34th Annual **INCOSE** international symposium

hybrid event

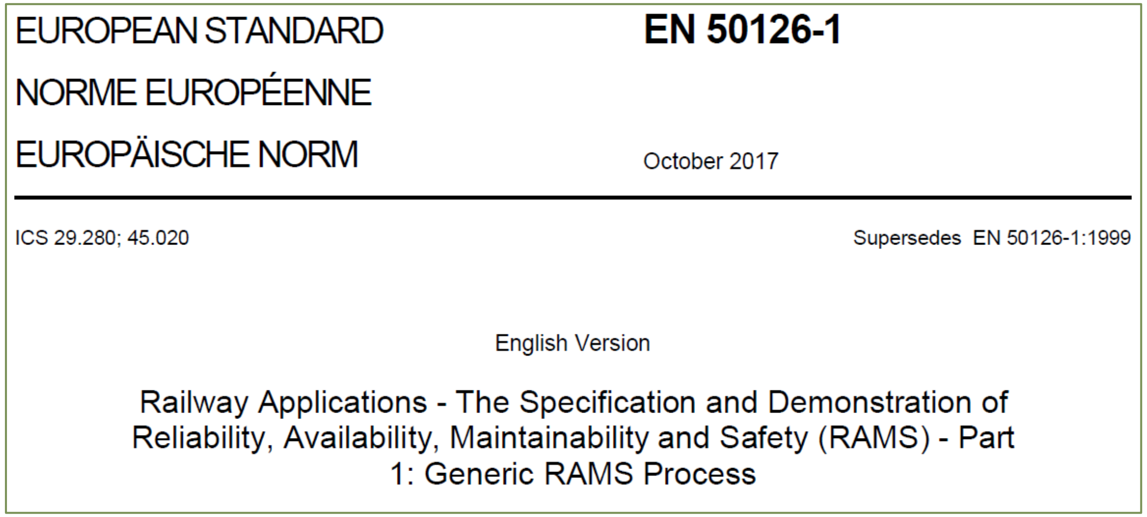
Dublin, Ireland
July 2 - 6, 2024

John Slowey – Think Systems

Application of the System-Theoretic Process Analysis (STPA) technique to enabling systems in the rail industry

Systems Safety in Rail

- Systems safety is well-established in the rail industry.
- Application of EN50126 (IEC 62278) suite of standards is BAU.
- Functional Safety approach – signalling systems, braking systems, tunnel ventilation systems.



EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN 50126-1

October 2017

ICS 29.280; 45.020

Supersedes EN 50126-1:1999

English Version

Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process

Enabling Systems

- System of Interest boundary not always drawn correctly → safety risk management of Enabling Systems not always adequate.
- Enabling systems found to contribute to multiple safety incidents.

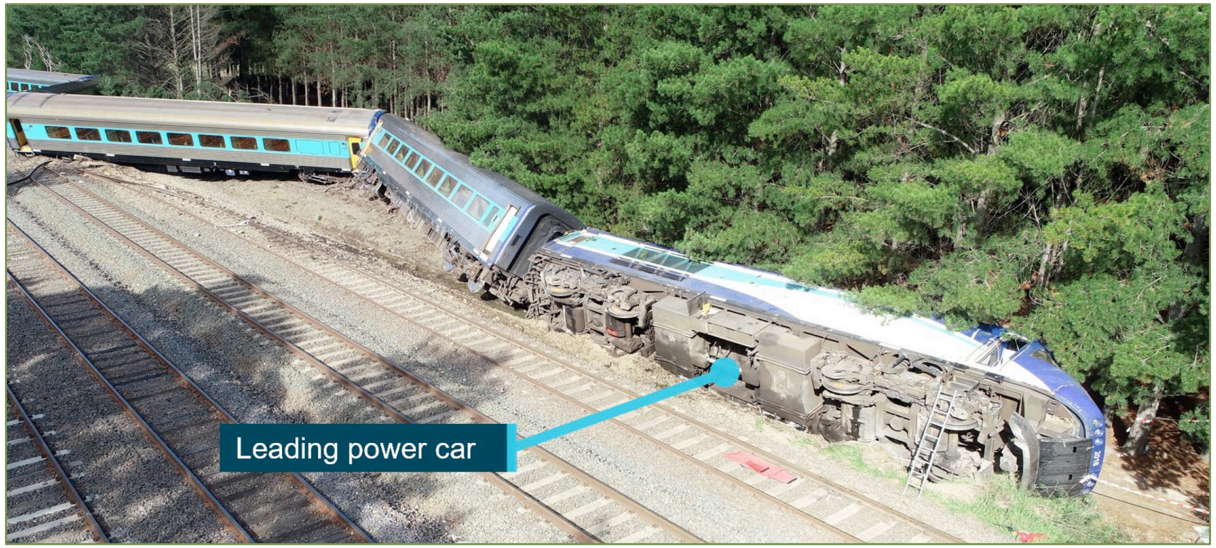
Derailment at Nana Glen, NSW.

Derailment at Carmont, Scotland.

The Wallan Incident

- Feb 2020 – railway operating in degraded mode.
- Passenger train entered 15km/h turnout at >114km/h and derailed.
- 2 fatalities, 8 serious injuries, 58 minor injuries.

- Enabling systems played a major role in the incident.
- How could safety have been better managed?



Derailment at Wallan, VIC.

The Train

- New South Wales XPT (eXpress Passenger Train)
- Class entered service in 1982.
- Localised version of British Rail HST (Intercity 125).
- Operated by NSW TrainLink.

