INTERNATIONAL RAILWAY SAFETY COUNCIL 2022

IRSC Spain

IRSC 2022

INTERNATIONAL RAILWAY
SAFETY COUNCIL

SEVILLA, OCTOBER 16-21, 2022

University of HUDDERSFIELD
Inspiring global professionals

ROCK rail united kingdom

UNIVERSITY OF BIRMINGHAM

BCRRE

EUROPEAN UNION AGENCY FOR RAILWAYS

AESF AGENCIA ESTATAL DE SEGURIDAD FERROVIARIA

adif

Coen van Gulijk / George Bearfield / Richard Thomas
University of Huddersfield / Birmingham & ROCK

IRSC Spain

IRSC 2022
INTERNATIONAL RAILWAY SAFETY COUNCIL
SEVILLA, OCTOBER 16-21, 2022

EUROPEAN UNION AGENCY FOR RAILWAYS
AESF AGENCIA ESTATAL DE SEGURIDAD FERROVIARIA
adif

University of HUDDERSFIELD
Inspiring global professionals

Security/Safety assessment with the STAIRCASE model

Transformation of rail Cyber/Safety and Security (paper 61, speaker 34)

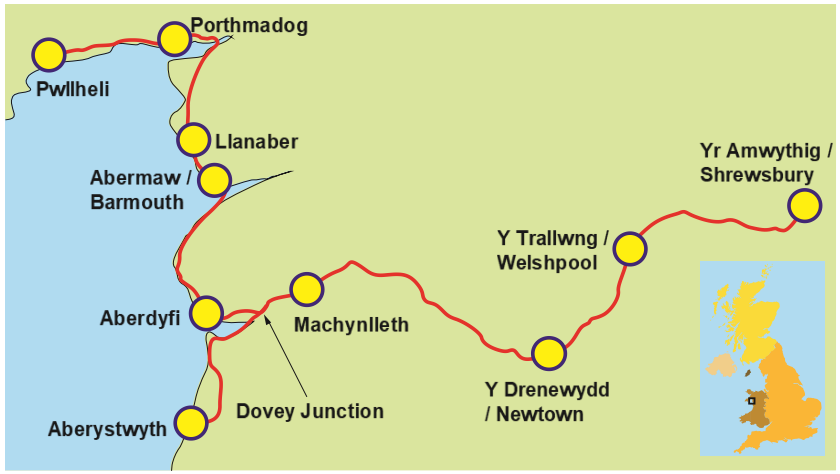
IRSC 2022
INTERNATIONAL RAILWAY SAFETY COUNCIL
SEVILLA, OCTOBER 16-21, 2022

INDEX

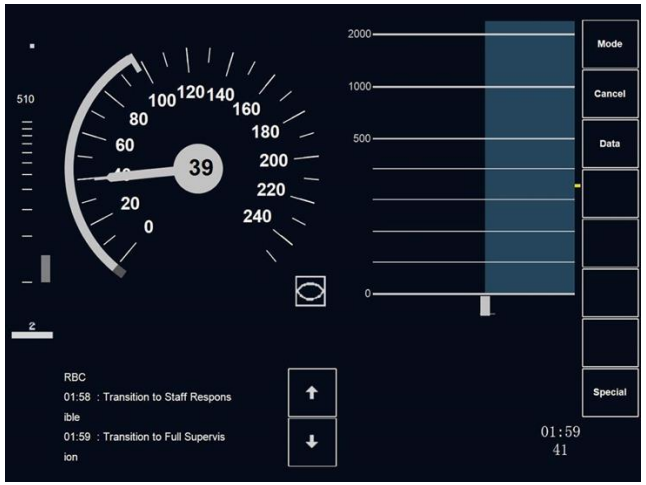
CHAPTER 1

ERMTS Cambrian Line

Preambule: ERMTS Cambrian line: Machynlleth signalling control centre [RAIB 17/2019]



