

System safety in rail:

The ATSB investigation into the 2018 Devonport cement train runaway and derailment

*Australian System Safety Conference (ASSC) 2024
Brisbane, Queensland*



Australian Transport Safety Bureau

Australia's national transport safety investigator

- Purpose is to improve safety of, and public confidence in, aviation, marine and rail transport through:
 - independent investigation of transport accidents and other safety occurrences
 - safety data recording, analysis and research
 - fostering safety awareness, knowledge and action
- Not for administrative, regulatory or criminal action, blame or liability
- In rail, OTSI (NSW) and OCI (Vic) also operate under the same rules (TSI Act 2003)

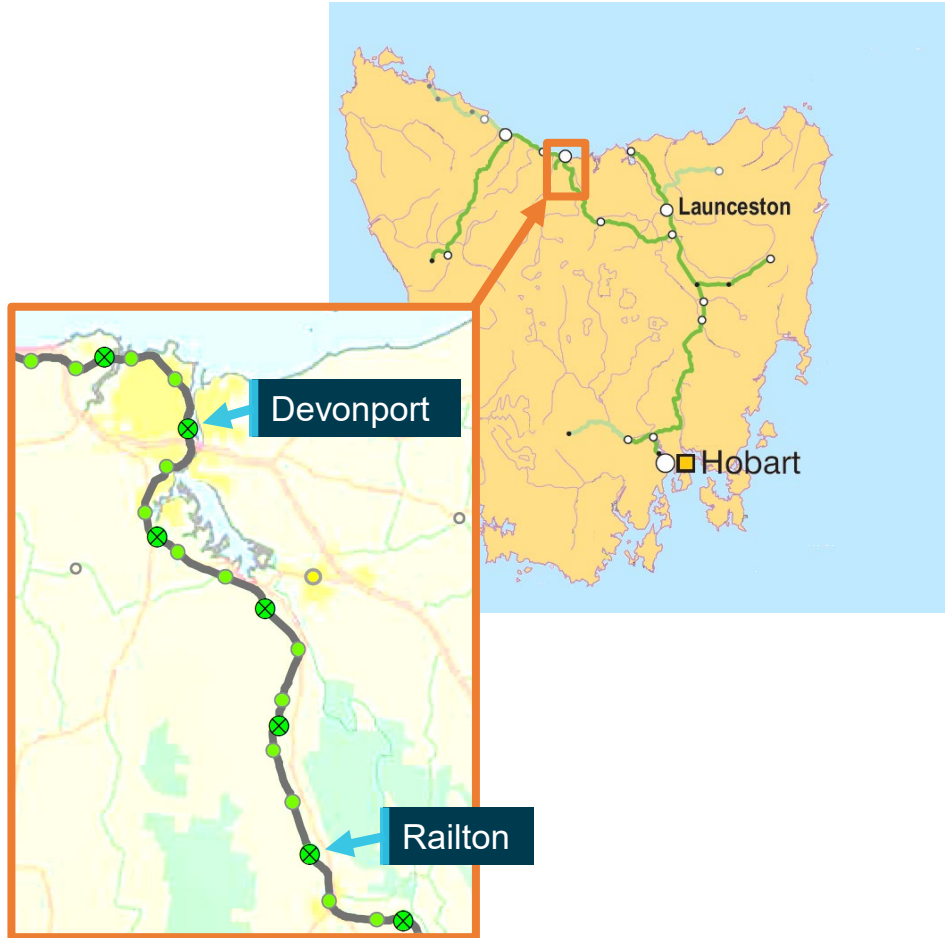


Today's topics

- Background
- What happened on the day of the accident?
- What were the organisational factors involved in the lead-up to the accident?
- What are the lessons we can learn?

