永不出軌

守護關鍵基礎設施中的軌道安全

Mars Cheng, Senior Threat Research Manager

Jair Chen, Sr. Threat Researcher

PSIRT and Threat Research, TXOne Networks Inc.

April 25, 2025 @CYBERSEC 2025

Mars Cheng and Jair Chen

Senior Threat Research Manager, PSIRT and Threat Research at TXOne Networks Inc.

- Executive Director of the Association of Hackers in Taiwan (HIT/HITCON)
- ICS/SCADA systems, malware analysis, threat intelligence and hunting, blue team, and enterprise security
- Delivered over 60 presentations at international cybersecurity conferences, including Black Hat USA, Europe, and MEA, RSA Conference, DEF CON, CODE BLUE, FIRST, HITB, HITCON, Troopers, NOHAT, SecTor, S4, SINCON, ROOTCON, among others.
- Successfully organized several notable HITCON events, such as the HITCON CISO Summit in 2024 and 2023, HITCON PEACE 2022, and HITCON 2021 and 2020.

Sr. Threat Researcher, PSIRT and Threat Research at TXOne Networks Inc.

- Jair Chen is a senior threat researcher of TXOne Networks PSIRT and Threat Research team. He specializes in building threat intelligence systems and tracking potential attack organizations as well as emerging attack techniques.
- Jair's research spans the detection and defense against malicious behaviors in virtualization environments, on-premises systems, and cloud environments. Jair has developed an enterprise-grade APT behavior analysis engine that uncovers hidden hacker attacks by correlating suspicious behaviors across multiple dimensions.

Outline

- Introduction to Railway Cybersecurity
- Potential Threats in Railway Industry Ecosystem
- Insights on Remote Hijacking of Railroads
- Takeaways

Outline

- Introduction to Railway Cybersecurity
  - A Common Yet Often Overlooked Infrastructure: Railways
  - Cyber Attacks on the Global Railway Sector
  - Business Trends in Railway Cybersecurity
- Potential Threats in Railway Industry Ecosystem
- Insights on Remote Hijacking of Railroads
- Takeaways

A Common Yet Often Overlooked Infrastructure

Railways

https://grou CSMonitor/album?id=28

Cyber Attacks on Railway Systems

Increase by 220% over the last five years

https://www.secureworld.io/industry-news/railway-cyber-attacks

Cyber Attacks on the Global Railway Sector - MEA

Iran - Tehran
Jul 2021

https://amwaj.media/media-monitor/iran-s-government-organisations-hit-by-multiple-cyberattacks

Cyber Attacks on the Global Railway Sector - EU

BBC

Home News Sport Business Innovation Culture Arts Travel Earth Video Live

Some trains were brought to a standstill for a few hours

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.

Polish - Szczecin

Aug 2023

txOne networks

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

Cyber Attacks on the Global Railway Sector - EU

Russian are accused of wanting to sabotage trains, including here in Prague EPA-EFE/MARTIN DIVISEK

News

5 April 2024

‘Russia trying to sabotage European railways,’ says Czech transport minister

Czechia, Baltic States, Romania

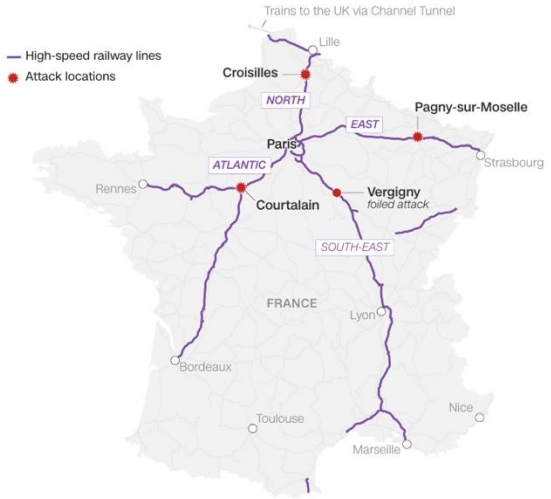
Apr 2024

https://brusselssignal.eu/2024/04/russia-trying-to-sabotage-european-railways-says-czech-transport-minister/

Cyber Attacks on the Global Railway Sector - Worldwide

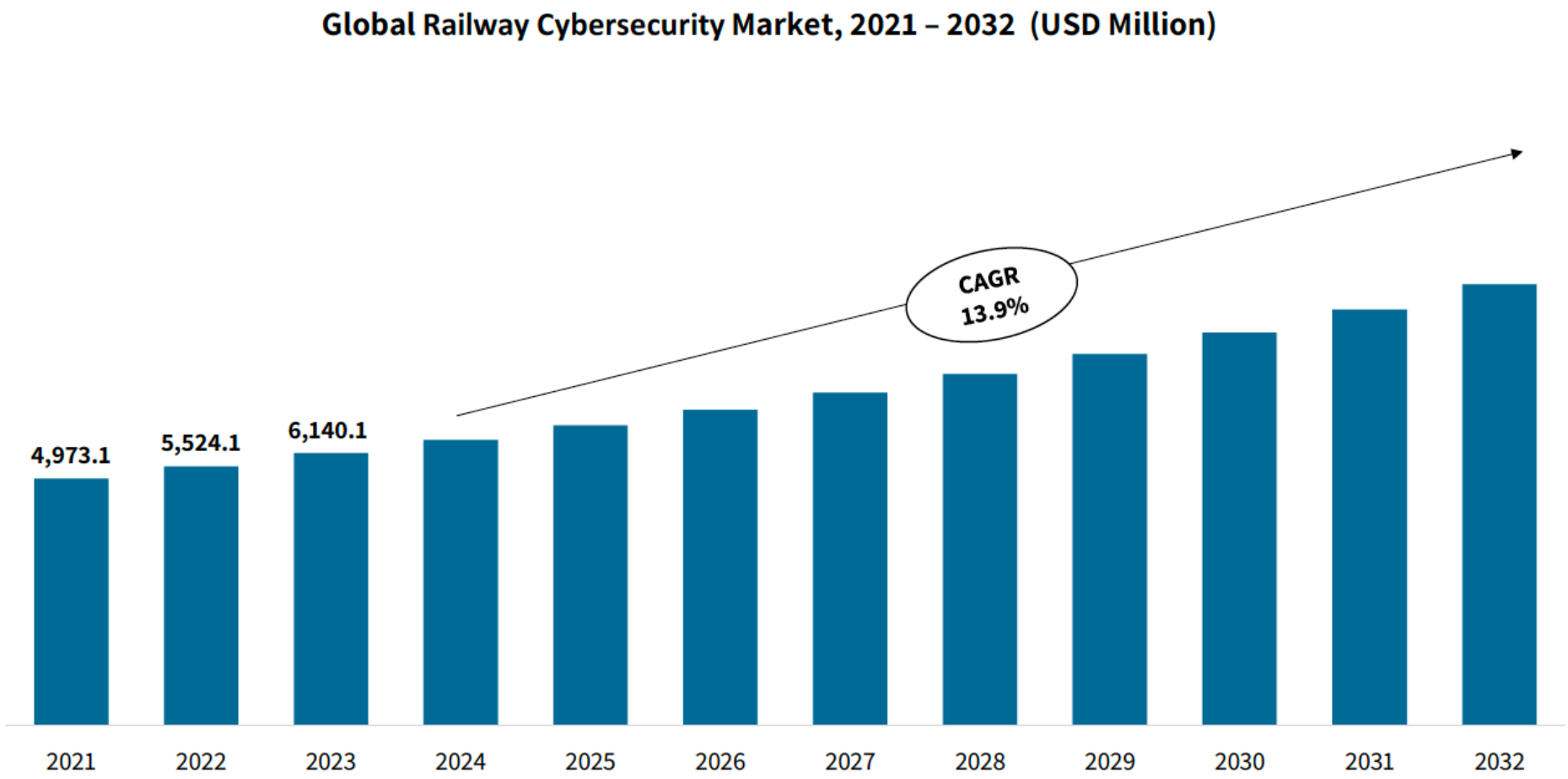
USA - Ohio
Feb 2023

France - Paris
Aug 2024



Japan - Tokyo
May 2024

Business Trends in Railway Cybersecurity – Global Market



https://www.gminsights.com/industry-analysis/railway-cybersecurity-market

Business Trends in Railway Cybersecurity – by Component

Segment	2021	2022	2023
Passenger Trains	2,293.1	2,549.9	2,837.3
Freight Trains	1,570.5	1,736.8	1,921.8
Metro/Monorail	1,109.5	1,237.4	1,380.9
Total	**4,973.1**	**5,524.1**	**6,140.1**

