An insight into Railway Security

Brian Butterly

@BadgeWizard

Disclaimer

- The content in this presentation is general / public knowledge
  - No secrets, just a bunch of nice wrapping paper and bows
- Please don‘t try to do anything stupid with trains or the train network, they are precious
- Opinions are my own, not the ones of my employer

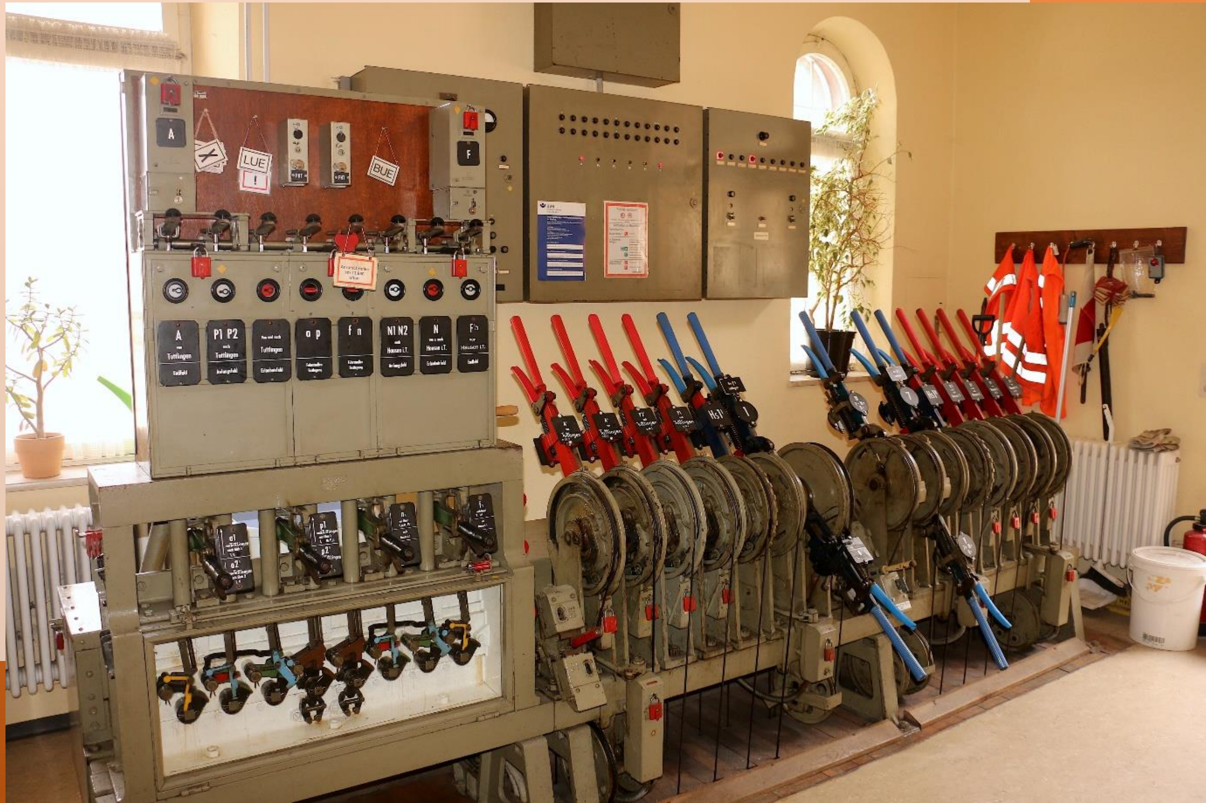
About Me

- Brian
  - Not my first H2HC
- Security Engineer
  - Hardware, Embedded, Telco, +OT
- Work in OT Security in Germany
  - And get to break really cool stuff!
- Had a short break from offensive
  - And did incident response
- Finally, back to offensive work
  - Finally, back in Brazil!

Railway – Steam, Noise and a lot of fun

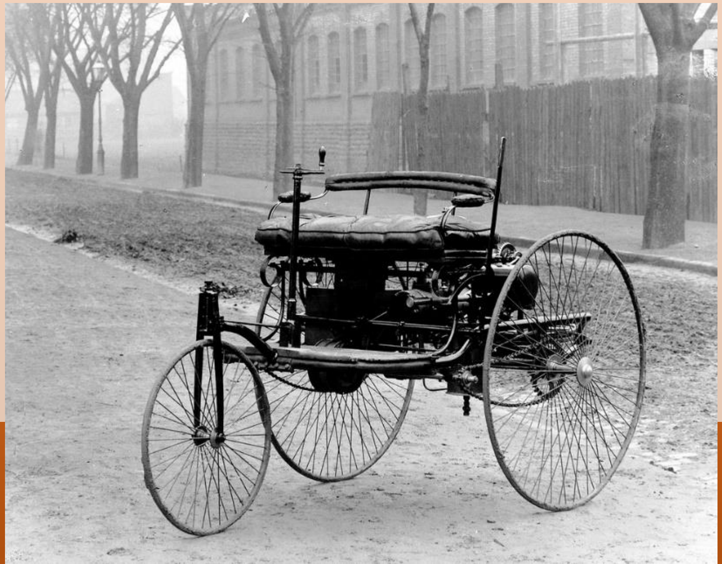
Back in the day…

- Everything was analog
- It was controlled with steel wires and pulleys
  - And levers and a lot of manual power