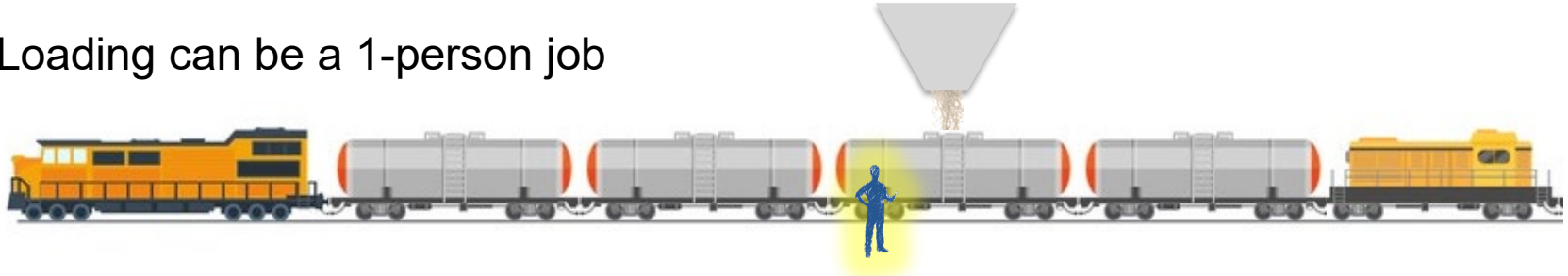
Background

- One job – haul dry cement from Railton to Devonport, and return empty for the next load
- 24/7/365 operation