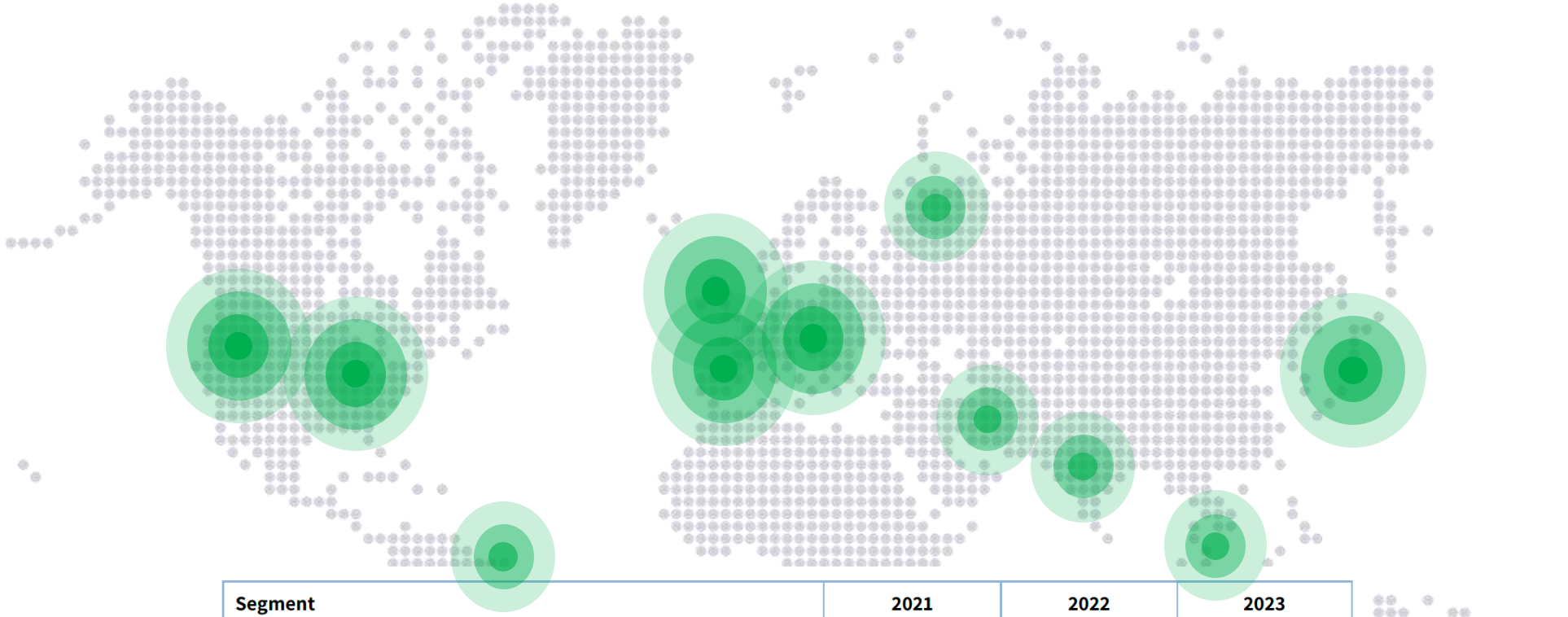
Source: Global Market Insights, Paid Databases, Primary Research

Segment	2021	2022	2023
Solution	3,347.9	3,712.2	4,118.8
Services	1,625.2	1,811.9	2,021.3
Total	**4,973.1**	**5,524.1**	**6,140.1**

Source: Global Market Insights, Paid Databases, Primary Research

https://www.gminsights.com/industry-analysis/railway-cybersecurity-market

Business Trends in Railway Cybersecurity – by Region



Segment	2021	2022	2023
North America	1,263.2	1,401.5	1,555.9
Europe	1,486.5	1,652.3	1,837.7
Asia Pacific	1,736.1	1,939.0	2,166.8
Latin America	279.0	305.5	334.6
MEA	208.4	225.9	245.0
Total	**4,973.1**	**5,524.1**	**6,140.1**

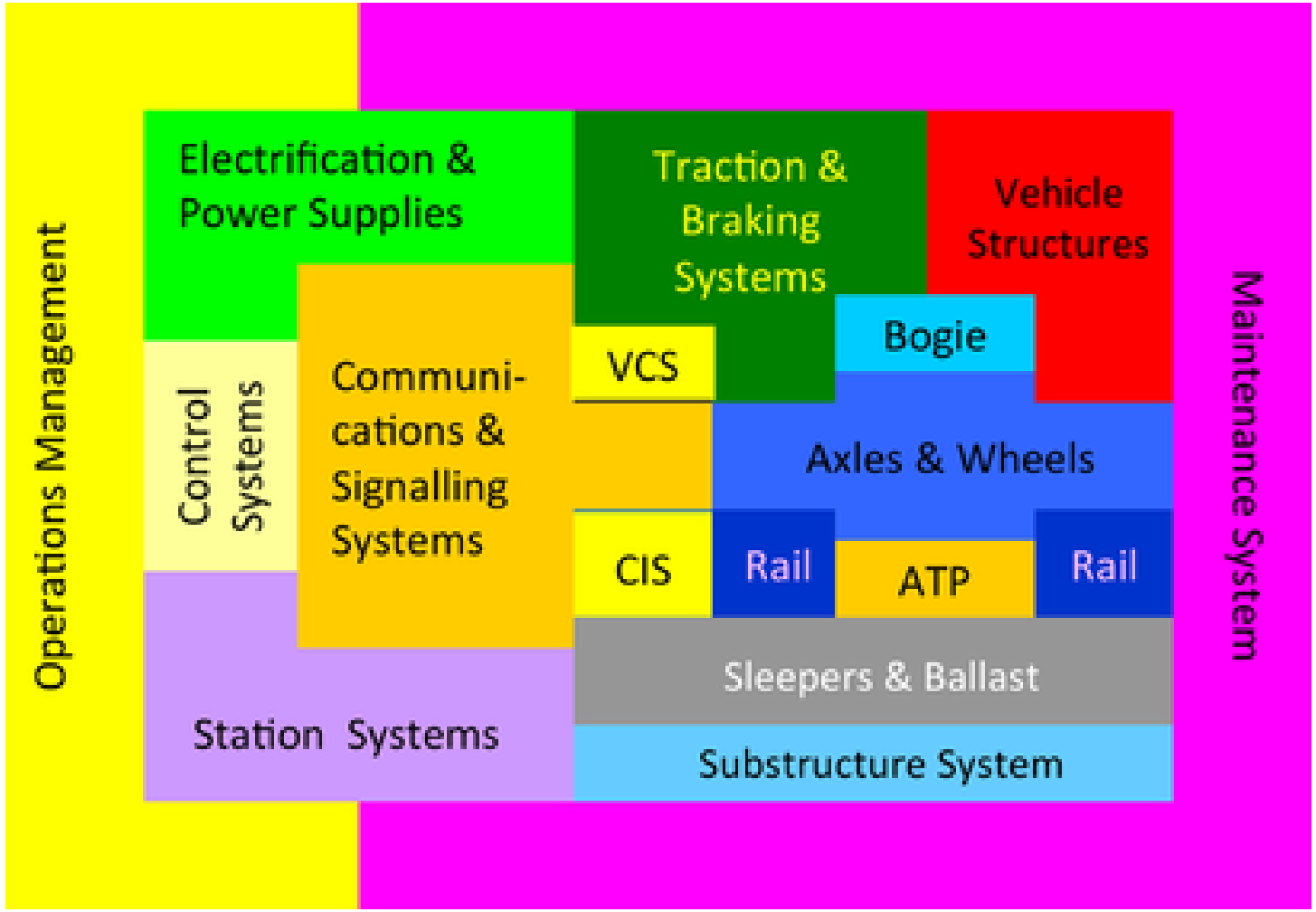
Source: Global Market Insights, Paid Databases, Primary Research

https://www.gminsights.com/industry-analysis/railway-cybersecurity-market

Outline

- Introduction to Railway Cybersecurity
- Potential Threats in Railway Industry Ecosystem
  - Overview of Railway Industry Ecosystem
  - Potential Threats in Train Stations
  - Potential Threats in Control Center
- Insights on Remote Hijacking of Railroads
- Takeaways

