Safety Solutions Designer

CRISIS
NOV2024

Security for safety critical systems in the railways

Thierry Lecomte
R&D Director

« This presentation examines the foundational principles of railway safety, followed by an analysis of how emerging digital threats could compromise them»

THIERRY.LECOMTE@CLEARSY.COM

Art mostly generated with *ChatGPT or similar*

Common Thread

How the distribution of

safety critical functions

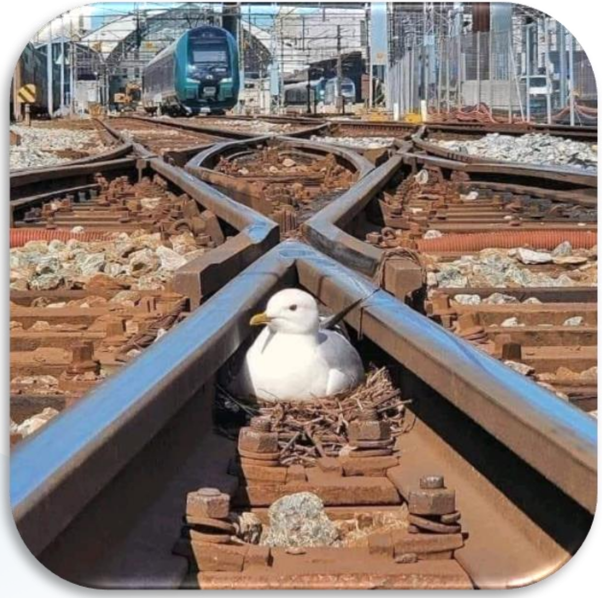
in the railway sector

creates security risks

that could lead to

disasters

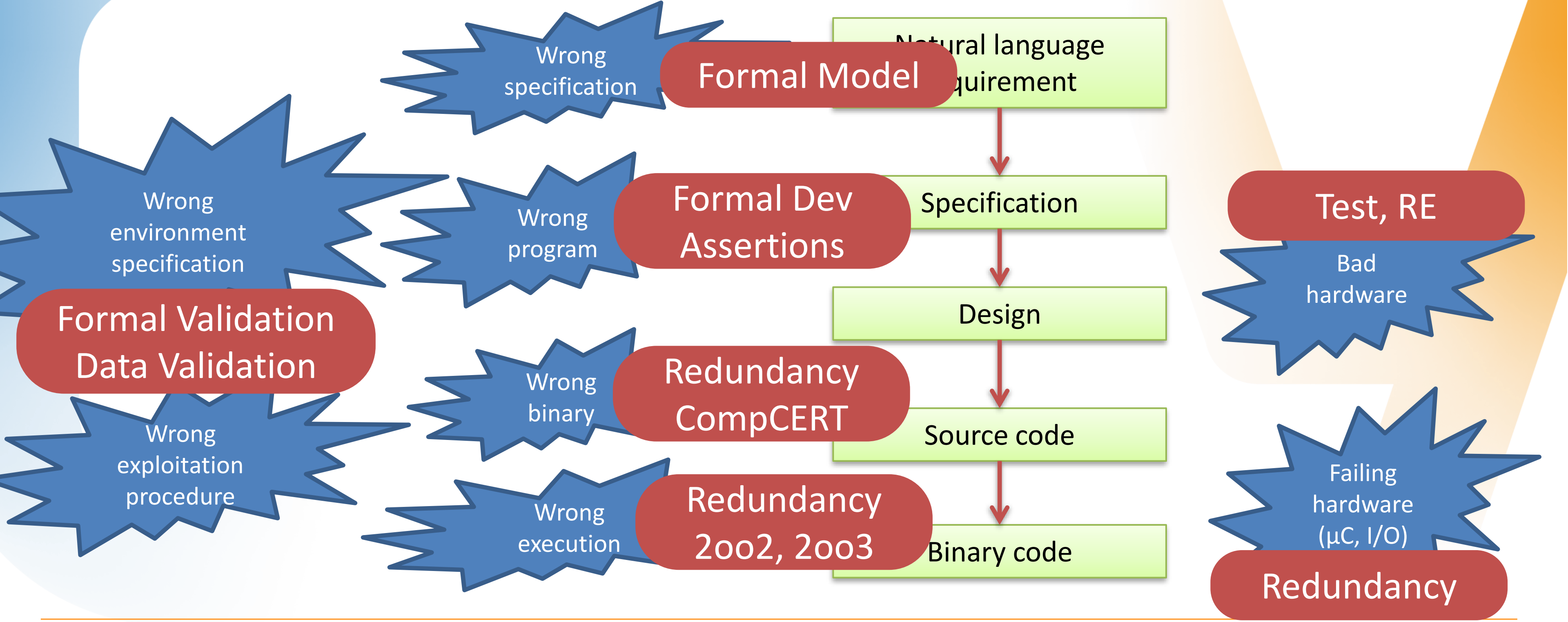
SAFETY



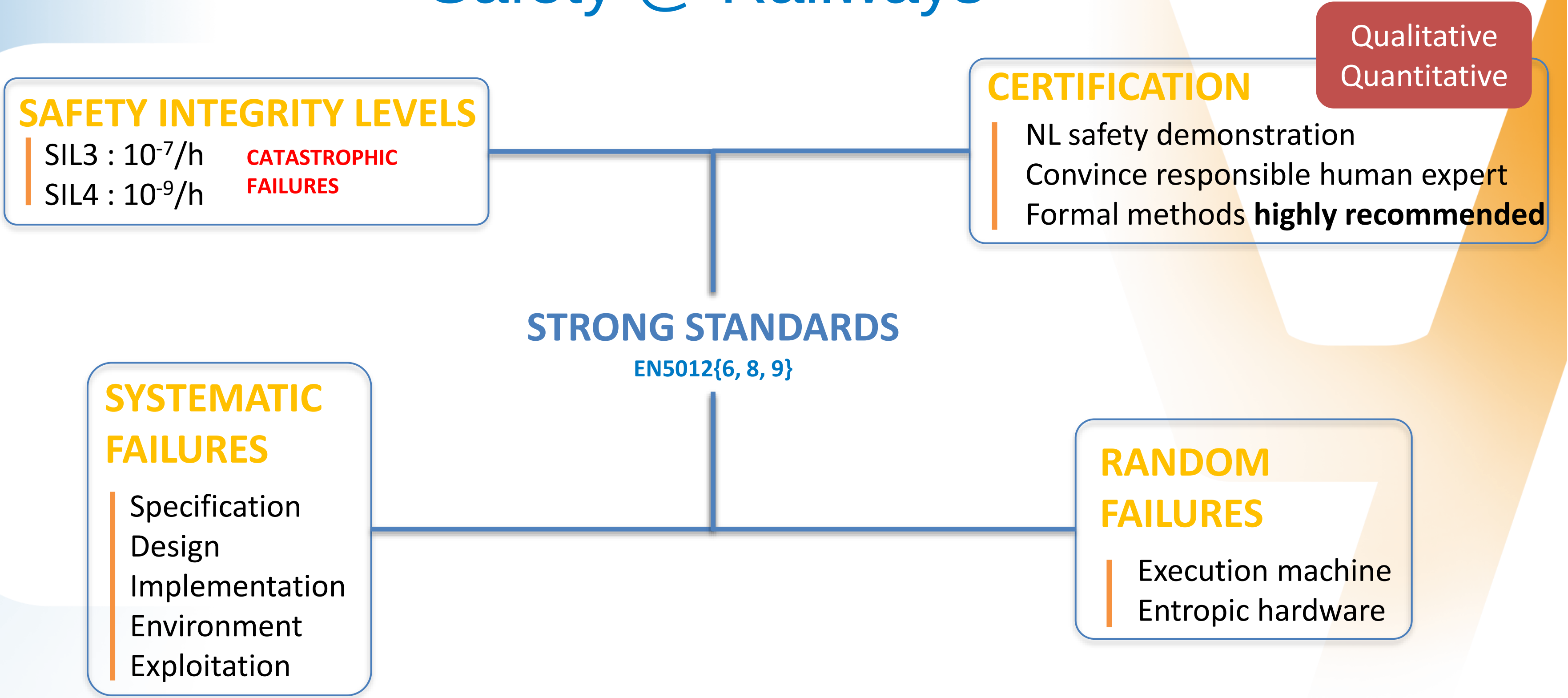
- Failing systems
- Safety critical
- Standards

Safety is about things that happen 1 in 1,000,000

Failing Software-Based Systems



Safety @ Railways



SAFETY INTEGRITY LEVELS

- SIL3 : 10^{-7}/h
- SIL4 : 10^{-9}/h

CATASTROPHIC FAILURES

CERTIFICATION

Qualitative
Quantitative

- NL safety demonstration
- Convince responsible human expert
- Formal methods **highly recommended**

STRONG STANDARDS

EN5012{6, 8, 9}

SYSTEMATIC FAILURES

- Specification
- Design
- Implementation
- Environment
- Exploitation

