Challenges and Research directions in Securing the Connected Rail infrastructure

Ritesh Kumar Kalle, Ph.D.
Hitachi India R&D Centre

Date
17 May 2025

Hitachi India R&D Center

Highly talented researchers working on cutting edge technologies like Cybersecurity, AI to invent the future

Agenda

1 — Expanding attack surface in connected rail infrastructure

2 — IoT/OT threats and risks

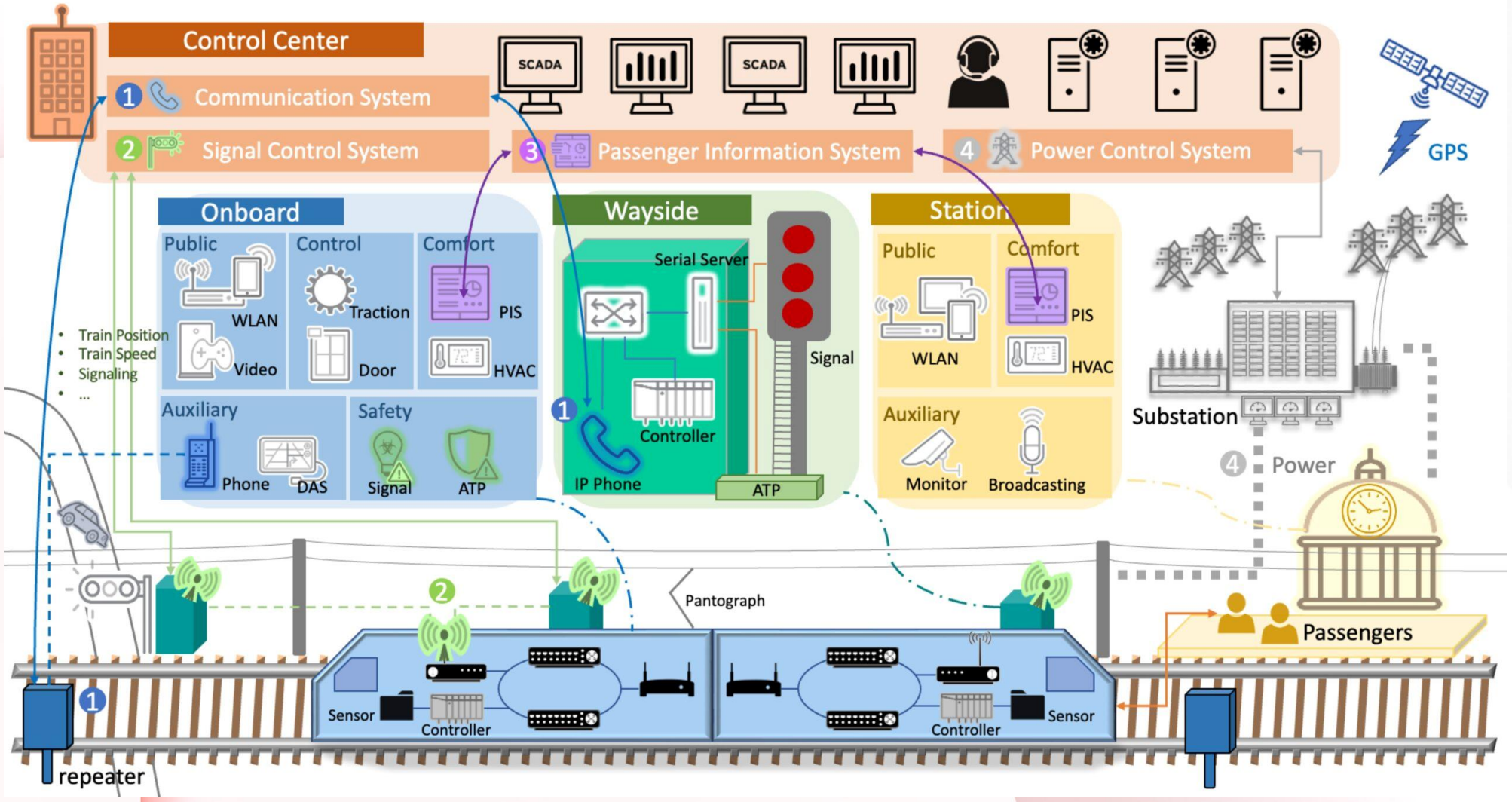
3 — Emerging trends and R&D opportunities