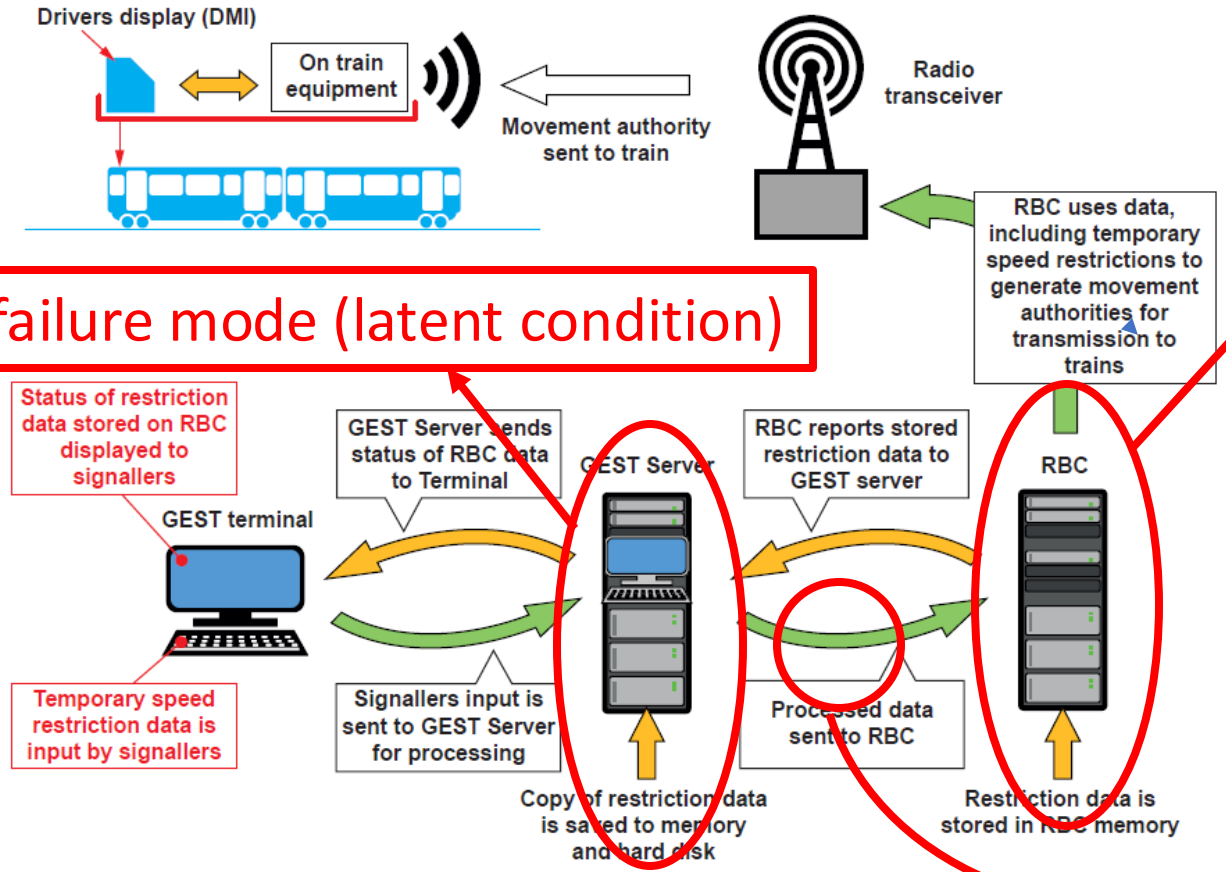
Signaling system stopped transmitting temporary speed restriction data after it had experienced a shutdown and restart at around 23:10 hrs the previous evening.



Drivers did not see the TSR in their display so they crossed TSR areas at speeds they shouldn't. No-one was hurt and no damage was done to equipment.

https://www.gov.uk/raib-reports/report-17-2019-loss-of-safety-critical-signalling-data-on-the-cambrian-coast-line

Complex digital system confounded safety assessment [RAIB 17/2019]



GEST in failure mode (latent condition)

Internally triggered software rollover (reset) due to conflincting movement authorities (10-12 per year!)
TSR in memory: lost.

TSR was not communicated to:
a) RBC/TMI/Driver
b) RBC/Signaller

Figure 6: Simplified arrangement of GEST and signalling control system interface

RAIB recommendations

IMs {..} aided by the wider rail industry, should **improve its safety assurance** process for high integrity software-based systems and **improve safety learning** from failures of such systems, and develop a process to **capture data** needed to understand these failures.

{..} should **review its safety assurance processes** in the light of the learning from this investigation, and should provide a technical solution for the Cambrian lines that avoids the need for signallers to verify automatically uploaded speed restrictions.

Drivers {..} **reporting inconsistencies information** provided to them; the need for ISA to **understand the scope of checks** undertaken by other bodies and to apply extra vigilance if documents form part of a non-standard process; the importance of **clients undertaking their client role when procuring high integrity software**; and achieving the specified level of safety when implementing temporary speed restrictions in ERTMS.

"Better safety assurance needed"