RANDOM FAILURES

- Execution machine
- Entropic hardware

Status (for automation)

- Perception-based behaviour (not in the Matrix)
  - Redundant sensors with different technos / from different providers
  - Moving 100x tons with up to 1000 passengers onboard
- Automatic metros worldwide
  - Simplified interactions => no « decision », no autonomy
  - Physical signals replaced by digital signalling
  - 10Bx passengers, no fatalities
- Autonomous trains
  - AutoHaul 2km mining train in the Australian bush (Rio Tinto)
  - Larger interfaces and more complex interactions
  - Replacing driver by computer and camera is still not enough for safety
- Accidents very often due to human error
  - Safe position == stop

PARADIGM SHIFT

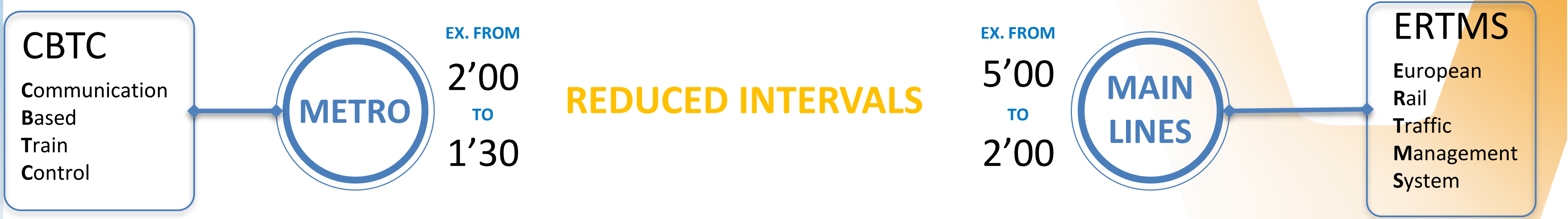
- Seeking performance
- Evolving railways
- Safe distance between trains
- Fixed and moving Bblocks

Seeking Performances

- Increased travel demand
  - Increasing urban population
  - Greener mobility
- Stations and tracks as fix points
  - Platforms, stations, tunnels, trains largely immutable
  - Replace Control Centers by distributed systems (ATO, ATP, ATS, ZC, etc.)