Chapter 1

Expanding attack surface in connected rail infrastructure

HITACHI

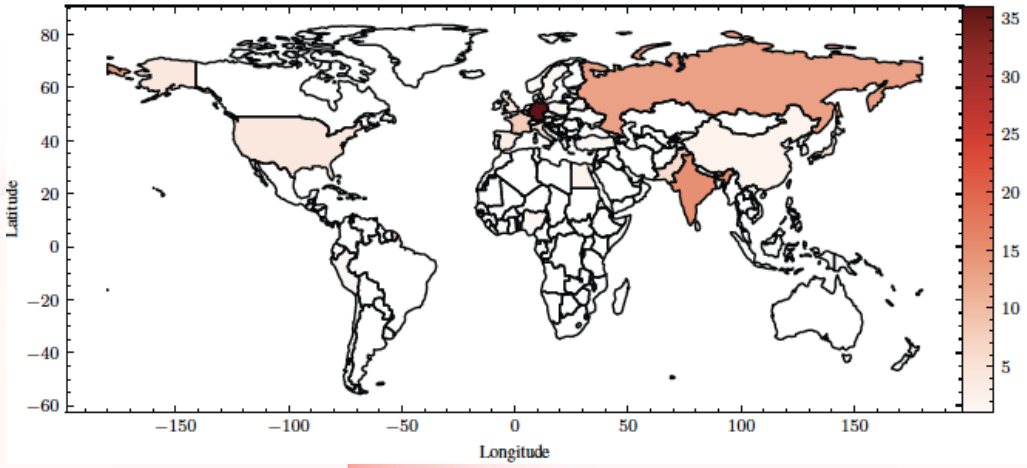
Modern rail is a highly complex cyber physical system. Every sub-system is a possible attack surface



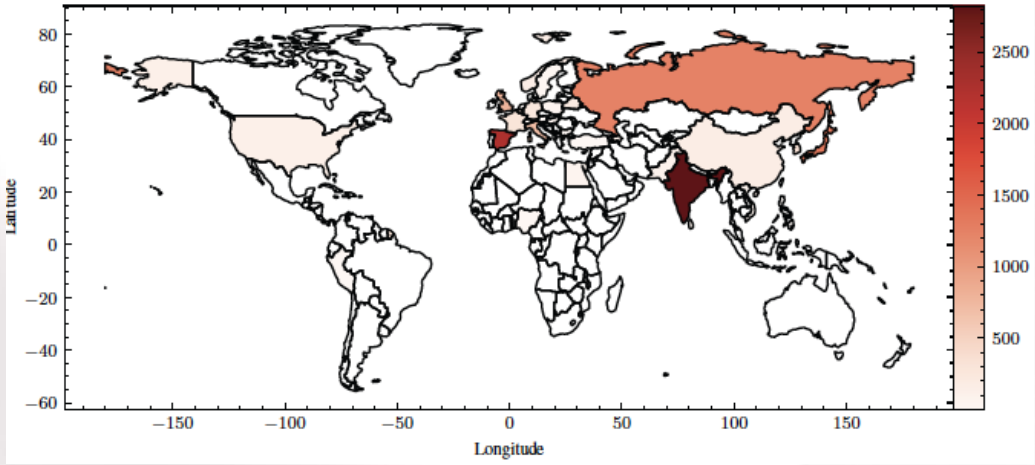
Ref: https://www.txone.com/blog/potential-threats-to-railway-industry/

HITACHI

Cyber attacks are an extension of the physical attacks on rail infrastructure



No. of attacks per country since the invention of railways



No. of casualties per country since the invention of railways

Ref: https://www.american-cse.org/csce2023-ieee/pdfs/CSCE2023-5LlpKs7cpb4k2UysbLCuOx/275900c419/275900c419.pdf

BLOGS › UNFETTERED BLOG

Cyber-related rail incidents have killed more than 490 people

Examples of catastrophic control system rail cyber incidents included the Big Bayou Canot rail accident. This was caused by displacement of a span and deformation of the rails when a tow of heavy barges collided with the rail bridge. The collision forced the unsecured end of the bridge span approximately three feet out of alignment and severely kinked the track. The track circuit controlling the bridge approach block signals remained closed (intact), and the nearest signal continued to display a clear (green) signal as the rail was not broken. 47 people were killed and 103 more were injured.

Ref: https://www.controlglobal.com/blogs/unfettered/blog/33015054/cyber-related-rail-incidents-have-killed-more-than-490-people

HITACHI

Recent attacks target digital railway infrastructure

Radio Stop signal over VHF 150 MHz in Poland

Polish intelligence services are investigating a hacking attack on the country's railways, Polish media say.

Hackers broke into railway frequencies to disrupt traffic in the north-west of the country overnight, the Polish Press Agency (PAP) reported on Saturday.

The signals were interspersed with recording of Russia's national anthem and a speech by President Vladimir Putin, the report says.

Poland is a major transit hub for Western weapons being sent to Ukraine.

Saturday's incident occurred when hackers transmitted a signal that triggered an emergency stoppage of trains near the city of Szczecin, PAP reported.

About 20 trains were brought to a standstill, but services were restored within hours.

Stanislaw Zaryn, a senior security official, said Poland's internal security service ABW was investigating. "For the moment, we are ruling nothing out," he told PAP.