Railway has come a long way since then…

- Locomotives, trains and the railway all in all have come a long way
  - Just as cars and planes, which both are great references



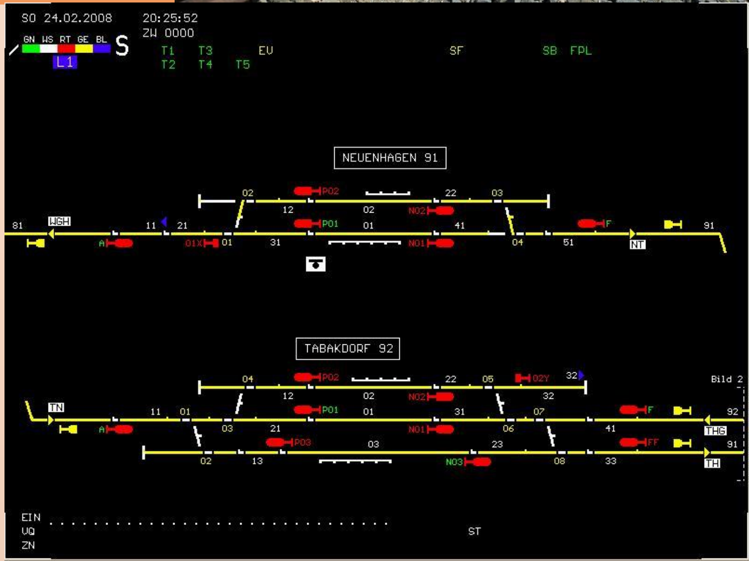
Railway has come a long way since then…

- Locomotives, trains and the railway all in all have come a long way
  - Just as cars and planes, which both are great references

- The “steel wires” have become electronic wires
  - With I/O, sensors, actors and everything that’s part of controlling a digital system

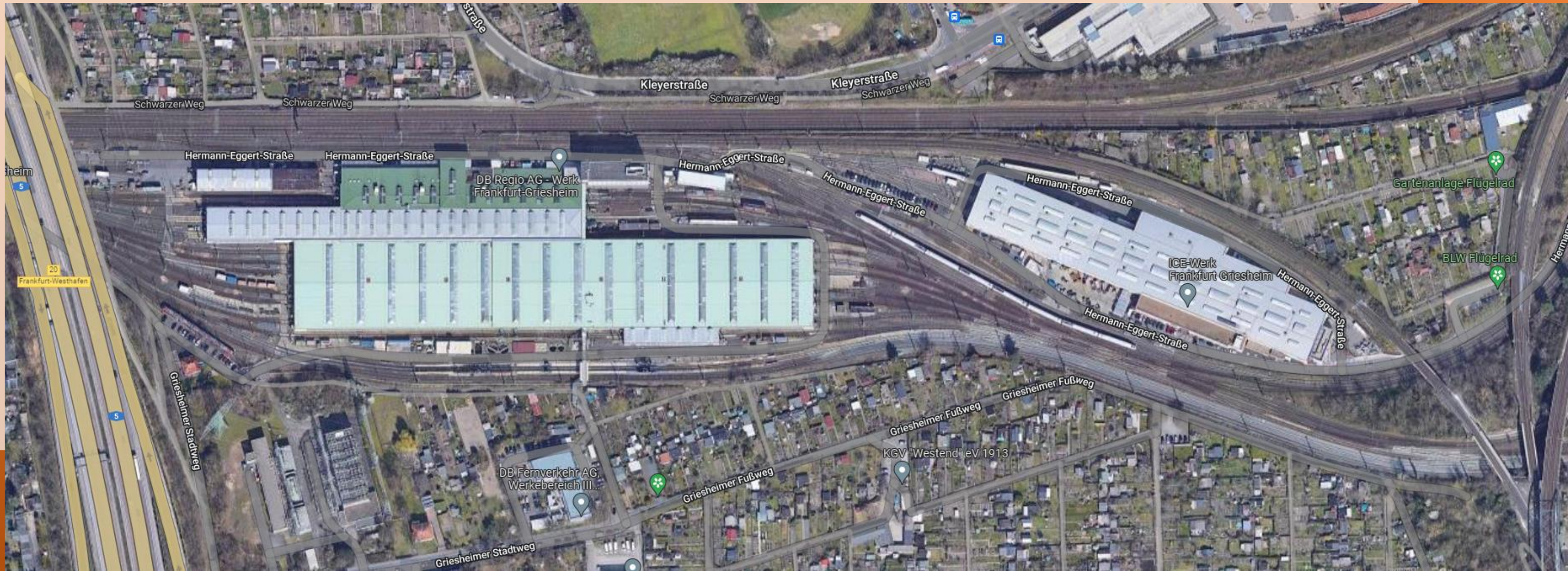
“The System”