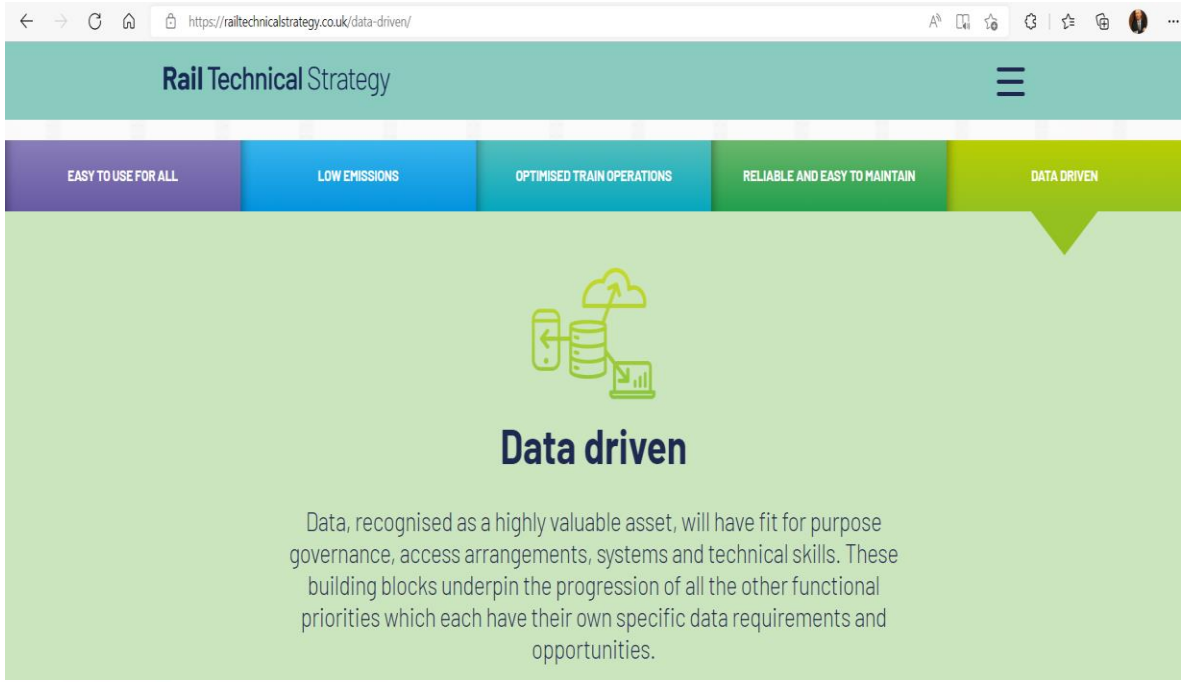
https://www.gov.uk/raib-reports/report-17-2019-loss-of-safety-critical-signalling-data-on-the-cambrian-coast-line

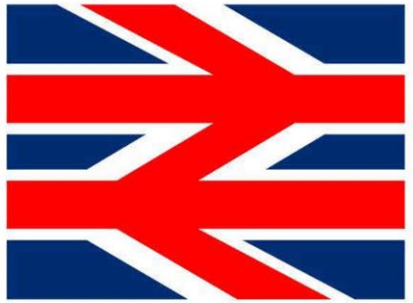
CHAPTER 2

Digitalisation of Rolling stock

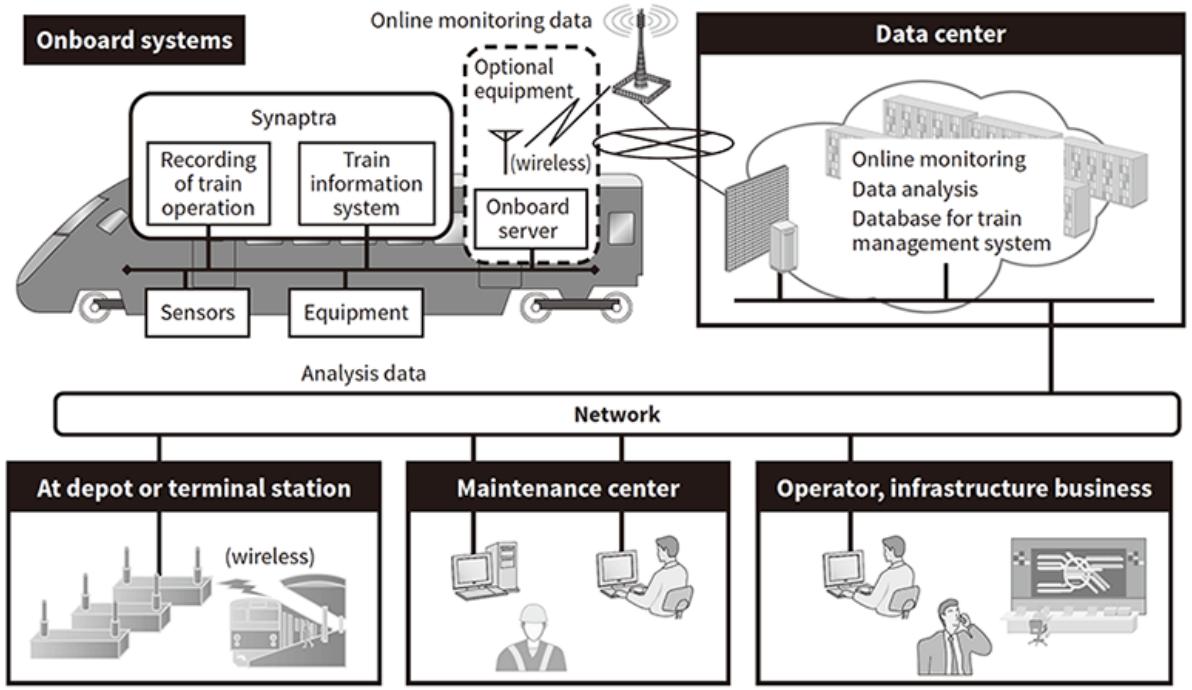
And software Solutions are promoted by industry in a broad sense

- Data becomes the proverbial oil that greases the wheels of progress
- It is a keystone technology in the UK's Rail Technical Strategy
- It introduces cybersecurity liabilities that are attracting attention