Evolving Railways

NEED FOR



CBTC

Communication
Based
Train
Control

METRO

EX. FROM

2’00

TO

1’30

REDUCED INTERVALS

EX. FROM

5’00

TO

2’00

MAIN LINES

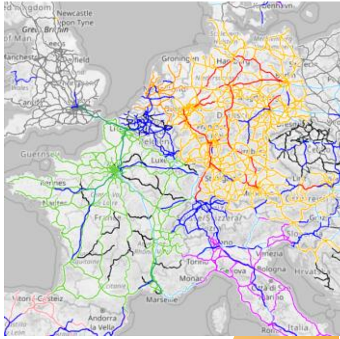
ERTMS

European
Rail
Traffic
Management
System

UP TO FULL AUTOMATION

MORE FLEXIBLE TRANSIT

Evolving Railways



NEED FOR

CBTC

Communication
Based
Train
Control

METRO

INTEROPERABILITY

MAIN LINES

ERTMS

European
Rail
Traffic
Management
System

UP TO FULL AUTOMATION
COMMON SPECIFICATION IN SOME CASES
RADIO BASED COMMUNICATION
DIGITAL SIGNALLING

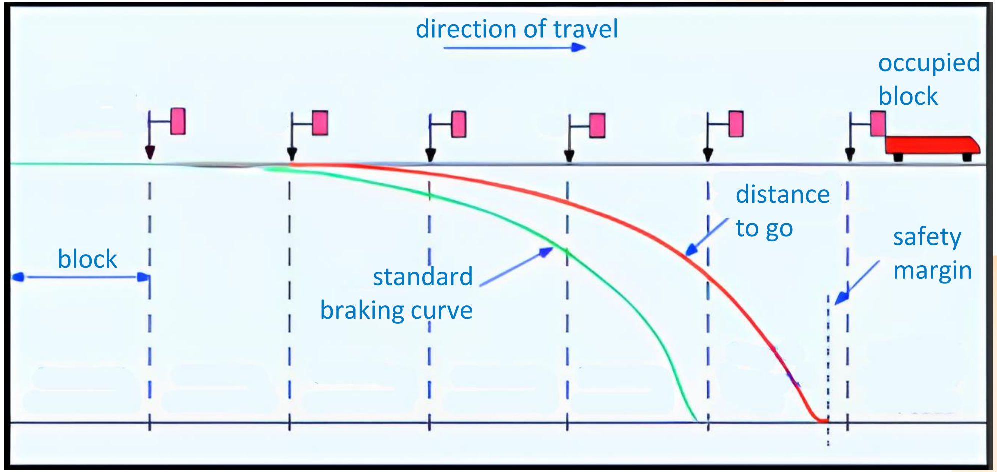
MORE FLEXIBLE TRANSIT
UNIQUE SIGNALLING SYSTEM
RADIO BASED COMMUNICATION
DIGITAL SIGNALLING
GNSS

Many DoF for Train Manufacturers

https://www.era.europa.eu/system/files/2023-09/index094_-_FRMCS_SRS_%28AT-7800%29_v100.pdf

Safe Distance Between Trains

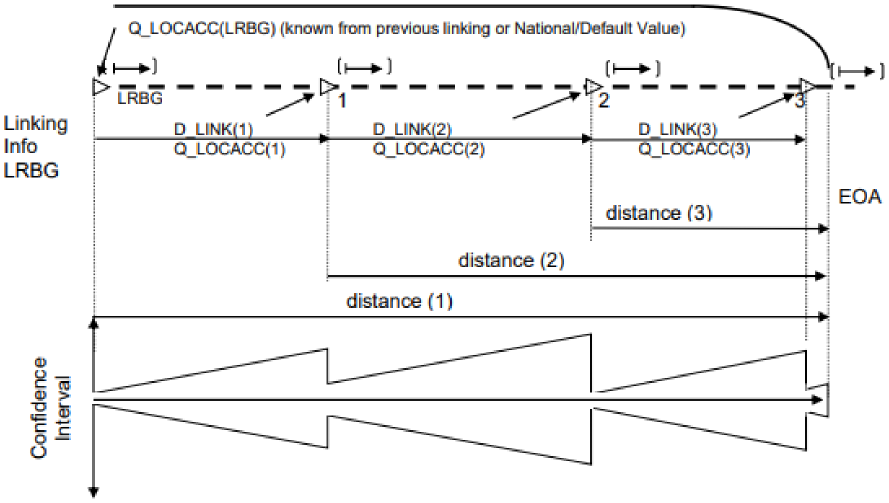
- ▶ No collision
- ▶ No overspeed
- ▶ No derailment



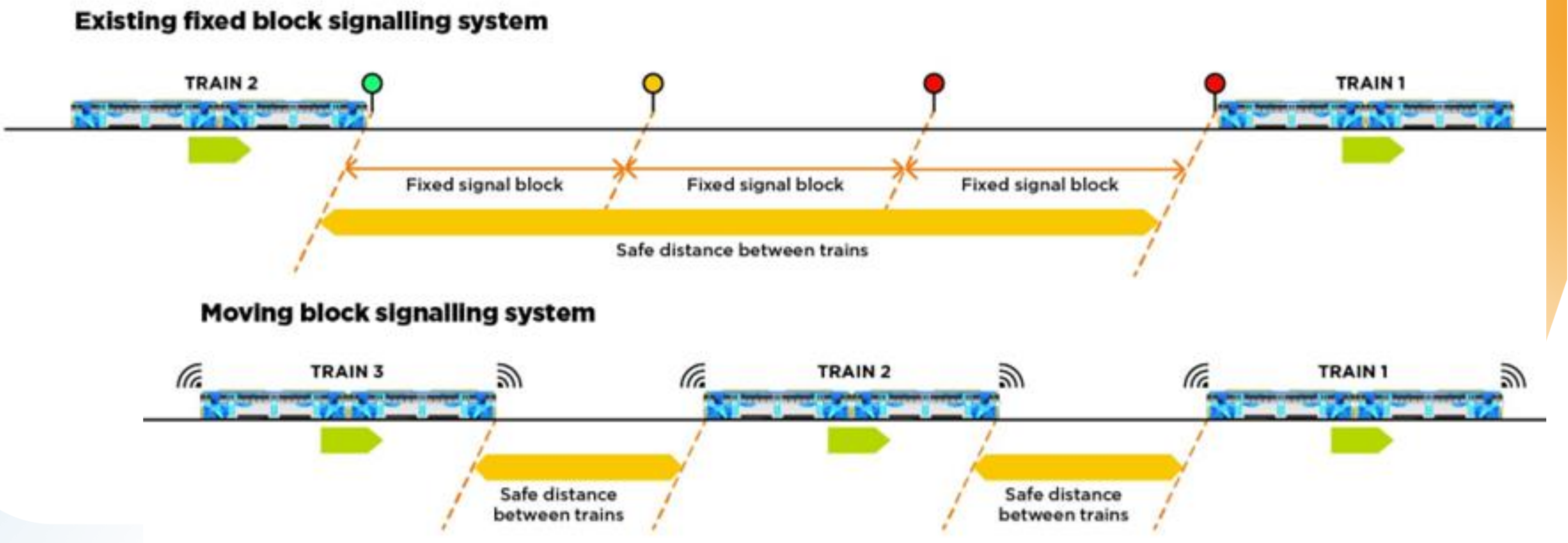
Braking curves

Train Localization !?

