

Hacking Trains

Not US vs Them. Just We!
This is OUR responsibility

Who am I?

- B.Eng in Computer Engineering from the University of Mumbai
- Engineer at R.U.D.R.A Cybersecurity
- Securing OSS, websites, orgs and Govs of the world.
- Helping build, breaking, and protect websites, apps, ICSs, SDRs, AI models, and much more
- Part time keyboardist/musician



Disclaimers!!!

- This is **OUR** responsibility
- This research was done in good faith because we care!
- Built off previous work done over years
- **I AM NOT AN OT Expert**
- All findings have been disclosed!
- **FOR EDUCATIONAL PURPOSES ONLY!**
- Please exercise sound judgement
- **Disclose your research to the authorities!**



COMMON SENSE

Just because you can, doesn't mean you should.

motivateusnot.com

So many findings! So little time!

A | 26 | Ask Copilot

-

+



1

of 50



Zombie Trains

Exploring vulnerabilities in the railways

In the interest of time: A kill chain

Questions...

- Is it possible for a low-skilled attacker to gain remote access, via the public internet, to sensitive systems of the railways?
- How difficult is it to pull this off? Can we prove that a novice with a few hours could replicate our work?
- If yes, what is the worst thing that an attacker could achieve using this access?

YES

Vulnerability we found

```
@Override // android.app.Activity
public void onCreate(Bundle savedInstanceState) {
    super.onCreate(savedInstanceState);
    setContentView(R.layout.password_view);
    this.blogin = (Button) findViewById(R.id.all);
    this.tusername = (TextView) findViewById(R.id.editText1);
    this.tpassword = (TextView) findViewById(R.id.editText2);
    this.blogin.setOnClickListener(new View.OnClickListener()
        @Override // android.view.View.OnClickListener
        public void onClick(View view) {
            password_view.this.username = password_view.this.tusername.getText().toString();
            password_view.this.password = password_view.this.tpassword.getText().toString();
            if (password_view.this.username.isEmpty() || password_view.this.password.isEmpty()) {
                password_view.this.alter_message("Enter All Entery");
            } else if (password_view.this.username.equalsIgnoreCase("admin") && password_view.this.password.matches("s[0-9]{4}")) {
                Intent sac1 = new Intent("android.intent.action.MAIN");
                password_view.this.startActivity(sac1);
                password_view.this.finish();
            } else {
                password_view.this.alter_message("Invalid Username/Password");
            }
        }
    });
}
```



Answer to question 1?

YES!

Context for answer 2:
2 years ago, at
NullCon Goa 2022...



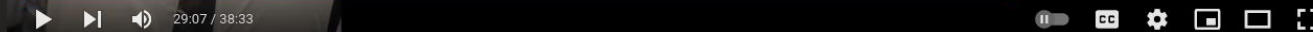
Developer's **Misconception !**

- Instances when a developer tried to protect from XSS
- Tried to protect from SQLi but it was still vulnerable to XSS
- Where the filters protected against XSS but still vulnerable to SQLi



SLIDE = 14

Raining CVEs On WordPress Plugins With Semgrep
- Shreya Pohekar and Syed Sheeraz Ali



Raining CVEs On WordPress Plugins With Semgrep by Shreya Pohekar & Sheeraz Ali | Nullcon Goa 2022



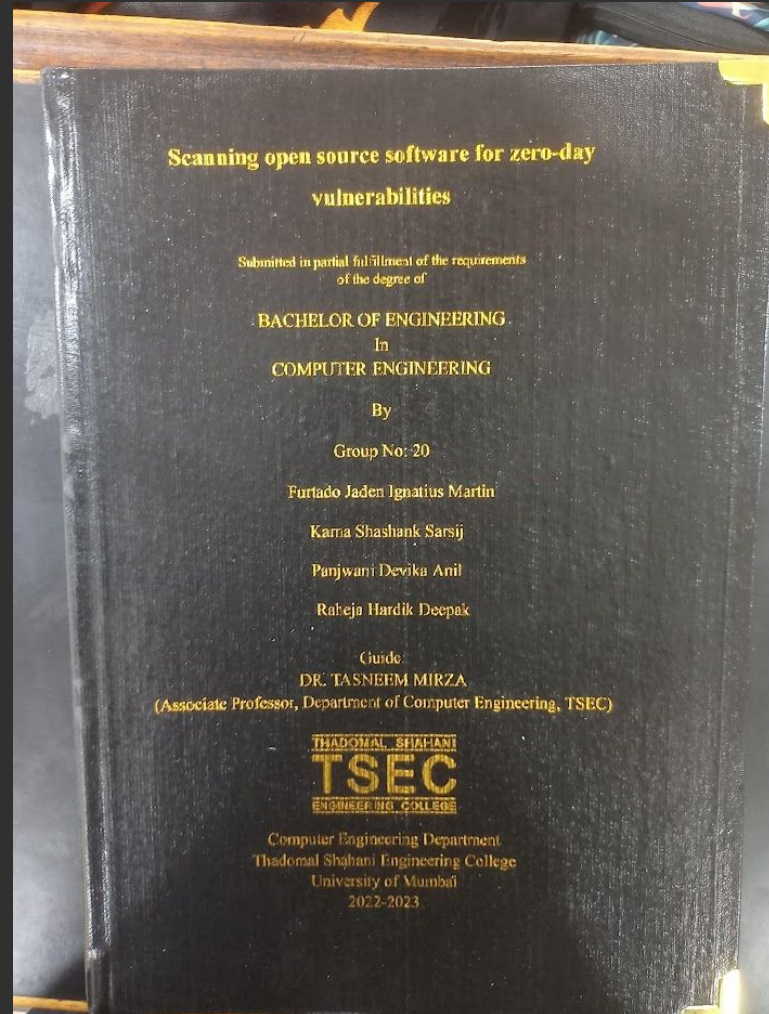
nullcon
11.1K subscribers



<https://www.youtube.com/watch?v=RvKLn2ofMAo>

Final Year Undergrad project:
Scanning OSS for 0-days

ScanRE:
<https://github.com/scanre/ScanRE>
a wrapper around Semgrep, ORT
and GPT-3



Side-quest?

Mass Scanning vulnerability in Google Play-Store app



On A Budget!

Stuff we found...

```
package server.#####.dataLayer.Redis; /* loaded from: classes3.dex */ public class RedisDBConfig { public static final String HOST = "13.232.1##.1##"; public static final String PASSWORD = "d41d8cd98f00b204e9800998ecf#####"; public static final int PORT = 6379; public static final int TIMEOUT = 10000; }
```

```
public static final String DISPATCH_TYPE_MANUAL = "Manual";
```

```
public static String DISPATCH_WEB_REASON = null;
```

```
public static final String ELASTIC_SEARCH_BASIC_AUTH_PASSWORD = "#####@123";
```

```
public static final String ELASTIC_SEARCH_BASIC_AUTH_USERNAME = "#####";
```

```
public static final String ELASTIC_SEARCH_FORWARD_URL = "http://13.232.##.#:9200/";
```

```
public static final String END_STOP_STOP_NAME = "endStopName";
```


Results...

- 23 of the 1000 apps scanned had critical vulnerabilities
- API-keys and passwords, galore
- Exposed Firebase DBs
- Many used outdated libraries with known vulnerabilities
- Apps had insecure permissions
- Apps used unencrypted communication
- All Findings were DISCLOSED!

We missed the Big Picture!