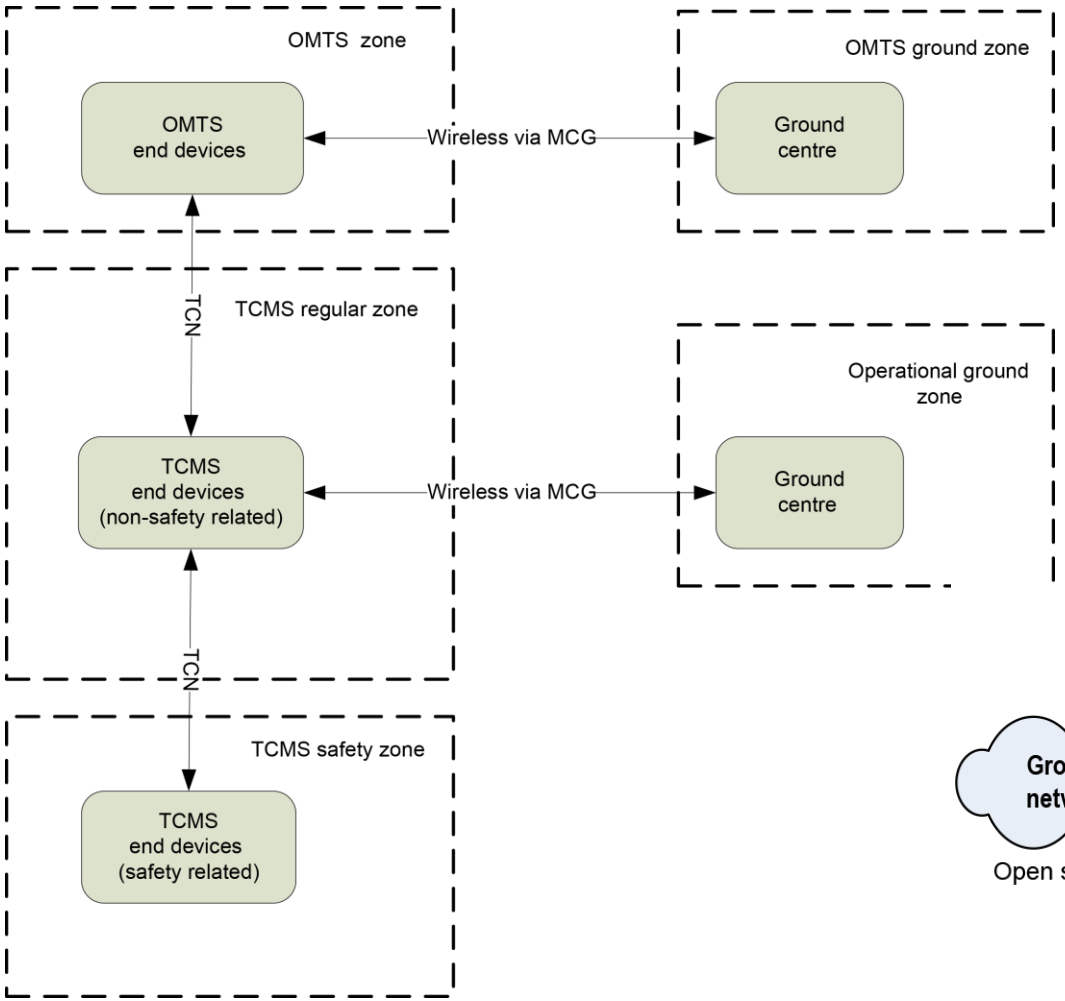
Rolling stock at the pinnacle of digitalization

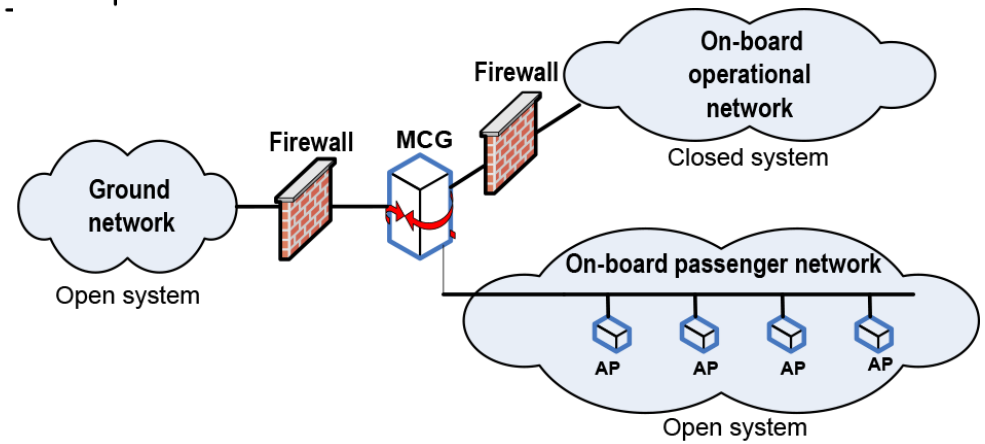


"Computer on Wheels?"