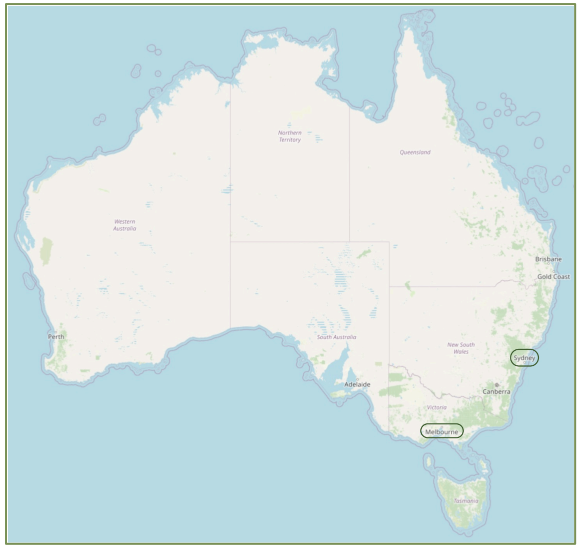
Typical XPT Consist

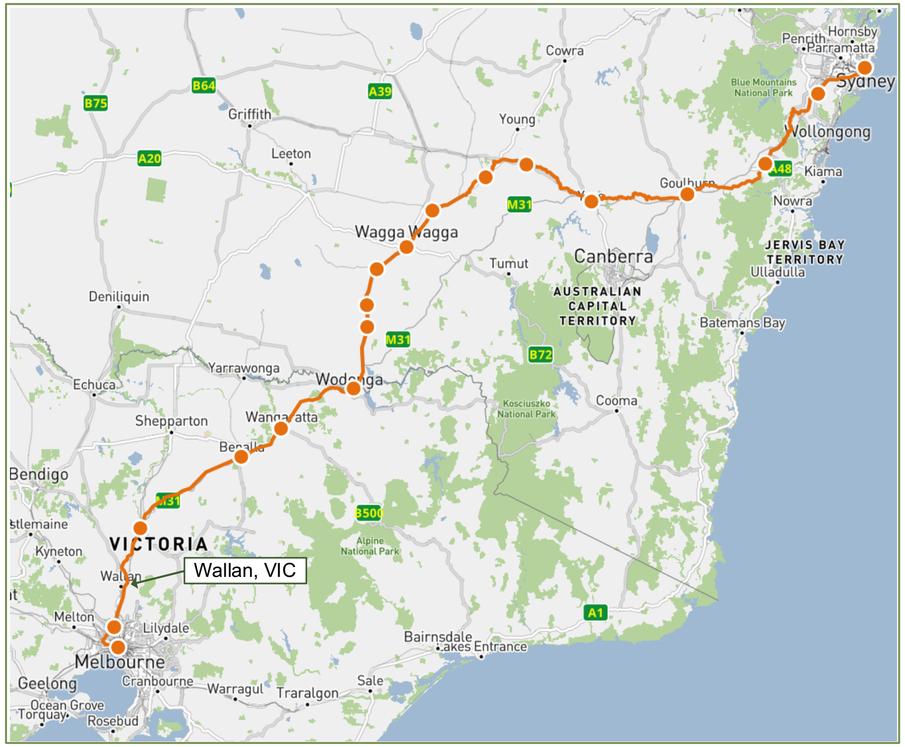
The Railway

- Incident occurred on Sydney to Melbourne line, approx. 45km north of Melbourne.
- Rail network operated by Australian Rail Track Corporation (ARTC).

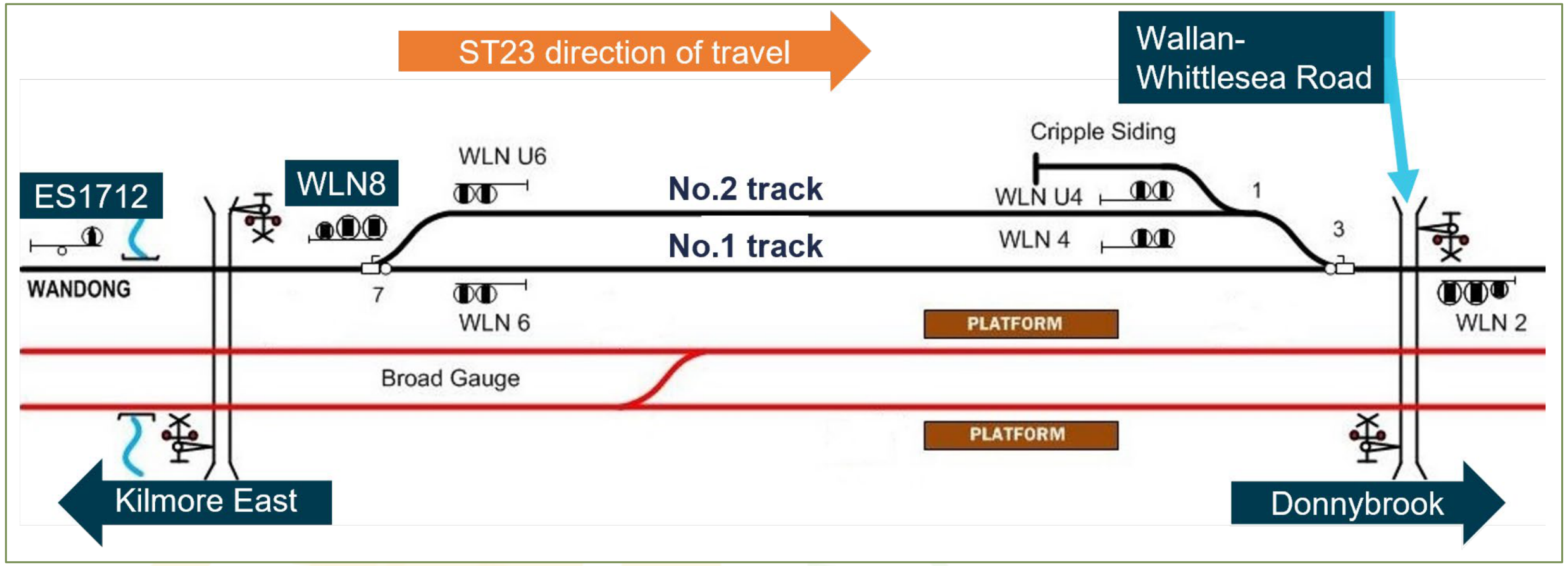
“Compared to other countries, our regional rail network is not at the standard expected of a modern rail system and is in urgent need of investment.”

Australasian Railway Association





Wallan Loop



Track Diagram – Wallan Loop

Typical Turnout

- Fire had destroyed signalling equipment normally used to control rail traffic.
- System had been operating in a degraded mode for 2 weeks.
- Trains had been routed straight ahead (No. 1 track), but this changed shortly before incident.

