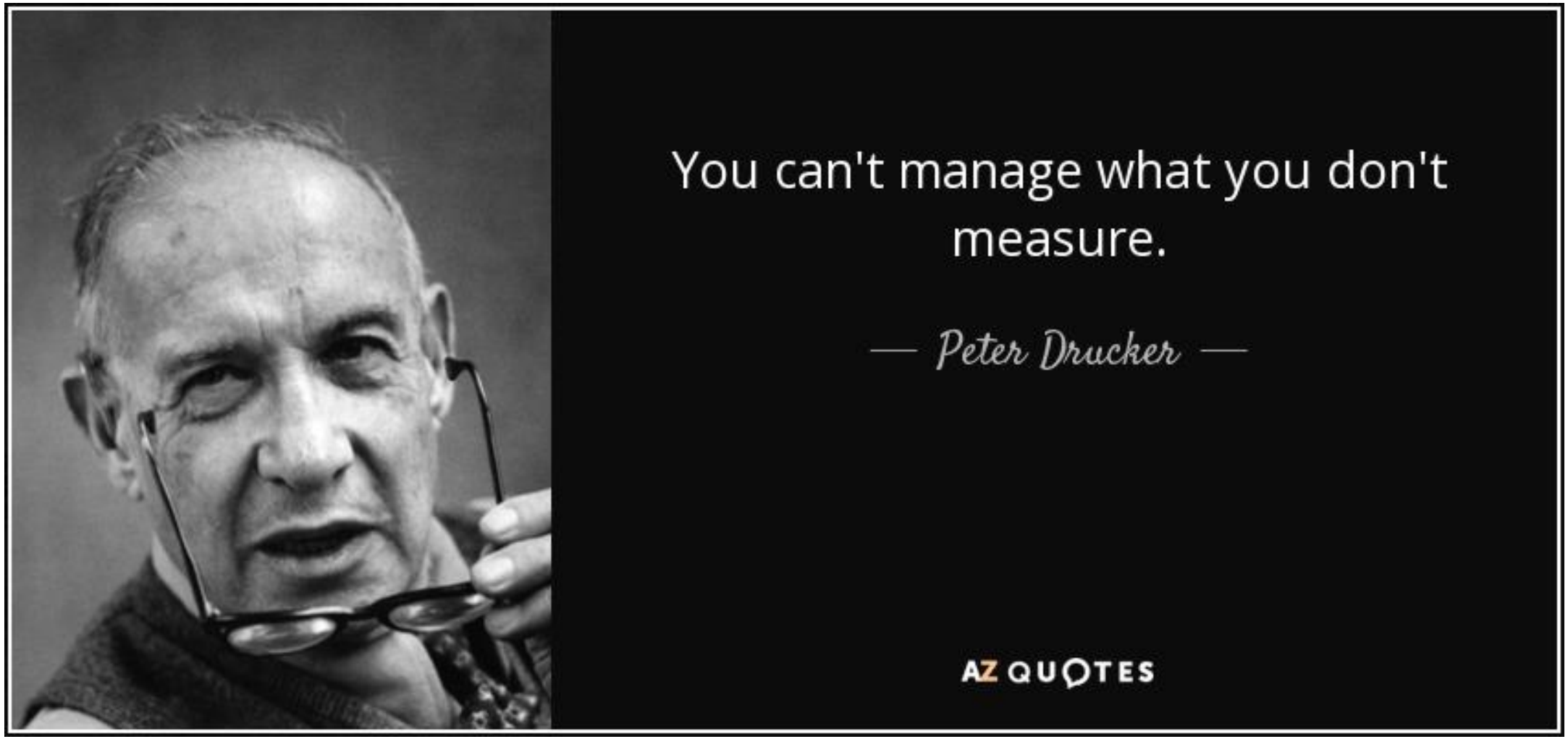
# Process


Define Risk Exposure
Identify suitable comparison
Determine 'acceptable'
Implement

# Operational Use & exposure to risks

- Passenger exposure
  - Planned maximum = 504 million passenger km / year
  - Design maximum = 756 million passenger km / year
- Worker exposure
  - ~300,000 worker hours per year

# Comparison to other railways



# Exploring the data: rail safety performance

- Auckland: Unknown
- New Zealand : Unknown
- Australia: Difficult to make a comparison
- USA: Good data, well presented
- UK: Good data and includes all European comparison