Railway as a System – A Visual Representation



http://www.railway-technical.com/

Railway Industry Ecosystem Overview

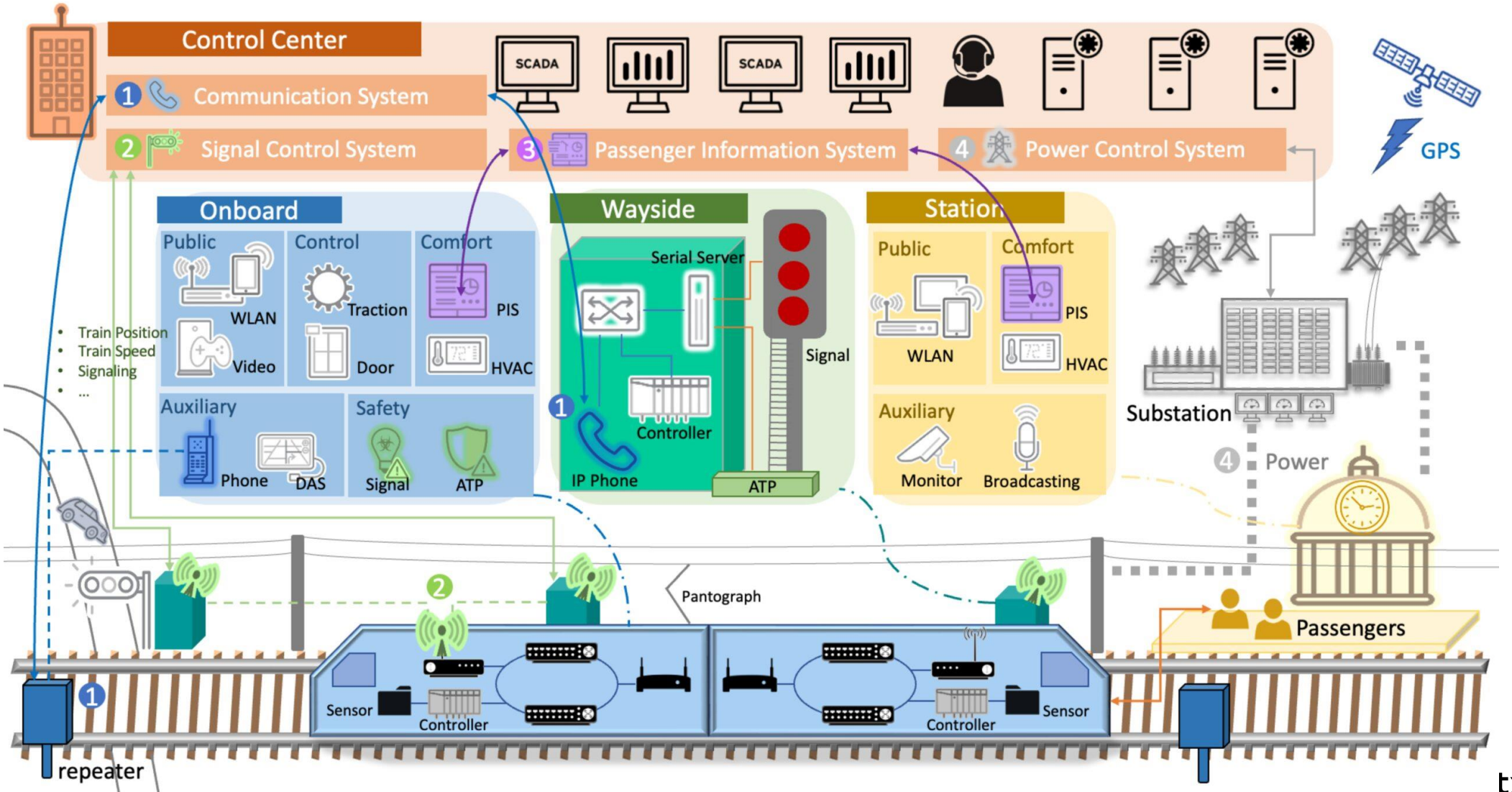
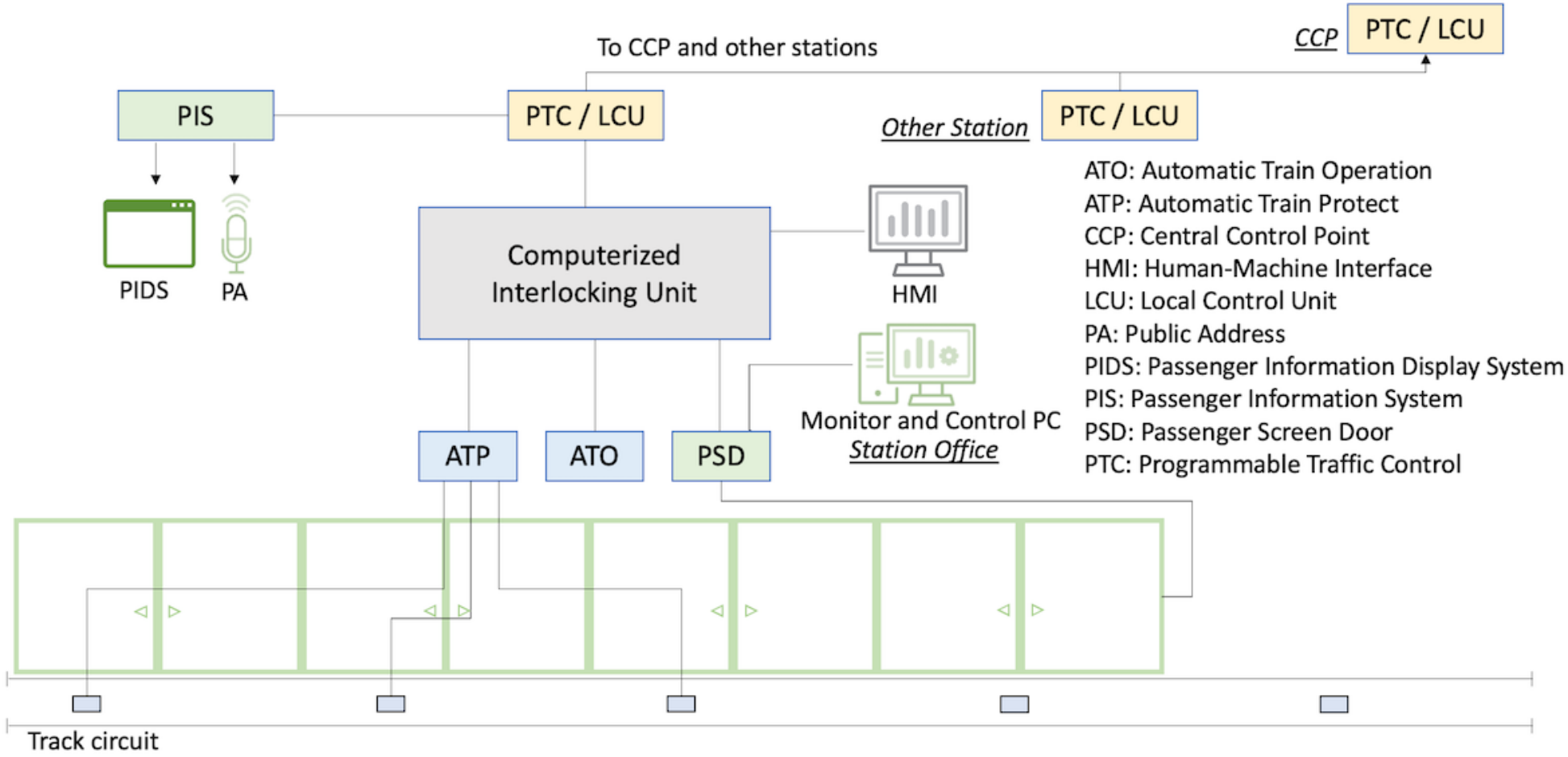
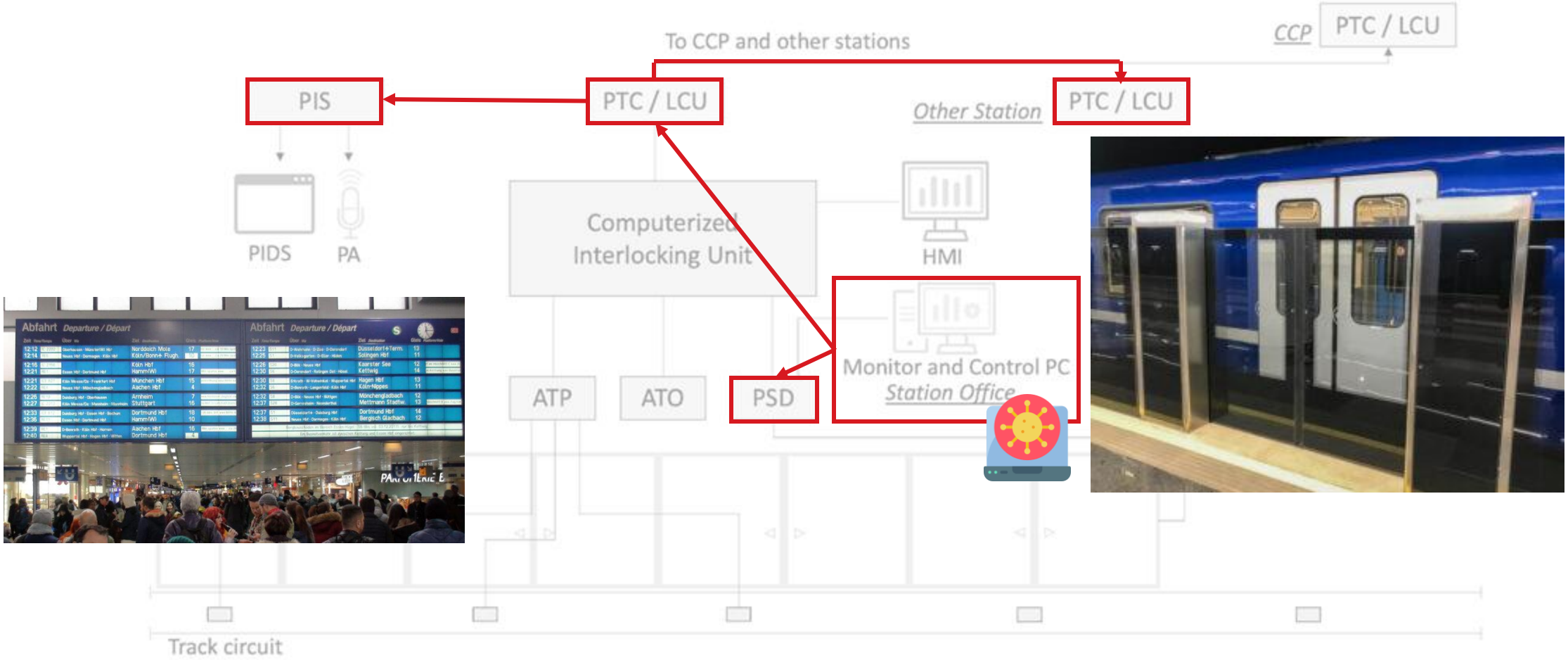