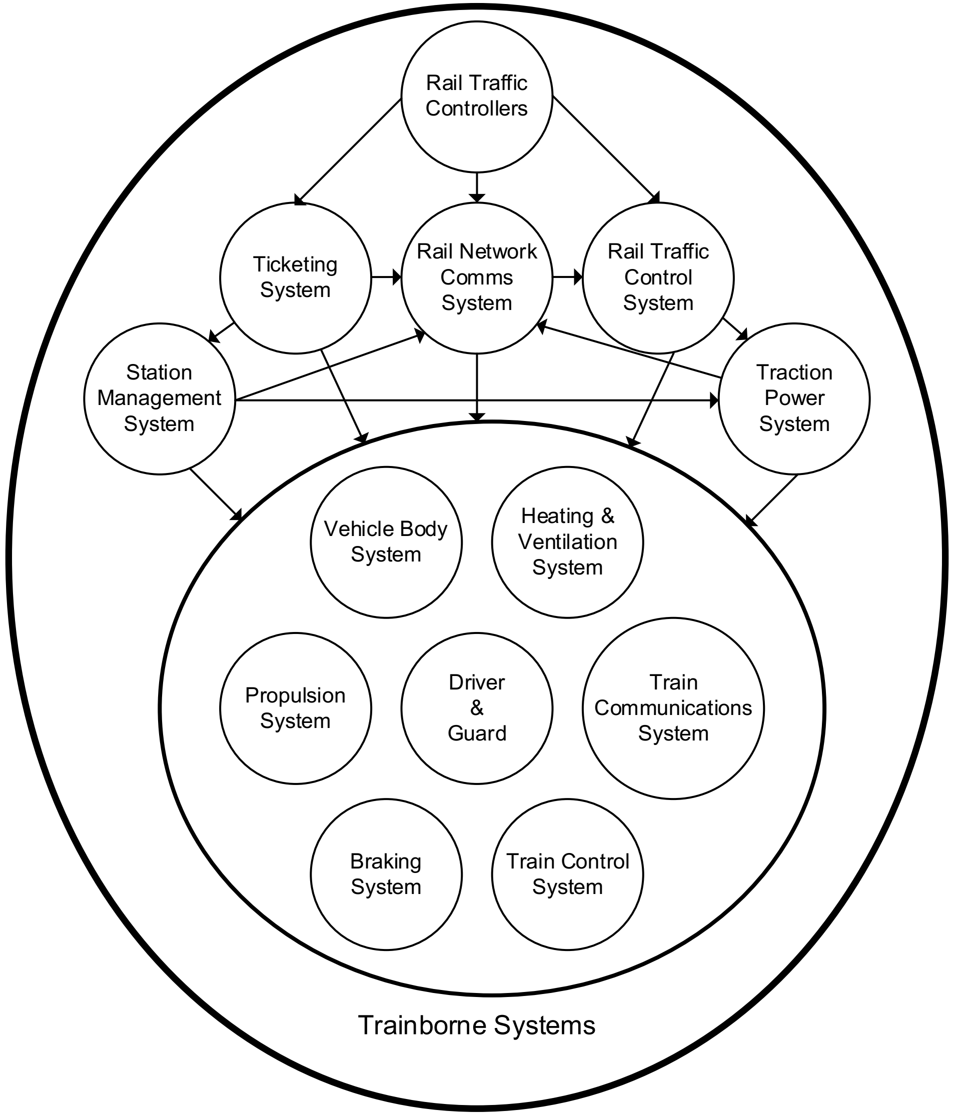
Degraded Mode

- “Manual train authority arrangements” – set of procedural controls controlling safety risks normally managed by signalling system.
- Effectively formed a temporary Safety Management System (SMS).
- Safety risk assessment was performed but had ‘significant weaknesses’.
- This enabling system was identified (amongst others) as a significant contributor to the incident.

British Transport Films – Single Line Working (1957)
https://www.youtube.com/watch?v=nMActDF-hBk

A Systems Approach

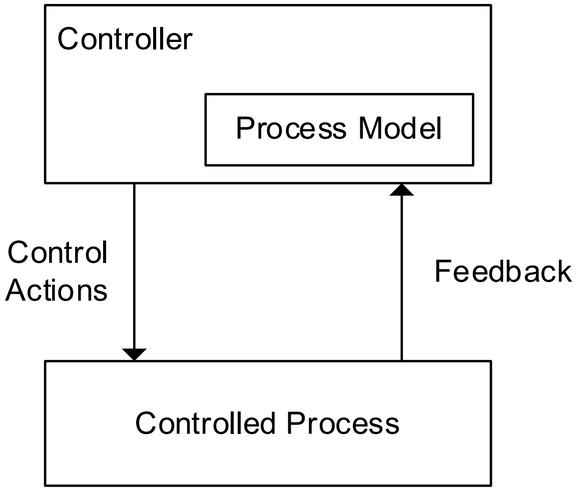
- Incident did not occur because of a system or component failure.
- A complex System of Systems (SoS) assured the safety of the Wallan XPT.
- Subsystem-level management of safety was not effective.
- Could an alternative approach have prevented the incident?