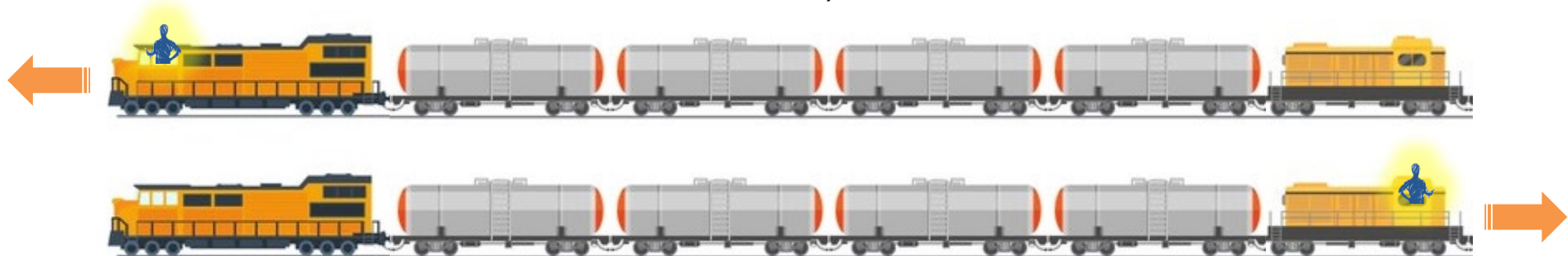


Remote control equipment

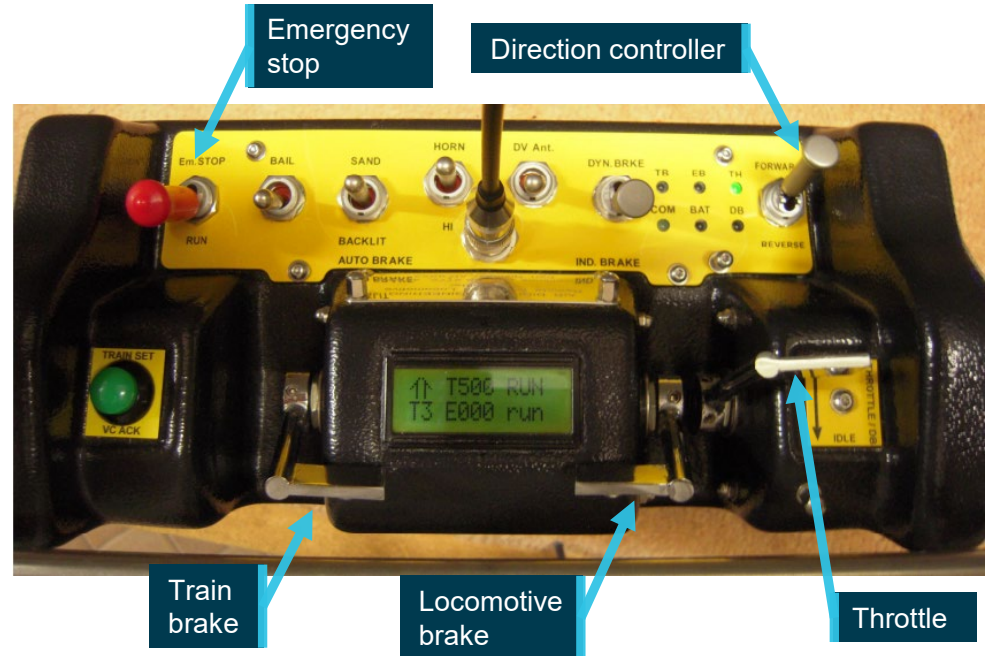
Loading can be a 1-person job



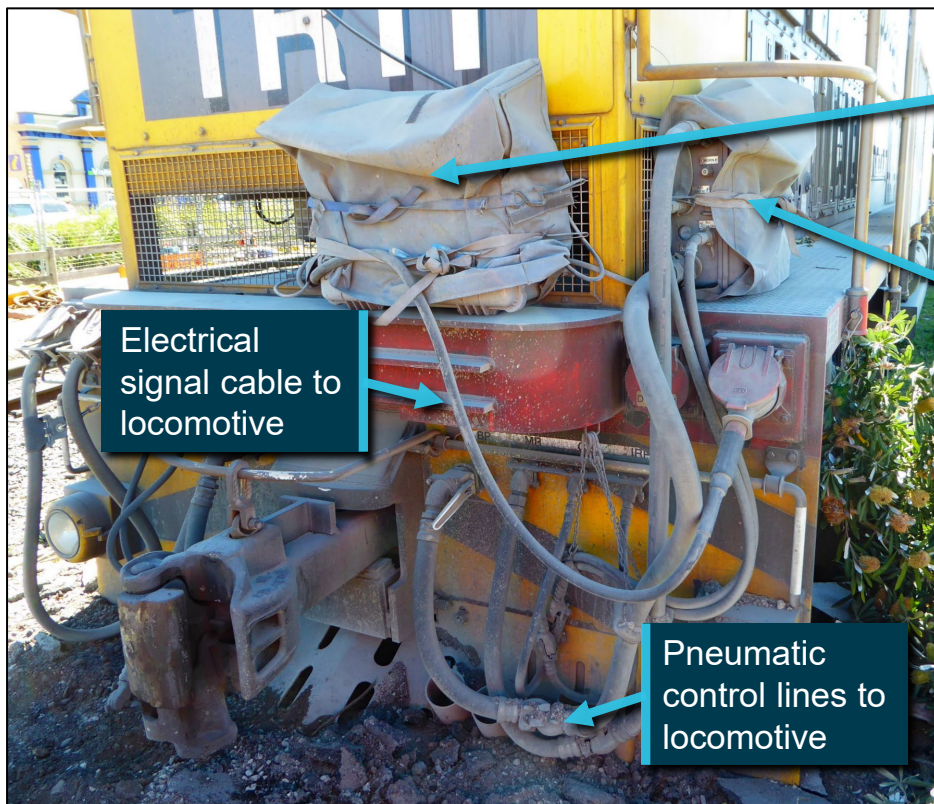
Train can be driven from a driver's van for the return trip (avoids the need to turn it around or use a second locomotive)