- Train position is not known precisely
  - Cumulative error with odometer (slipping, sliding)
  - Beacons on the ground to indicate position
- GNNS info unable to descriminate two parallels tracks



From Fixed to Moving Block

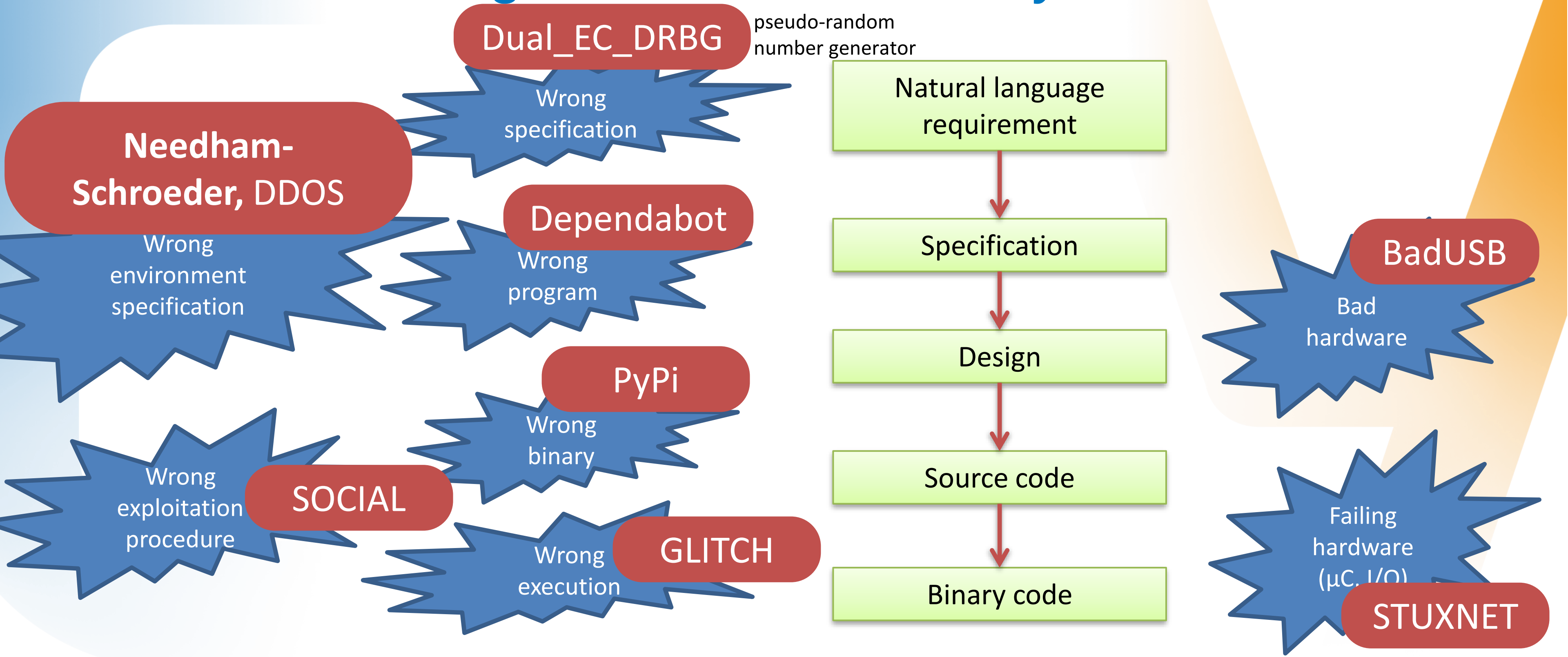

Existing fixed block signalling system
TRAIN 2
TRAIN 1
Fixed signal block
Fixed signal block
Fixed signal block
Safe distance between trains
Moving block signalling system
TRAIN 3
TRAIN 2
TRAIN 1
Safe distance between trains
Safe distance between trains

Courtesy: METROTUNNEL

SECURITY

- Failing systems
- Railways’ nightmare
- Standards
- It happens

Failing Software-Based Systems



Natural language requirement

Specification

Design

Source code

Binary code

Dual_EC_DRBG

pseudo-random number generator

Wrong specification

Needham-Schroeder, DDOS

Wrong environment specification

Dependabot

Wrong program

PyPi

Wrong binary

Wrong exploitation procedure

SOCIAL

Wrong execution

GLITCH

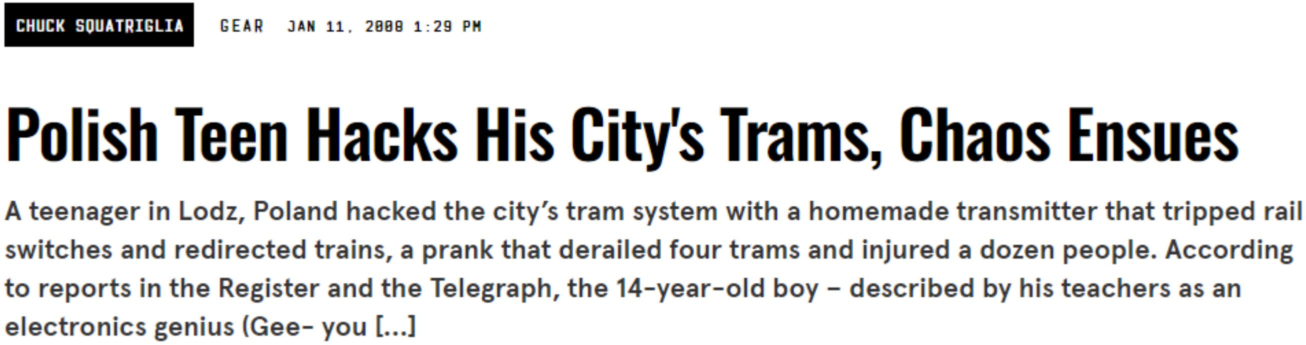
BadUSB

Bad hardware

Failing hardware (µC, I/O)

STUXNET

Railways’ Nightmare: Altering State of Signalling



CHUCK SQUATRIGLIA GEAR JAN 11, 2008 1:29 PM

Polish Teen Hacks His City's Trams, Chaos Ensues

A teenager in Lodz, Poland hacked the city’s tram system with a homemade transmitter that tripped rail switches and redirected trains, a prank that derailed four trams and injured a dozen people. According to reports in the Register and the Telegraph, the 14-year-old boy – described by his teachers as an electronics genius (Gee- you [...]