STAMP

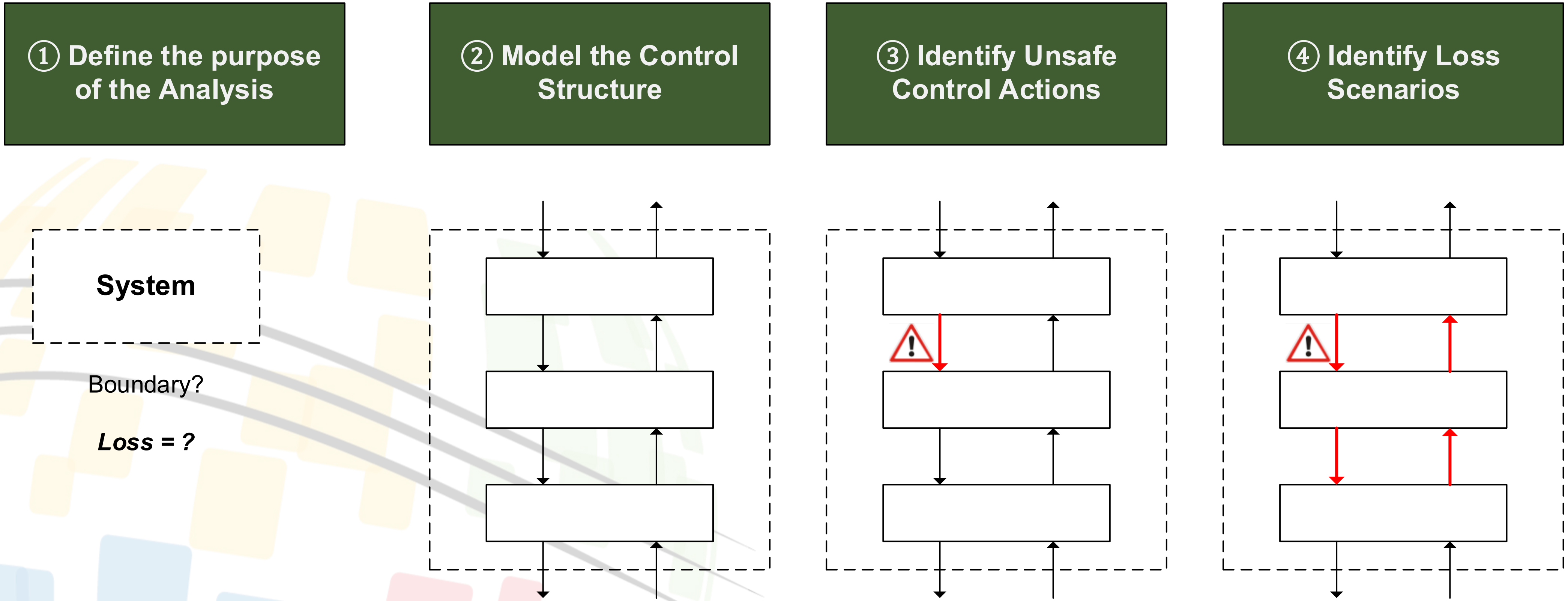
- System-Theoretic Accident Model and Processes.
- Developed in response to increasing complexity of SoS and inadequacy of traditional event-chain models.

- STAMP enables safety to be viewed as a control problem:
  - ➢ Safety is an emergent property of systems.
  - ➢ Emergent properties are controlled by a set of constraints (control laws).
  - ➢ Accidents result from interactions among components that violate the safety constraints.



STPA

- STPA (Systems-Theoretic Process Analysis)
- Hazard analysis technique based on STAMP causality model.
- Aims to identify how safety constraints (control laws) can be violated.