Illustration of Railway Station Architecture



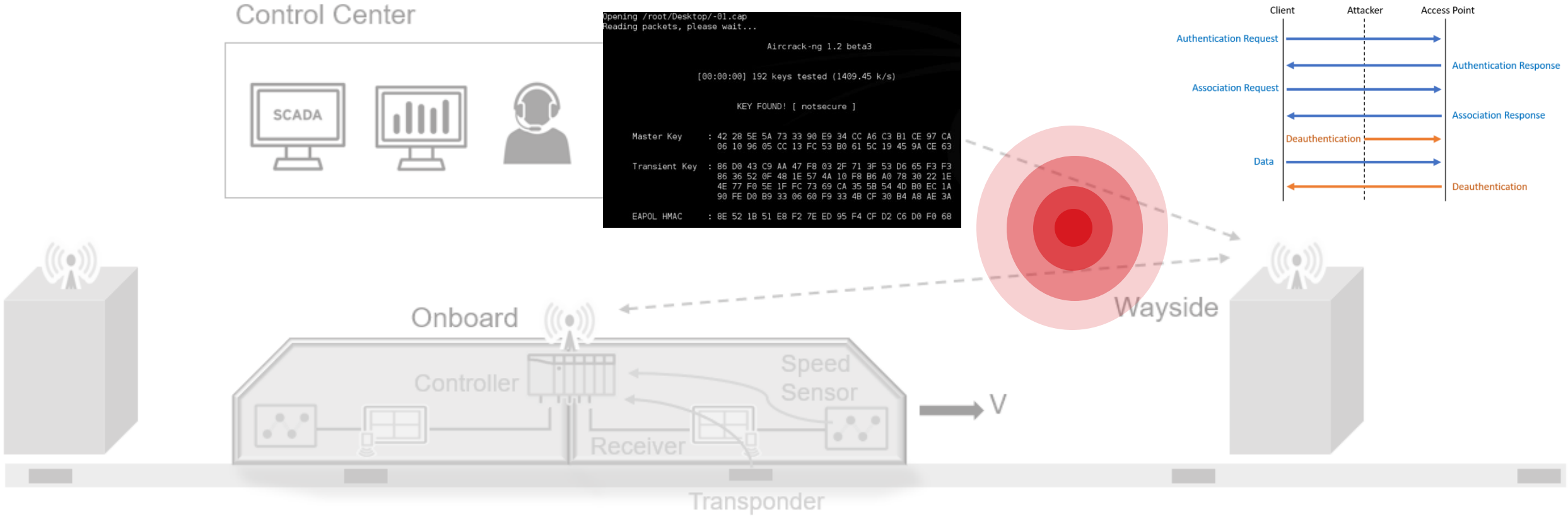
Potential Threats in Railway Station



When infected devices are brought to station office, PSD and PIS could be at risk

Illustration of Railway Control Center

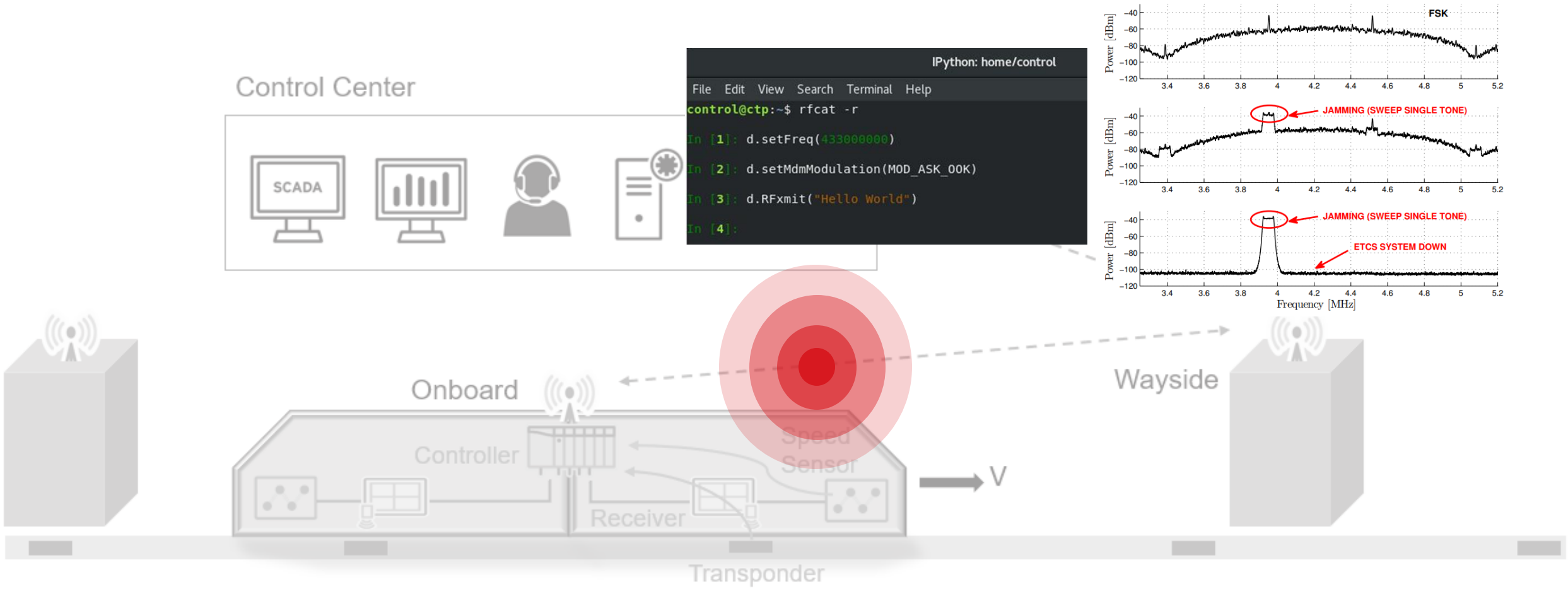
Potential Threats in Control Center - WLAN



Vulnerabilities in WLAN transmission will cause CBTC communication disruption

https://www.researchgate.net/publication/283354063_An_Automated_Approach_to_Detect_Deauthentication_and_Disassociation_Dos_Attacks_on_Wireless_80211_Networks

Potential Threats in Control Center - Transponder



Transponder interference attacks prevent trains from receiving location information

https://www.researchgate.net/publication/282907734_Cyber_Security_Analysis_of_the_European_Train_Control_System

Outline

- Introduction to Railway Cybersecurity
- Potential Threats in Railway Industry Ecosystem
- Insights on Remote Hijacking of Railroads
  - History and Technology of Air Brakes
  - EOT (End-of-Train Telemetry) / HOT (Head-of-Train Telemetry)
  - Deep Dive into EOT packet
- Takeaways

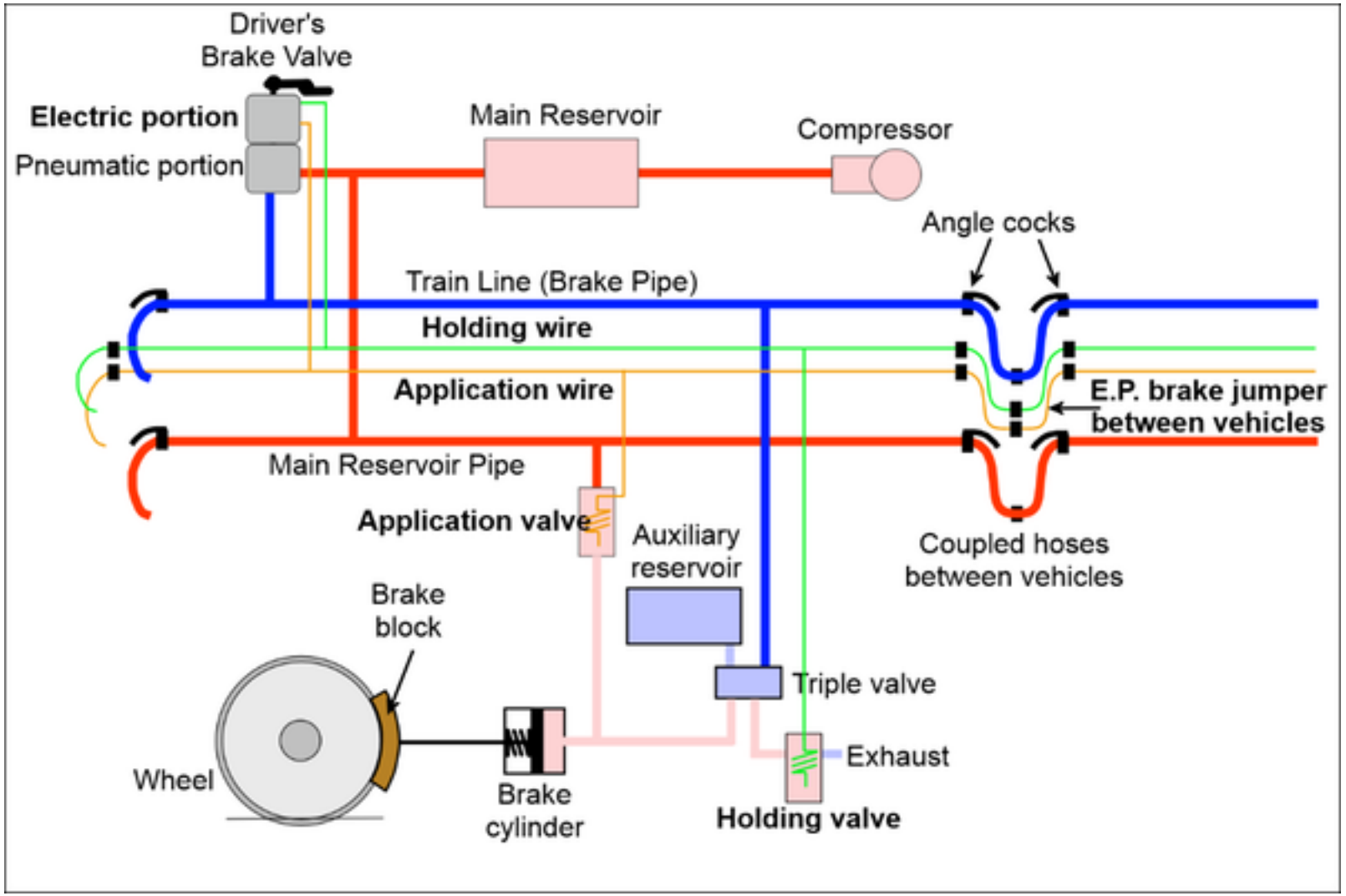
Brakeman of Railway Vehicle

A "PICNIC."