Remote control transmitter



Remote control receiver



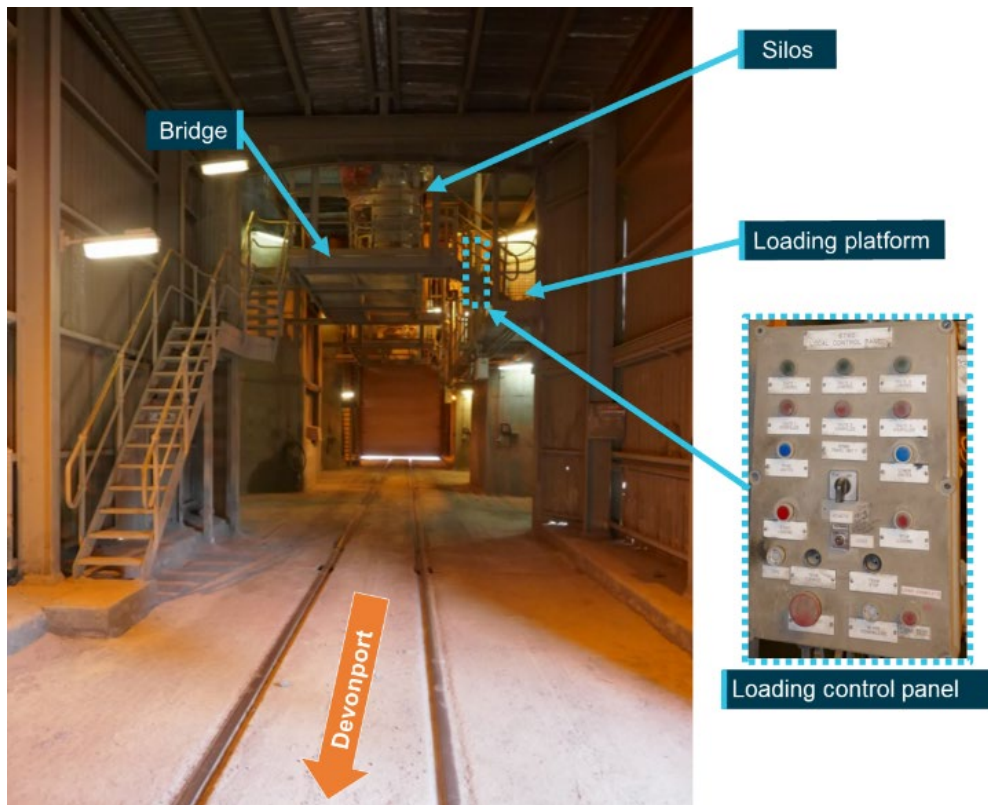
Receiver

Air box for
pneumatic
control

Electrical
signal cable to
locomotive

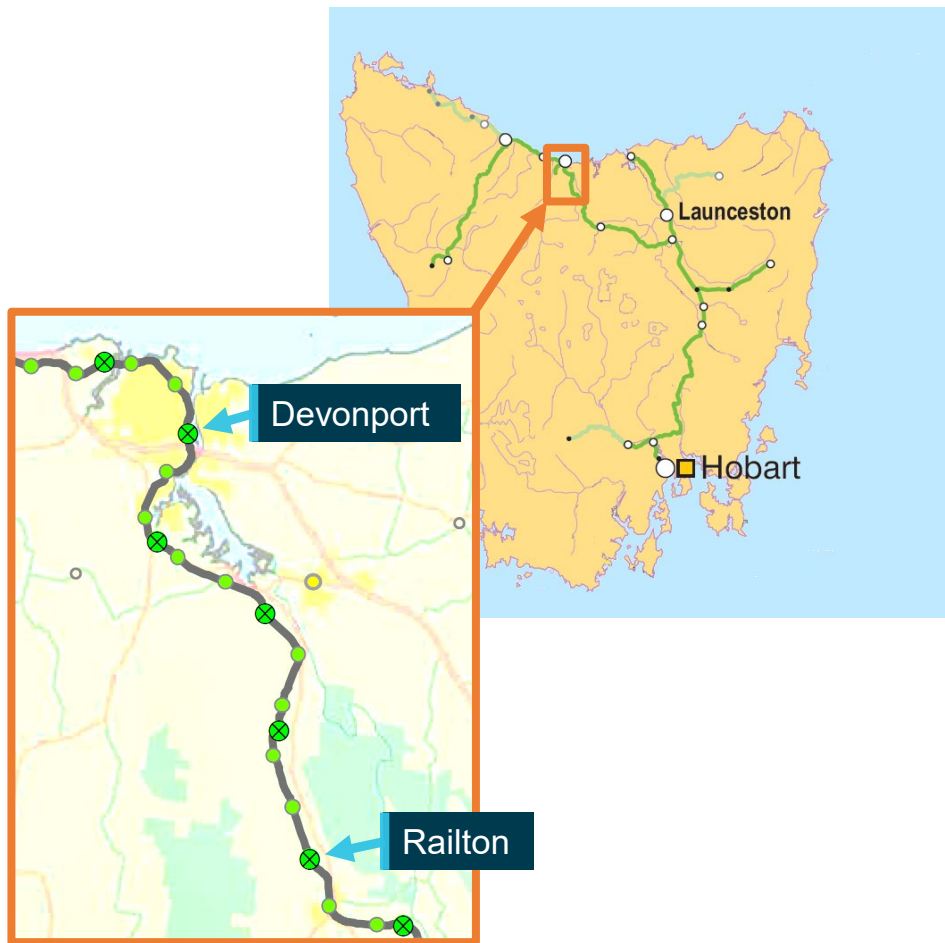
Pneumatic
control lines to
locomotive

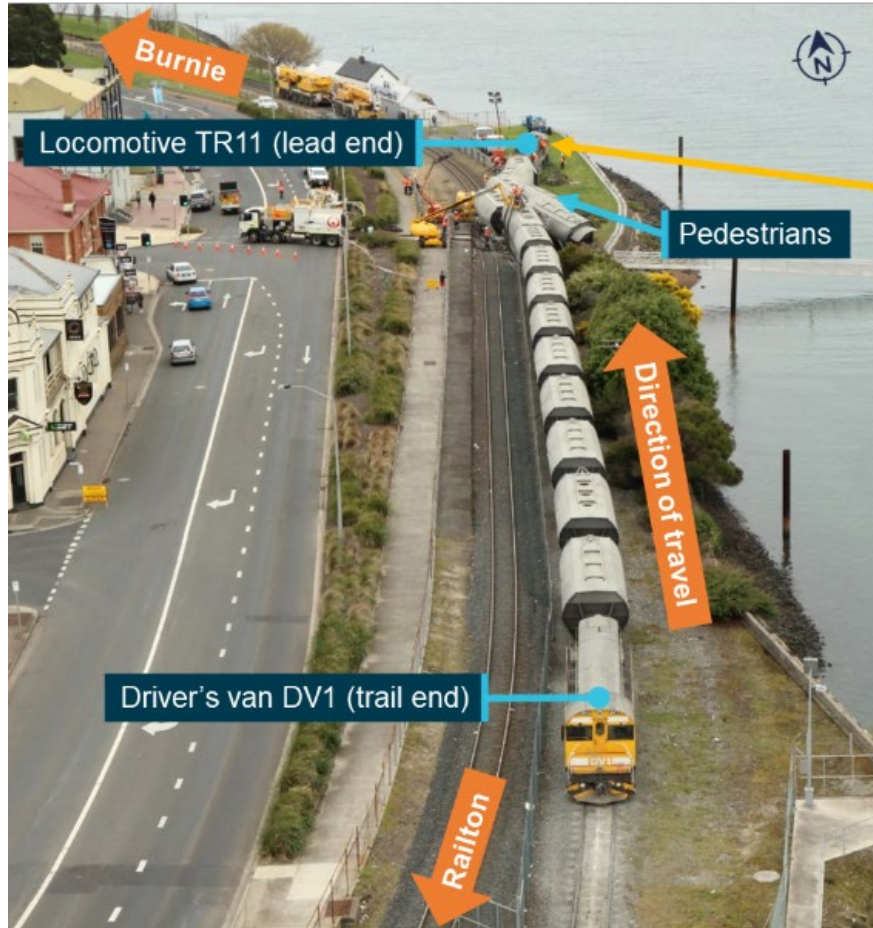
What happened



- Sole driver/operator loading cement at night
- Train overshot marker by a small amount
- Driver selected reverse direction
- Remote control equipment stopped responding
- Attempts to activate safeties were unsuccessful
- Brakes were repeatedly applied and released, uncontrolled
- Eventually the brakes remained released and the train rolled away

- Train ran onto the main line and gathered speed
- Speeds mostly higher than the maximum track speed at each point – up to 87.5 km/h
- Continued for about 20 km
 - through several populated areas
 - through 13 public level crossings (10 active and 3 passive)
 - beneath a highway overpass
- Operator alerted police, who blocked major level crossings from public access
- No collisions





- Track operator diverted train away from the centre of Devonport into Devonport Yard
- About 23 minutes after the train rolled away, it collided with a concrete footing at the end of the line
- 2 bystanders slightly injured by debris