① Define the purpose of the Analysis

② Model the Control Structure

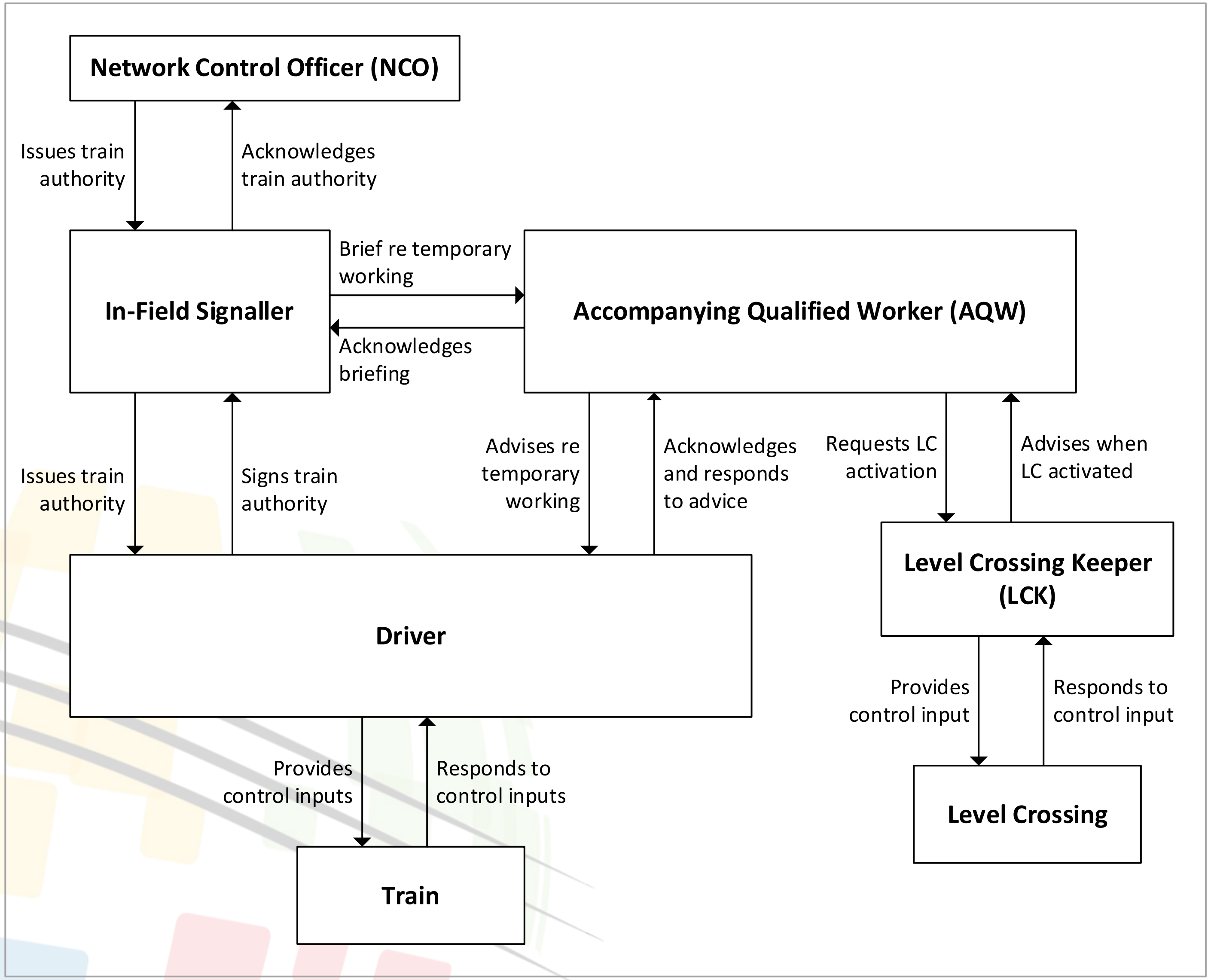
③ Identify Unsafe Control Actions

④ Identify Loss Scenarios

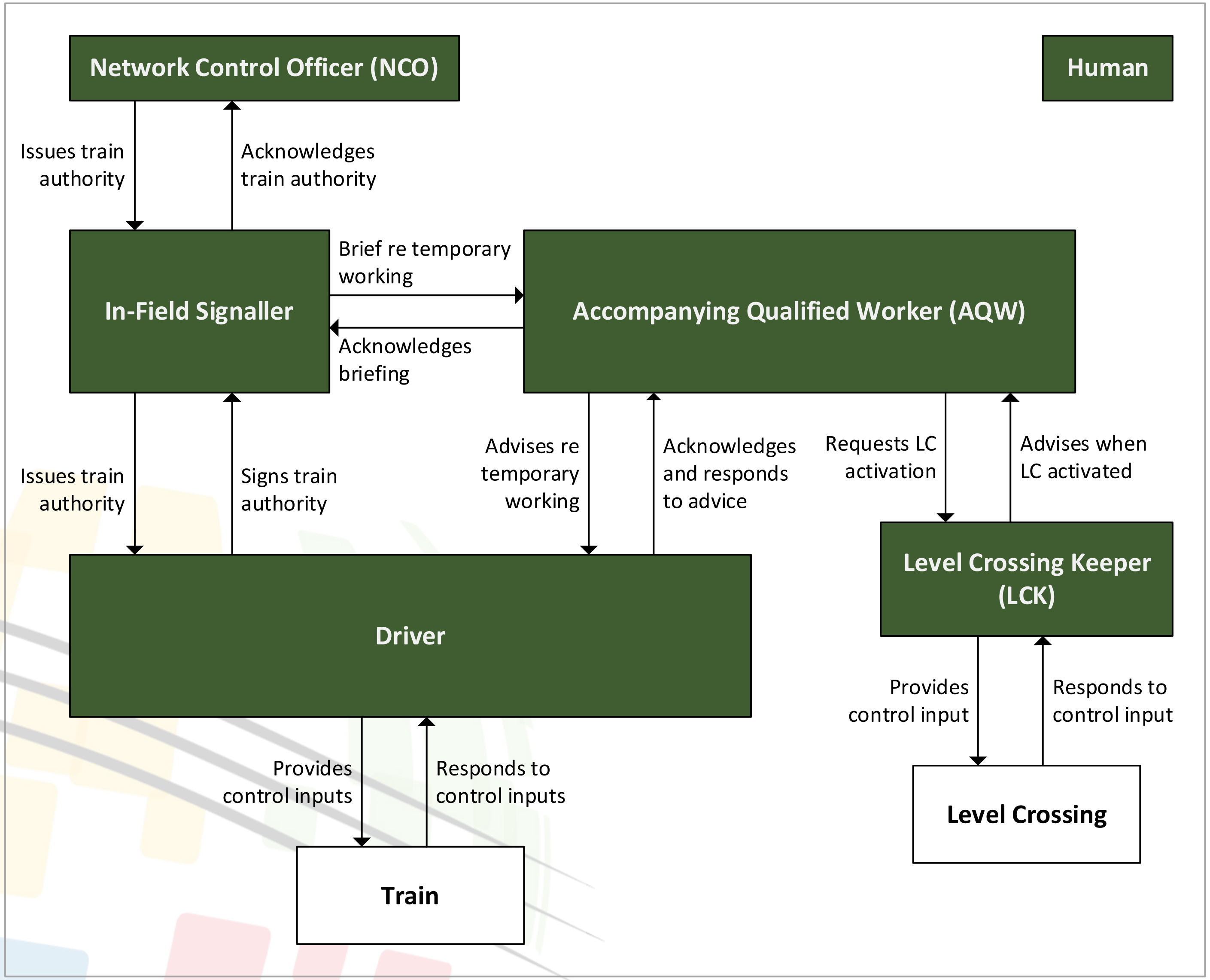
STPA – What if?

- Temporary SMS is well-documented in investigation report.
- STPA was used to identify loss scenarios for this subsystem.
- Aimed to see if better safety outcome was achievable.