- Railways consist of various different components / parts / subsystems
- There mainly are
  - Actual steel / tracks
  - Railroad switches, traffic lights and everything that controls them
  - Maintenance sites
  - The actual vehicles
    - Locomotives
    - Carriages
    - Integrated vehicles



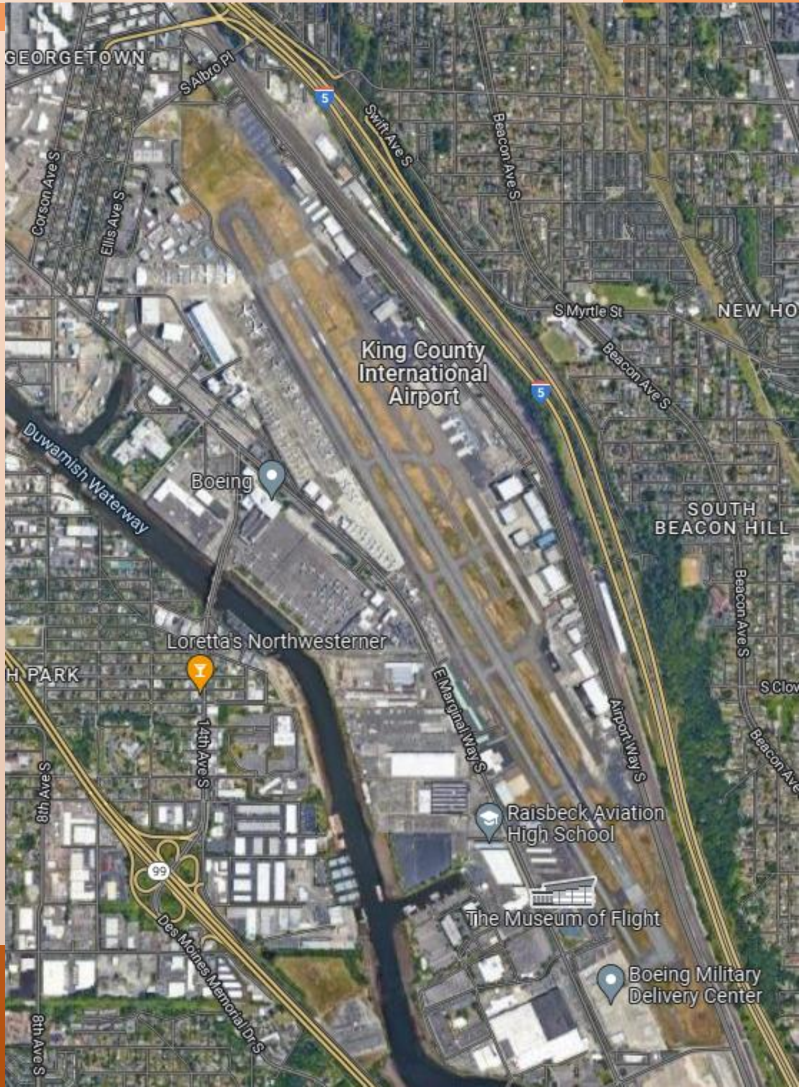
Simple first: Maintenance Sites

- Maintenance sites include all tools to maintain the vehicles
  - Oh, really? – Yes!
- With trains these just are a little bit bigger
  - The pictures shows about 1km – the white train is 200m long



Maintenance Sites

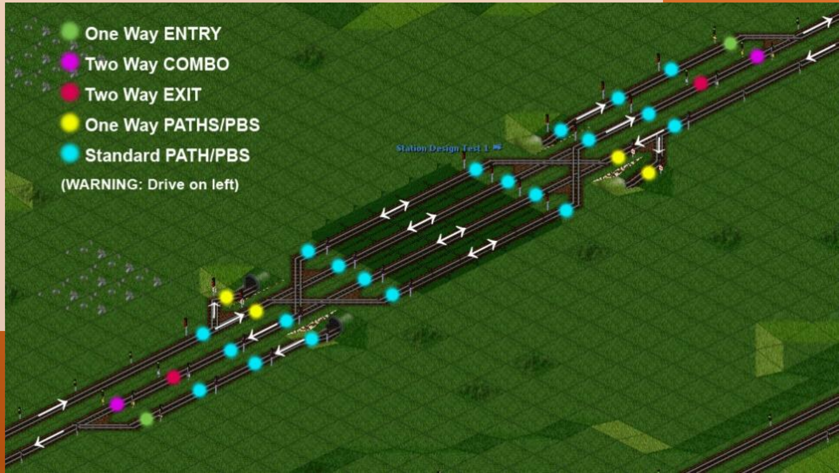
- While being bigger than car garages
  - Boeing Field still is a lot bigger (3.27km runway)
- It contains basics tools for any kind of repairs and a big collection of spare parts
- Obviously, in modern times, various jobs are run on machines which are digitally controlled
  - i.e. CNC equipment etc.
- Typical operational technology