Mysterious breakdowns due to controller logic in Poland

Coordinate pairs define the workshop areas. A condition has been written in the computer code to disable the ability to run a train if it spends at least 10 days in one of these workshops. One of the workshops belongs to Newag itself – but a different logical condition was defined for its coordinates, presumably for testing purposes.

Other surprises were soon discovered. Among them was the blocking of a train when one of its components is replaced (verified by its serial number). An option to undo the lockout was also discovered – this did not require setting flags at computer memory level, just the right sequence of button clicks in the cab and on the on-board computer screen. When news of the successful launch of the Impulse hit the media, the trains received a software update that removed this 'fix' option. On another train, a code was found instructing it to 'break down' after a million kilometres.

Disabling Automatic Train Control System in Belarus

First, the group conducts cyberattacks on the Belarusian and Russian regimes. They have undertaken several notable operations, including a successful campaign against the Belarusian Railways. This cyber operation began in December 2020 and continued with a second attack on January 23, 2021. The goal was to disrupt the work of freight trains, thereby indirectly impacting the Russian transportation of troops, weapons, and other equipment to the Ukrainian border. Following the escalation of the Russian-Ukrainian conflict, the Cyber Partisans executed additional attacks on February 26, 2022, and March 2, 2022. These attacks disabled the Automatic Train Control system, which is responsible for guiding trains and managing railway infrastructure. This disrupted Russian military train movements in Belarus for approximately two weeks.

Russian attack on Czech Signaling systems

Russia has made "thousands" of attempts to interfere with European rail networks in a campaign to destabilise the EU and sabotage critical infrastructure, the Czech Republic's transport minister has said.

Martin Kupka told the Financial Times Moscow was suspected of having made "thousands of attempts to weaken our systems" since Russian President Vladimir Putin ordered the full-scale invasion of Ukraine in February 2022.

The hacking campaign included attacks on signalling systems and on the networks of the Czech national railway operator České dráhy, Kupka said. Past attacks have put ticketing systems out of service and raised concerns about successful interference with signals causing serious accidents.

Arson attacks to destroy cabling boxes in France

What happened on Friday?

SNCF said three arson attacks overnight had destroyed cabling boxes at strategic junctions on the rail network.

Traffic on the high-speed line between Lille and Paris was stopped after "a malicious act in the Arras area."

On the route between Paris and eastern France, the company said vandalism between Metz and Nancy was seriously disrupting traffic.

Traffic was also cut on the Atlantic line, after sabotage where the tracks divide for Brittany and southwestern France.

Attempts to sabotage the southeastern line from Paris were thwarted.

"Following this massive attack aimed at paralyzing the high-speed line network, a large number of trains were diverted or canceled," SNCF tweeted earlier in the day.

The operator added that the situation would last "at least all weekend while repairs are conducted."