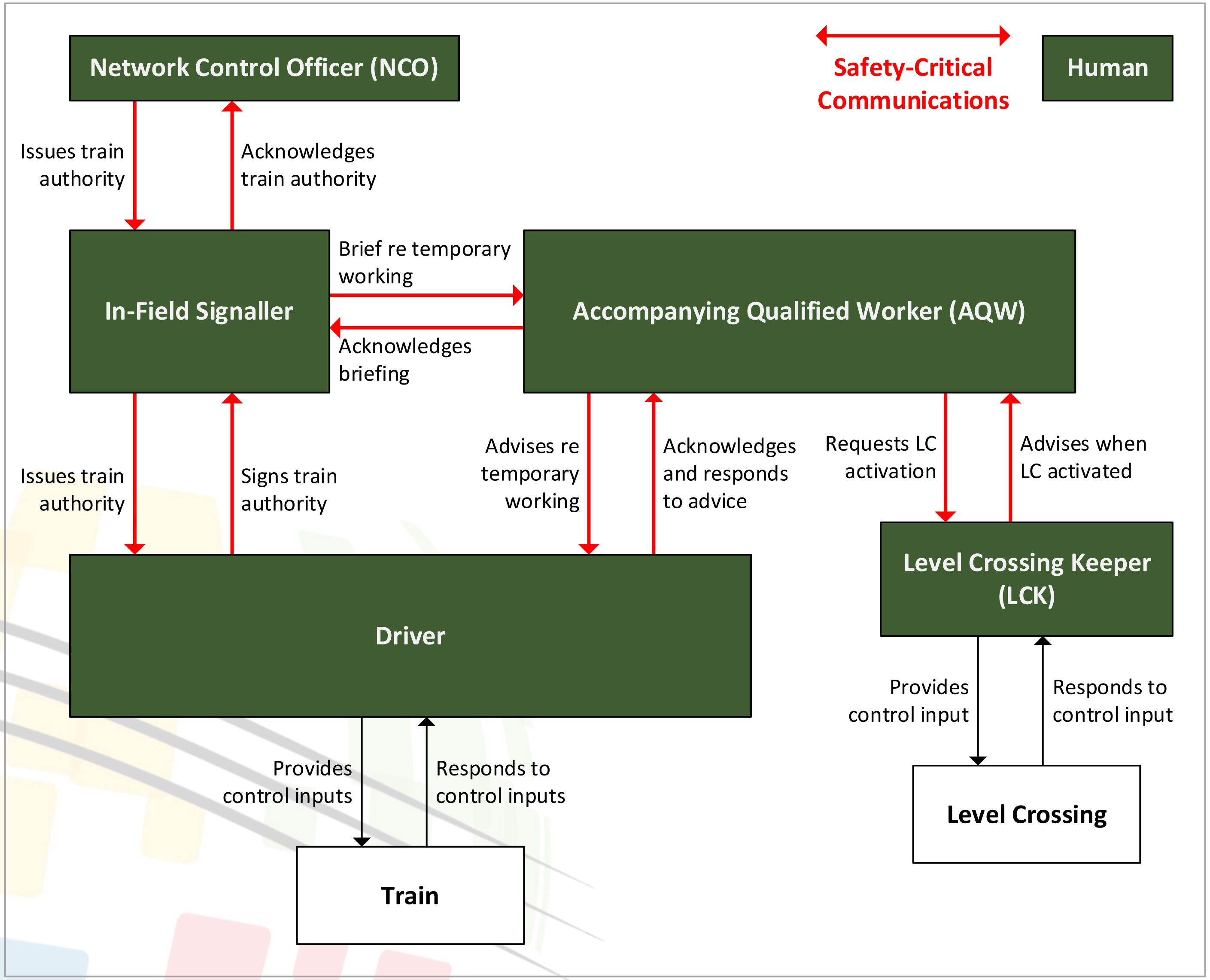
Temporary SMS – Control Structure


Network Control Officer (NCO)
Issues train authority
Acknowledges train authority
In-Field Signaller
Brief re temporary working
Acknowledges briefing
Accompanying Qualified Worker (AQW)
Issues train authority
Signs train authority
Advises re temporary working
Acknowledges and responds to advice
Requests LC activation
Advises when LC activated
Level Crossing Keeper (LCK)
Driver
Provides control input
Responds to control input
Provides control inputs
Responds to control inputs
Train
Level Crossing