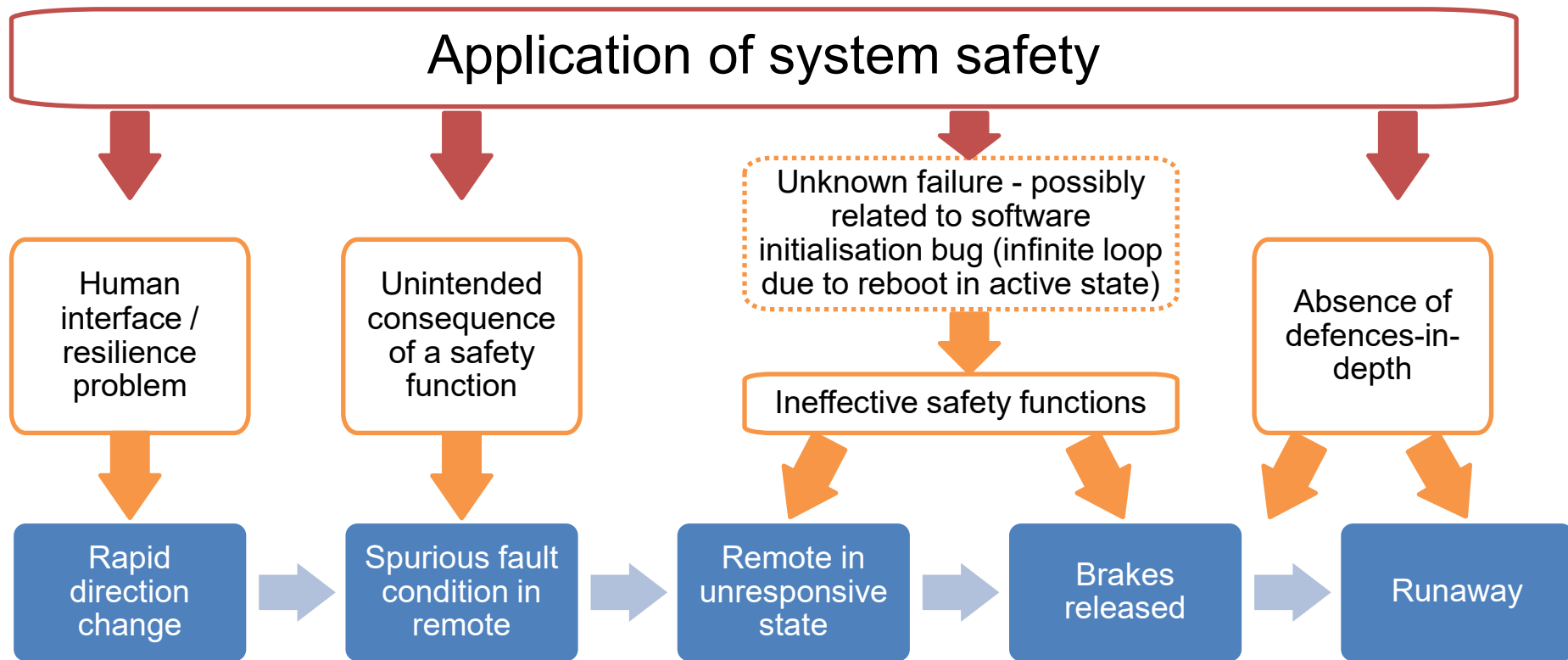
“Fail-safe”...?

- Remote control equipment was designed with multiple safety features
- Had been used for 19 years with no accidents attributable to the equipment
- Remote control equipment had recently undergone a **near-total redesign** using new hardware and software
- Design team of **two people** (one did the hardware design, manufacture, and customer liaison work, the other designed the software)
- Large number of “minor” **in-service issues** after the latest version was introduced



What went wrong on the day of the accident?





- All originate from design and integration issues: 'human error' in design
- Problems were associated with both the supplier and client

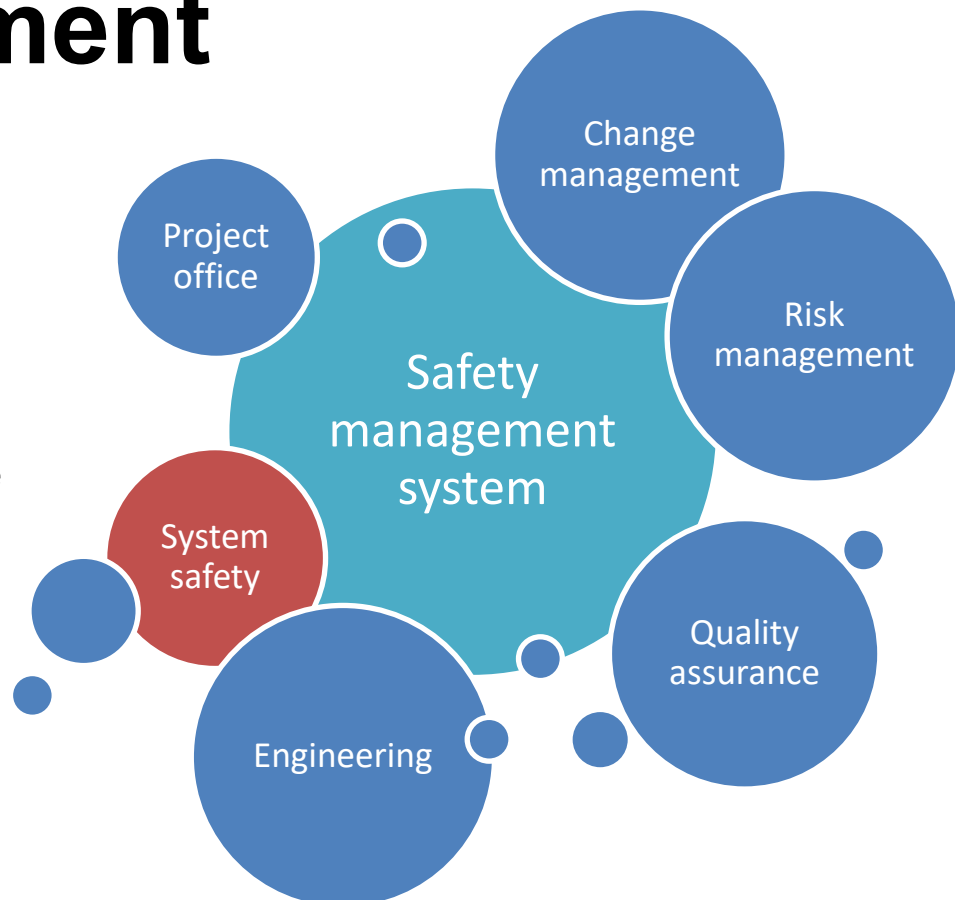
What were the organisational factors involved?