Chapter 2

IoT/OT threats and risks

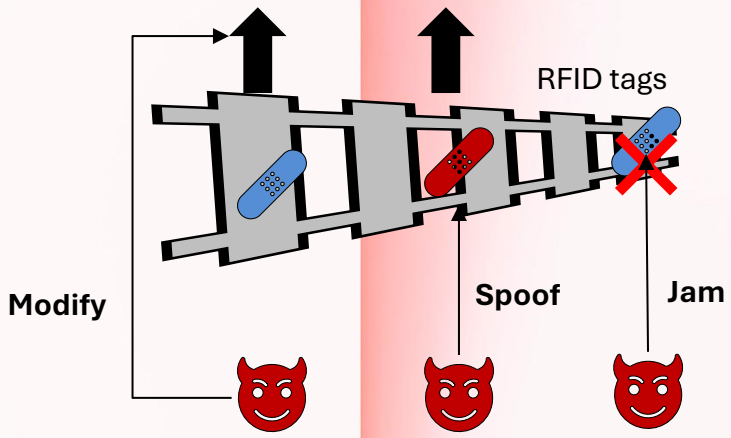
IoT/OT threats and risks

Train control system can be moved to unsafe states

Delhi Metro ATO Trial incident in 2017

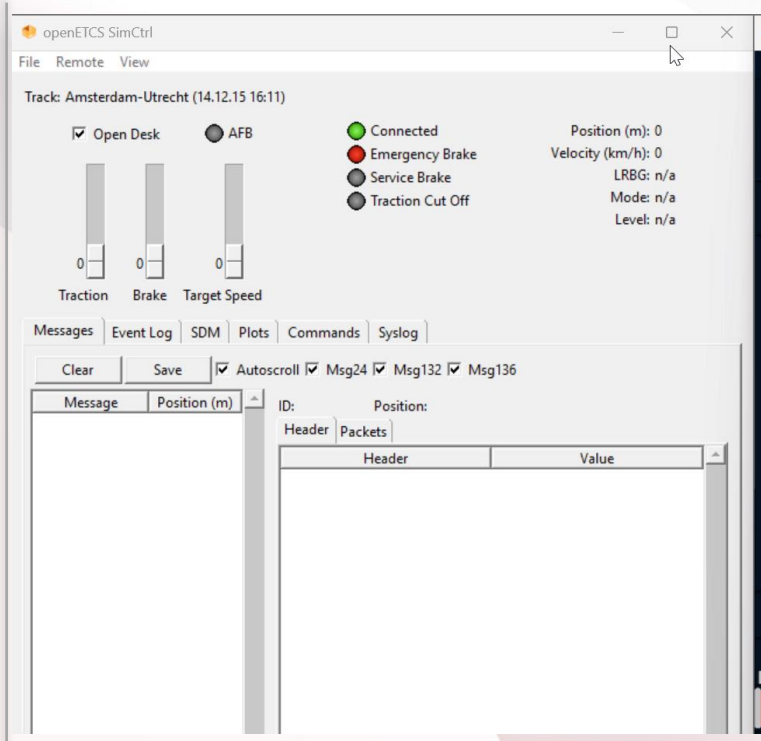
Erroneous track data to calculate movement authority can lead to accidents!

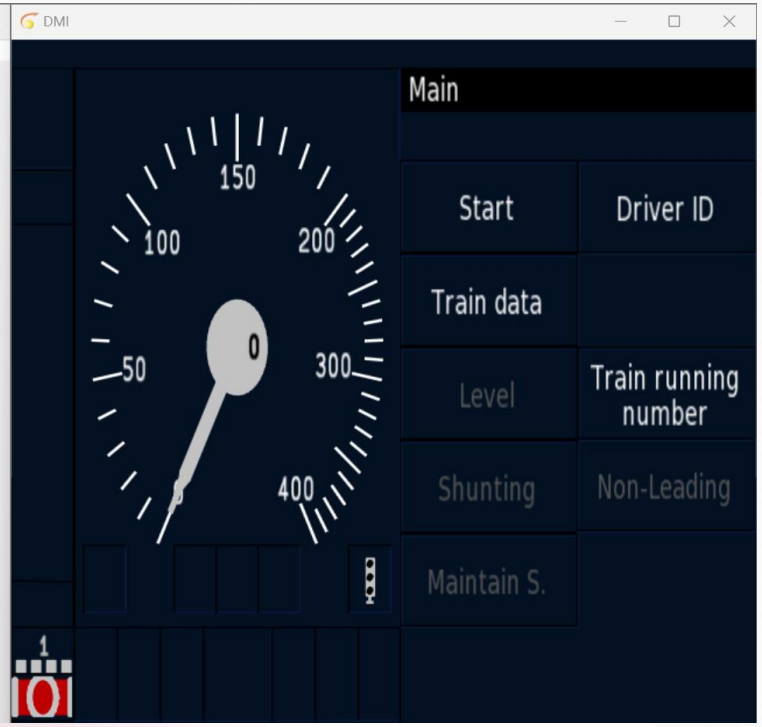
Malicious RFID data
- Can imply wrong movement authority
- Can lead to fatalities



Physical threat

- Eurobalise has been repeatedly shown to be a very viable threat vector [1,2]
- Same can apply for RFID tags