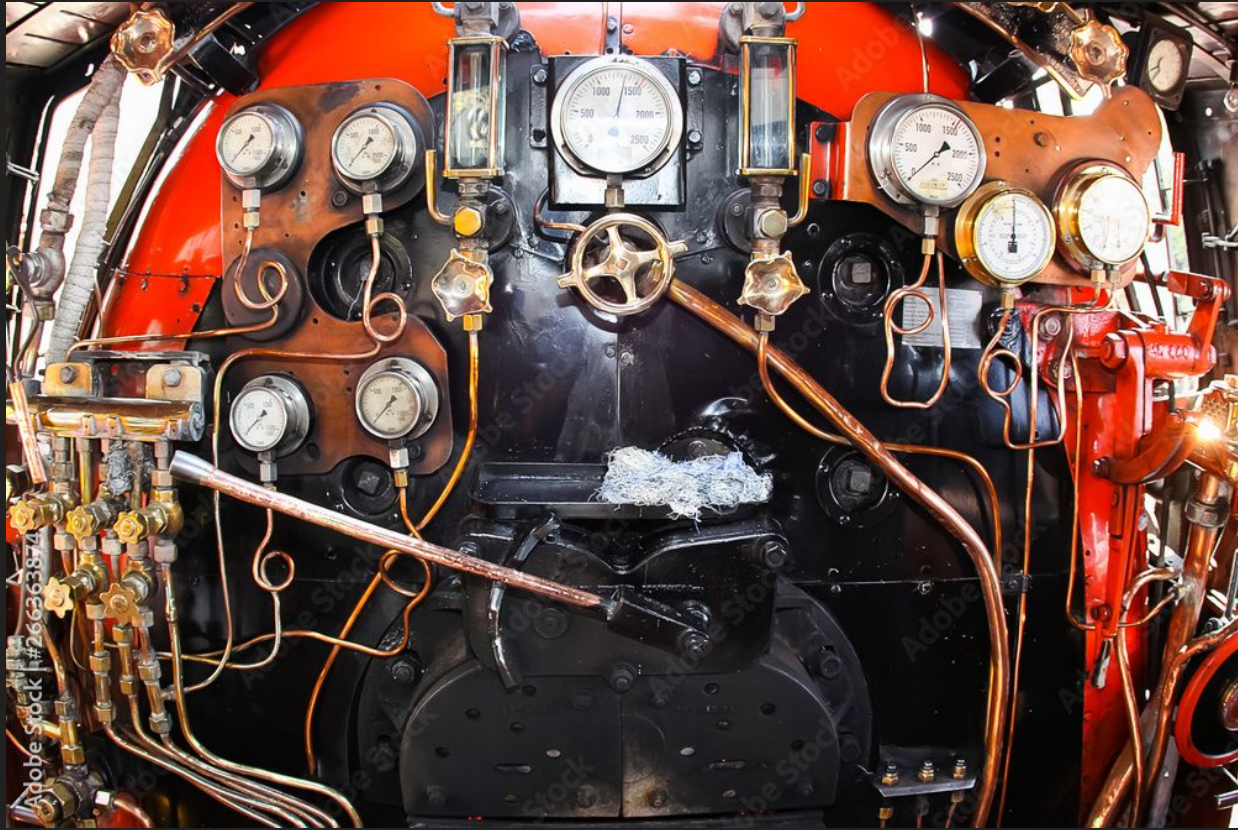
There was **so much more...**



Let's go back in time

Past





Adobe Stock #266363874



<https://nainitaltourism.com/homes.asp?iid=47799524&cid=42>

A few 100 years
later...

Present





One Big Difference?
A lot more computers!

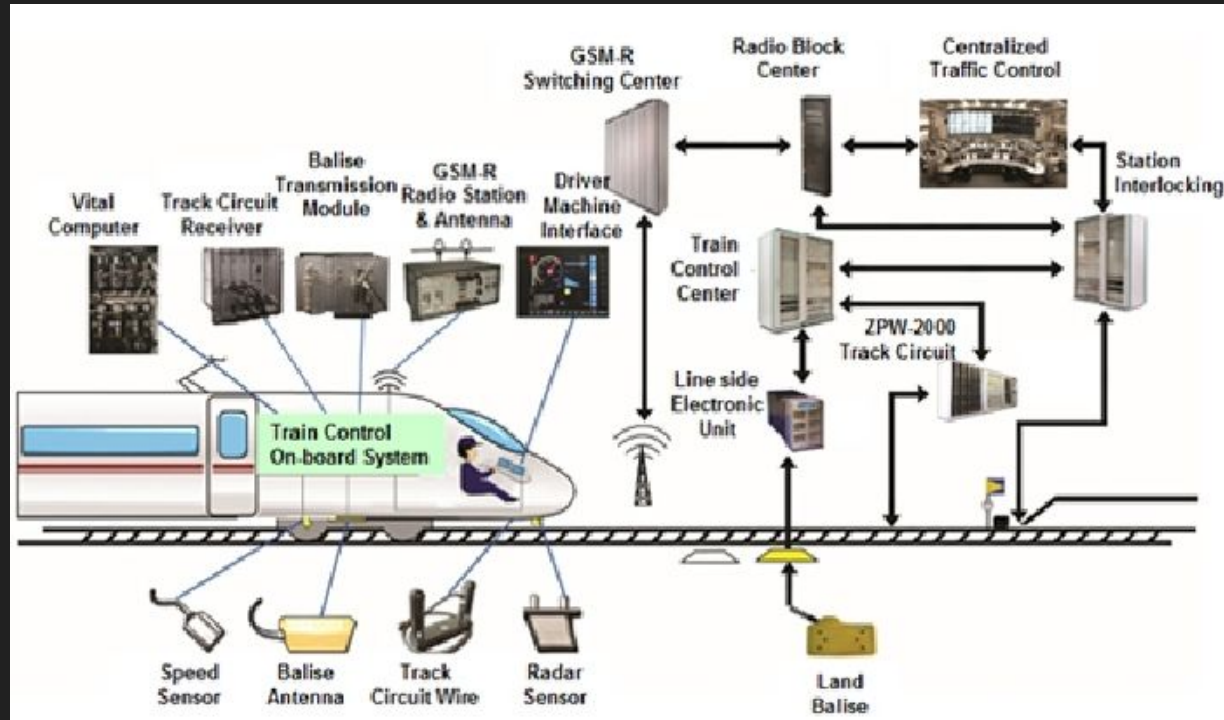
Let's **analyze** the
system

Say we were to design the system from scratch, given requirements...

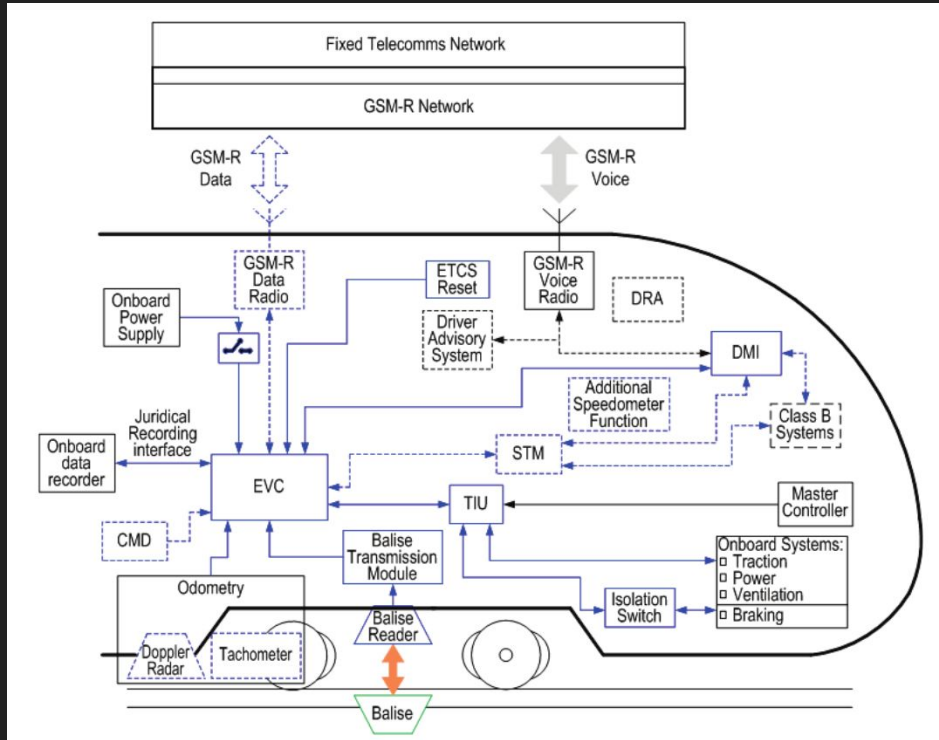
- Control room needs to know the current position of trains
- Driver needs to know their location on the track
- Signals and track switching should operate in a way that ensures graceful failure
- Control room needs to be able to manually override signals/track switches
- Drivers and control rooms need to communicate

...