Tracks

- Real tracks and control systems are very similar to the way they are in games
  - Like oTTD → forget to set a signal and two trains collide :)

- Only work with various sensors and actors along the tracks



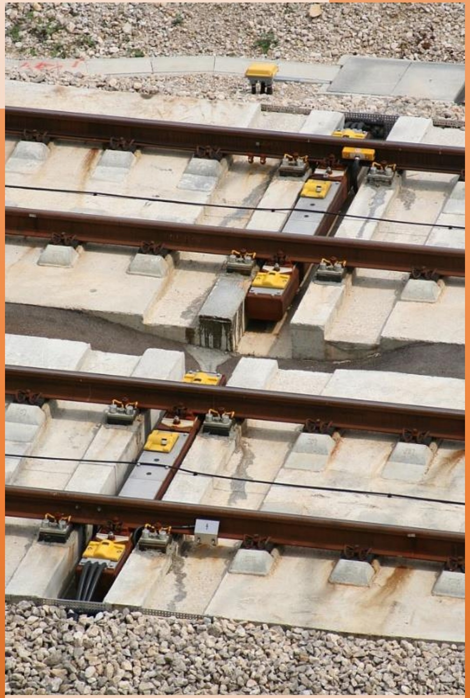
Track-Side Sensors & Actors

Axle counter, to keep safe distances between trains

Signals / traffic lights

Switches

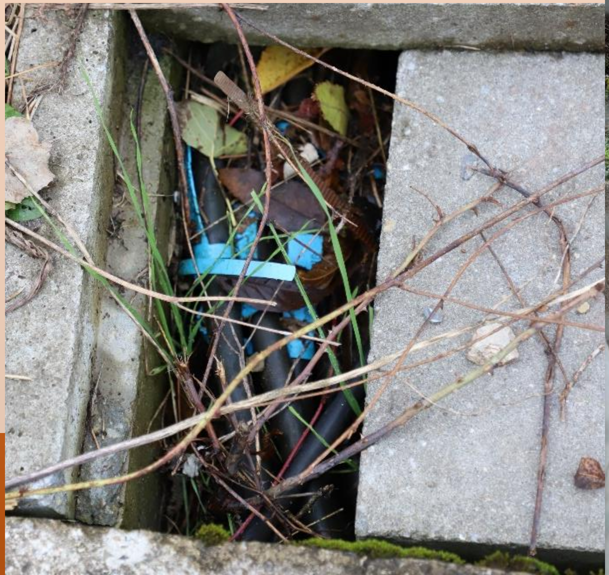
Railroad crossing



Detection for overheated wheels

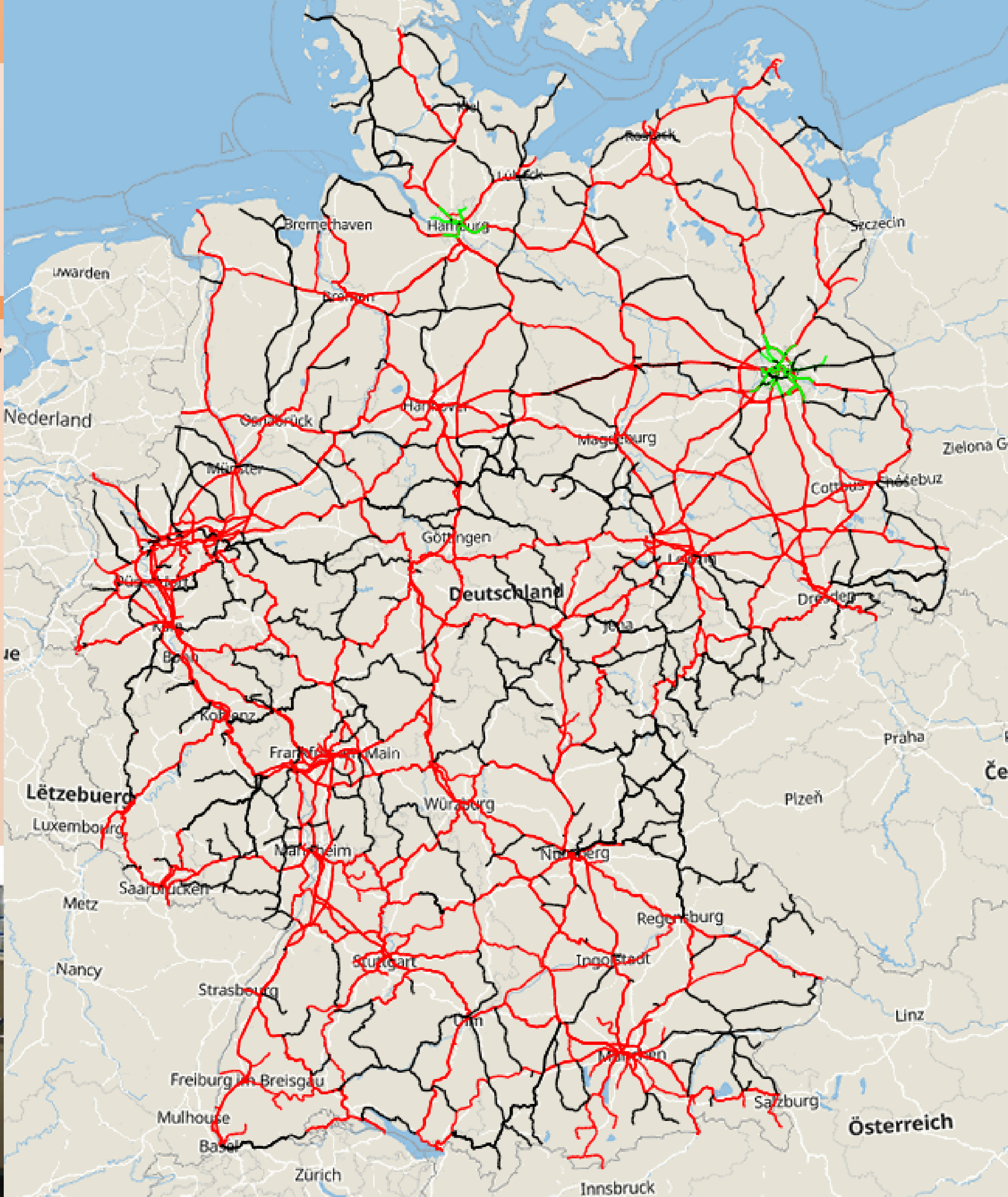
Track-Side Connectivity

- “Being critical” next to all connectivity is wired
- Thus, you can find vast cable trenches along railway tracks
  - Some old, some new
  - And if you look long enough: some open
- In the end it’s a wild mix of copper and fiber
  - Both analog and digital communication