Brakeman was abolished in1920s with introduction of air brakes, which can be controlled by engine driver

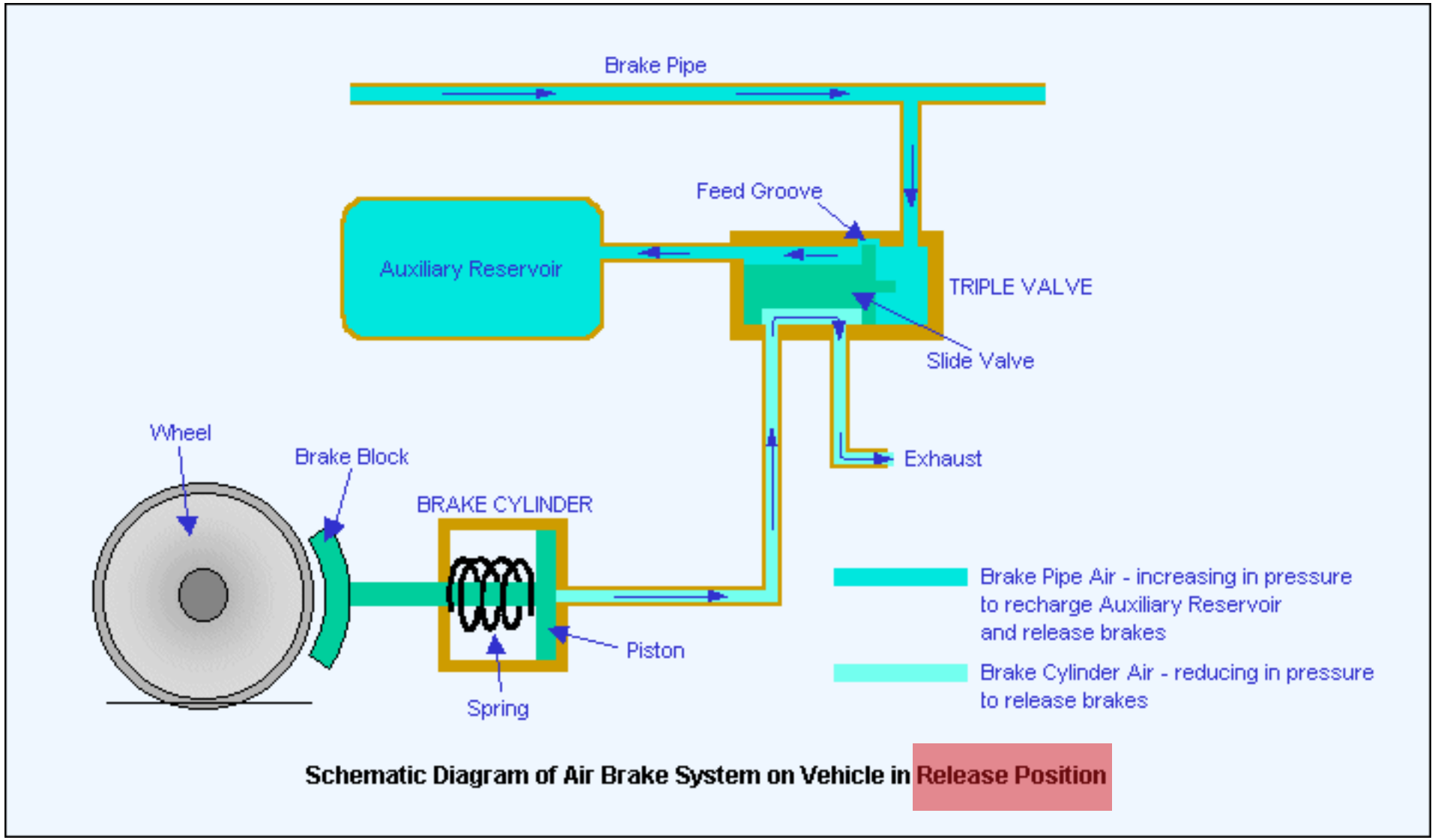
https://en.wikipedia.org/wiki/Brakeman

Air Brake of Railway Vehicle



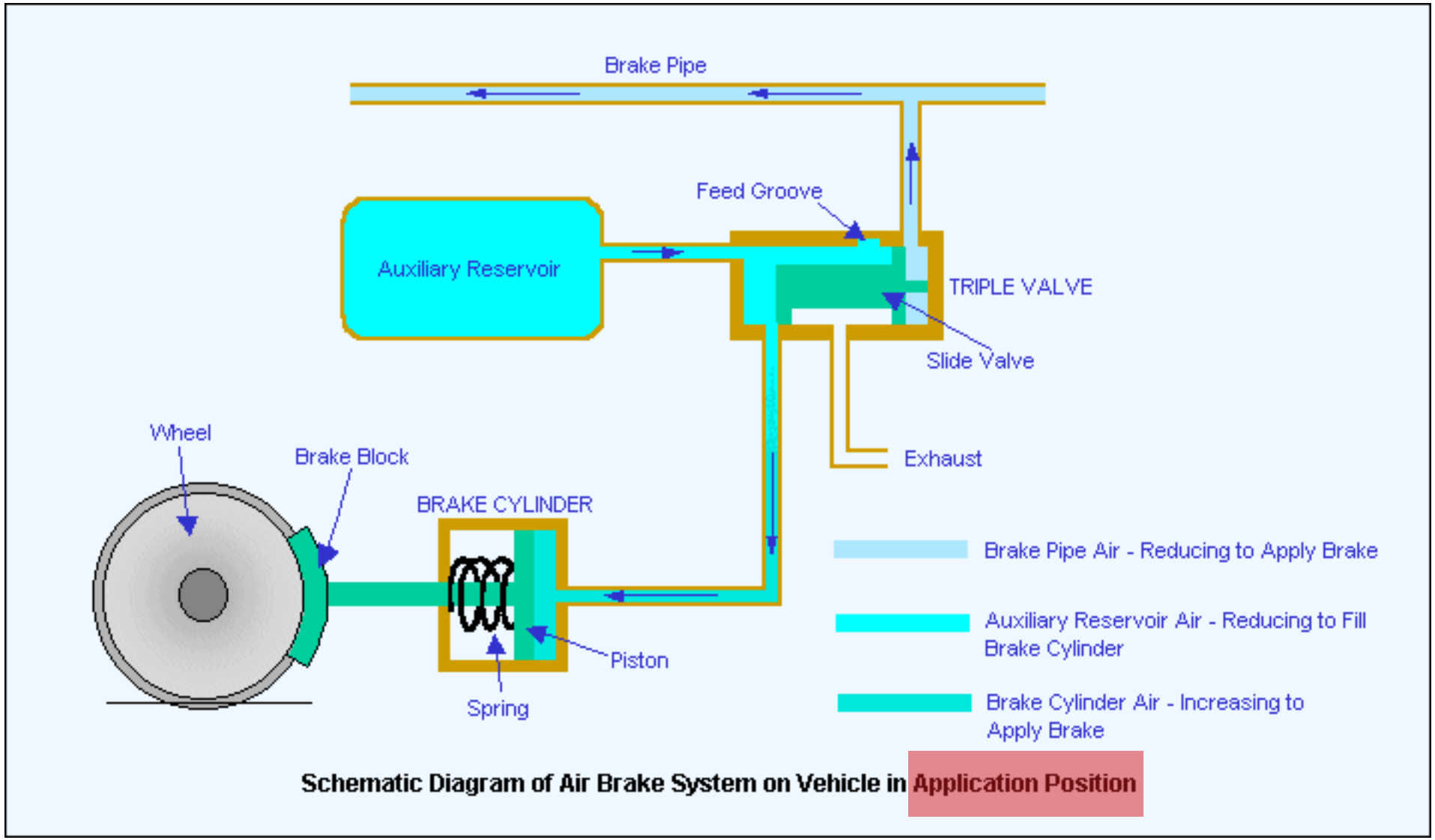
http://www.railway-technical.com/trains/rolling-stock-index-l/train-equipment/brakes/electro-pneumatic-brakes-d.html

Air Brake of Railway Vehicle



http://www.railway-technical.com/trains/rolling-stock-index-I/train-equipment/brakes/

Air Brake of Railway Vehicle



http://www.railway-technical.com/trains/rolling-stock-index-I/train-equipment/brakes/

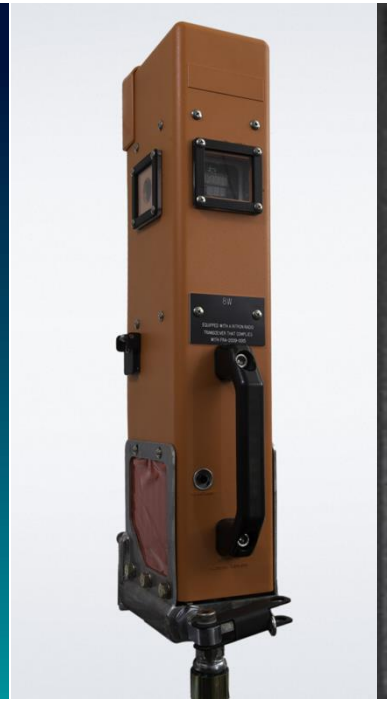
Monitoring Brake Pressure

The caboose was replaced in the 1980s by the EOT, a device attached to the end of the train

https://en.wikipedia.org/wiki/Caboose

EOT / HOT - Device

- Two-part system:
  - End-of-Train Device (EOT) attached to last car
  - Head-of-Train Device (HOT) in locomotive



https://www.inteletrack.co.za/PageEOTs.htm

EOT / HOT - Installation

- Modern units allow full-duplex two-way communication
  - Control Data 452.9375 MHz
  - Telemetry Data 457.9375 MHz

https://www.inteletrack.co.za/PageEOTs.htm

EOT / HOT - Function

- Pressure + Status
- ARM Request
- ARM Confirm
- Communication Test Reply
- Position