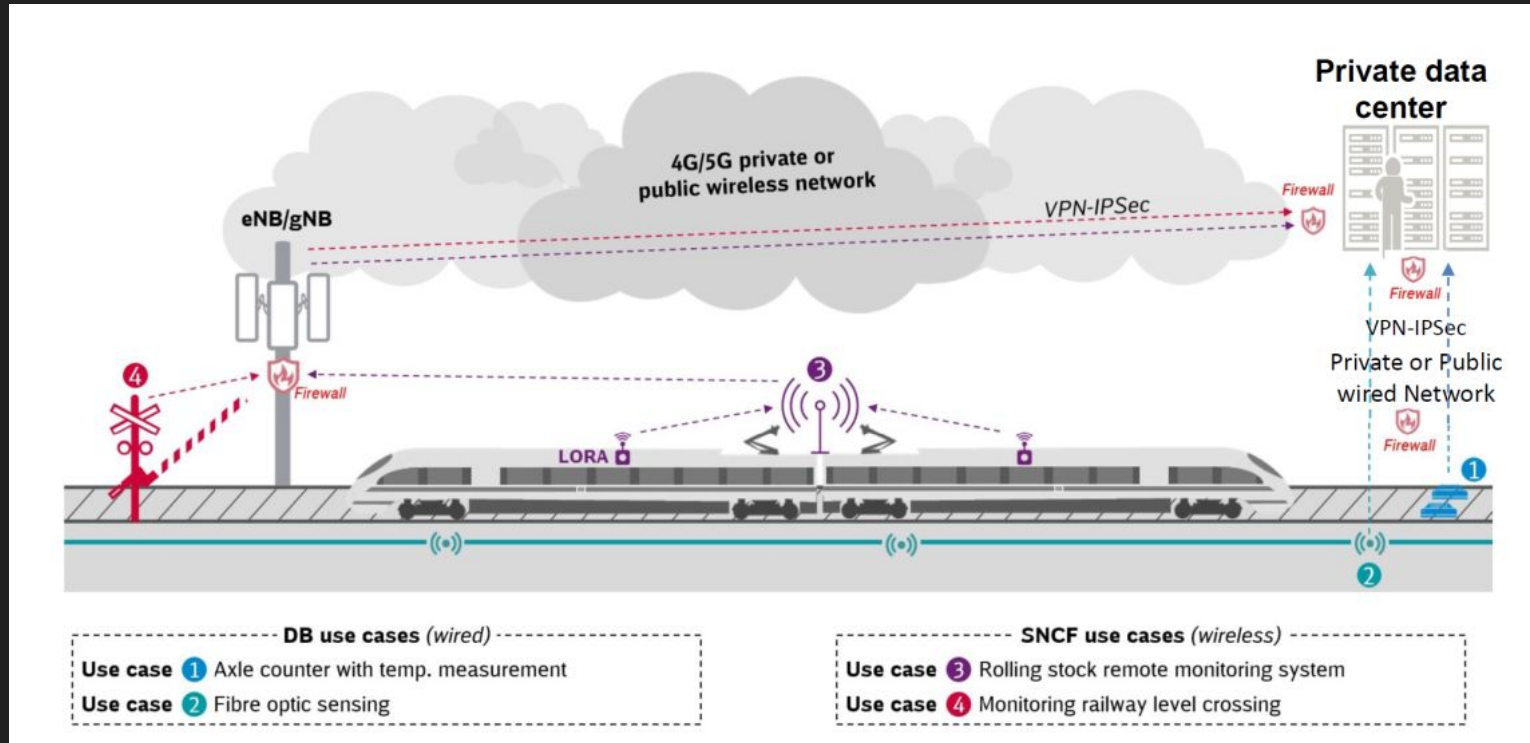
ETCS(European train control system)



ETCS(European train control system) OnBoard Equipment

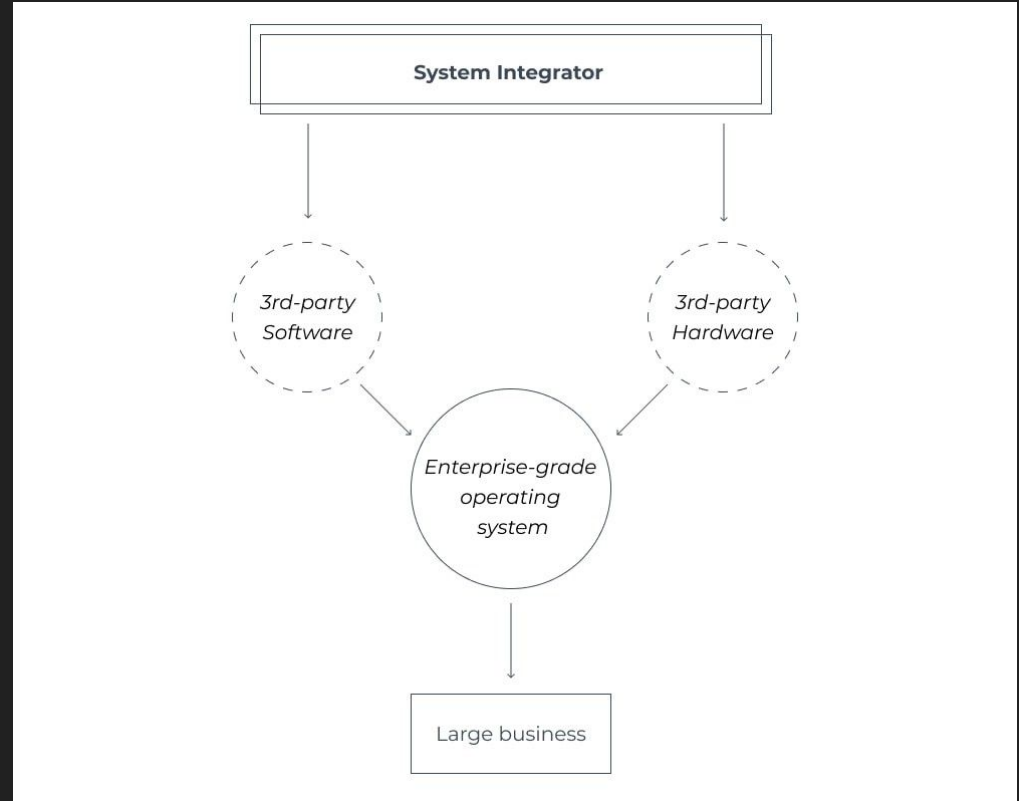


High level architecture



From a business perspective

- 3rd party Hardware components
- 3rd party Software components
- The Hardware+Software = Operating System, in this case is trains