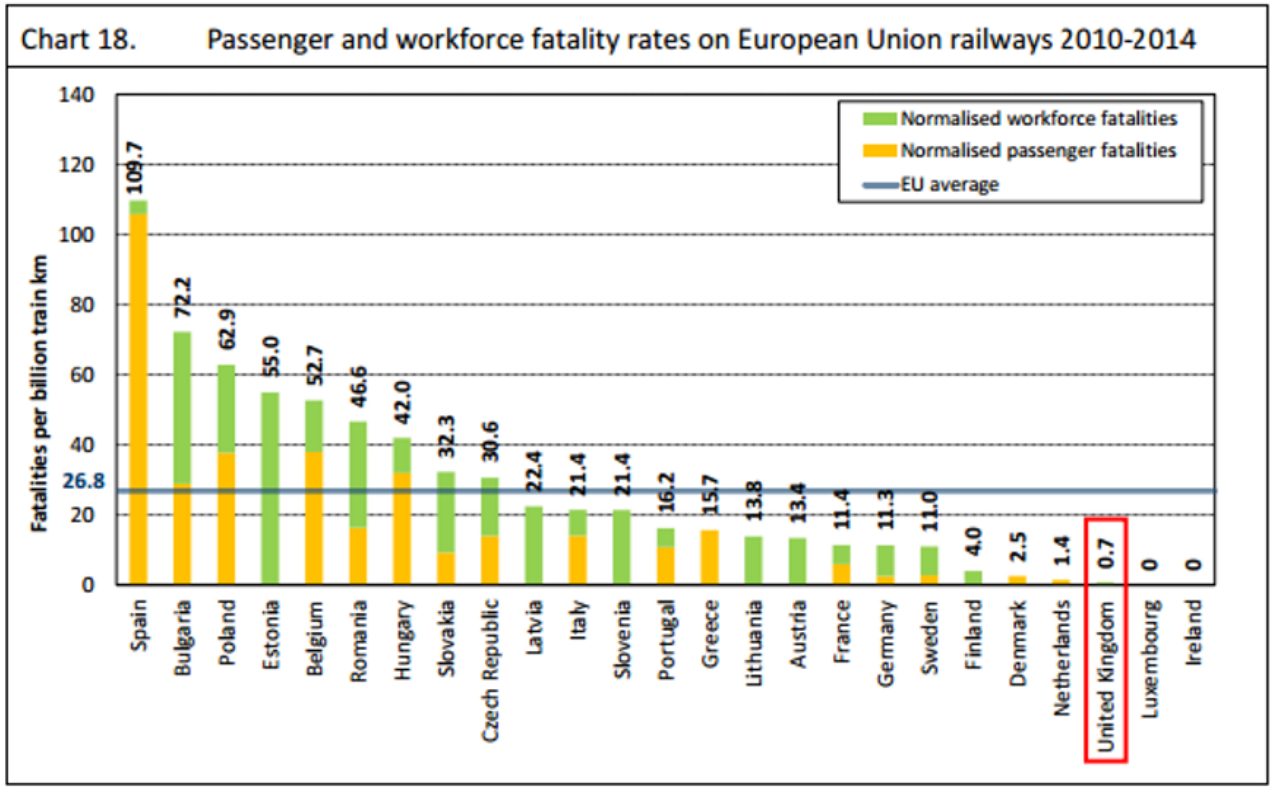



*Figure 2 - Passenger and workforce fatality rates on European Union railways 2010-2014 (RSSB, 2016)*