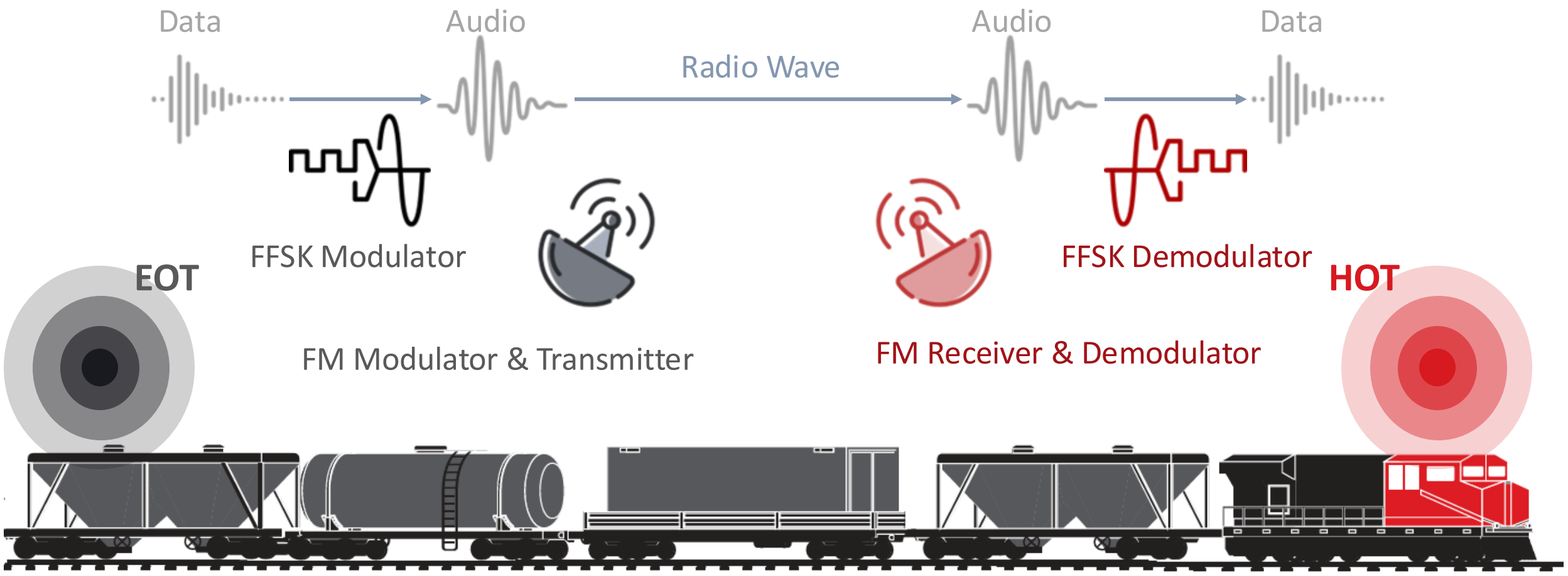
- ARM Reply
- Communication Test
- Emergency Command

EOT

HOT

https://assets.new.siemens.com/siemens/assets/api/uuid:f90685a5-3bec-49fc-8bfe-16d403032bed/Trainguard-EOT-Instruction-and-Installation-Manual-OBE-00-17-06A.pdf

Fast Frequency Shift Keying (FFSK)