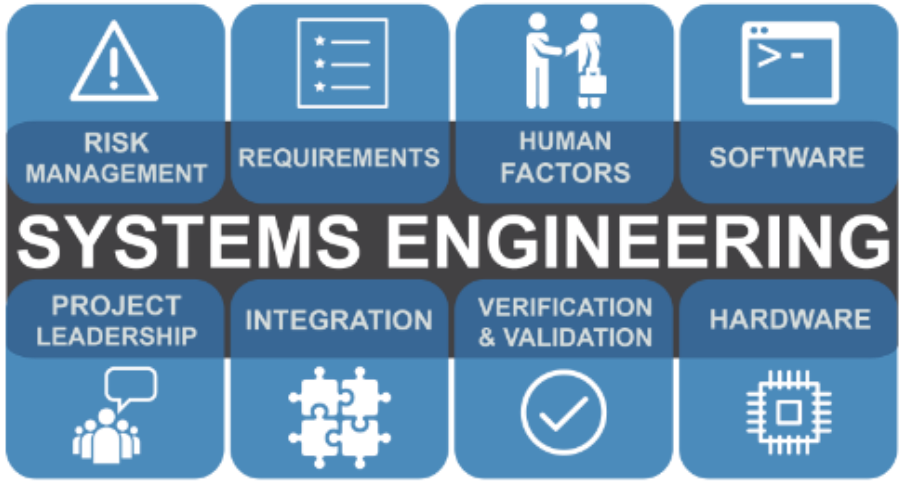
https://www.hitachi.com/rev/archive/2018/r2018_07/07a03/index.html