1. Change management
2. Client-side assurance
3. Design process issues
4. Challenges for small teams & projects



Change management

- Problems associated with project management and change management processes
- Limited appreciation of the safety significance of the design change (treated as 'like-for-like')
- Not a 'systemic view' of safety



Application of safety standard

- Supplier advised the client: '[The equipment] is designed with failsafe features following [Australian Standard] AS61508.'
- One document from 1999, applying some AS 61508 principles to the emergency stop function of a different, earlier design
- No other records for the application of AS 61508 or other safety design standards
- No structured approach to the equipment's design and little documentation
- No documented hazards/risks
- No requirements specifications, hazard/risk analyses, or safety case
- **Summary: the supplier used elements of AS 61508 to estimate the reliability of the emergency stop function for the earlier design but this was not equivalent to having developed the equipment to that standard**

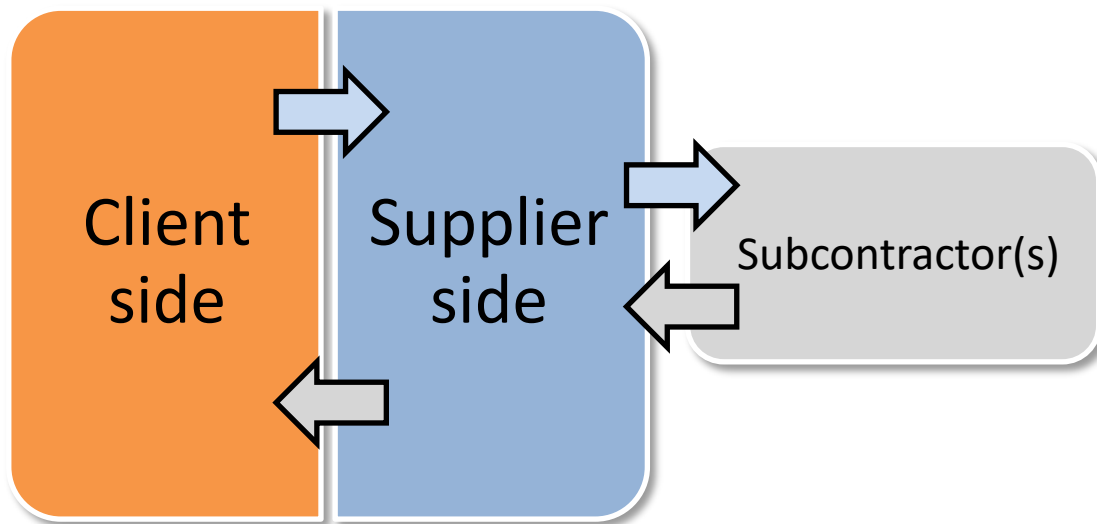


Application of safety standard

- Supplier did not address critical considerations such as:
 - the equipment's reliance on radio communications
 - start-up state
 - software reliability
 - reliability and effectiveness of some safety functions
- Not a 'systemic view' of safety

Client-side assurance

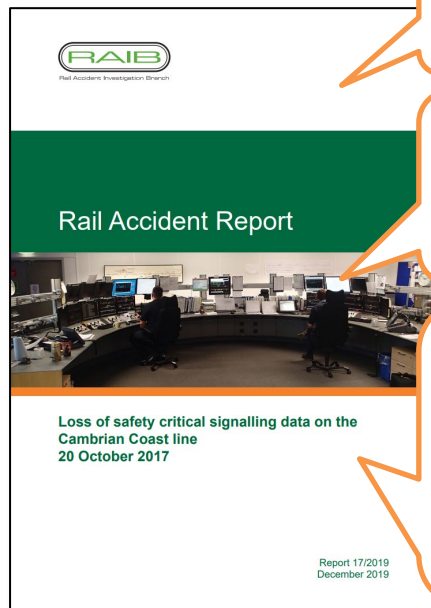
- No stated safety objectives
- Limited oversight by the client
- Client provided limited information about systems being integrated



The year before this...