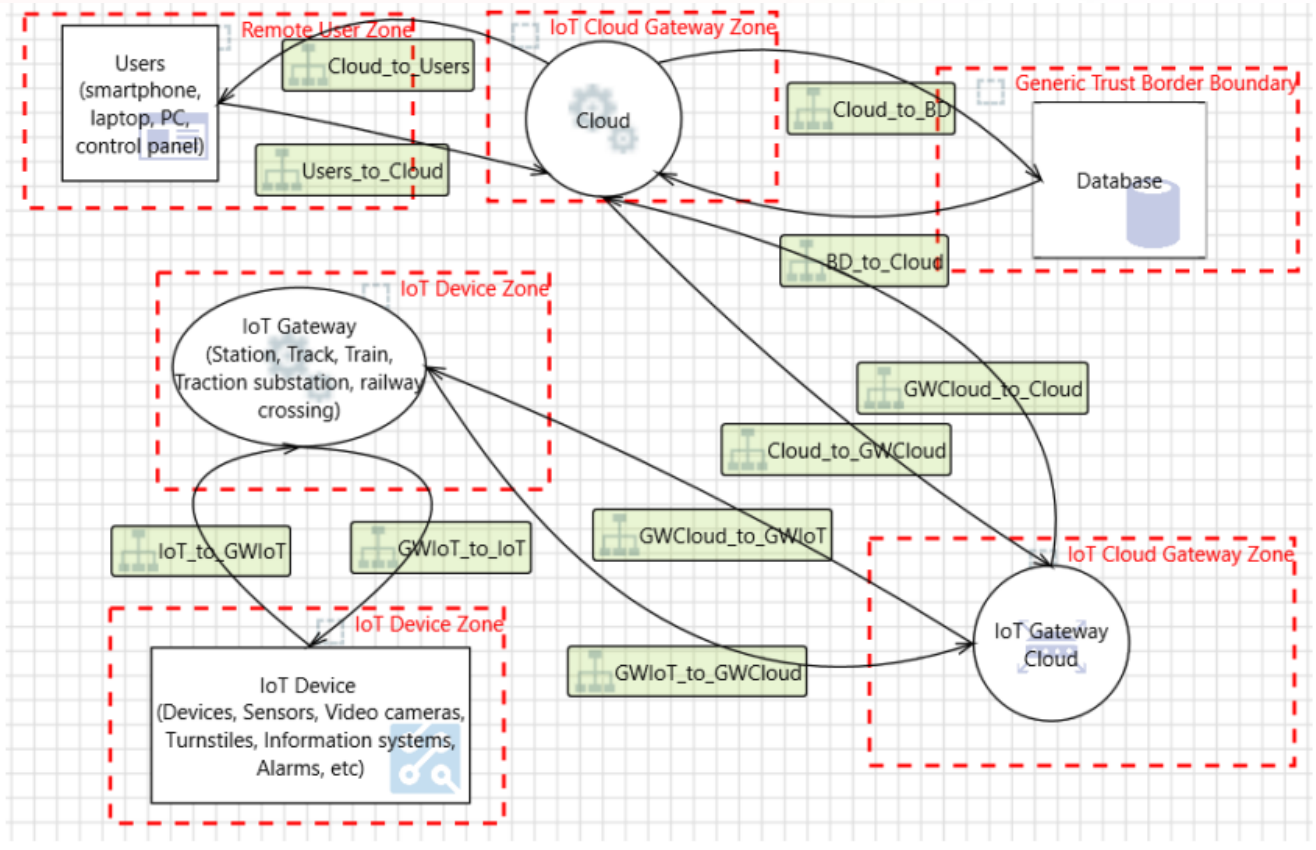


openETCS is designed to meet the requirements for Safety Integrity Level 4 (SIL 4) according to the EN 50128 standard

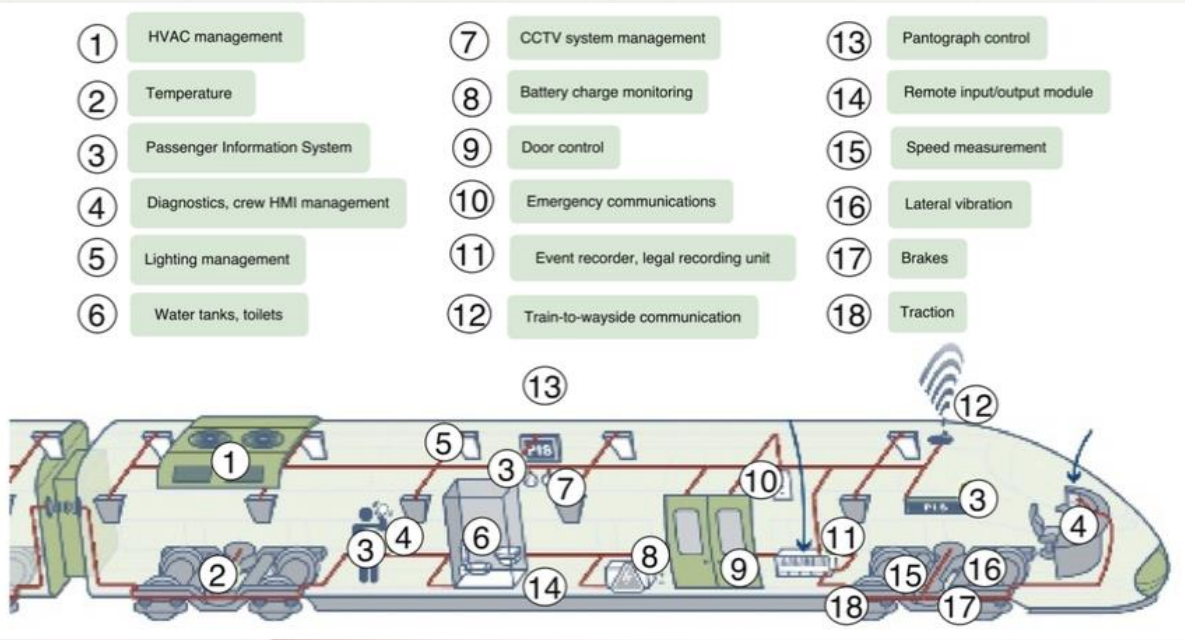
[1] S. Soderi, D. Masti, M. Hämäläinen, and J. Iinatti, "Cybersecurity Considerations for Communication Based Train Control," *IEEE Access*, vol. 11, pp. 92312–92321, 2023, doi: 10.1109/ACCESS.2023.3309005.
[2] "How secure is ERTMS.pdf," Accessed: Jun. 13, 2024. [Online]. Available: https://openaccess.city.ac.uk/id/eprint/1522/1/How%20secure%20is%20ERTMS.pdf