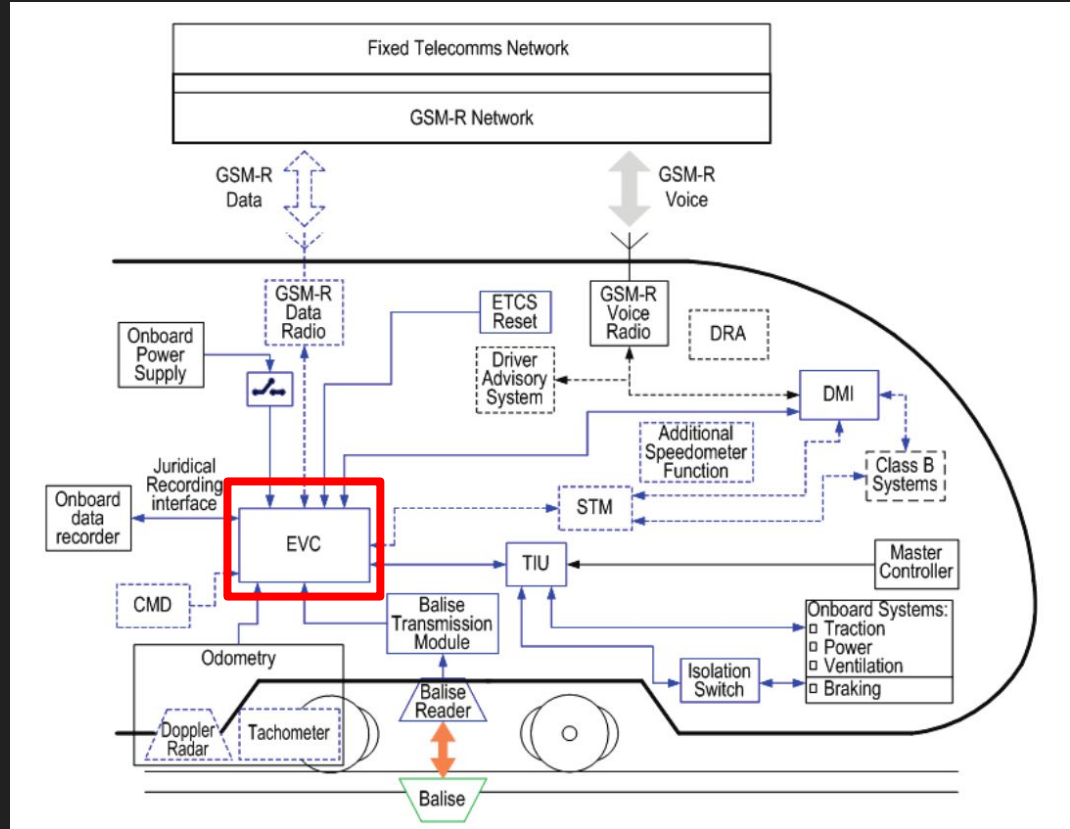


The EVC



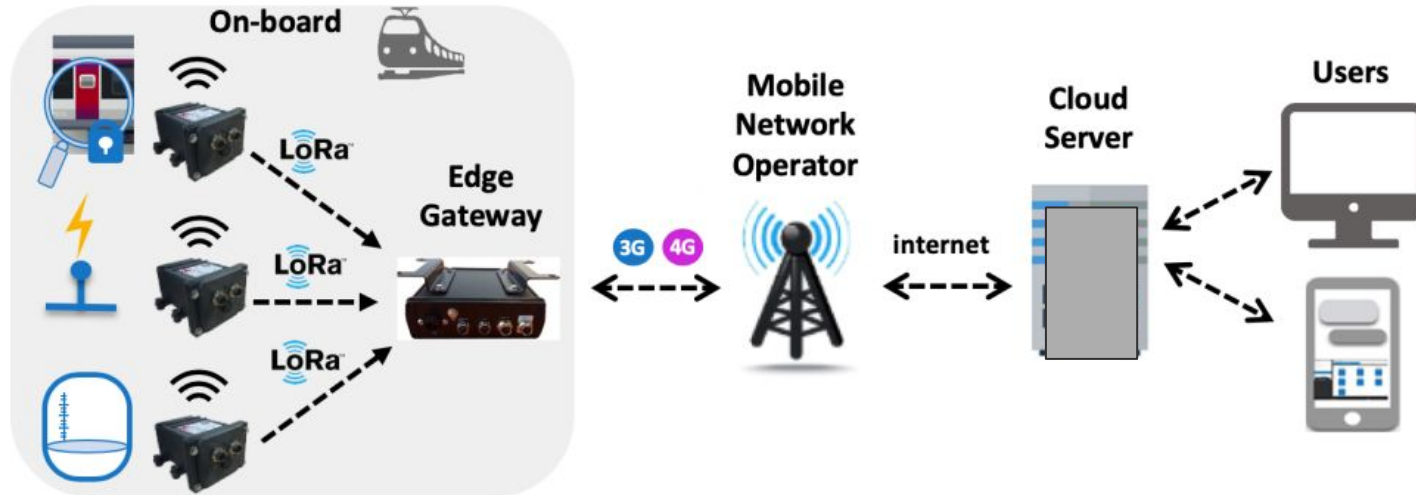
What is the EVC?

- The European Vital Computer (EVC), sometimes referred to as Eurocab, is the heart of train's on-board ETCS equipment
- THE onboard computer
- Heart of the locomotive
- All data flows(into and exits the train) through the EVC

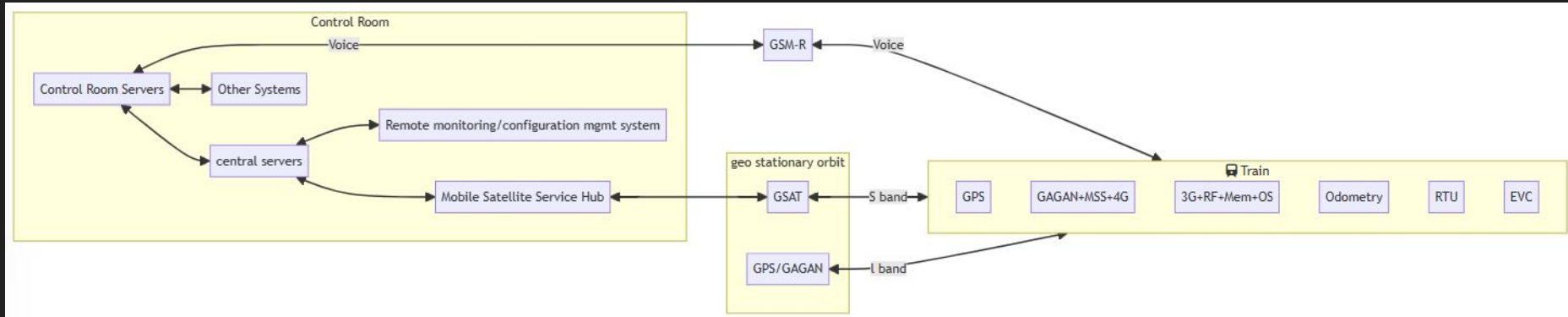


A more detailed look
into the **diagnostics**
systems in use

Remote Monitoring System



Behind the scenes



Remote monitoring of trains/their components???

What all functionality is exposed?

Can we reach it from the internet?

Can we find a vulnerability in this piece of code?



Where does one find
such software
publicly?



GET IT ON

Google Play

Vulnerability in the android app

```
@Override // android.app.Activity
public void onCreate(Bundle savedInstanceState) {
    super.onCreate(savedInstanceState);
    setContentView(R.layout.password_view);
    this.blogin = (Button) findViewById(R.id.all);
    this.tusername = (TextView) findViewById(R.id.editText1);
    this.tpassword = (TextView) findViewById(R.id.editText2);
    this.blogin.setOnClickListener(new View.OnClickListener()
        @Override // android.view.View.OnClickListener
        public void onClick(View view) {
            password_view.this.username = password_view.this.tusername.getText().toString();
            password_view.this.password = password_view.this.tpassword.getText().toString();
            if (password_view.this.username.isEmpty() || password_view.this.password.isEmpty()) {
                password_view.this.alter_message("Enter All Entery");
            } else if (password_view.this.username.equalsIgnoreCase("admin") && password_view.this.password.matches("s[0-9]{4}")) {
                Intent sac1 = new Intent("android.intent.action.MAIN");
                password_view.this.startActivity(sac1);
                password_view.this.finish();
            } else {
                password_view.this.alter_message("Invalid Username/Password");
            }
        }
    });
}
```



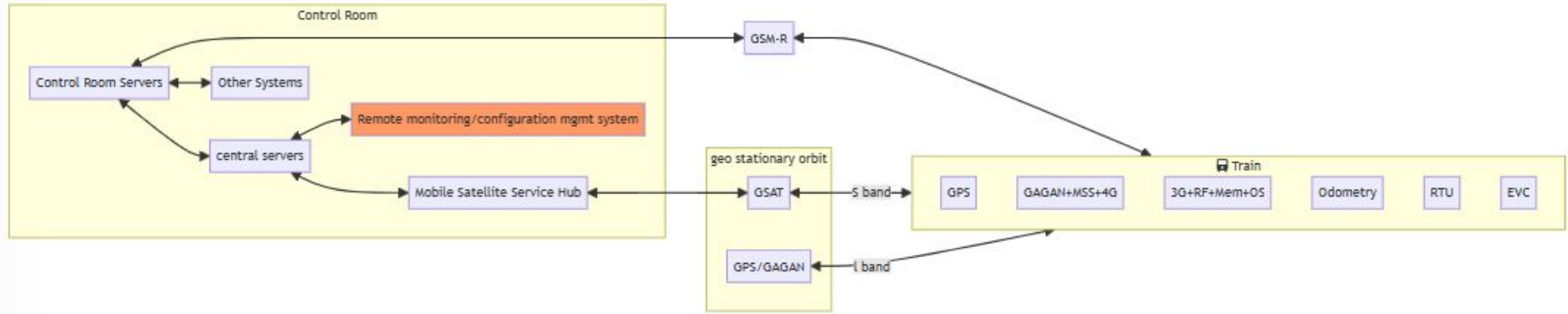
What is documented...

- READ ONLY app of metrics, location, and diagnostic information *
- Should be separate from the rest of the system *
- Considered as NOT safety critical *

The monitoring system
should be “iSoLaTeD”
from safety critical
systems*

But is it?

Expectations...



Undocumented
functionality allowed
software
updates(Over The
Air) to EVC!