Security zones

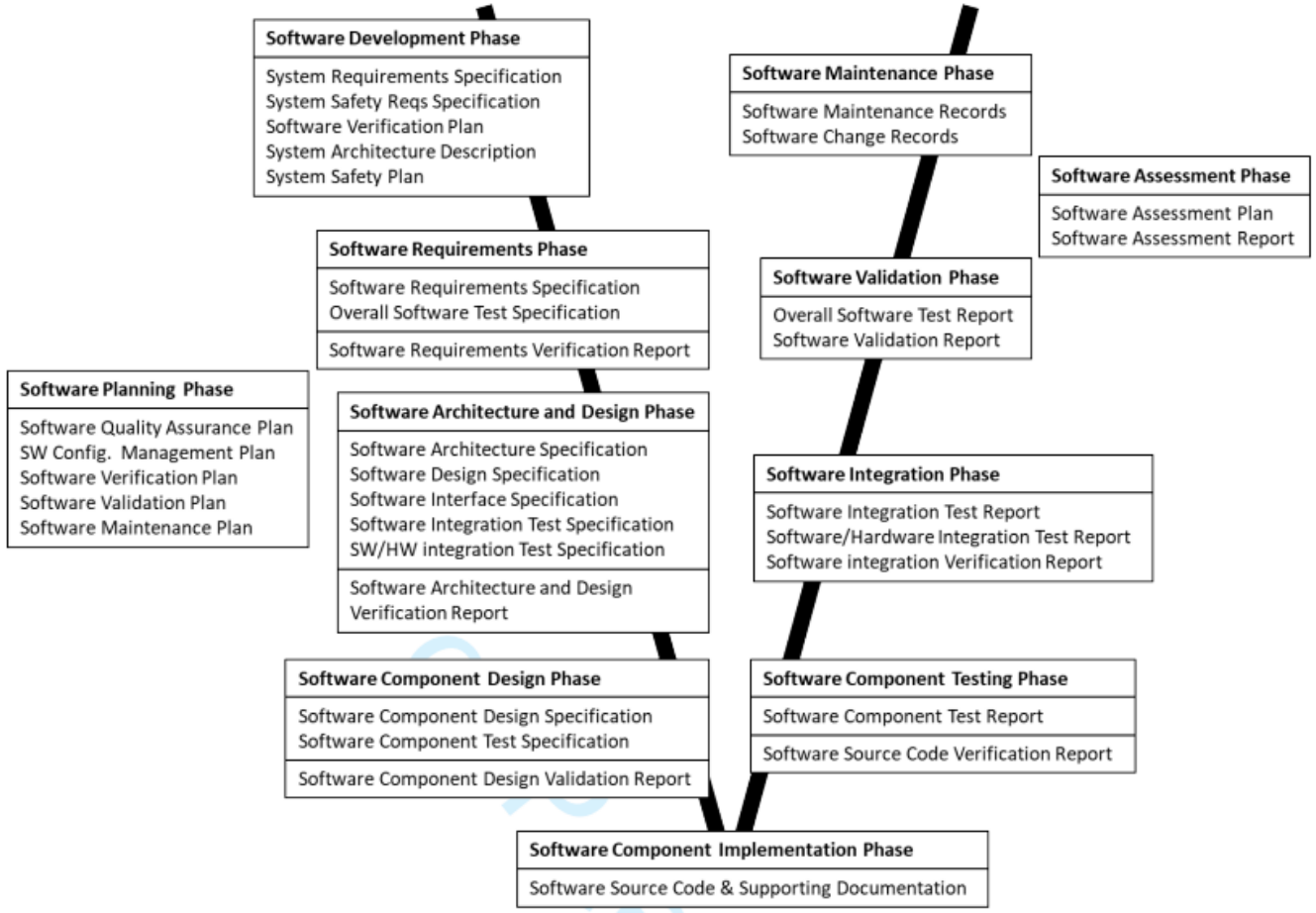




Safety Standards built on systems engineering with V&V cycle



https://www.incose.org/systems-engineering



Based on EN50128

https://journals.sagepub.com/doi/full/10.1177/09544097221102292

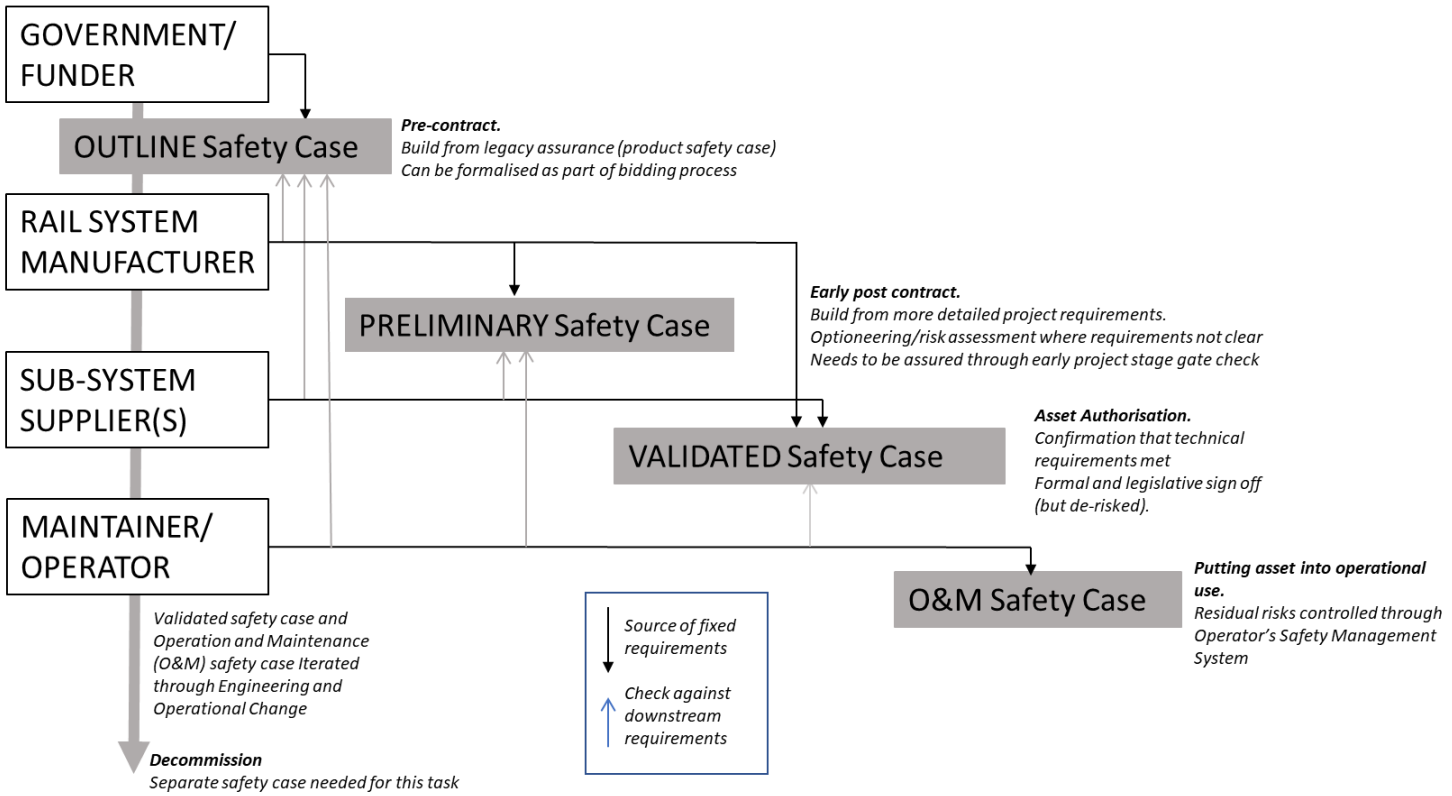
But software engineering is quite a different animal