IoT Threat modeling applied to trains

All interfaces between untrusted zones are subject to threats



Example systems monitored or controlled using IoT in trains



https://tst.duit.in.ua/index.php/tst/article/view/397

https://www.mdpi.com/1424-8220/17/6/1457

With Great Power comes Great Responsibility

Ministry of Railways

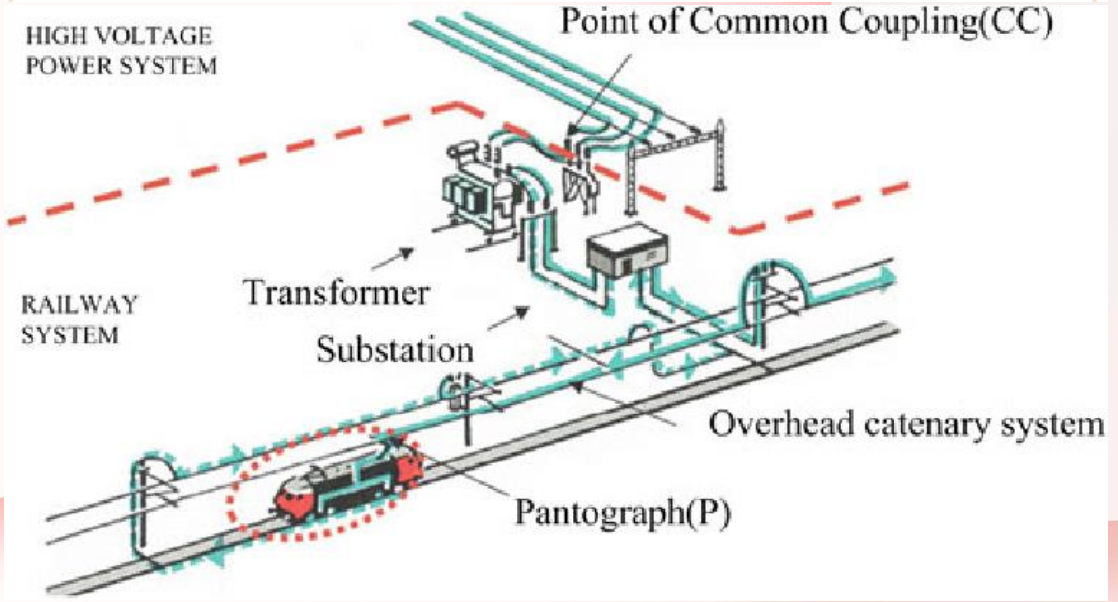
Azadi Ka Amrit Mahotsav

Railway Electrification Gains Momentum: 100% Network Electrified in 22 out of 29 States/UT, Work Progressing Rapidly in the Remaining 7 States

136 Crore Liters Reduction in Traction Fuel Consumption from 2018-19 to 2023-24

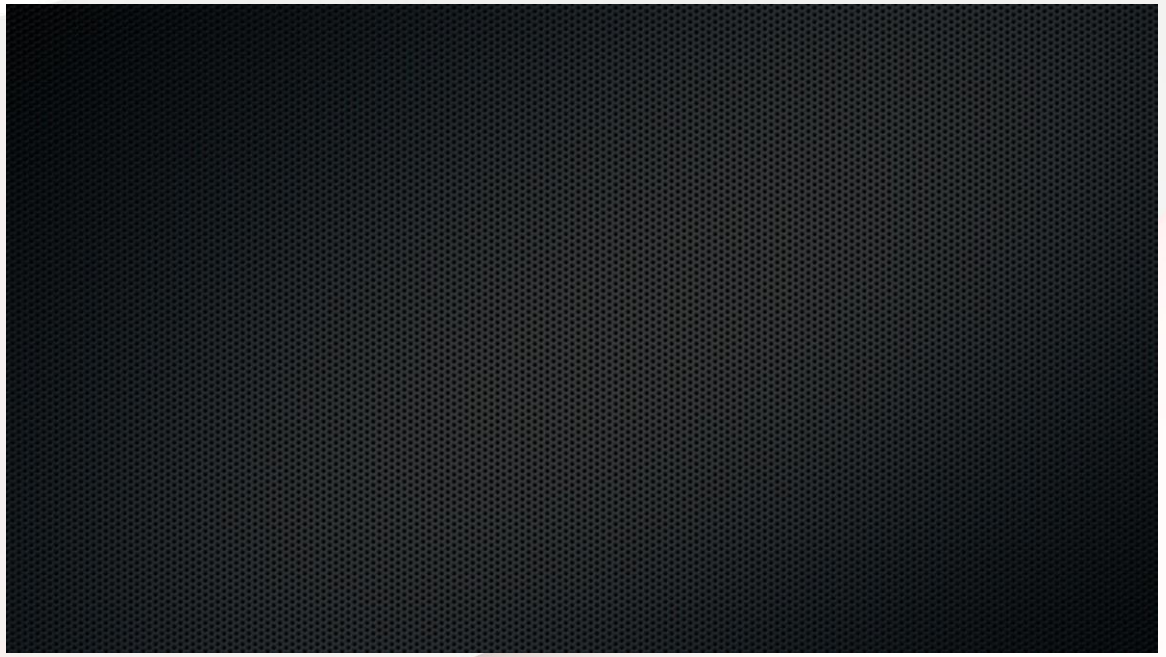
Posted On: 26 MAR 2025 8:13PM by PIB Delhi