Software updates



Some manufacturers have the ability to push remote code and configs to their hardware *

Secure Update Edge devices should facilitate the possibility to update their firm- and software to roll-out new functionality and to patch security vulnerabilities. Unpatched systems are left vulnerable to attacks. Such an update should be performed in a secure manner so that it does not constitute an additional attack surface. ENISA recommends that updates can be performed over-the-air, the connection used to transmit the update is secure, that the update does not contain sensitive data, and that the update is digitally signed to be verified by the updated device [12].

Reality!

SingleLoco MultipleLocos

Remote Programming

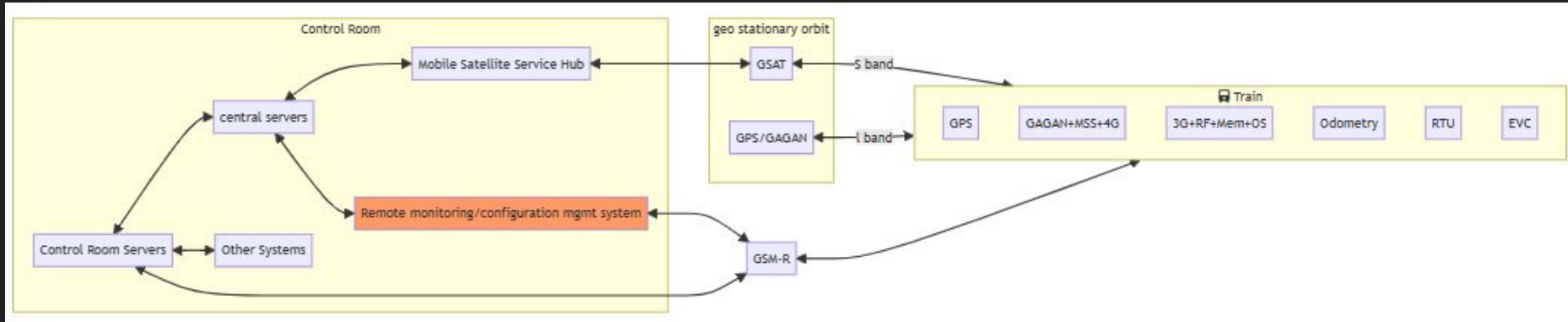
Select the Loco No

Enter the Password

Select the file No file selected.

Entered By

What was happening



Could someone use the monitoring system to abuse the EVC? YES!

- **Manufacturers re-use the monitoring software as a means of sending out software updates/config changes**
- Modern devices/sensors on trains use Linux
- Probability of a successful supply chain attack is high!

Doable by a novice?

Possibly

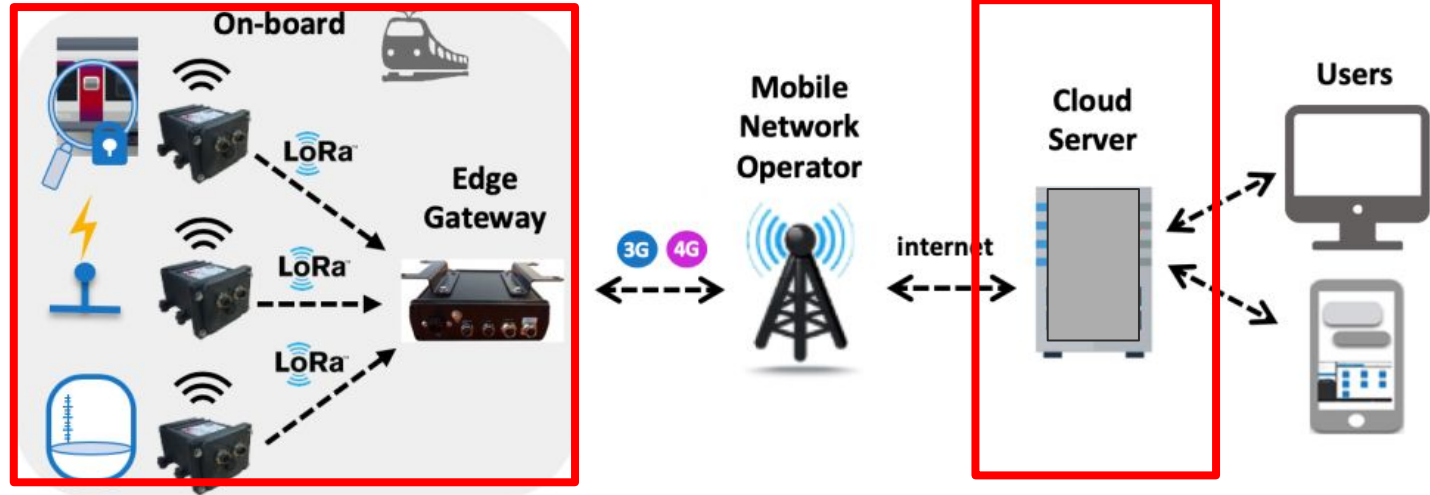
Say at some time T , a malicious attacker K conducts an attack A by performing a set of steps S that succeeds in controlling the EVC.

What is the worst that
could happen?

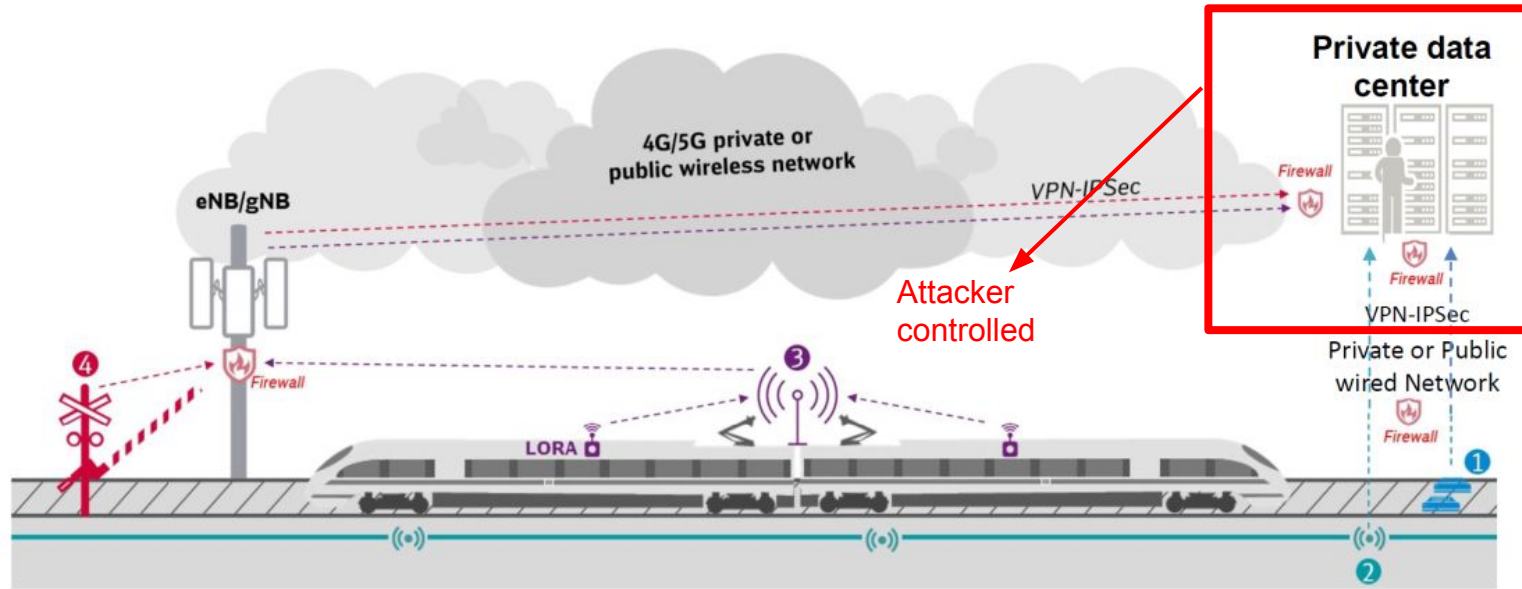
Cause collisions?