# Result

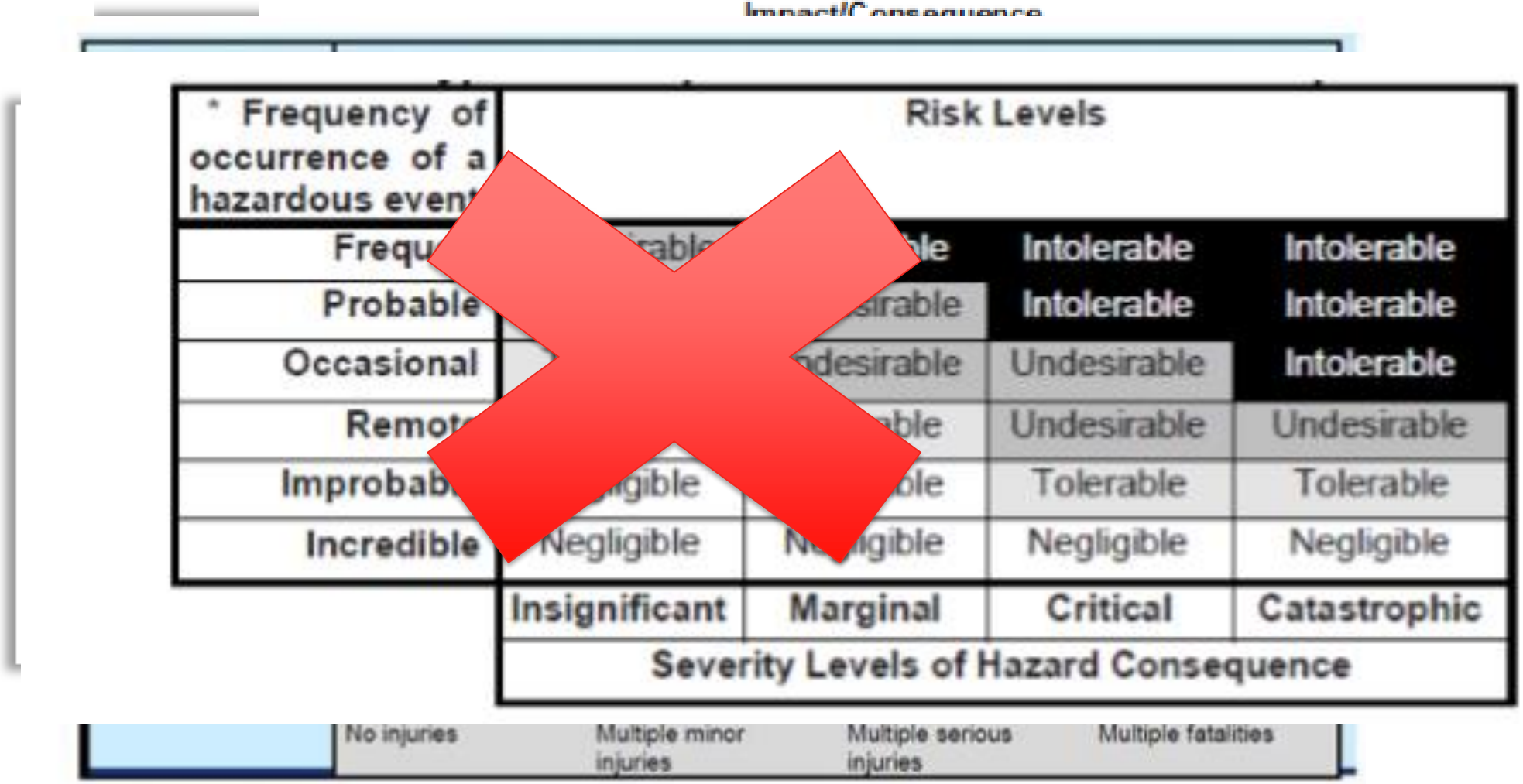
- Comparable CRL safety:
  - If CRL is comparable to USA
    -> 1.38 ‘EqF per year’
  - If CRL is comparable to UK
    ->  0.60 ‘EqF per year’

# How do we deal with this?

| | | | Consequence Level | | | | |
|---|---|---|---|---|---|---|---|
| | | | 1 | 2 | 3 | 4 | 5 |
| | | | 0 | 0.005 | 0.01 | 1 | 10 |
| Frequency Level | 1 | 0.001 | Desirable | Intolerable | Intolerable | Intolerable | Intolerable |
| | 2 | 0.01 | Desirable | Intolerable | Intolerable | Intolerable | Intolerable |
| | 3 | 0.1 | Desirable | Intolerable | Intolerable | Intolerable | Intolerable |
| | 4 | 1 | Desirable | Intolerable | Intolerable | Intolerable | Intolerable |
| | 5 | 10 | Desirable | Intolerable | Intolerable | Intolerable | Intolerable |