Two-stage Modulation and demodulation

EOT Packet Format

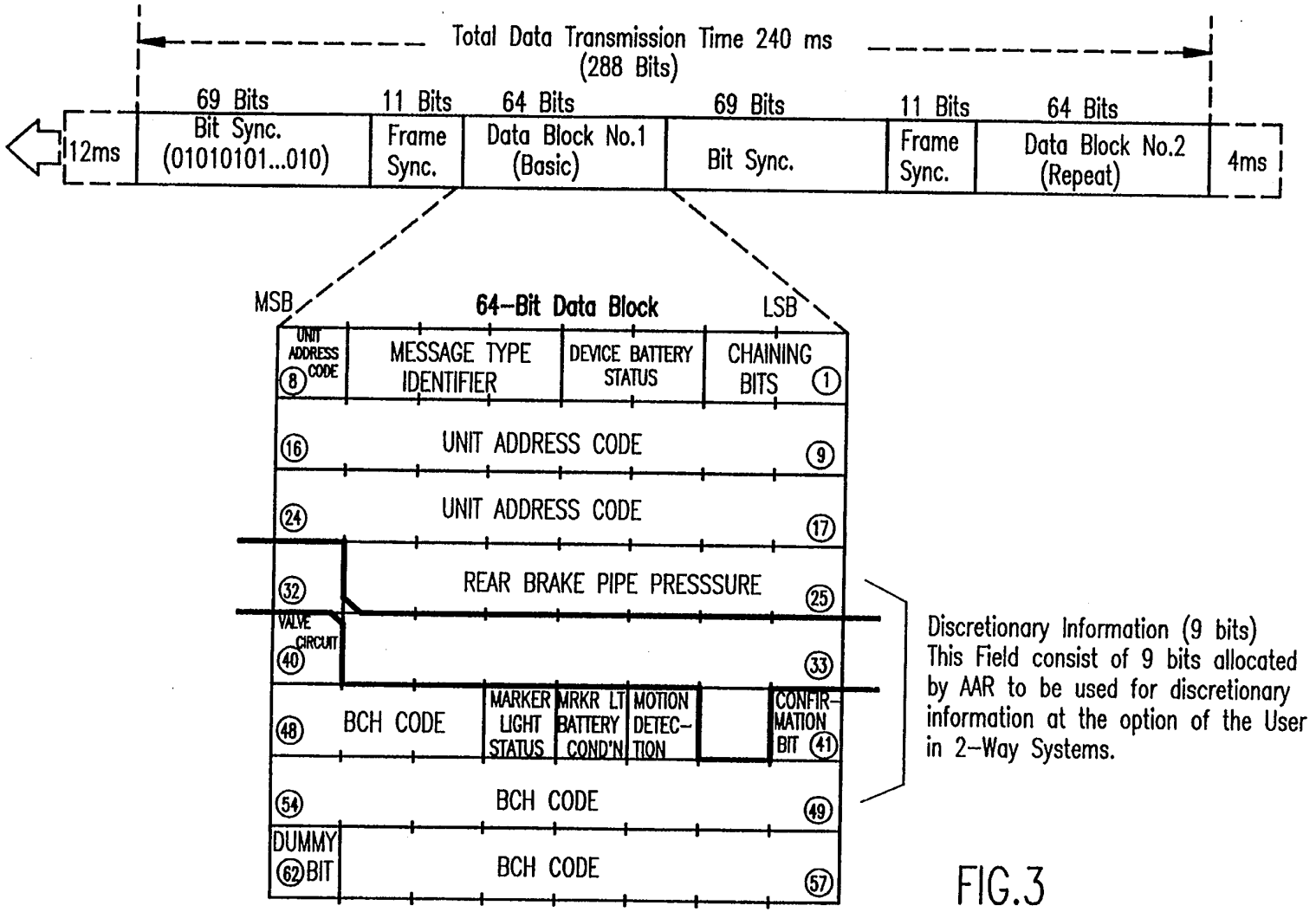


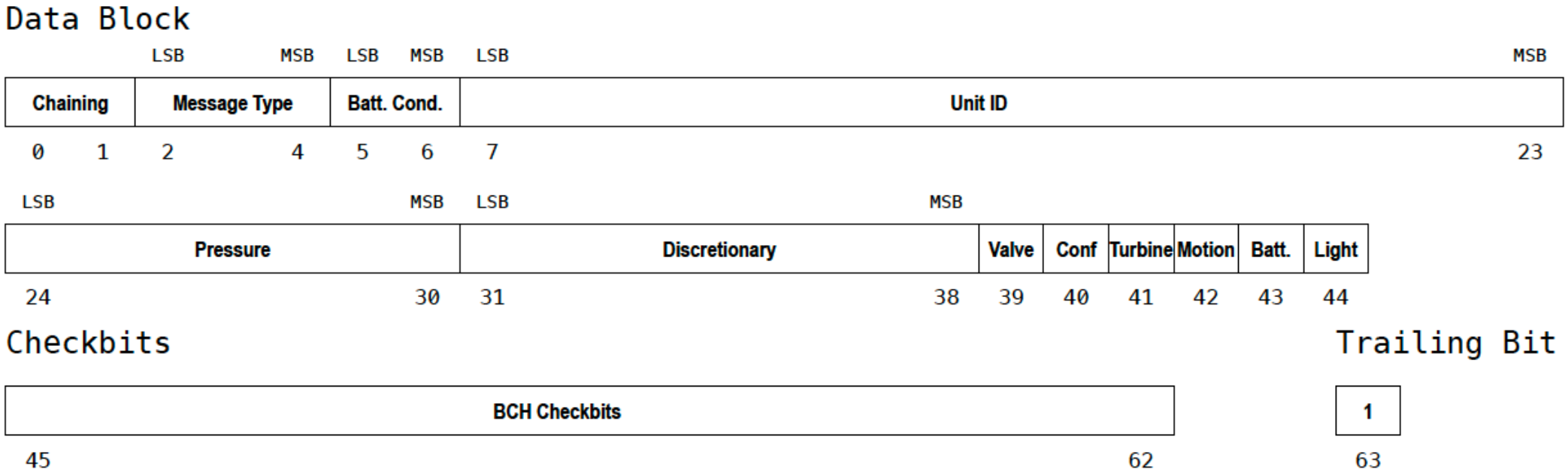
FIG.3

txOne networks

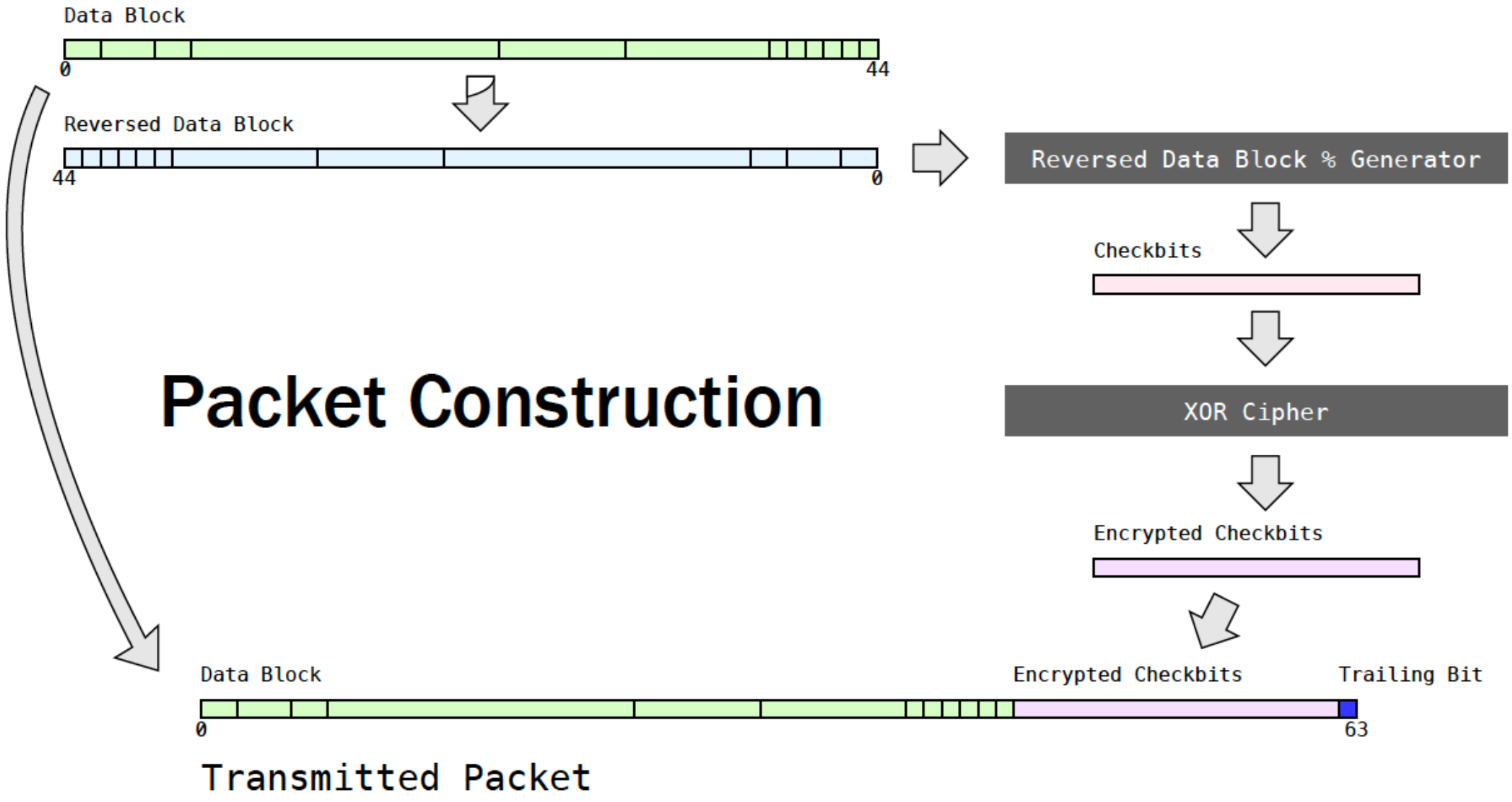
https://patents.google.com/patent/US5374015A/en

BCH encoding

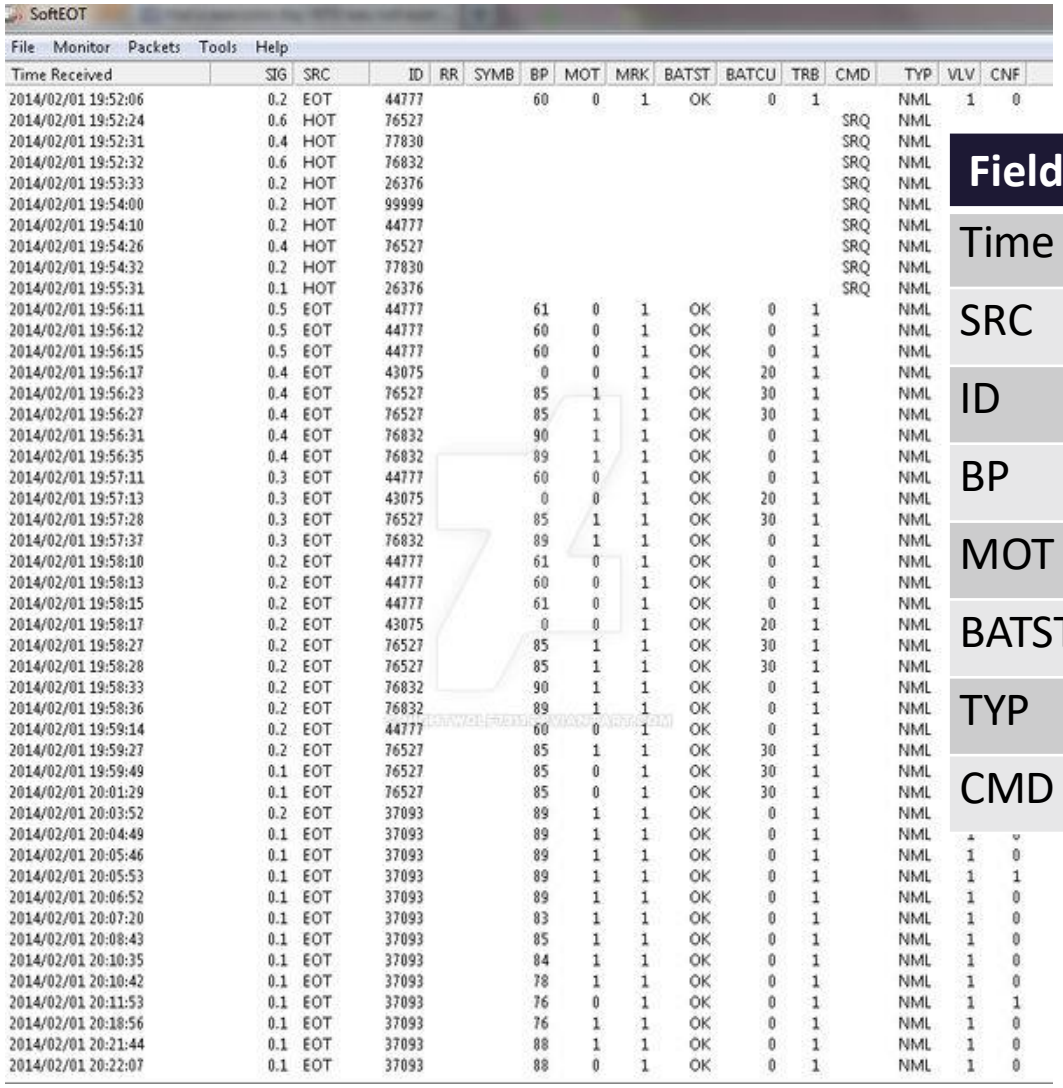
- BCH code is of (63, 45) Type
- g(x) = (x18+x17+x16+x15+x9+x7+x6+x3+x2+x+1) = 1111000001011001111