- So, what’s so special?



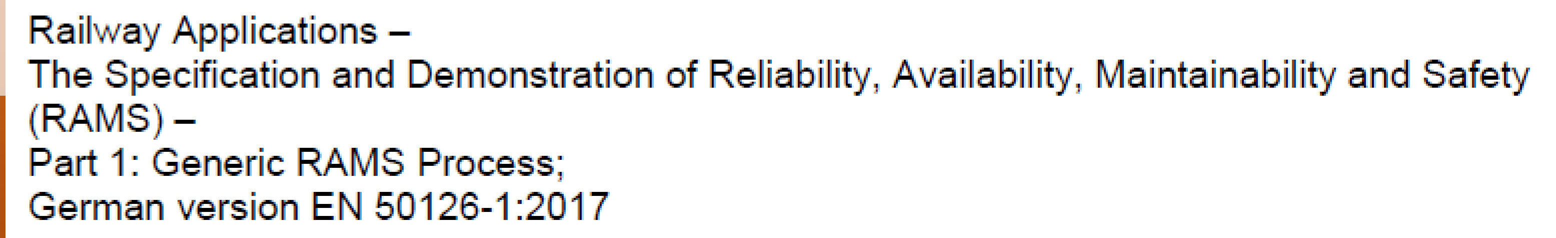
Tracks & Components

- The map shows DB’s own tracks only
    - It should be around 33400km
- There are around 2600 “Stellwerke”
    - Switching stations
    - Some of which are manned, some controlled from central locations
- “Does it scale” is a fun question



Lower Levels

- Switching from dedicated wires into the IP world brings a lot of challenges
  - Engineers have a lot of ideas how to do something like this
- One solution: RaSTA – Rail Safe Transport Application
  - You start by using a processor fulfilling DIN EN 50126-1
    - Fulfilling RAMS
  - Then using UDP, you implement a redundancy layer and implement sessions
  - And then you add the actual protocol on top and make it “sicher” by adding MD4!