# Goal

- New hazards don't increase 'total harm' above 0.6 EqF/annum



| * Frequency of occurrence of a hazardous event | Risk Levels | | | |
|---|---|---|---|---|
| Frequ | [illegible] | [illegible] | Intolerable | Intolerable |
| Probable | [illegible] | [illegible]irable | Intolerable | Intolerable |
| Occasional | [illegible] | [illegible]desirable | Undesirable | Intolerable |
| Remot | [illegible] | [illegible] | Undesirable | Undesirable |
| Improbab | [illegible]igible | [illegible] | Tolerable | Tolerable |
| Incredible | Negligible | N[illegible]igible | Negligible | Negligible |
| | Insignificant | Marginal | Critical | Catastrophic |
| | Severity Levels of Hazard Consequence | | | |

| | No injuries | Multiple minor injuries | Multiple serious injuries | Multiple fatalities |
|---|---|---|---|---|

# Created our own

- Assuming ~300 top level events, can we fill in the gaps?

| | | | Consequence | | | | |
|---|---|---|---|---|---|---|---|
| | | | No effect | Minor | Major | Critical | Catastrophic |
| | | | 0 | 0.005 | 0.1 | 1 | 10 |
| Likelihood | Incredible | 1.E-09/hr | Desirable | Likely tolerable | Likely tolerable | Likely tolerable | Possibly tolerable? |
| | Rare | 1.E-07/hr | | Likely tolerable | ? | ? | Intolerable |
| | Remote | 1.E-06/hr | | Likely tolerable | ? | Intolerable | Intolerable |
| | Occasional | 1.E-05/hr | | ? | ? | Intolerable | Intolerable |
| | Probable | 1.E-04/hr | | ? | ? | Intolerable | Intolerable |
| | Frequent | >1.E-04/hr | | Possibly intolerable? | Likely intolerable? | Intolerable | Intolerable |

# Manual table and sensitivity testing

**"Worst case" where all hazards are biased toward most likely**

Total hazard risk for CRL is about 53 Equivalent Fatalities in 100 years, (less than 0.6 EqF per year) where the largest contributor to this is minor injuries.

Of note, the table is very sensitive to regular minor events.

| | EQF | Tolerable | Hazard distribution | Events in CRL Life (Total Hazards) Assuming a high risk distribution of residual risk (near worst case but tolerable) (column E) | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | no / consequence | Event in life | EQF (SFAIRP) 100 yrs | Event in life | EQF (SFAIRP) 100 yrs | Event in life | EQF (SFAIRP) 100 yrs | Event in life | EQF (SFAIRP) 100 yrs | Event in life | EQF (SFAIRP) 100 yrs | Event in life | EQF (SFAIRP) 100 yrs |
| Catastrophic | 10 | 1.00E-09 | 10 | 0.01 | 0.09 | 0.01 | 0.07 | 0.00 | 0.02 | 0.00 | 0.01 | 0.00 | 0.00 | 0.00 | 0.02 |
| Critical | 1 | 1.00E-09 | | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| Critical | 1 | 1.00E-07 | 20 | 1.75 | 1.75 | 1.46 | 1.46 | 0.38 | 0.38 | 0.15 | 0.15 | 0.05 | 0.05 | 0.38 | 0.38 |
| Major | 0.1 | 1.00E-09 | | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| Major | 0.1 | 1.00E-07 | | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| Major | 0.1 | 1.00E-06 | 75 | 65.70 | 6.57 | 54.75 | 5.48 | 14.40 | 1.44 | 5.48 | 0.55 | 1.80 | 0.18 | 14.40 | 1.44 |
| Minor | 0.005 | 1.00E-09 | | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| Minor | 0.005 | 1.00E-07 | | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| Minor | 0.005 | 1.00E-06 | 100 | 87.60 | 0.44 | 73.00 | 0.37 | 19.20 | 0.10 | 7.30 | 0.04 | 2.40 | 0.01 | 19.20 | 0.10 |
| Minor | 0.005 | 1.00E-04 | 100 | 8760.00 | 43.80 | 7300.00 | 36.50 | 1920.00 | 9.60 | 730.00 | 3.65 | 240.00 | 1.20 | 1920.00 | 9.60 |
| No effect | 0 | | 155 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| | | | 460 | | 53 | | 44 | | 12 | | 4 | | 1 | | 12 |