Source: https://www.wired.com/2008/01/polish-teen-hac/

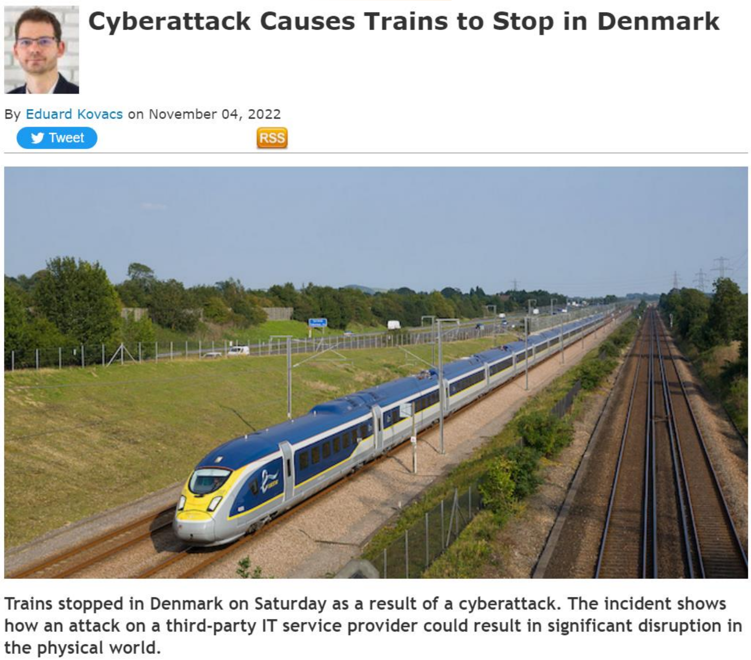
Standards for Secure Critical Systems

- ▶ Domain-specific standards ((very) recent)
- ▶ Recommandations (REX, best practices)
  - ▷ No definitive recipe to produce secure systems
  - ▷ Cover SW, HW and development process
- ▶ Security problem
  - ▷ Security target, threat model, protection profile
  - ▷ Quality & correct development required
  - ▷ **Security by-design !**

- CLC/TS 50701: railways
- IEC 62433: industry
- CC/CSPN: µelectronics

It happens

- Railway infrastructure under attack
  - Threats: safety, availability
- Huge surface of attack
- **State-level attackers**
- Heterogeneous equipement installed for decades
- PLCs not fit for security

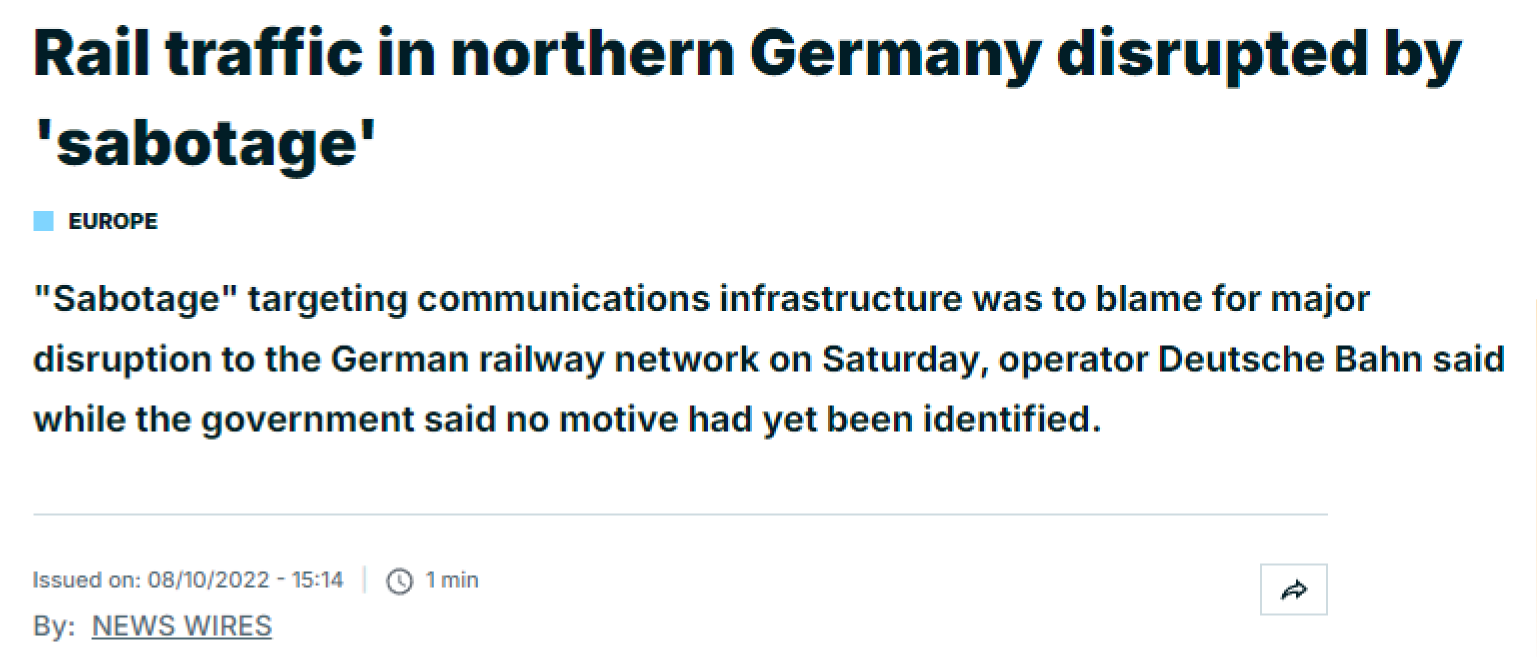


Cyberattack Causes Trains to Stop in Denmark

By Eduard Kovacs on November 04, 2022

Trains stopped in Denmark on Saturday as a result of a cyberattack. The incident shows how an attack on a third-party IT service provider could result in significant disruption in the physical world.

It happens – still no safety issue



Rail traffic in northern Germany disrupted by 'sabotage'

EUROPE

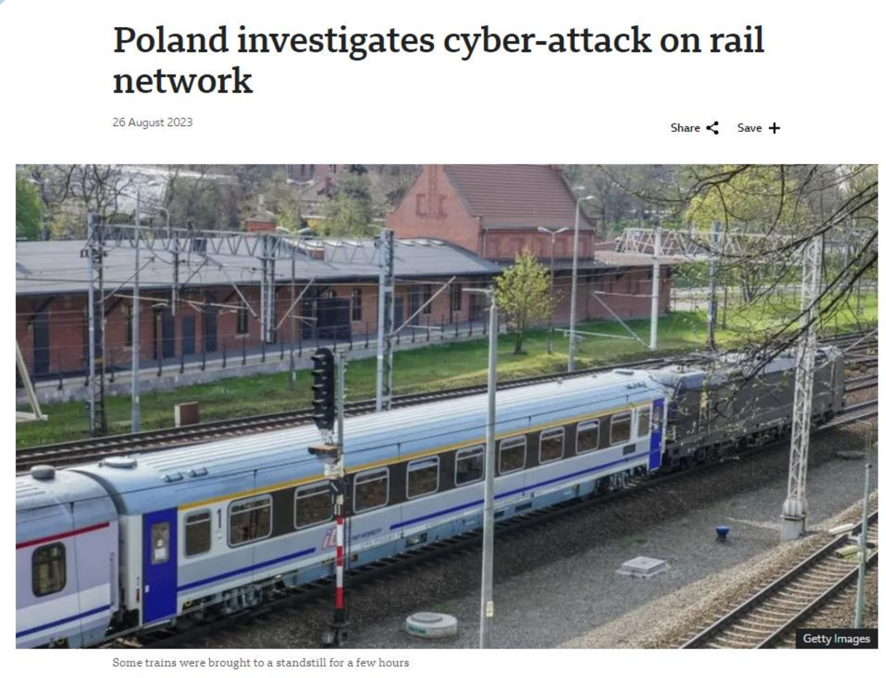
"Sabotage" targeting communications infrastructure was to blame for major disruption to the German railway network on Saturday, operator Deutsche Bahn said while the government said no motive had yet been identified.