https://www.digite.com/agile/scrum-methodology/

CHAPTER 3

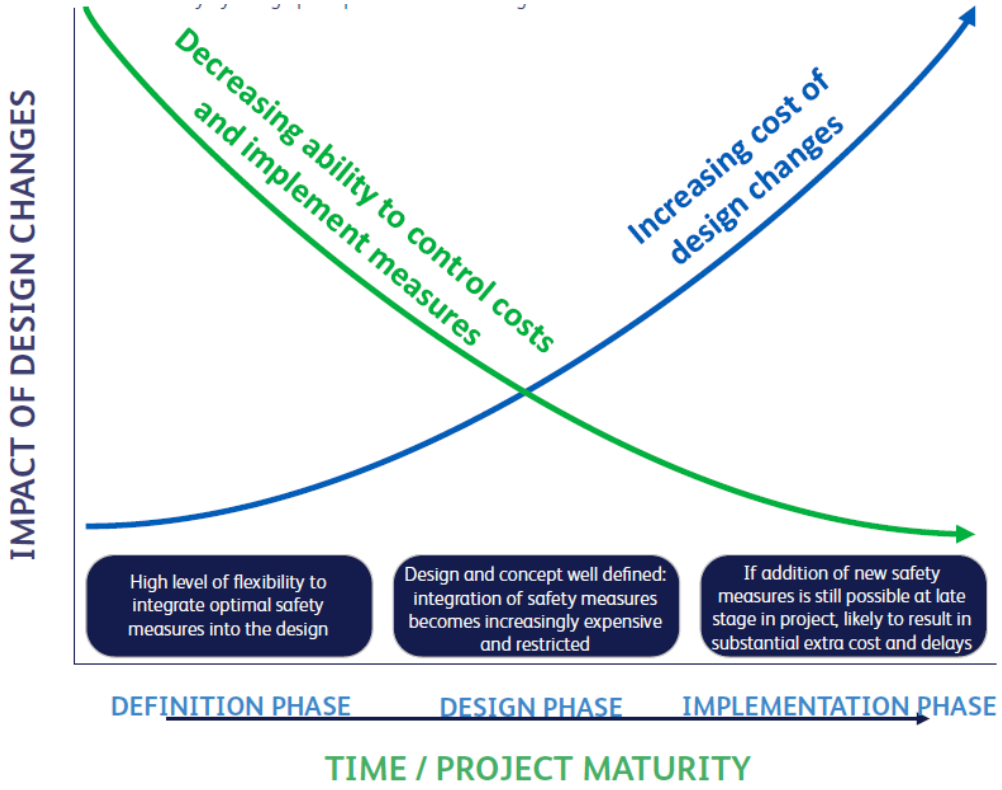
Proposal for strengthening verification process; the STAIRCASE

So we want to bring the validation forward in steps: the STAIRCASE



https://journals.sagepub.com/doi/full/10.1177/09544097221102292

When fundamental changes are needed



Outline safety case: pre contract

We propose that the first significant evaluation of the (outline) safety case should be a part of the tender process, and a basis on of which the contract is selected

This puts some (more) onus on train manufacturers on formulating core safety arguments and a commercial incentive to enhance safety and security by design.

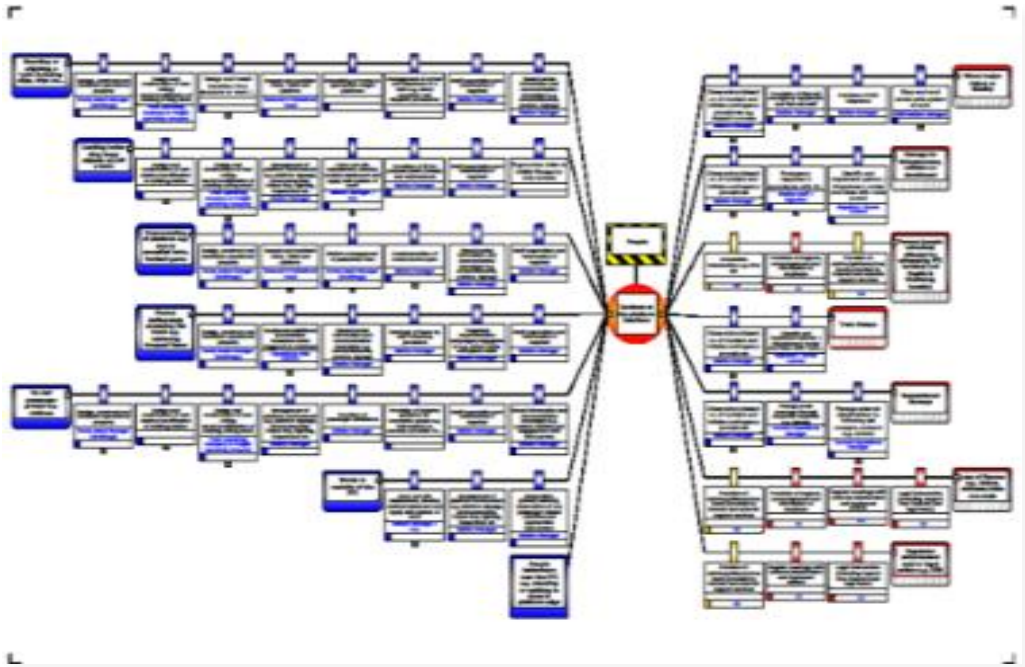
It also offers opportunities to gather initial ideas and architectures to address the rapidly evolving digital assurance risks and (dynamic) software updates and, as a bonus, thoughts about how to deal with emerging design assurance issues.