# Final Result

| | | | CONSEQUENCE | | | | |
|---|---|---|---|---|---|---|---|
| | | | No effect | Minor | Major | Critical | Catastrophic |
| | | | | 0.005 EqF | 0.1 EqF | 1 EqF | 10 EqF |
| LIKELIHOOD | Incredible | 1.E-09/hr | 0 | 1 | 3 | 4 | 5 |
| | Rare | 1.E-07/hr | | 2 | 4 | 5 | 6 |
| | Remote | 1.E-06/hr | | 3 | 5 | 6 | 7 |
| | Occasional | 1.E-05/hr | | 4 | 6 | 7 | 8 |
| | Probable | 1.E-04/hr | | 5 | 7 | 8 | 9 |
| | Frequent | >1.E-04/hr | | 6 | 8 | 9 | 10 |

*Table 5 - CRL safety risk matrix*

Red = Intolerable Risk

Orange = Risk must be reduced SFAIRP

- Each sell presents ‘EqF/Annum’

# Sum the Top Events!

A1

+ A2

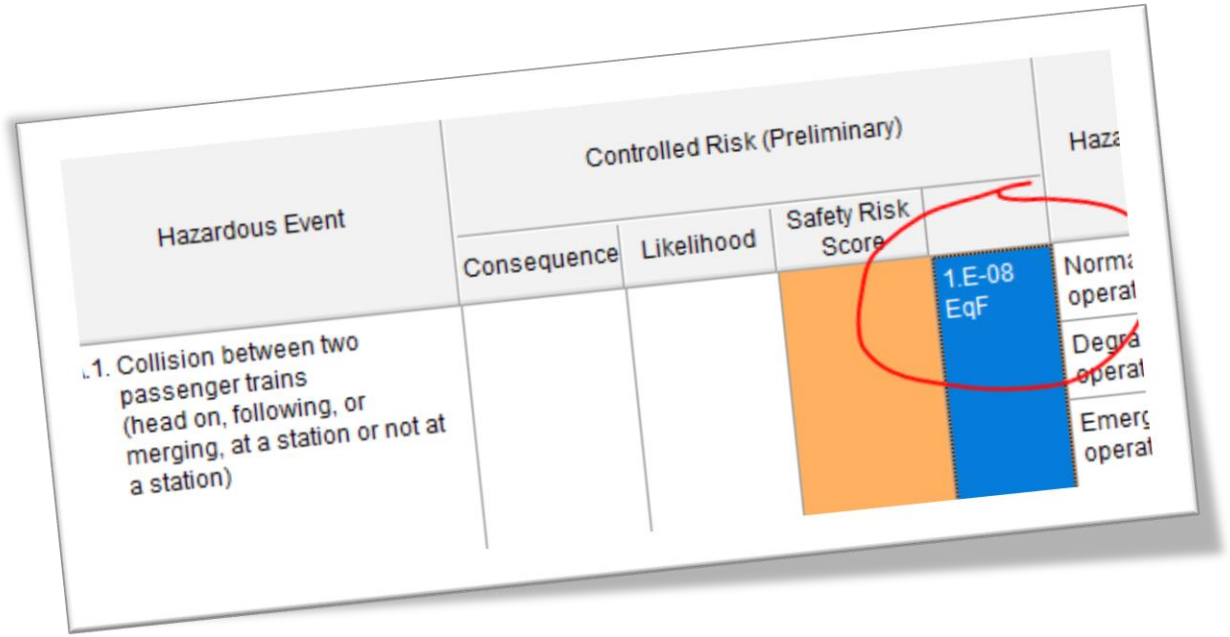
+ A3

+ ….

+ Z99

---

Less than 0.6EqF / annum?



# Summary

- Absolute
  - What is an acceptable limit? = 0.6 EqF / Annum
- Comparative
  - Not worse than current NZ? = "demonstrable level of (design) safety"
  - 'As safe as an internationally safe railway'? = "aim: as safe as UK, which is one of the safest"
  - NZ best practice or International best practice? = follow International best practice safety standards
- Relative
  - Safer than other modes (car / bus / cycle) = Yes
- SFAIRP
  - HSWA (2015) / Railways Act (2005) require SFAIRP = SFAIRP included in safety requirements
- Implied acceptability
  - What are the 'features' that imply acceptability? = NZ building code + UK rail safety features
- *Fiat*
  - Do all the approval authorities agree on the acceptance criteria? = we've hedged our bets!