Issued on: 08/10/2022 - 15:14 | 1 min

By: NEWS WIRES

Source: https://www.france24.com/en/europe/20221008-rail-traffic-in-northern-germany-disrupted-by-sabotage

It happens – still no safety issue



Poland investigates cyber-attack on rail network

26 August 2023

Share Save +

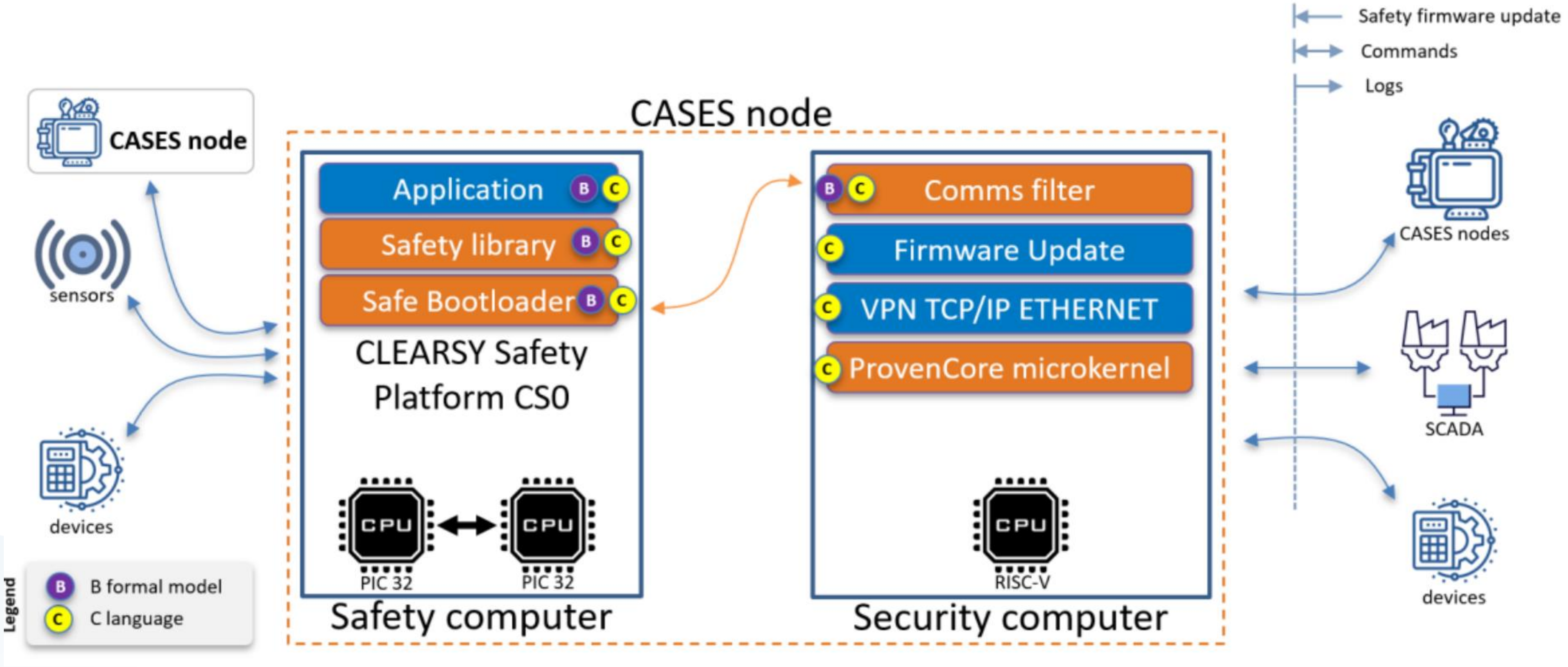
Getty Images

Some trains were brought to a standstill for a few hours

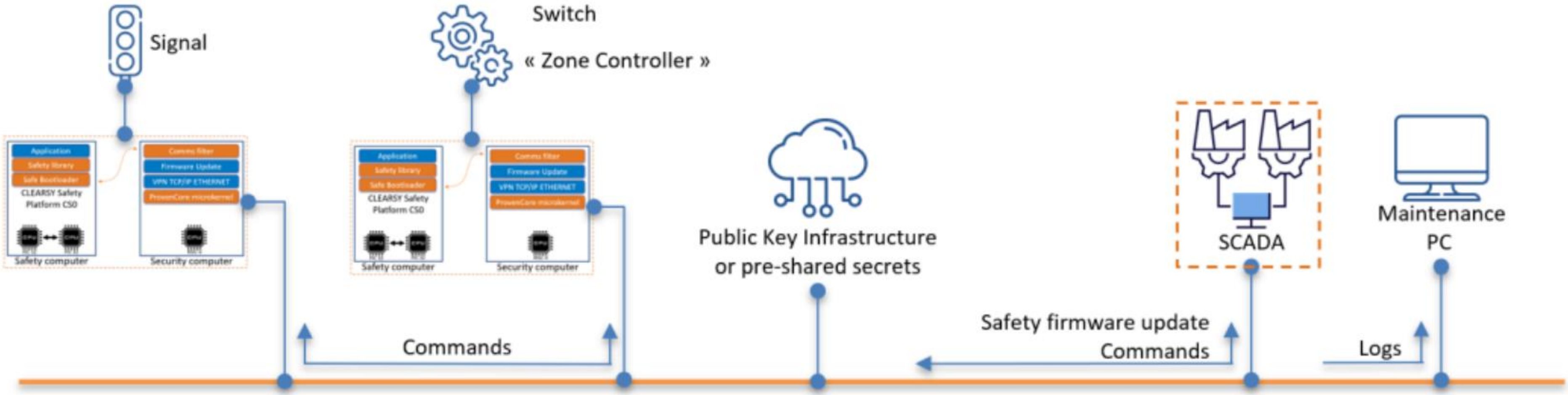
Source: https://www.bbc.com/news/world-europe-66630260