Temporary SMS – Control Structure

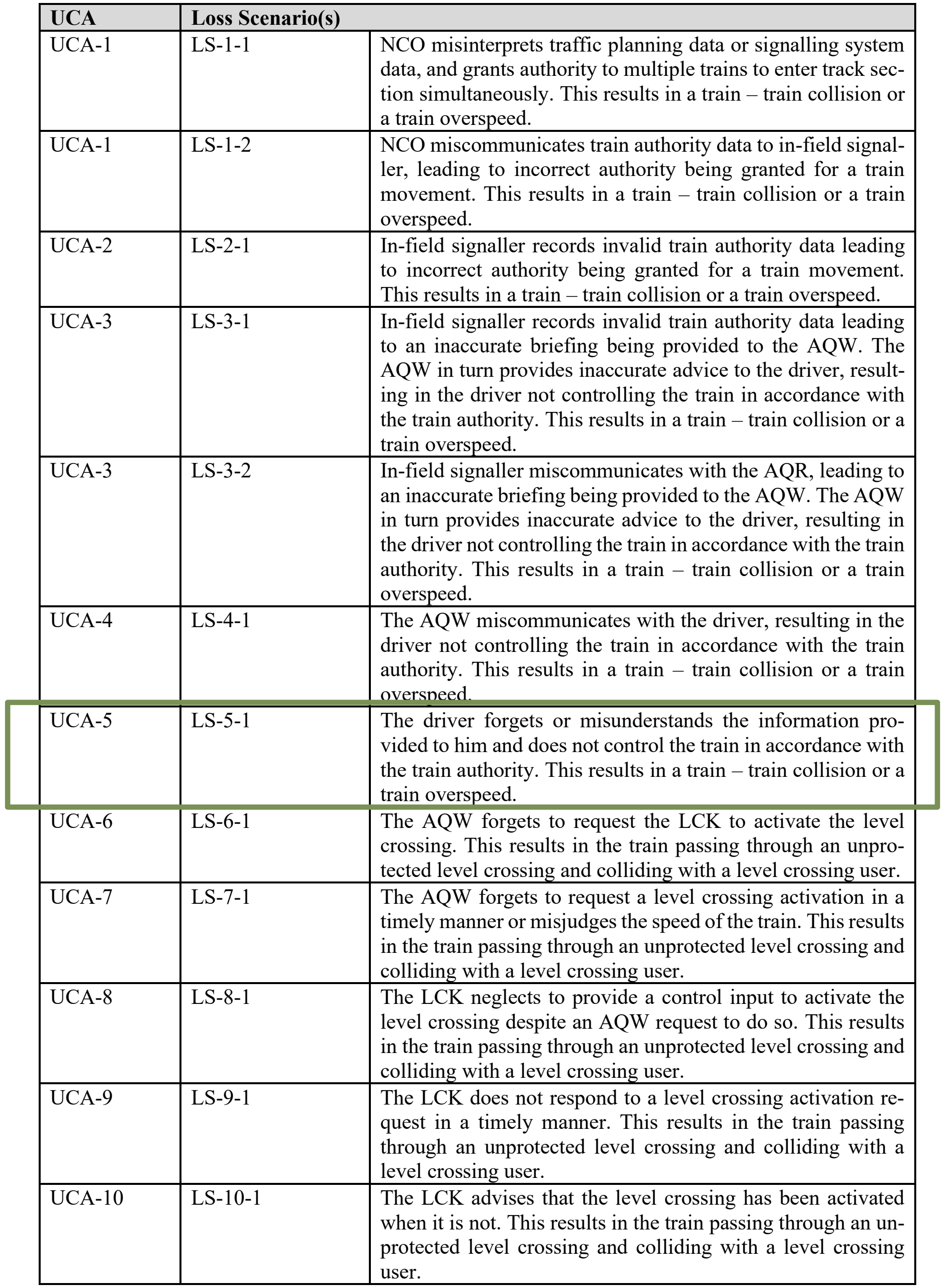

Network Control Officer (NCO)
Human
Issues train authority
Acknowledges train authority
In-Field Signaller
Brief re temporary working
Acknowledges briefing
Accompanying Qualified Worker (AQW)
Issues train authority
Signs train authority
Advises re temporary working
Acknowledges and responds to advice
Requests LC activation
Advises when LC activated
Driver
Level Crossing Keeper (LCK)
Provides control inputs
Responds to control inputs
Provides control input
Responds to control input
Train
Level Crossing

Temporary SMS – Control Structure


Safety-Critical Communications
Human
Network Control Officer (NCO)
Issues train authority
Acknowledges train authority
In-Field Signaller
Brief re temporary working
Acknowledges briefing
Accompanying Qualified Worker (AQW)
Issues train authority
Signs train authority
Advises re temporary working
Acknowledges and responds to advice
Requests LC activation
Advises when LC activated
Driver
Level Crossing Keeper (LCK)
Provides control inputs
Responds to control inputs
Provides control input
Responds to control input
Train
Level Crossing

Temporary SMS Loss Scenarios

- List of loss scenarios was long.
- Loss scenario that eventuated at Wallan was identified.



UCA	Loss Scenario(s)	
UCA-1	LS-1-1	NCO misinterprets traffic planning data or signalling system data, and grants authority to multiple trains to enter track section simultaneously. This results in a train – train collision or a train overspeed.
UCA-1	LS-1-2	NCO miscommunicates train authority data to in-field signaller, leading to incorrect authority being granted for a train movement. This results in a train – train collision or a train overspeed.
UCA-2	LS-2-1	In-field signaller records invalid train authority data leading to incorrect authority being granted for a train movement. This results in a train – train collision or a train overspeed.
UCA-3	LS-3-1	In-field signaller records invalid train authority data leading to an inaccurate briefing being provided to the AQW. The AQW in turn provides inaccurate advice to the driver, resulting in the driver not controlling the train in accordance with the train authority. This results in a train – train collision or a train overspeed.
UCA-3	LS-3-2	In-field signaller miscommunicates with the AQR, leading to an inaccurate briefing being provided to the AQW. The AQW in turn provides inaccurate advice to the driver, resulting in the driver not controlling the train in accordance with the train authority. This results in a train – train collision or a train overspeed.
UCA-4	LS-4-1	The AQW miscommunicates with the driver, resulting in the driver not controlling the train in accordance with the train authority. This results in a train – train collision or a train overspeed.
UCA-5	LS-5-1	The driver forgets or misunderstands the information provided to him and does not control the train in accordance with the train authority. This results in a train – train collision or a train overspeed.
UCA-6	LS-6-1	The AQW forgets to request the LCK to activate the level crossing. This results in the train passing through an unprotected level crossing and colliding with a level crossing user.
UCA-7	LS-7-1	The AQW forgets to request a level crossing activation in a timely manner or misjudges the speed of the train. This results in the train passing through an unprotected level crossing and colliding with a level crossing user.
UCA-8	LS-8-1	The LCK neglects to provide a control input to activate the level crossing despite an AQW request to do so. This results in the train passing through an unprotected level crossing and colliding with a level crossing user.
UCA-9	LS-9-1	The LCK does not respond to a level crossing activation request in a timely manner. This results in the train passing through an unprotected level crossing and colliding with a level crossing user.
UCA-10	LS-10-1	The LCK advises that the level crossing has been activated when it is not. This results in the train passing through an unprotected level crossing and colliding with a level crossing user.