Metro
THE MERCURY

# Applied to infrastructure (or anything)

1. Understand expected usage / capacity / operations
    - i.e. number of people x activity x time (or distance)
2. Understand what ‘good’ looks like
    - Industry stats for activity  (local / international)
    - Rate per hour, or person, or km or per hour for total harm
3. Determine ‘good’ for the local application
    - Work out total harm which would be tolerable for use case
4. Implement ‘good’ in the hazard / risk model for total harm
    - Set tolerability in the risk matrix & measure total score

# One more thing…..

# Risk Matrix Generator

**RISK MATRIX GENERATOR**

Please note: you must use a consistent ***time period*** and ***unit of harm*** across all of your inputs. Your unit of harm could be, for instance, dollars of damage, or equivalent fatalities. Your time period could be, for instance, a fortnight or a year.

**How many levels of likelihood/frequency should your matrix** [ ]
(where frequency describes how often you expect a particular hazard to occur during one time

**How many levels of consequence should your matrix have?** [ ]
(where consequence describes the harm you expect one instance of the hazard to generate)

**Enter the maximum total amount of harm that it would be acceptable for your activity to generate (across all hazards)** 2

Enter your input in the box above right, input should be numeric only, in terms of the same harm unit as you used to define your consequence levels.

**Optional: if you would like to build in a tolerance margin (for instance, if you believe there are a reasonable number of hazards which you have not yet identified), then slide to select your preferred margin (as a percentage of**

10 %

**Please fill in the matrix using the directions given below:**

1. In each yellow square, enter the number of hazards that you have identified that fall within that category (e.g. if you know of zero hazards which have a frequency of level 5 and a consequence of level 2, then you should enter the number 0 into cell (5,2) of the matrix below)
2. In each blue square, enter the amount of harm generated by a hazard with that consequence. Again, this should be in terms of the same unit of harm used above.
3. In each green square, enter how often you expect a hazard of that frequency to recur in a single time period. For example, a hazard you expect to occur about once every 4 time periods would have a frequency of 0.25.
4. For consistency, a level one frequency is the least likely, and a level one consequence should be the smallest level of consequence.

All inputs should be numeric only

| | | | Consequence Level | | | | |
|---|---|---|---|---|---|---|---|
| | | | 1 | 2 | 3 | 4 | 5 |
| | | | 0 | 0.005 | 0.1 | 1 | 10 |
| Frequency Level | 1 | 0.001 | 0 | 0 | 0 | 0 | 0 |
| | 2 | 0.01 | 0 | 0 | 0 | 0 | 0 |
| | 3 | 0.1 | 0 | 0 | 0 | 0 | 0 |
| | 4 | 1 | 0 | 100 | 5 | 0 | 0 |
| | 5 | 10 | 0 | 0 | 0 | 0 | 0 |

**f there are any cells in the matrix that you would like to fix as intolerable, click**

| | | | Consequence Level | | | | |
|---|---|---|---|---|---|---|---|
| | | | 1 | 2 | 3 | 4 | 5 |
| Frequency Level | 1 | | | | | | |
| | 2 | | | | | | |
| | 3 | | | | | | |
| | 4 | | | | | | |
| | 5 | | | | | | |

**Once you have completed and checked all of the inputs (left), click to generate your risk matrix. You can adjust your inputs and re-generate the matrix as many times as you wish. Note:**

Generate Risk Matrix

| | | | Consequence Level | | | | |
|---|---|---|---|---|---|---|---|
| | | | 1 | 2 | 3 | 4 | 5 |
| | | | 0 | 0.005 | 0.1 | 1 | 10 |
| Frequency Level | 1 | 0.001 | Desirable | Tolerable | Tolerable | Intolerable | Intolerable |
| | 2 | 0.01 | Desirable | Tolerable | Tolerable | Intolerable | Intolerable |
| | 3 | 0.1 | Desirable | Tolerable | Tolerable | Intolerable | Intolerable |
| | 4 | 1 | Desirable | Tolerable | Intolerable | Intolerable | Intolerable |
| | 5 | 10 | Desirable | Tolerable | Intolerable | Intolerable | Intolerable |

| | |
|---|---|
| Desirable | Hazards in this category produce no harm; it is acceptable not to treat these hazards. |
| Tolerable | Hazards in this category do not pose problems for the aggregate risk profile, but should still be minimised where possible (or legally compulsory). |
| Intolerable | Hazards in this category must have controls applied until they fall within a tolerable category, otherwise the aggregate risk profile will be |


Metro
Metro