Packet Construction



EOT Packet Analysis



SoftEOT

File Monitor Packets Tools Help

Time Received	SIG	SRC	ID	RR	SYMB	BP	MOT	MRK	BATST	BATCU	TRB	CMD	TYP	VLV	CNF
2014/02/01 19:52:06	0.2	EOT	44777			60	0	1	OK	0	1		NML	1	0
2014/02/01 19:52:24	0.6	HOT	76527									SRQ	NML		
2014/02/01 19:52:31	0.4	HOT	77830									SRQ	NML		
2014/02/01 19:52:32	0.6	HOT	76832									SRQ	NML		
2014/02/01 19:53:33	0.2	HOT	26376									SRQ	NML		
2014/02/01 19:54:00	0.2	HOT	99999									SRQ	NML		
2014/02/01 19:54:10	0.2	HOT	44777									SRQ	NML		
2014/02/01 19:54:26	0.4	HOT	76527									SRQ	NML		
2014/02/01 19:54:32	0.2	HOT	77830									SRQ	NML		
2014/02/01 19:55:31	0.1	HOT	26376									SRQ	NML		
2014/02/01 19:56:11	0.5	EOT	44777			61	0	1	OK	0	1		NML		
2014/02/01 19:56:12	0.5	EOT	44777			60	0	1	OK	0	1		NML		
2014/02/01 19:56:15	0.5	EOT	44777			60	0	1	OK	0	1		NML		
2014/02/01 19:56:17	0.4	EOT	43075			0	0	1	OK	20	1		NML		
2014/02/01 19:56:23	0.4	EOT	76527			85	1	1	OK	30	1		NML		
2014/02/01 19:56:27	0.4	EOT	76527			85	1	1	OK	30	1		NML		
2014/02/01 19:56:31	0.4	EOT	76832			90	1	1	OK	0	1		NML		
2014/02/01 19:56:35	0.4	EOT	76832			89	1	1	OK	0	1		NML		
2014/02/01 19:57:11	0.3	EOT	44777			60	0	1	OK	0	1		NML		
2014/02/01 19:57:13	0.3	EOT	43075			0	0	1	OK	20	1		NML		
2014/02/01 19:57:28	0.3	EOT	76527			85	1	1	OK	30	1		NML		
2014/02/01 19:57:37	0.3	EOT	76832			89	1	1	OK	0	1		NML		
2014/02/01 19:58:10	0.2	EOT	44777			61	0	1	OK	0	1		NML		
2014/02/01 19:58:13	0.2	EOT	44777			60	0	1	OK	0	1		NML		
2014/02/01 19:58:15	0.2	EOT	44777			61	0	1	OK	0	1		NML		
2014/02/01 19:58:17	0.2	EOT	43075			0	0	1	OK	20	1		NML		
2014/02/01 19:58:27	0.2	EOT	76527			85	1	1	OK	30	1		NML		
2014/02/01 19:58:28	0.2	EOT	76527			85	1	1	OK	30	1		NML		
2014/02/01 19:58:33	0.2	EOT	76832			90	1	1	OK	0	1		NML		
2014/02/01 19:58:36	0.2	EOT	76832			89	1	1	OK	0	1		NML		
2014/02/01 19:59:14	0.2	EOT	44777			60	0	1	OK	0	1		NML		
2014/02/01 19:59:27	0.2	EOT	76527			85	1	1	OK	30	1		NML		
2014/02/01 19:59:49	0.1	EOT	76527			85	0	1	OK	30	1		NML		
2014/02/01 20:01:29	0.1	EOT	76527			85	0	1	OK	30	1		NML		
2014/02/01 20:03:52	0.2	EOT	37093			89	1	1	OK	0	1		NML		
2014/02/01 20:04:49	0.1	EOT	37093			89	1	1	OK	0	1		NML		
2014/02/01 20:05:46	0.1	EOT	37093			89	1	1	OK	0	1		NML	1	0
2014/02/01 20:05:53	0.1	EOT	37093			89	1	1	OK	0	1		NML	1	1
2014/02/01 20:06:52	0.1	EOT	37093			89	1	1	OK	0	1		NML	1	0
2014/02/01 20:07:20	0.1	EOT	37093			83	1	1	OK	0	1		NML	1	0
2014/02/01 20:08:43	0.1	EOT	37093			85	1	1	OK	0	1		NML	1	0
2014/02/01 20:10:35	0.1	EOT	37093			84	1	1	OK	0	1		NML	1	0
2014/02/01 20:10:42	0.1	EOT	37093			78	1	1	OK	0	1		NML	1	0
2014/02/01 20:11:53	0.1	EOT	37093			76	0	1	OK	0	1		NML	1	1
2014/02/01 20:18:56	0.1	EOT	37093			76	1	1	OK	0	1		NML	1	0
2014/02/01 20:21:44	0.1	EOT	37093			88	1	1	OK	0	1		NML	1	0
2014/02/01 20:22:07	0.1	EOT	37093			88	0	1	OK	0	1		NML	1	0

Field	Full Name	Description
Time	Time Received	The time when the packet was received
SRC	Packet Source	Indicates if the packet is from an EOT or HOT
ID	ID Code	The unique identifier code for EOT or HOT device
BP	Brake Pipe Pressure	The brake pipe pressure reported by the EOT
MOT	Motion Status	Indicates whether the train is in motion or not
BATST	Battery Status	Displays battery condition: OK, LO, DE, NM
TYP	Message Type	Indicates the message type: NRM or ARM
CMD	Command	Indicates the command sent by HOT packets

txOne networks

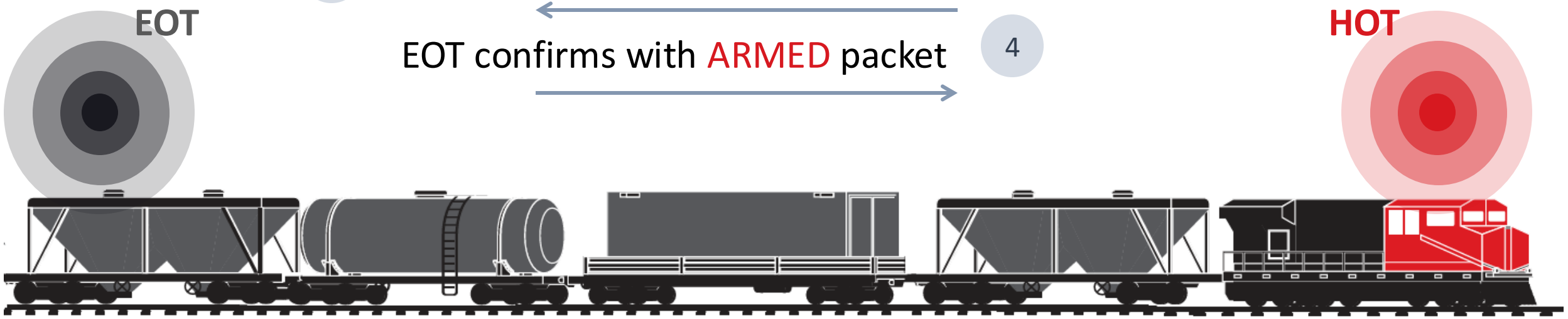
HOT / EOT Emergency Command

1 HOT number dials set to match EOT ID

EOT sends ARMING packet to HOT 2

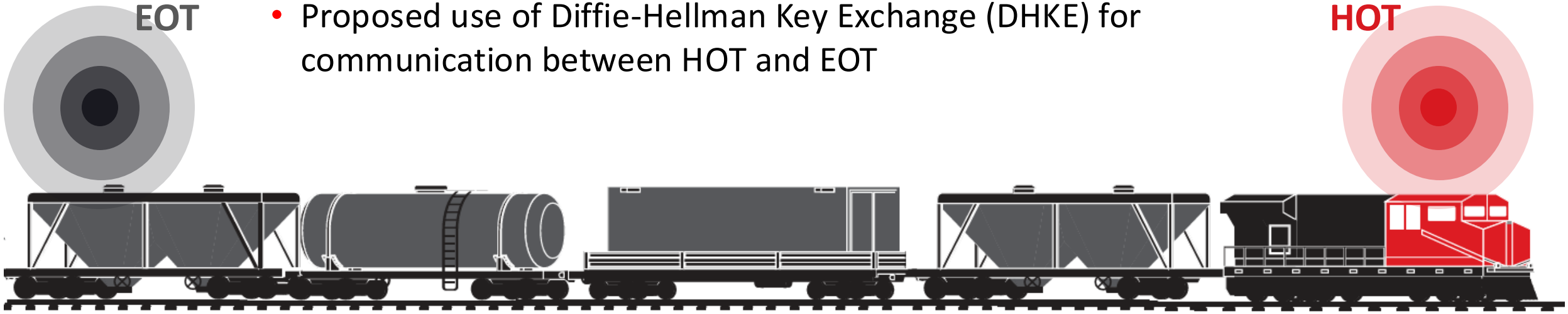
3 HOT sends ARM REPLY packet to EOT

EOT confirms with ARMED packet 4



HOT / EOT Emergency Command Attacking

- Unarmed HOT will transmit status request but not emergency cmd
- Arming sequence prevents rogue HOT from sending
- Presumed to be vulnerable to spoofing
- Proposed use of Diffie-Hellman Key Exchange (DHKE) for communication between HOT and EOT



Outline

- Introduction to Railway Cybersecurity
- Potential Threats in Railway Industry Ecosystem
- Insights on Remote Hijacking of Railroads
- Takeaways
  - Compliance and Regulations on Railway Cybersecurity
  - Strategies to Mitigate Railway Cybersecurity Threats

TSA Security Directive Upgraded

Release	Security Directive	Key Points
May 2021	**SD Pipeline–2021–01**	Requires operators to designate a 24/7 cybersecurity coordinator and report incidents promptly to strengthen incident response capabilities.
July 2021	**SD Pipeline–2021–02B**	Introduced mandatory cybersecurity mitigation measures to protect against known threats and improve response preparedness.
July 2022	**SD Pipeline–2021–02C**	Emphasized continuous monitoring and anomaly detection to safeguard critical cyber systems effectively.
July 2023	**SD Pipeline–2021–02D**	Strengthened resilience by requiring annual cybersecurity plan updates and regular testing of incident response objectives.
July 2024	**SD Pipeline–2021–02E**	Focused on clarifying responsibilities for MSSPs, submission deadlines for cybersecurity assessments, and updated compliance definitions.

TSA impose cyber risk management (CRM) requirements on certain pipeline and rail owner/operators

https://www.federalregister.gov/documents/2024/11/07/2024-24704/enhancing-surface-cyber-risk-management

Strategies to Mitigate Railway Cybersecurity Threats

- Implementing a **network segmentation** policy and controls to prevent operating disruption to OT systems if IT systems are compromised and vice versa
- Create **access controls** to secure and prevent unauthorized access to critical cyber systems
- Rail operators must ensure that critical systems are **continuously monitored** for cyber threats

https://groups.io/g/ATCSMonitor/album?id=285443

Strategies to Mitigate Railway Cybersecurity Threats

- Reduce the risk of unpatched systems being exploited by using a risk-based approach to **apply timely security patches** and updates to operating systems, applications, drivers, and firmware on critical network systems
- **Establish a rail cybersecurity assessment plan** to proactively test and periodically audit the effectiveness of cybersecurity measures and identify and address vulnerabilities in equipment, networks, and systems

https://groups.io/g/ATCSMonitor/album?id=295904


txOne
networks