Conclusions

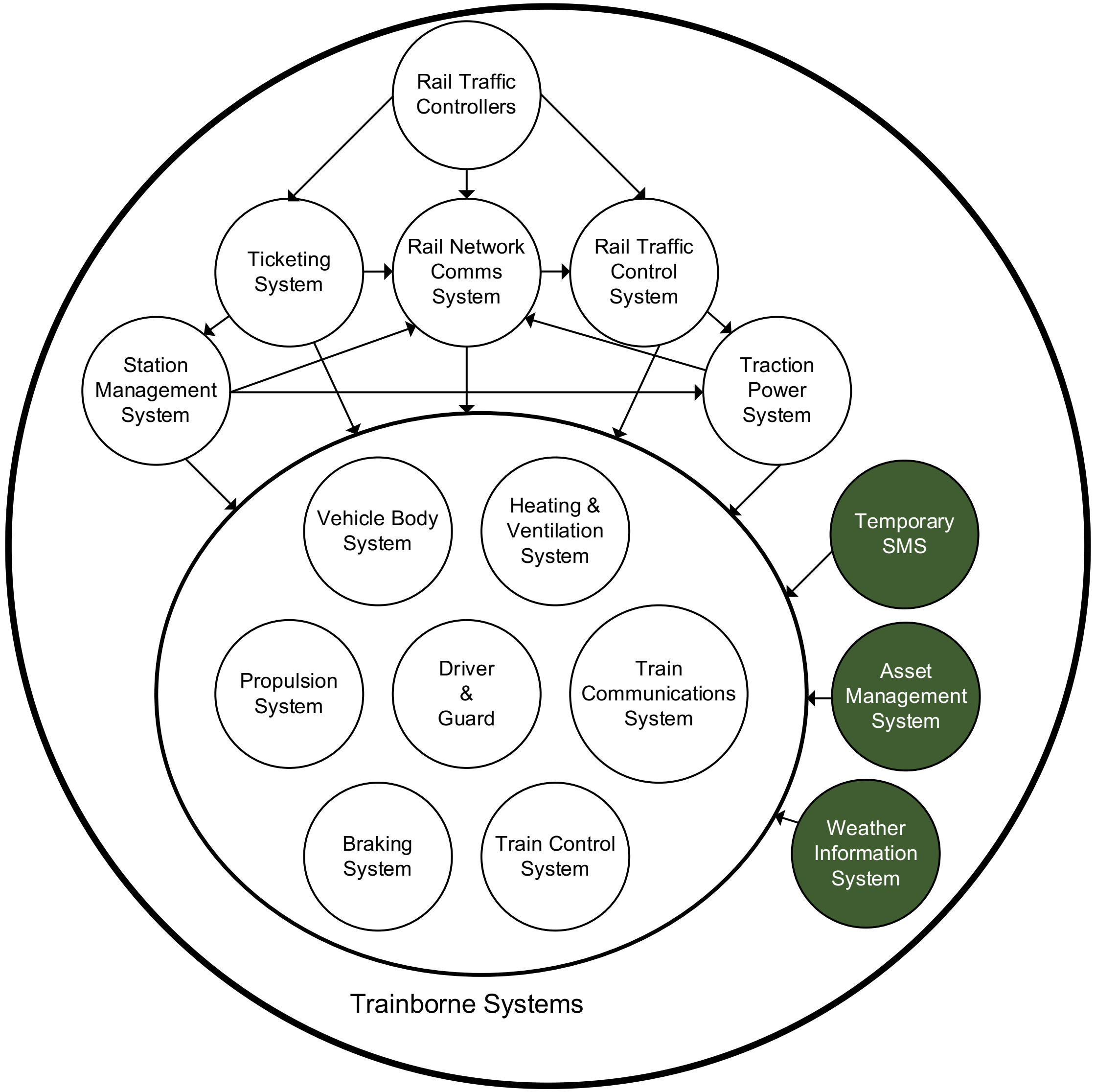
- Using STPA to analyse the Temporary SMS would have added value.

  - ➢ STPA requires thought and analysis, inherently incompatible with copy-and-paste approach.
  - ➢ Pictures more powerful than spreadsheets → Modelling of control structure provides insights.
  - ➢ Systematic identification of loss scenarios.

- Could use of STPA have prevented loss? Possibly.
  - ➢ Would have highlighted lack of higher-integrity controls for safety risk.

Recommendations

- MBSE being increasingly adopted in rail – enabling systems being modelled for first time.
- Obvious opportunity for model re-use.
- Real power of STPA could be realised at system level.

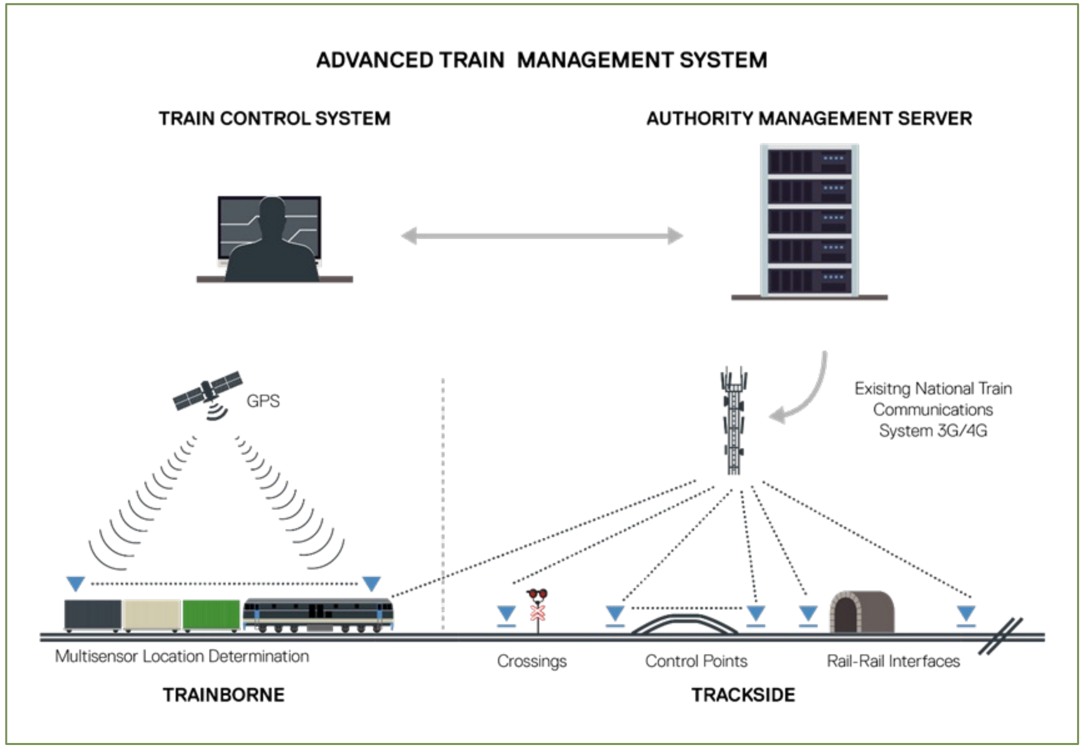


What could have been done differently?

Potential additional controls:

- Temporary Speed Restriction signage.

- Reduction of trackside assets.
- Automatic Train Protection.
- Crashworthiness of Rolling Stock.


ADVANCED TRAIN MANAGEMENT SYSTEM
TRAIN CONTROL SYSTEM
AUTHORITY MANAGEMENT SERVER
GPS
Exisitng National Train Communications System 3G/4G
Multisensor Location Determination
Crossings
Control Points
Rail-Rail Interfaces
TRAINBORNE
TRACKSIDE

Advanced Train Management System
Australian Rail Track Corporation

Thank You!

34th Annual INCOSE international symposium

hybrid event

Dublin, Ireland
July 2 - 6, 2024

www.incose.org/symp2024
#INCOSEIS