Currently, about 98% of the Indian Railways' (IR) Broad Gauge (BG) network has been electrified and balance sections have been taken up. Significant progress has been made in railway electrification in recent years, a comparison of electrification before and after 2014 is as follows:



[11]Ref: https://link.springer.com/chapter/10.1007/978-981-13-6589-8_1

Demonstration



CVE – 2023-2625. CVSS 8 (NIST). CVSS 9 (Hitachi Energy)
URL: https://nvd.nist.gov/vuln/detail/CVE-2023-2625

HITACHI

Chapter 3

Emerging trends and R&D opportunities

Regulatory guidance to industry

Department for Transport

Rail Cyber Security
Guidance to Industry

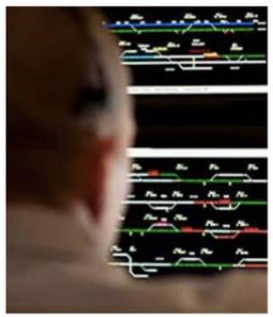
Top 10. Whichever development approach is chosen, it is important you ensure that the following key areas are included:

- threat modelling / architectural risk analysis
- attack surface reduction[3]
- 'fuzz' testing[4]
- static analysis[5]

ASSOCIATION OF AMERICAN RAILROADS (AAR)

Rail Information Security Committee

Cyber Security Effective Practices for Information Technology Procurements



Provide a Quality Assurance program and validate that the software and firmware of the procured product have undergone Quality Control testing to identify and correct potential cybersecurity weaknesses and vulnerabilities. This testing shall include fuzz testing, static testing, dynamic testing, and penetration testing. Use positive and appropriate negative tests to verify that the procured product operates in accordance with requirements and without extra functionality, as well as monitor for unexpected or undesirable behavior during these tests. This testing may be done by the Supplier or an independent entity. Provide summary documentation of the results of the testing that includes unresolved vulnerabilities and recommended mitigation measures.

Iterative automated threat modeling using LLM

LLM PROMPT BASED THREAT MODELING INTERFACE

RI You

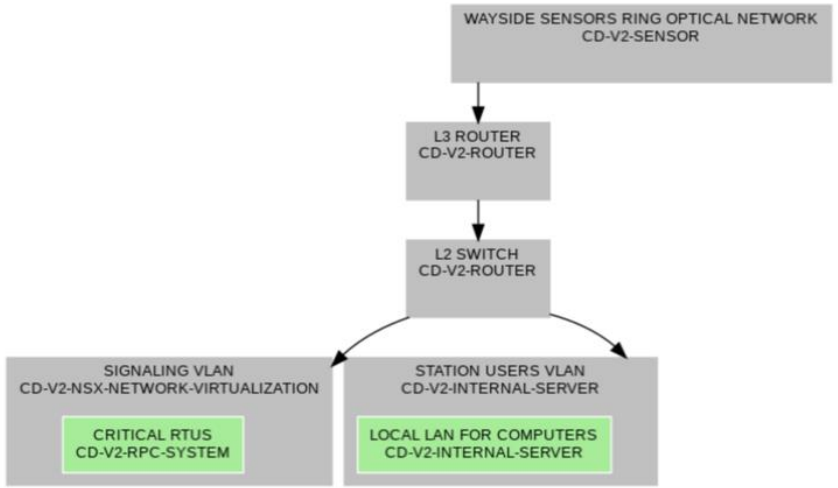
A railway signaling network consists of wayside 10 sensors connected in a ring topology optical network terminating at the railway station. The stations network consists of an L3 router that terminates the optical fiber. The connectivity is extended the local LAN using an additional L2 switch. the VLAN for signaling network is separated from the VLAN for station users computer. The signaling network in the station consists of additional REmote Telemetry Unit (RTU) which are critical to operations.