Preliminary safety case: early post-contract

With the core safety arguments of the outline safety case as a starting point, the safety case can develop as a preliminary safety case to provide transparency.

This offers opportunities for early engagement with the future user/ operator on operational risks and controls for the cyber safety, cybersecurity and sensitivities for the local operation conditions. Clear safety requirements can then be cascaded into the tier 1 and tier 2 supply chain.

The preliminary safety case offers ongoing clarity on progress in compliance, project delivery and the assurance process. It also offers clarity in things that might have been missed and how they were solved.



Validated safety case: asset authorisation

The validated safety case remains a well defined process associated with the key regulatory stage gate; but it follows from earlier stages in a relatively straightforward manner.

It should be about gathering the necessary information to evidence the safety argument and provide assurance that is already in place since the preliminary safety case

The STAIRCASE makes authorization a more mechanical process, bringing greater assurance, ensuring that there is a clear audit trail for the safety argument and a solid basis for risk transfer into the operation and maintenance phases.

O&M safety case: operating in a dynamic environment

With a robust validated safety case there is room for an O&M safety case which is envisaged as a space where the asset owner, the operator and the maintenance supplier deal with the dynamic (cyber) safety/security world.

It offers a platform where residual risks are transferred into an operators/infrastructure manager's SMS that provides space for attention to (weak) signals of software failures and breaches.

Returning to RAIB recommendations

IM/Man {..} aided by the wider rail industry, should **improve its safety assurance** process for high integrity software-based systems and **improve safety learning** from failures of such systems, and develop a process to **capture data** needed to understand these failures.

{..} should **review its safety assurance processes** in the light of the learning from this investigation, and should provide a technical solution for the Cambrian lines that avoids the need for signallers to verify automatically uploaded speed restrictions.

Drivers {..} **reporting inconsistencies information** provided to them; the need for ISA to **understand the scope of checks** undertaken by other bodies and to apply extra vigilance if documents form part of a non-standard process; the importance of **clients undertaking their client role when procuring high integrity software**; and achieving the specified level of safety when implementing temporary speed restrictions in ERTMS.

Conclusions for the STAIRCASE

- It changes the safety culture by talking about core safety arguments throughout the asset lifecycle
- Interactions with stakeholders are improved
- Gives room to discussing digital risks early stage
- Puts owners and operators in a better position to understand and control dynamic risks

- ALSO: it builds on current practice (doesn't replace it)
- It addresses concerns that RAIB expressed and
- When done well shouldn't take excessive amounts of time
- The staircase codifies what you could consider 'better practice'

Call to Action.

We propose research to develop the STAIRCASE addressing:

- Collate cyber **threats landscape** for rolling stock and its sprawling networks
- Assess vulnerabilities for cyber safety and cyber security to inform **software architectures**
- Investigate cyber safety/security **barriers** and mechanisms
- Rules to set **performance levels** for integrated (cyber)safety and cyber security systems and

UKRRIN
UK RAIL RESEARCH AND INNOVATION NETWORK

University of HUDDERSFIELD
Inspiring global professionals

UNIVERSITY OF BIRMINGHAM | BCRRE

ROCK rail united kingdom

Further reading

Check for updates

Case Study

Institution of MECHANICAL ENGINEERS — Journal of RAIL AND RAPID TRANSIT

Proc IMechE Part F:
J Rail and Rapid Transit
2022, Vol. 0(0) 1–9

Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/09544097221102292
journals.sagepub.com/home/pif
SAGE

Redefining rail systems verification and validation: The safety/security STAIRCASE model

George Bearfield[1], Coen Van Gulijk[2] and Richard James Thomas[3]

Abstract

Safety critical functions of the engineered railway need to perform at levels of integrity that are so high that an acceptable failure rate cannot be demonstrated through testing alone. Where such functions need to be implemented in complex programmable electronic systems certain design, build and test requirements are defined in technical standards and these are deemed to ensure that the correct level of systematic integrity is achieved. These approaches are based on assumptions around how system requirements are managed and delivered which are increasingly challenging to meet in practice. In particular the V&V lifecycle used in functional safety standards and emerging cyber security design standards is idealised. It assumes a top-down cascade of requirements for each delivery project. The approaches have become the de-facto standard internationally and are now mandated to an extent in European railway safety regulations. This paper proposes a different approach: a new lifecycle model that aligns better with the reality of the modern global supply chain and the order in which asset design and project delivery activities are actually undertaken to improve the ability to proactively manage safety.This leads to a fundamental change in the assurance philosophy to bring a simpler and more understandable approach. A framework for applying this approach is set out along with further research objectives to deliver the solution in practice.

Keywords

Railways, railway technology, RAMS, risk analysis, safety/safety engineering, safety-critical software, security, cyber security, safety assurance

Date received: 3 December 2021; accepted: 3 May 2022

https://journals.sagepub.com/doi/full/10.1177/09544097221102292

Thank you!

c.vangulijk@hud.ac.uk

www.irsc2022.com

EUROPEAN UNION AGENCY FOR RAILWAYS

AESF AGENCIA ESTATAL DE SEGURIDAD FERROVIARIA

adif