Maybe! *

Attacker can poison data



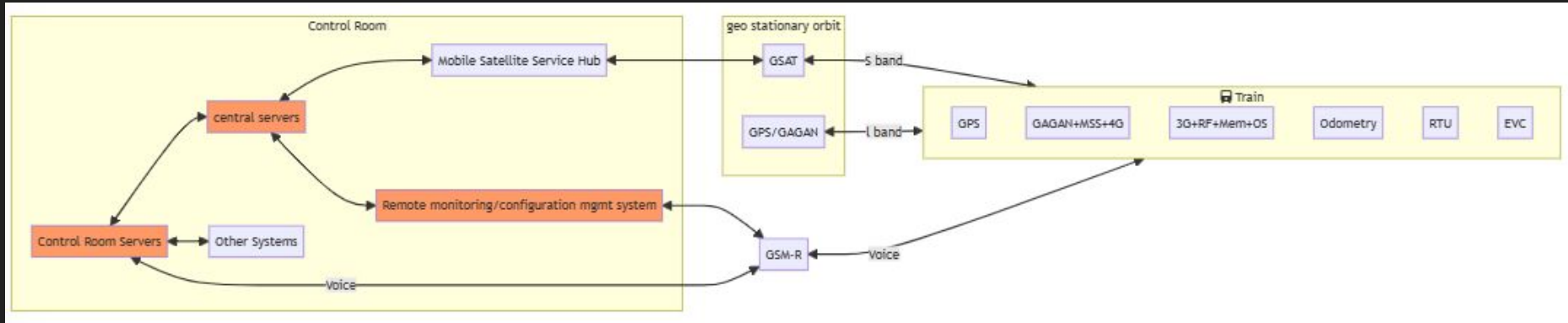
Send false data back to the control rooms



- DB use cases (wired)**
- Use case 1 Axle counter with temp. measurement
 - Use case 2 Fibre optic sensing

- SNCF use cases (wireless)**
- Use case 3 Rolling stock remote monitoring system
 - Use case 4 Monitoring railway level crossing

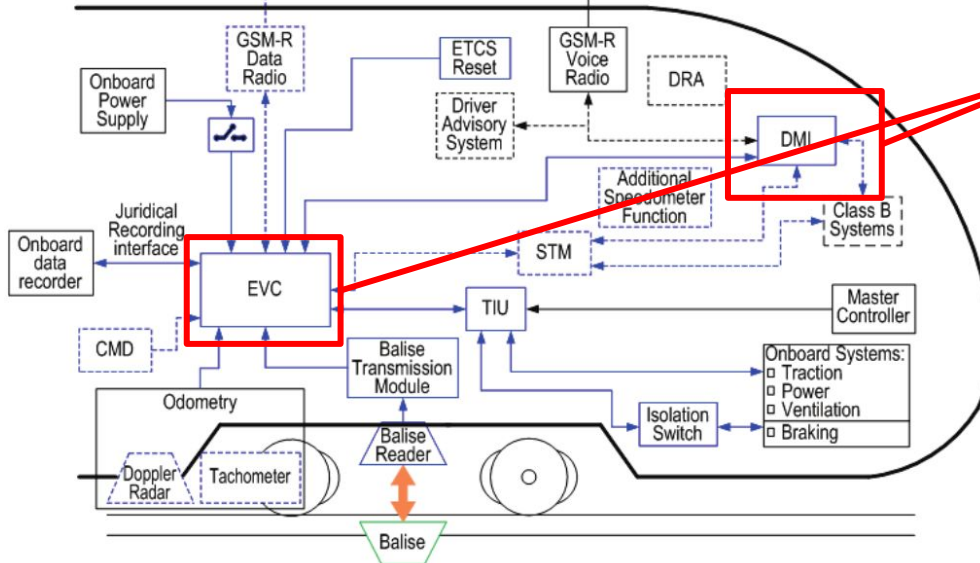
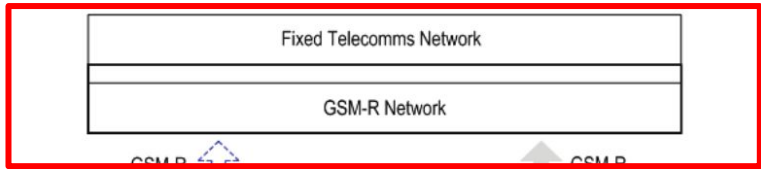
In effect



Why is this a big deal?

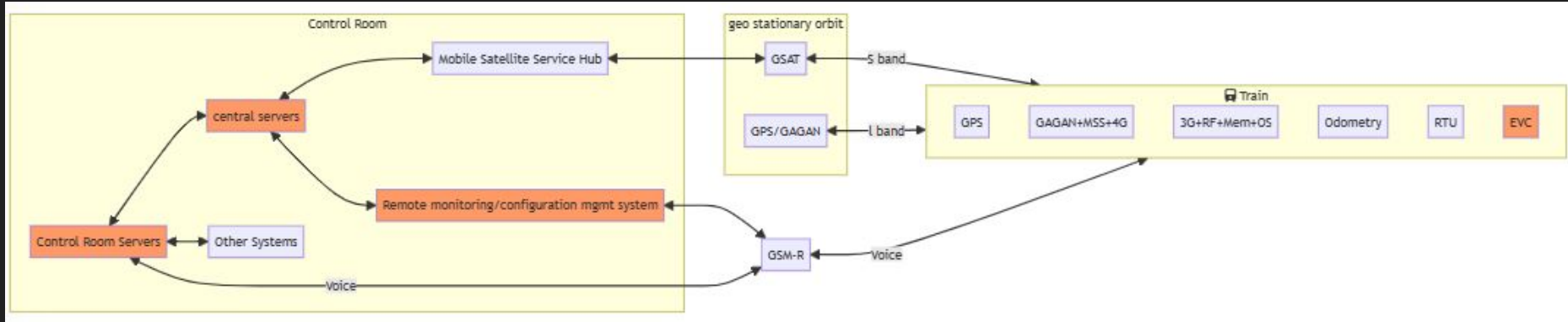
- Attacker controls EVC, Central data servers, and control room servers
- Attacker sends false data to the control room
- Attacker sends false data to the trains
- Formal verification fails as data can't be trusted

A Botnet of trains!



Attacker controlled

A botnet



To sum it up

- Over 2000 locomotives affected
- Operators/SIs/Drivers/Regulators in the dark about this functionality
- Poor engineering decisions
- Lack of proper security testing
- Multiple glaring security issues
- Software used as a fix
- On paper != Reality

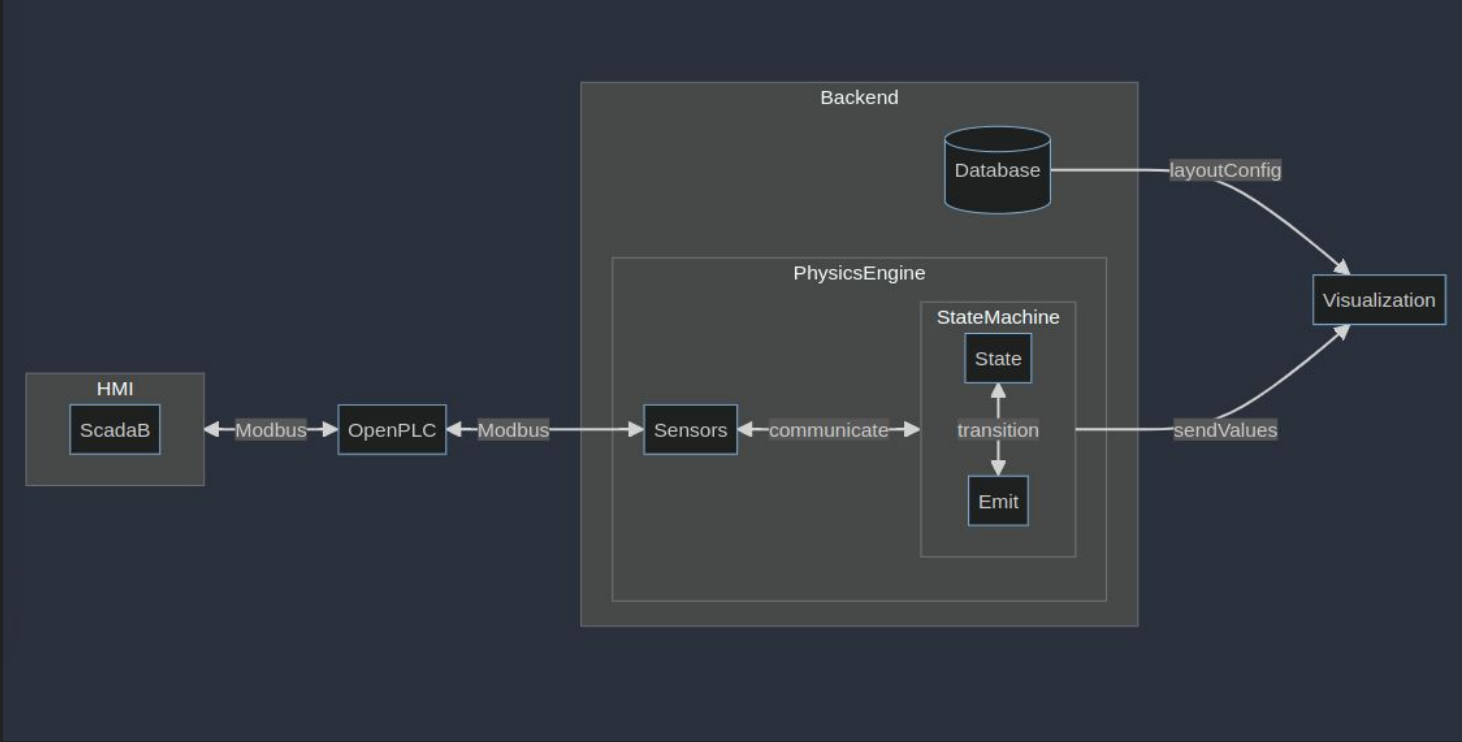
Can we simulate this?