- Hackers broke into railway frequencies to disrupt traffic
- Signals interspersed with recording of Russia's national anthem and a speech by President Vladimir Putin
- 20 trains brought to a standstill for hours

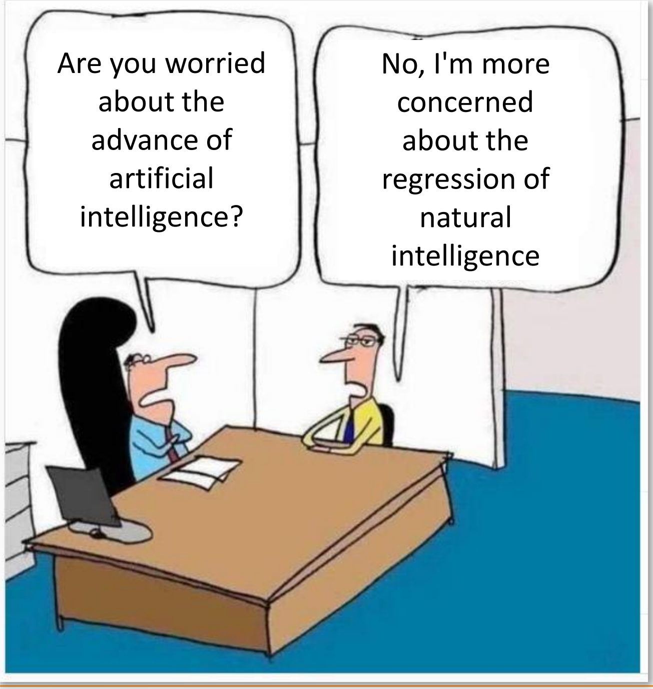
Wired Equipements on the Tracks



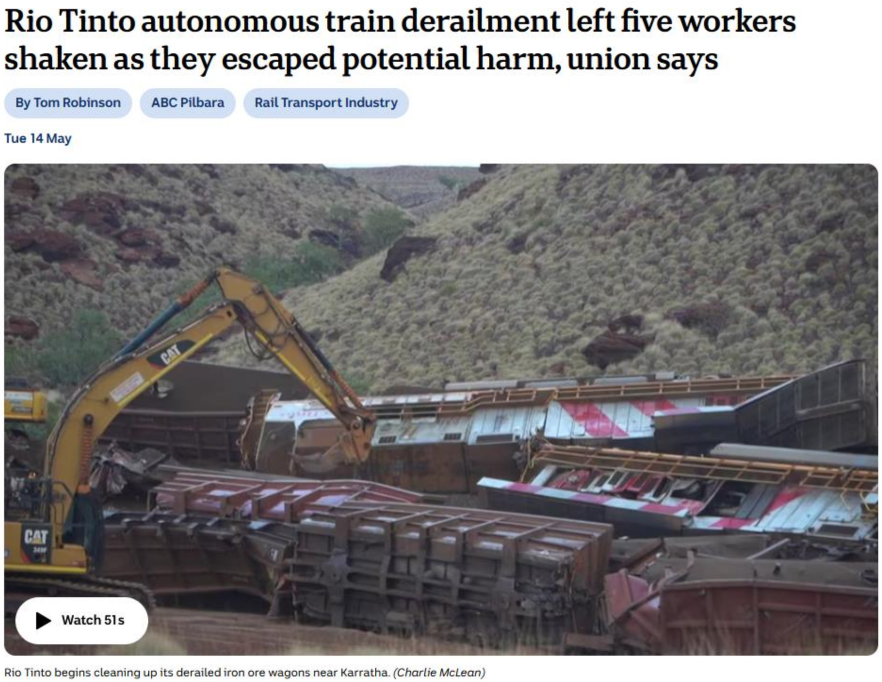
Wired Equipements on the Tracks



ARTIFICIAL INTELLIGENCE


Are you worried about the advance of artificial intelligence?
No, I'm more concerned about the regression of natural intelligence

AUTONOMOUS MOBILITY



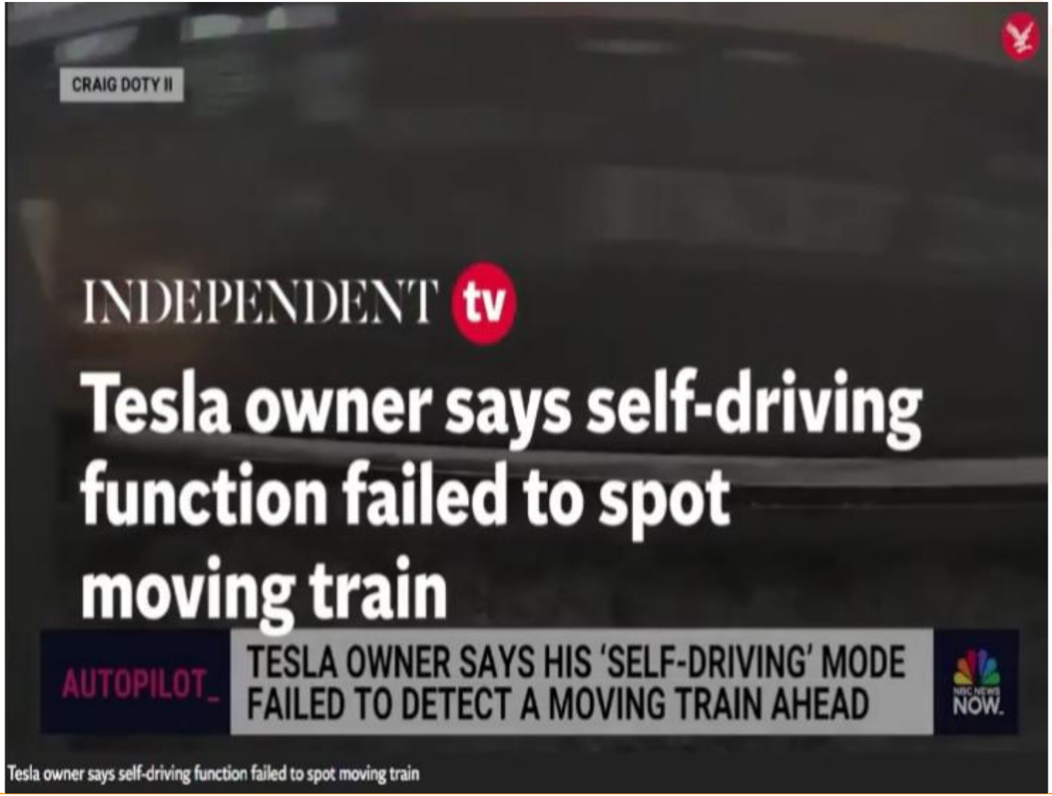
Rio Tinto autonomous train derailment left five workers shaken as they escaped potential harm, union says