Railway Applications –
The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) –
Part 1: Generic RAMS Process;
German version EN 50126-1:2017

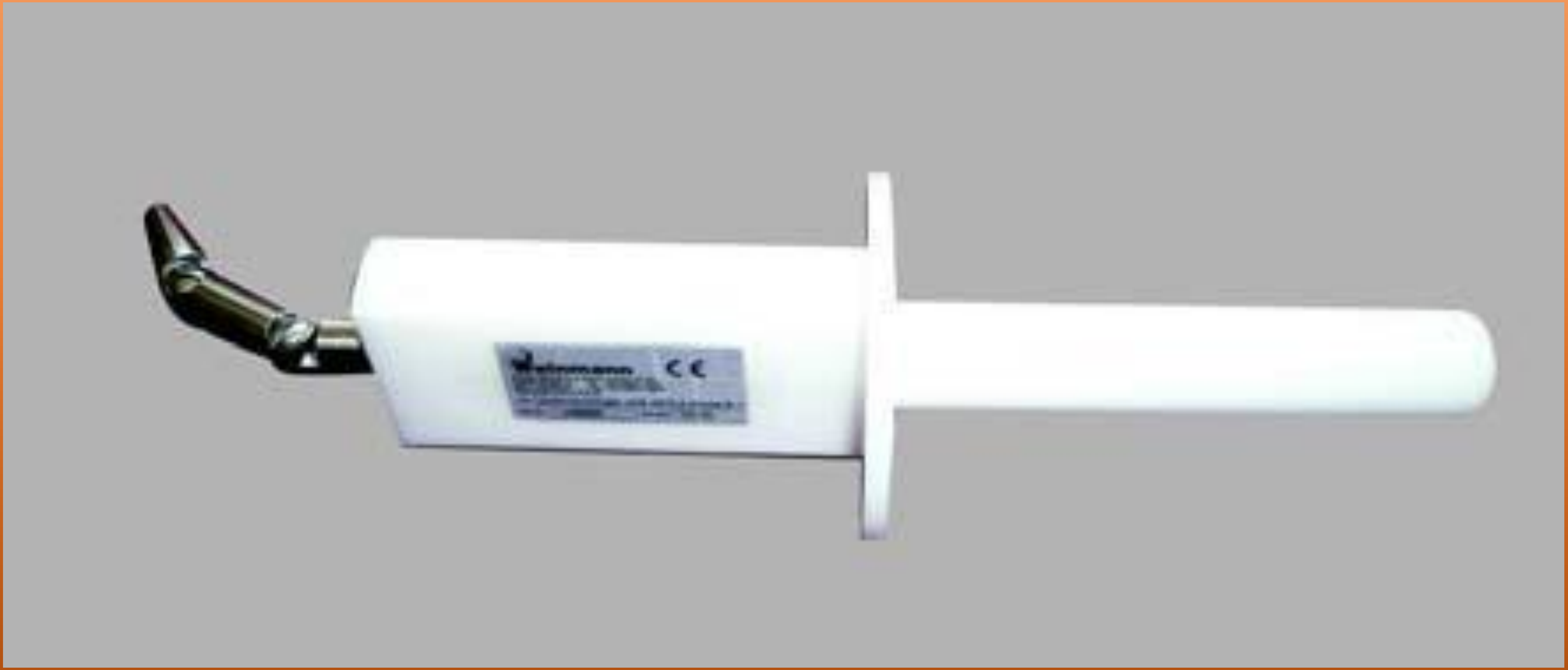
A little issue with the German Language

- In Germany we have the word “Sicherheit”
- Sicherheit ist in Deutschland sehr wichtig
    - “Sicherheit” is very important in Germany
- “Ausfallsicherheit” → usually redundancy
- “Übertragungssicherheit” → usually integrity protection
- “Fingersicher” → Finger-proof
- “Sicherheit” → Security
- “Sicherheit” → Safety

A Random Laugh

- Yes, “Fingersicher” really exists
  - Yes, “Finger-proof” isn’t the best translation :P
- Yes, “Fingersicher” is officially described in a standard
  - VDE-0660-514
- Yes, there is a standard for a standard finger
  - VDE 0470-1

Yes, I have a Picture



Yes, I have a Picture

No this is not a joke
but an insight into safety standards

Safety!

- Engineering has a long history of ensuring safety throughout highly complex processes
  - Nobody may get hurt due to single or double faults
- Most of these systems were developed as standalone or air gapped
  - Using dedicated wires for direct communications
- Thus, bad intent required physical access
- While digitizing and connection systems a lot of the old protocols were simply wrapped with TCP/IP
  - “Problem solved”

Safety through Security

- The concept that in modern systems security is a base necessity is only slowly growing
  - EULYNX – Security, standardization entity behind RaSTA, as only started with it in 2022 after an actual security guy (my former boss) joined the team
- Yet again not specific to the railway sector but to all industrial areas
  - Being able to properly F-up a car while driving via CAN was a known issue, but it took Miller and Valasek to give it some spotlight
- In railway security, there are a few advocates trying to push everything in the right direction

EULYNX

Adding Security

- Adding security to a running system will break it
    - I know we always say it doesn’t, but let's be honest, it’s a rocky path
    - But it’s usually worth the work
- Including security in the development process would be the way to go!
    - Trivial!