Loss of safety critical signalling data on the Cambrian Coast line (UK), 20 October 2017

Four trains travelled over the line without temporary speed restriction data being sent from the signalling system.



- Multiple design issues
- Multiple design process issues

“.... did not include effective client role checks to identify the design process shortcomings.”

“The importance of clients understanding and undertaking their role in procuring safety critical high integrity software is demonstrated by this investigation.”

RSSB (UK) standard, 2022

RIS-0745-CCS Iss 1

Client Safety Assurance of High Integrity Software-Based Systems for Railway Applications

...sets out requirements for safety assurance of high integrity software-based systems for railway applications

Challenges for small teams & projects

- Numerous challenges in attaining justified confidence in a system's safety
- Generally, system safety standards were/are:
 - aimed at larger organisations and more complex projects
 - abstract and/or complex
 - require specific expertise
 - significant resources to implement
 - not adapted to Australian standards or not widely used in Australia (limited visibility)
 - not rail-oriented, or only for control/signal systems and not rolling stock
- **Smaller organisations may not have a sufficient understanding of system safety to recognise when their approaches fall short**



Findings specific to this operation: supplier

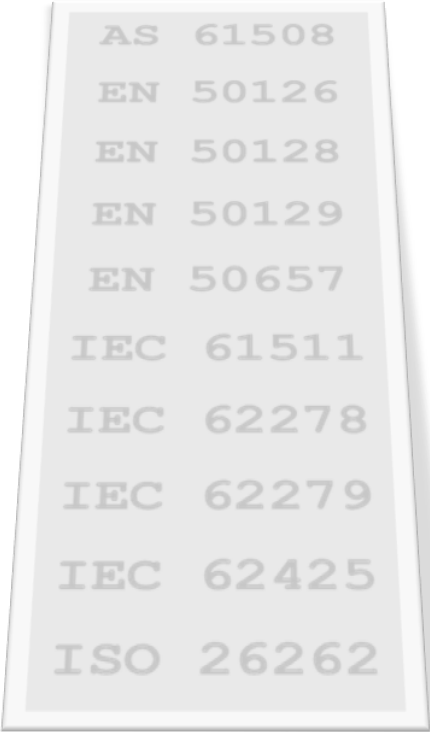
- The remote control equipment had several safety-related **design and integration problems**, which were readily identifiable
- Although [the supplier] had safety as a design objective, **system safety assurance activities appropriate to its application were not conducted**

Findings specific to this operation: client

- The client **did not identify or fully assess the safety implications** of remotely-controlled train operations generally, or those of their specific implementation (i.e. how they used it)
- The client commissioned the equipment with **insufficient systematic assurance of safety**, leading to excessive reliance on the supplier, and did not:
 - fully engage with the development process
 - explicitly identify and impose safety requirements, or
 - verify that the overall system met a specified level of safety.

Rail industry findings

- There was no explicit **regulatory requirement** or expectation to demonstrate an objective evaluation of design safety or apply system safety principles in rail
- Standards and guidance for system safety available at the time were **too abstract, complex, costly and/or impractical** for widespread recognition and acceptance by the Australian rail industry



AS	61508
EN	50126
EN	50128
EN	50129
EN	50657
IEC	61511
IEC	62278
IEC	62279
IEC	62425
ISO	26262



*It's the 'unknown
unknowns' that tend
to be difficult.*

– D. Rumsfeld

What are the lessons we can learn?

- ‘Good intent’ is not enough
- System safety can’t be added later
 - Needs specific expertise that is embedded in the organisations
 - Needs to make a real difference to the process
 - Needs to be measurable
 - Needs to be scalable
- Need to understand changes to systems



New standards

- RISSB (safety standards board):
 - AS 7474 Rail industry – System safety
 - AS 7473 Complex system integration in railways
 - System Safety Guideline
 - Rolling Stock Safety Assessment Guideline
- ONRSR (regulator):
 - System safety not mandated (yet)



Thank you!

(Search for “ATSB Devonport derailment”)