YES!

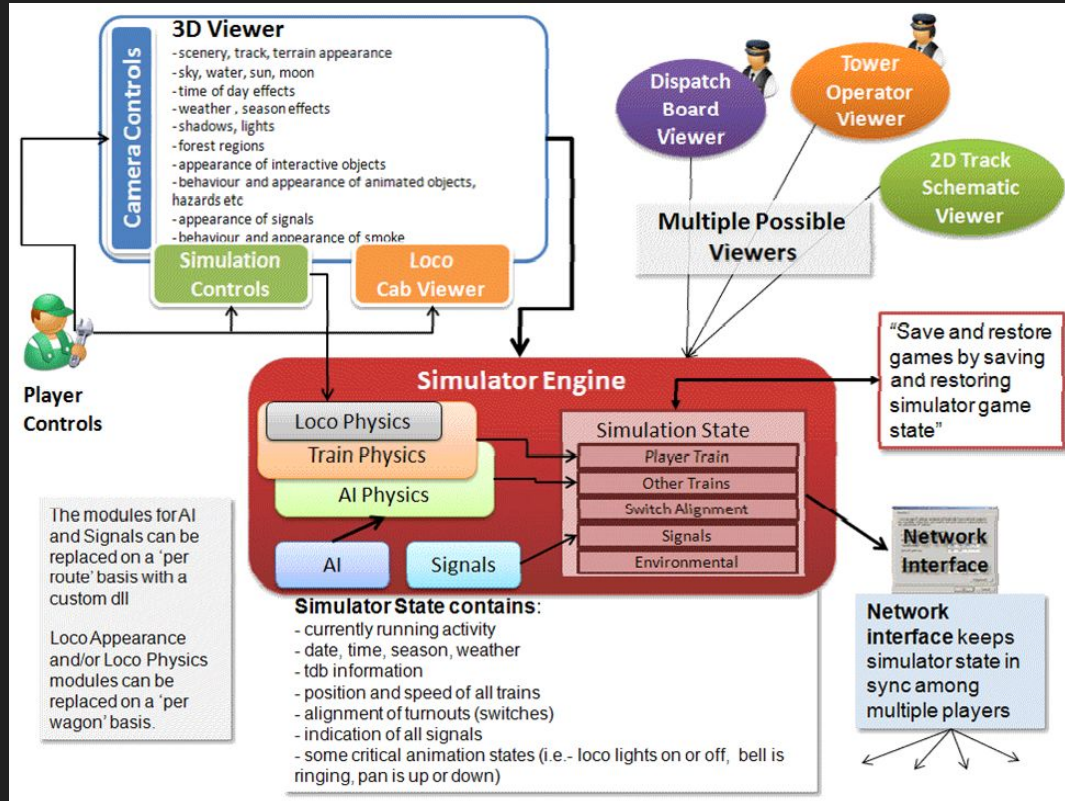
Microsoft Train Simulator/Open rails



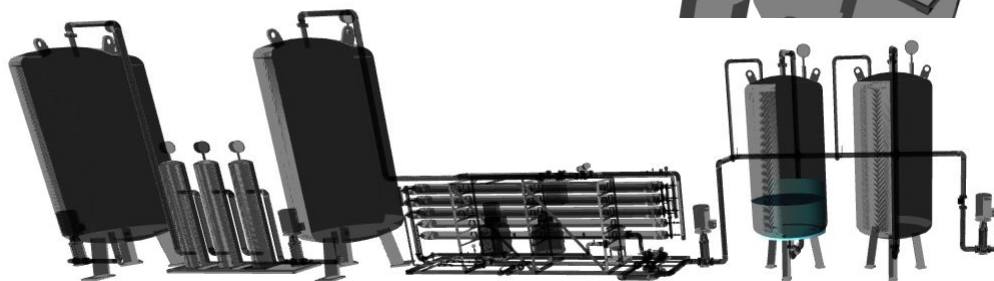
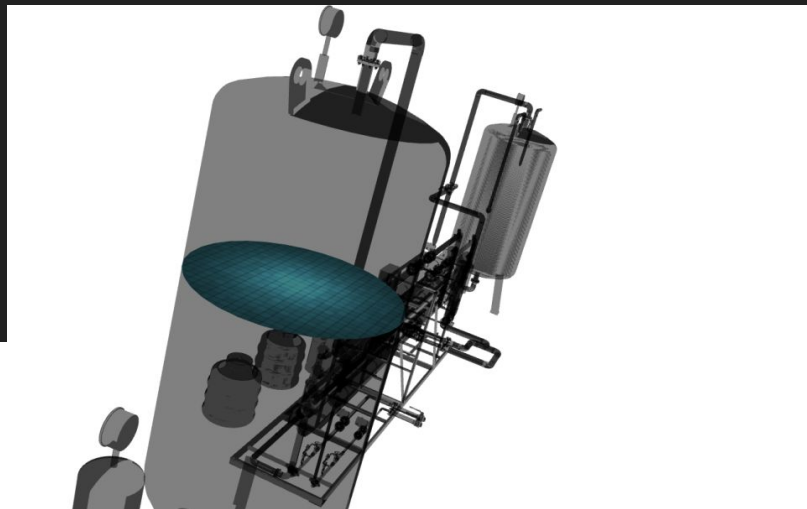
Our solution



Architecture of openrails



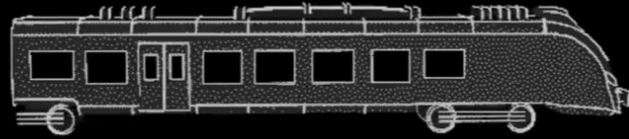
Some cool stuff!



What about other
manufactures?

Newag's DRM ...

Breaking "DRM" in Polish Trains



37C3



0:48 / 1:01:45 • Introduction >



37C3 - Breaking "DRM" in Polish trains



media.ccc.de
206K subscribers

Subscribe

18K

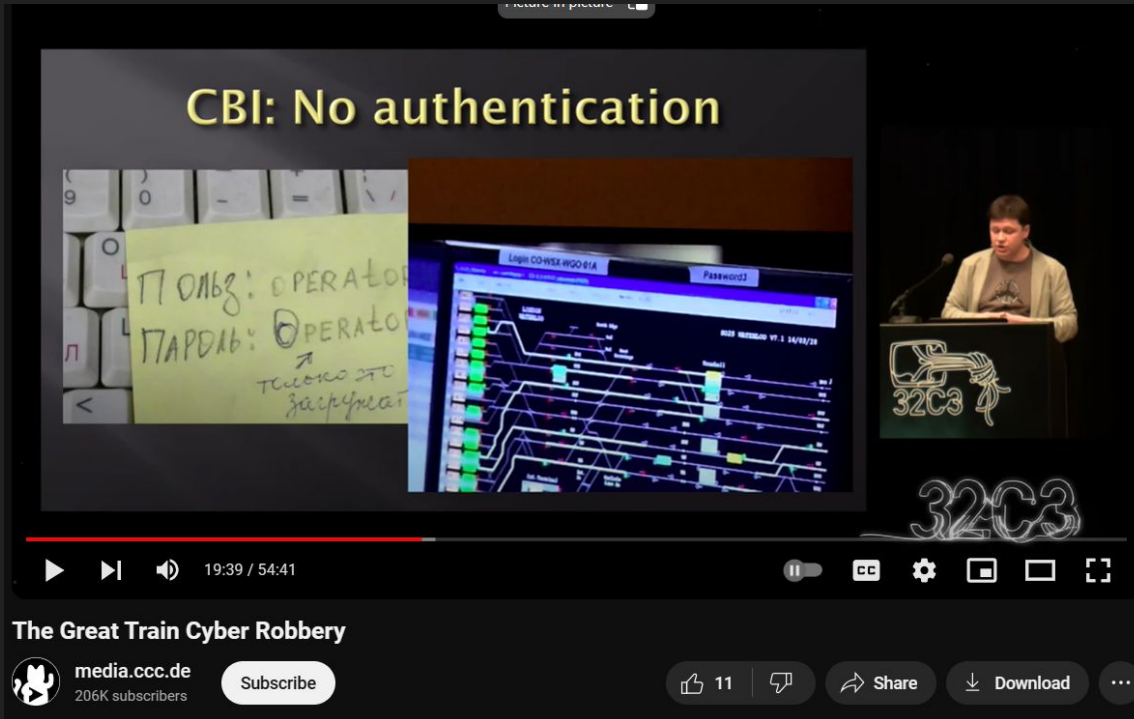


Share

Download



SCADA StrangeLove: The Great Cyber Train Robbery



The video player displays a presentation slide with the following content:

- Title:** CBI: No authentication
- Image 1:** A close-up of a computer keyboard with a yellow sticky note placed over it. The note contains handwritten Russian text: "Польз: OPERATOR", "Пароль: OPERATOR", and "↑ тшкккккк загрузка".
- Image 2:** A screenshot of a SCADA system interface showing a complex network diagram with various colored nodes and connections. The interface includes a login form with fields for "Login" (containing "CO-HSE-WGO-014") and "Password", and a date field showing "01/23 10:00:00 07.1.2018/18".

The video player interface includes a progress bar at 19:39 / 54:41, a speaker icon, and standard YouTube controls (play, pause, full screen, etc.). The video title is "The Great Train Cyber Robbery" and the channel is "media.ccc.de" with 206K subscribers. The video has 11 likes and options for share, download, and more.

Have we seen a
similar thing happen
before?

MCAS in Boeing



How can we make this comparison?

- MCAS was considered NOT safety critical
- NOT documented in manuals or part of training
- Initially relied only on AOA sensors
- Management pressured engineering for workarounds
- Poor engineering decisions

Result?



Software being used as a “Fix”

What can we do about
it?

For the engineers

Say **YES** to:

- Safety
- Testing your systems
- Sound design and engineering solutions

Say **NO** to:

- Hiding functionality/safety issues using software!
- “Hacky” solutions
- Cutting corners
- Unneeded complexity

For the **System Integrators**

- People make mistakes! **Ensure redundancy!**
- Understand everything going into your end product!
- **Audit the software/hardware** before using it
- Test the end system exhaustively

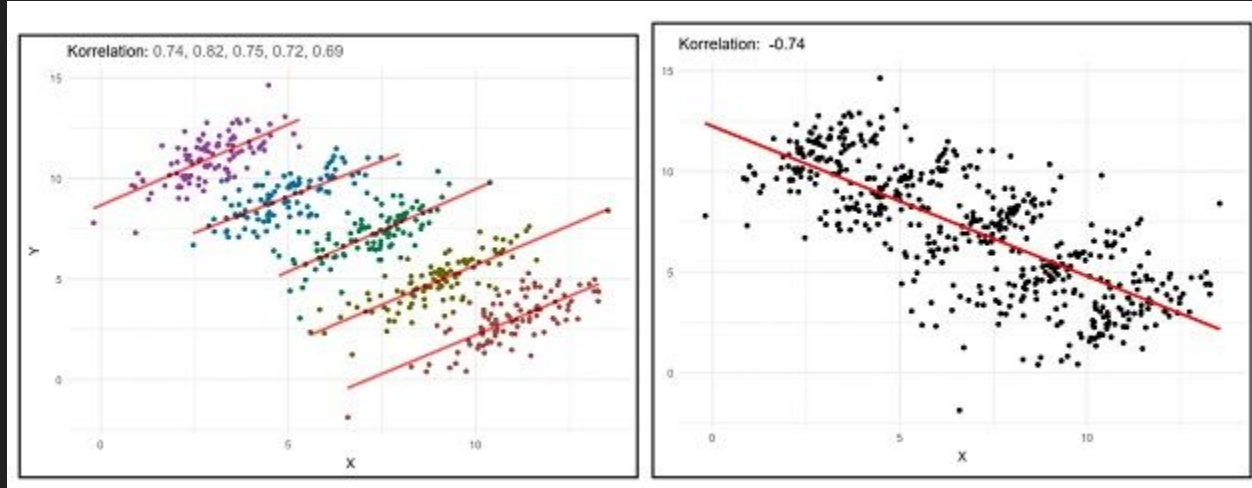
For the executives

- Would you travel on your trains?
- Work WITH, and NOT AGAINST your engineers
- Do NOT Pressurize your engineers to cut corners
- Understand risk!
- Good for Business != Good Engineering

Regulators

Do you have a **complete oversight** of what is truly going on?
The **app shown was supposedly pentested and manufacturer was iso 27001 certified**

NOT misrepresentation, BUT, incorrect interpretation!



Regulators/Engineers/Executives, **have you read this?**

The Internet of Railway Things Security

Whitepaper

Full version

June 2020



Financial impact? **Just in USA!**

**ESTIMATED COST OF A
NATIONWIDE FREIGHT
RAILROAD SHUTDOWN:
MORE THAN \$2 BILLION A DAY!!!**

What is the **true cost**
of getting things
wrong?

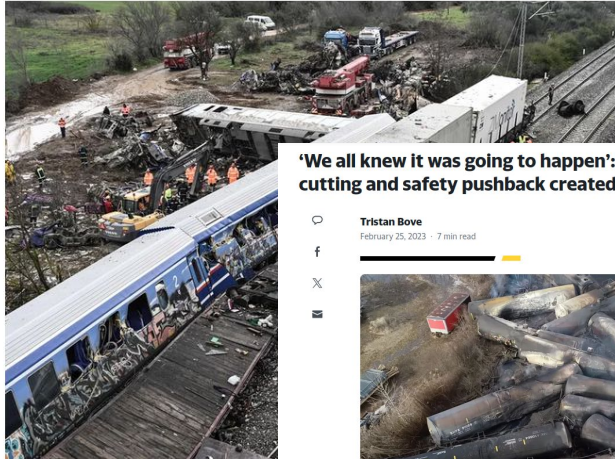
Cost of Life

EUROPE

A Greek train driver was told to ignore a red light before a head-on crash killed 57

MARCH 3, 2023 - 1:18 PM ET

 Juliana Kim



'We all knew it was going to happen': Railroad workers and unions say years of cost-cutting and safety pushback created the Ohio train disaster

 **Tristan Bove**
February 25, 2023 · 7 min read



NTSB.gov/Handout via REUTERS

CATASTROPHE

Germany recalls the Eschede train disaster

06/02/2018

Germany's worst train accident, 20 years ago, is being remembered at Eschede, northeast of Hanover. A high-speed ICE train derailed, killing 101 people, and left Deutsche Bahn facing deep scrutiny over design and safety.



Image picture-alliance/gpa/KeyStone/i. Wagner

HUMAN INTEREST

At Least 280 People Dead and Hundreds More Injured in Three-Way Train Crash in India: 'Deep Sorrow'

Prime Minister Narendra Modi wrote that he is "committed to providing all possible assistance to those affected"

By **Brechen Blanchet** Published on June 3, 2023 01:45PM EDT



Source of today's train crash in India. PHOTO: AP PHOTO/AMERICAN ASSOCIATION



R.U.D.R.A.

Main takeaways from this talk... expectations vs reality of ICS security!

- Genius hacker
- 0-day exploit
- Stealthy persistence
- Exfiltration
- Custom ICS exploit
- Physical process takeover



- RDP from public internet
- PLC's in read state
- Default passwords

So many more questions that remain to be answered!

- What else is out there?
- How many such apps are there on Google Play Store/Apple's App Store?
- What CII is affected by such apps? Transport, Energy, Medical Devices, waste treatment?
- What is the impact of abuse?
- Can Google/Apple do something to help with this?

Why should you care? Let's make the world a better place



“For a successful
technology, reality
must take precedence
over public
relations, for nature
cannot be fooled.”



Richard Feynman

To everyone:
Safety and Sound
Engineering First!

Thank you :)