Lifespans

- DB's prestigious high-speed train is the ICE
  - Inter City Express
- The ICE 1 hit the tracks 30 years ago and is still running
  - Together with ICE2, ICE3, ICE4 and multiple variants
- The ICE-L was just presented a few weeks ago at InnoTrans
  - The project started around 2015
- This june DB opened bidding for a project on developing the new HGV3.0 (highspeed vehicle)
  - Looking at the ~10year project span of the ICE-L the HGV3.0 would hit the tracks around 2032

Lifespans

- On the vehicle side we're currently looking at around 70 years of potential issues with vehicles
  - The ICE1 is obviously pre-security
    - Built over 30 years ago
  - The ICE-L is pre-OT-security focus
    - If on the tracks for 30 years that'll be 2052
  - The HGV 3.0 is about to be designed with security
    - If on the tracks for 30 years that'll be 2062

What Measures will we need in 40 Years?

- No F***ing clue!
- So, what do we do?
  - Modularization
  - Make sure that the overall system (yes, a train is just a system) is designed in such a way, that the components can be updated (modularization in software) and components can be swapped against newer version (modularization of the system)
- But…
  - Certification

Certification

- The EBA, federal office for railway affairs, makes sure>everything< used in the railway environment is certified
  - Even the walls placed along tracks against noise must be certified for railway use
- While certification keeps up quality, old processes can barely be applied to modern tech
  - Having a whole train certified as an integrated system makes updates really hard
  - Change one part, loose the overall certification…

Eisenbahn-Bundesamt

Certification & Changes

- Changes as is are a challenge, due to the quality requirements from safety
- They become close to impossible, when requiring new certification
  - Worst case: Re-certify after every MS Patch day
    - … nope…
- Yet again, by applying modularization, splitting critical security functions from general features can be a way to ensure that safety-critical functions always work
  - Worth a try…
- There is a bypass: If the manufacturer takes responsibility, they can swap a part…

Development

- As in all areas, “digitalization” and “The BlockChain” and “AI” are finding their way into the railway world
  - Some being smart choices, some being, well….”BINGO”
- Condition based and predictive maintenance for example are trivial approaches and result in good output
  - But require regular logs from a vehicle
- Moving forward to a “Digital Twin” offer even deeper insights
  - But live log / bus / status / data streams from a vehicle become a necessity
  - Thus the vehicle will be online 24/7

UIC Plug

- Most vehicles and their carriages are connected using special cables
  - Initially 13 pins, including a few in reserve
- Each vehicle has two sockets to create a redundant coupling
- Initially being designed for trivial use cases: controlling lights, PA/sound, door control
  - Defined by UIC memo 568
- Free wires were used for custom features
  - I.e. DB implemented time-multiplexed coms for controlling a locomotive from the other side of the train in 1974/1975 (“ZWS”) on pins 17/18
    - For trains going back and forth without turning

UIC Plug

- The plugs were expanded in UIC 558 to a compatible 18 pin version
  - Expanded to support a full TCN – Train Communication Network by supporting signal lines for WTB – Wire Train Bus
  - Based on RS-485, 1Mbit/s on pins 17/18
- In 2017 it was updated again to IRS 50558 to a 24 pin cable
  - Pins 17/18 were removed and replaced by ethernet
  - Now supports the ETB – Ethernet Train Bus
  - Full IP :)
- Now most vehicles have both a 18 pin and a 24 pin socket
  - Well, two each actually…redundancy

Ideas & Sources

- Feeling like a very closed eco-system, ideas and solutions often come from within the railway eco-system
- As such they will have a strong focus on safety and show hints of security in early stages
- Other approaches come from i.e. the car industry
  - Which openly said is also still learning security
- Even though they exist, good, new, and actually secure products feel extremely rare

Railway in General

- Having specific standards, and references, and individual approaches, and an own federal office many components are specific to railway
  - Partially a special set of firmware, partially even specific hardware
- As with many topics, being a segregated and traditional ecosystem, rail tends to “re-invent the wheel”
  - Instead of following known approaches, they do things themselves
  - They’ll be very similar, buuuut different enough…
- Thus, it also lacks a few “crazy new ideas” in certain situations
  - It’s a very conservative environment
    - Well, making wrong decisions will end in people dying. . . .

Security in Railway

- A lot of modern security was driven by conferences by this one, publications, hacking and sharing
- The security community as made sure, that security as in most parts become part of the IT world
  - Even though some might not live it, them having to make up a lot of excuses not do any security is also a good sign
- Looking at 30-year-old vehicles, security in railway is still on the rise
  - And being “special” with the same fights we’ve had in the IT world

Preventive Work

- IT has learned from WannaCry, Conficker, various hacks and is still learning from ransomware
  - Thus, security in most areas is moving forward
- Automotive also had its incidents
- Rail has learned how import safety is the hard way and still is…
  - We’re trying to make sure, that rail won’t have to learn the necessity for security the hard way…..