By Tom Robinson · ABC Pilbara · Rail Transport Industry

Tue 14 May

Rio Tinto begins cleaning up its derailed iron ore wagons near Karratha. *(Charlie McLean)*

Train vs Autonomous Car



Tesla owner says self-driving function failed to spot moving train

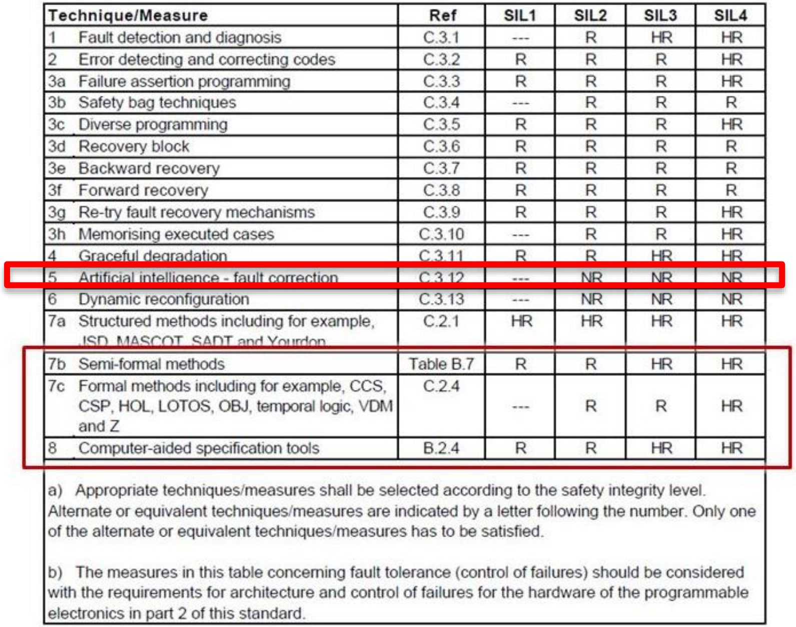
TESLA OWNER SAYS HIS 'SELF-DRIVING' MODE FAILED TO DETECT A MOVING TRAIN AHEAD

Tesla owner says self-driving function failed to spot moving train

Standards for Safety Critical Systems

- ▶ Combination of techniques
  - ▷ Recommanded, Highly recommended
  - ▷ AI not recommended (read as « not accepted ») by default

IEC 61508: Software design and dev. (table A.2)



Technique/Measure		Ref	SIL1	SIL2	SIL3	SIL4
1	Fault detection and diagnosis	C.3.1	---	R	HR	HR
2	Error detecting and correcting codes	C.3.2	R	R	R	HR
3a	Failure assertion programming	C.3.3	R	R	R	HR
3b	Safety bag techniques	C.3.4	---	R	R	R
3c	Diverse programming	C.3.5	R	R	R	HR
3d	Recovery block	C.3.6	R	R	R	R
3e	Backward recovery	C.3.7	R	R	R	R
3f	Forward recovery	C.3.8	R	R	R	R
3g	Re-try fault recovery mechanisms	C.3.9	R	R	R	HR
3h	Memorising executed cases	C.3.10	---	R	R	HR
4	Graceful degradation	C.3.11	R	R	HR	HR
5	Artificial intelligence - fault correction	C.3.12	---	NR	NR	NR
6	Dynamic reconfiguration	C.3.13	---	NR	NR	NR
7a	Structured methods including for example, JSD, MASCOT, SADT and Yourdon	C.2.1	HR	HR	HR	HR
7b	Semi-formal methods	Table B.7	R	R	HR	HR
7c	Formal methods including for example, CCS, CSP, HOL, LOTOS, OBJ, temporal logic, VDM and Z	C.2.4	---	R	R	HR
8	Computer-aided specification tools	B.2.4	R	R	HR	HR

a) Appropriate techniques/measures shall be selected according to the safety integrity level. Alternate or equivalent techniques/measures are indicated by a letter following the number. Only one of the alternate or equivalent techniques/measures has to be satisfied.

b) The measures in this table concerning fault tolerance (control of failures) should be considered with the requirements for architecture and control of failures for the hardware of the programmable electronics in part 2 of this standard.

AI for Autonomous Trains

- Several European demonstrating projects
- In France,
  - 3 SNCF projects for high speed, regional, and freight trains
  - Several projects for low-traffic, regional lines
- Various safety problems
  - 3 km to stop a TGV at 320 km/h – dangers outside camera view
  - Low speed, 1 train / line, limited risks on low traffic lines

AI & Cybersecurity for Certified Trains

- UIC has started a 3-year project « New Methods for Safety Demonstration » (2022-2025)
  - Usual safety assessment methods are no longer fully adequate
  - Safety demonstrations based on introducing limited innovations into already accepted designs
  - New methods must be found to effectively assess the safety of systems (ex: decentralised computing, AI, sensor fusion, deep learning, and intelligent sensing)
  - Goal: examine, nominate and select potential methods for conducting safety demonstrations in a context of rapidly evolving technologies.
  - Deliverable: TS that could become Standard

Conclusion

- What is the current status?
  - Heterogenous legacy components lasting decades
  - Domain with lot of inertia: ERTMS currently based on 2G (“soon” on 5G)
  - Huge safety culture and experience, lots of engineering
  - Lack of security culture
  - Large surface of attack: 2G/5G, Wifi onboard, wired technical networks
  - Impact only on availability (at the moment)
- What perspective ?
  - Requires security-aware decision makers and practitioners (BT and RT)
  - “New Methods for Safety Demonstration” project to propose TS for certification of AI and Cybersecurity safety features

CLEARSY
Safety Solutions Designer

CRISIS
NOV2024

AIX
LYON
PARIS
STRASBOURG

WWW.CLEARSY.COM

Thank you
for your attention

https://mooc.imd.ufrn.br/

MOOC
massive open
online course

THIERRY.LECOMTE@CLEARSY.COM