AUTO GENERATE PRELIMINARY THREAT MODELS

RI You

create threat model

Jeff



Wayside Sensors Ring Optical Network

- Type: CD-V2-SENSOR
- *Description:* Ring topology optical network consisting of 10 connected wayside sensors deployed along the railway line, terminating at the railway station.

https://community.iriusrisk.com/

CRITICAL THREAT FILTERING and AUTOMATED PRIORITIZATION

Threat details

Wayside Sensors Ring Optical ... / Tampering

Signal injection and manipulation

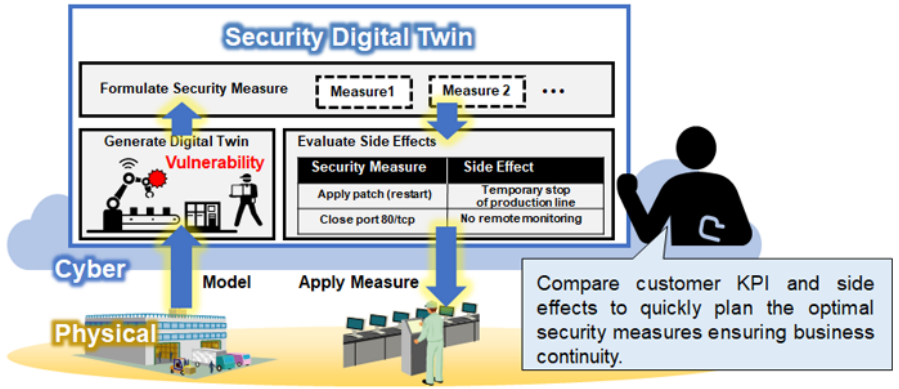
Critical risk

Threat Agents/Attack Vectors

- Malicious Actors: Individuals using specialized equipment to generate and inject false signals into the sensor.
- Physical Access: Attackers gaining physical access to sensor wiring or circuitry to manipulate the signals directly.
- Interference Exploitation: Exploiting design vulnerabilities where insufficient filtering or isolation allows unauthorized signal interference.

Impacts

- Data Integrity Compromise: Altered sensor signals can result in inaccurate or misleading data being recorded.
- Operational Disruption: False readings may trigger incorrect system responses, leading to operational failures.
- Reduced Trust: Compromised sensor data undermines confidence in the system's reliability and decision-making processes.



https://rd.hitachi.com/_ct/17701263

HITACHI

Greybox Fuzzing IoT/OT software

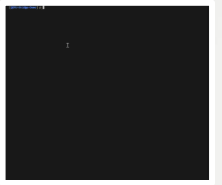
CiA® 421 series: CANopen application profile for train vehicle control systems

The application profile specifies the communication within the integration network that facilitates information exchange between sub-systems located in a single rail vehicle or a consist of rail vehicles. It provides a detailed specification of the application data communicated by rail vehicle sub-systems, such as the door control system, passenger information system, HVAC (heating, ventilation, and air conditioning), and others.

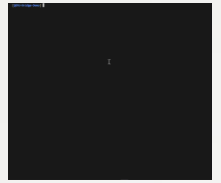
For instance, when it is necessary to close all doors of a rail vehicle, the train operating system needs to know how to send the appropriate command to the door control system. From a CANopen perspective, this involves determining which object in the CANopen object dictionary of the door controller should receive the "close all doors" command. Additionally, the door controller has to understand the structure of the command (e.g., which bit specifies the requested action). This and other related information are specified in the CiA 421.

Demonstration

Running without bridge

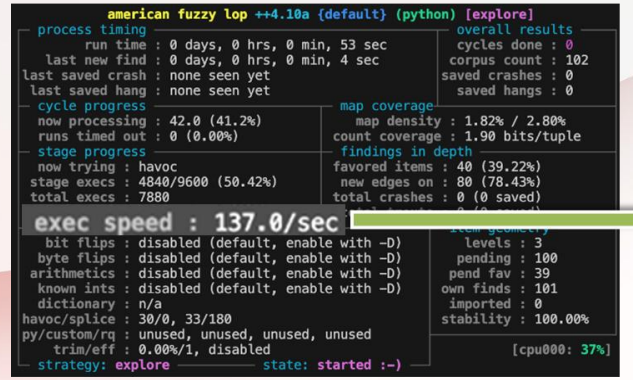


Running with bridge



Performance boost

RUNNING WITH PYTHON-BASED QILING/UNICORN



RUNNING WITH THE BRIDGE

Test setup: 64-bit Ubuntu 22.04 + 8 GB RAM + Intel(R) Core(TM) i7-4790 CPU @ 3.60GHz with 8 logical CPUs
Test program: Same as the demo but reading from standard input

Press Release: https://rd.hitachi.com/_ct/17722949
URL: https://github.com/AFLplusplus/AFLplusplus/tree/stable/qemu_mode/hooking_bridge
Presentation at Linux Foundation SOSS'24 event, Atlanta, USA
URL: https://www.youtube.com/watch?v=qx1PCjQ1bCA&t=307 s

HITACHI

Thank you

Follow us

www.hitachi.com

QUIZ

HITACHI

What do you think is the major cyber threat to Indian Railways?

A. Nation state hack to cripple the system, cause accident

B. Ransomware attack on Ticketing Portal, personal information

C. Physical attack on wayside signals impacting the operations

D. Cyber attack on the Rolling stock IoT devices