Being Special

- It’s often hard to explain why measures are necessary
- There are only few references for the question “…but does it affect >us<!?”
- Not being able to patch in short time windows makes sharing really hard
- There aren’t a lot of others to properly learn from
  - In the specific industry
- There is next to no external pressure to apply security
  - With exceptions for critical infrastructure
    - Which are partially good, partially not…

Hacking Rail

- A LOT of fun
  - As always when you get to hack something nobody as ever touched
- Can be overwhelming concerning potential impact and resulting risk
  - Especially if one as a tester takes things personally
- Partially boring, because you can easily drown in low hanging fruits
- Very rewarding, as you can actually still change something

Hardening Rail

- Very frustrating, as processes and cycles are very long
- Scary, when seeing what others implement as “state of the art”
- Very demanding as non-security personnel relies heavily on security
- Challenging if you actually want to give useable / pragmatic recommendations
  - I personally hate these “Do security!” recommendations, without input on the how
- Offers work for many years, until security has become part of railway DNA

Why am I here Today?

- Share an insight into something I’ve grown very passionate about
- Get more people into thinking about rail and industrial security
- Teach rail that sharing is caring
  - And the hacking community is nice people
- Teach the hacking community, to keep a safe distance
  - Rail isn’t scaring off hackers because they want to hide issues, but because they understand certain implications
- Create some more transparency

Questions?

Brian Butterly

@BadgeWizard

brian@security-bits.de

Sources

3: my own

4: Von Chianti - Eigenes Werk, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=54073883

5: Von Olga Ernst &amp; Hp.Baumeler - Eigenes Werk, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=67943062

6: Von William M. Connolley (Diskussion · Beiträge) - Diese Datei hat keine Quelle.Bitte ergänze die Dateibeschreibung und gib eine Quelle an.Übertragen aus en.wikipedia nach Commons mithilfe des CommonsHelper / PushForCommons.Eigenes Werk, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=1233520

6: Public Domain, https://commons.wikimedia.org/w/index.php?curid=49836

6: By John T. Daniels - https://commons.wikimedia.org/w/index.php?curid=6224251

7: Von Roger Green from BEDFORD, UK, derivative work Lämpel - Airbus A380, CC BY 2.0, https://commons.wikimedia.org/w/index.php?curid=65623145

7: Von u/Kruzat modified by Periwinklewrinkles - https://imgur.com/a/tp7JG6P but modified, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=84985335

7: Von Martin Lechler - Eigene Aufnahme mit Handy, Gemeinfrei, https://commons.wikimedia.org/w/index.php?curid=44976930

8: Von Andre_de - Eigenes Werk, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=27550812

8: Von Falk2 - Eigenes Werk, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=71029261

8: Von Funkruf - selbst fotografiert aus der ESTW-Simulation Neuenhagen von B. Schneider, CC-by-sa 2.0/de, https://de.wikipedia.org/w/index.php?curid=3355398

9,10: Google Map Screenshot

11: https://wiki.openttd.org/de/Manual/Bahnhof

11: Von Kilian Salzer, Attribution, https://commons.wikimedia.org/w/index.php?curid=7649602

12: Von Sebastian Terfloth - Selbst fotografiert, CC BY-SA 2.0 de, https://commons.wikimedia.org/w/index.php?curid=31669093

12: https://de.wikipedia.org/wiki/Eisenbahnsignale_in_Deutschland#/media/Datei:Railway_signal.jpg

12: Von MdE aus der deutschsprachigen Wikipedia (→ Benutzerseite auf Commons) - Eigenes Foto, CC BY-SA 3.0 de, https://commons.wikimedia.org/w/index.php?curid=3679782

13: my own ☺

14: https://geovdbn.deutschebahn.com/isr

14: https://fahrweg.dbnetze.com/fahrweg-de/kunden/betrieb

18,19: https://www.weinmann-online.de/produkt/elektrische-sicherheit-zugangssonden-nach-vde-0470/

21: https://eulynx.eu/

23: Von S. Terfloth (Sese Ingolstadt at de.wikipedia) - selbst fotorafiert, CC BY-SA 2.0 de, https://commons.wikimedia.org/w/index.php?curid=16312116

24: Von Martin Lechler - Eigene Aufnahme mit Handy, Gemeinfrei, https://commons.wikimedia.org/w/index.php?curid=44976930

25: https://www.eba.bund.de/DE/home_node.html

29,30: my own

34: Von Nils Fretwurst - Eigenes Werk, Gemeinfrei, https://commons.wikimedia.org/w/index.php?curid=359420

34: Von Feuerwehr Mittelkalbach - Feuerwehr Mittelkalbach (http://www.feuerwehr-mittelkalbach.de/), CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=4008465

34: Gemeinfrei, https://commons.wikimedia.org/w/index.php?curid=474858

34: Von Sûreté du Québec - https://twitter.com/sureteduquebec/status/353519189769732096/photo/1, CC BY-SA 1.0, https://commons.wikimedia.org/w/index.php?curid=27152159