



Cybersecurity on rails: A look at the connected train

Jesus Molina

jesus@waterfall-security.com

@verifythetrust



About Waterfall



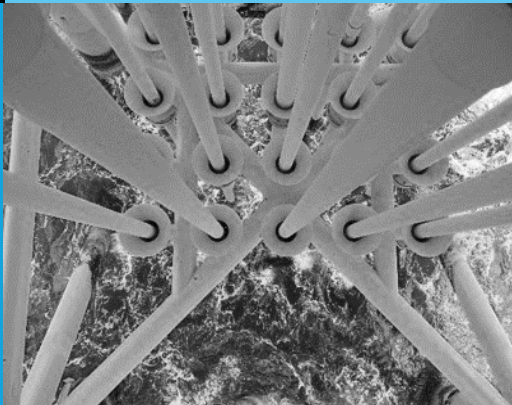
**Founded in
2007**



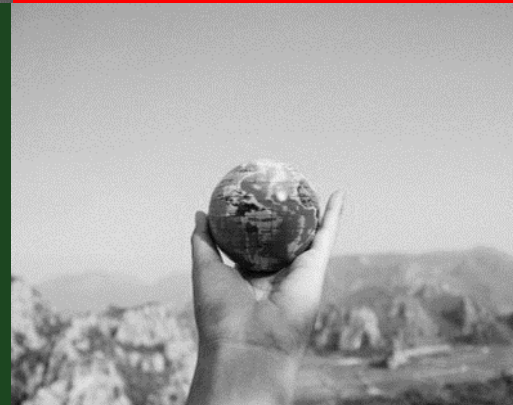
**1000+ sites
worldwide**



**Headquarters
in Israel**



**Deployed in
all critical
infrastructure
sectors**



**Sales &
operations
in the USA,
EU & APAC**



**Multiple
registered
US patents**



**Technology
& sales
collaboration
with global
partners**



**Spanish hacker
manages to control
every room at a luxury
hotel remotely**



Use Cases in Rail

Equipment Maintenance

Maintenance of equipment across stations.

Emergency Messaging & Dispatch from CTC

Provide real time alerts for people on the ground.

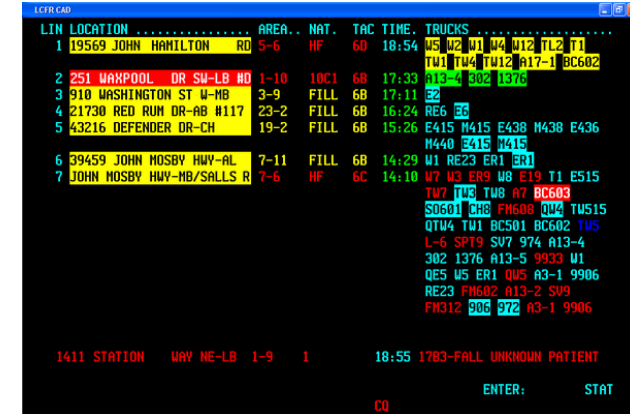
Onboard Train

Provide information from control to comfort zones, and/or protect critical subsystems.

Asset Management

Evaluate current status of equipment.

And many, many more...



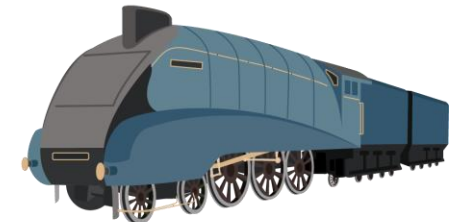
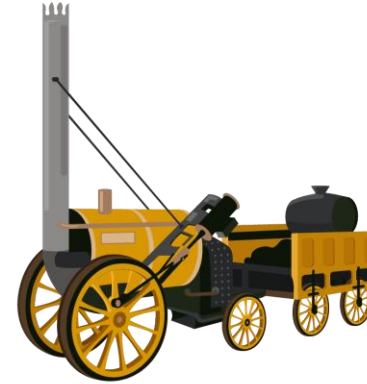
LIN	LOCATION	AREA	NAT	TAC	TIME	TRUCKS
1	19569 JOHN HAMILTON RD	5-6	HF	60	18:54	WS M2 W1 W4 W12 TL2 T1 TU1 TU4 TU12 A17-1 BC602
2	251 WAXPOOL DR SW-LB RD	1-10	10C1	68	17:33	A13-4 302 1876
3	910 WASHINGTON ST W-MB	3-9	FILL	68	17:11	32
4	21730 RED RUN DR-AB H117	23-2	FILL	68	16:24	RE6 33
5	43216 DEFENDER DR-CH	19-2	FILL	68	15:26	E415 M415 E438 M438 E436 M440 E415 M415
6	39459 JOHN NOSBY HWY-AL	7-11	FILL	68	14:29	W1 RE23 ER1 ER1
7	JOHN NOSBY HWY-MB/SALLS R	7-6	HF	6C	14:10	W7 W3 ER9 W8 E19 T1 E515 TW7 TWE TW8 A7 BC603 S0601 CH8 FH608 QW4 TW515 QTW4 TW1 BC501 BC602 TWS L-6 SPT9 SV7 974 A13-4 302 1376 A13-5 9933 W1 QE5 WS ER1 QWS A3-1 9906 RE23 FH602 A13-2 SW9 FH312 306 972 A3-1 9906

1411 STATION WAY NE-LB 1-9 1 18:55 1783-FALL UNKNOWN PATIENT
ENTER: STAT
CO



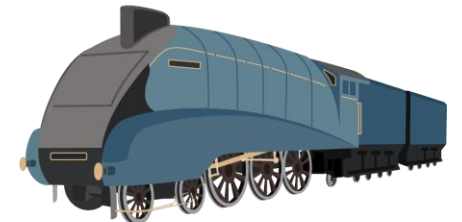
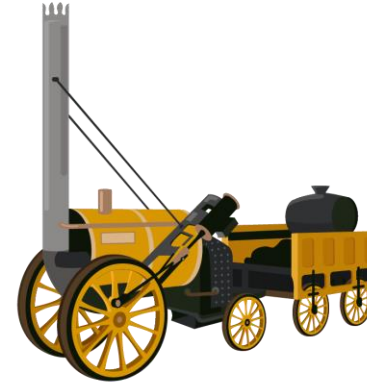
Rolling Stock Evolution

- Invented in the 1800s
- A reflection of the industrial revolutions
- In the 3rd revolution, IT was added to trains, in the form of computers and buses
- In the 4th industrial revolutions, information is collected by hundreds of sensors



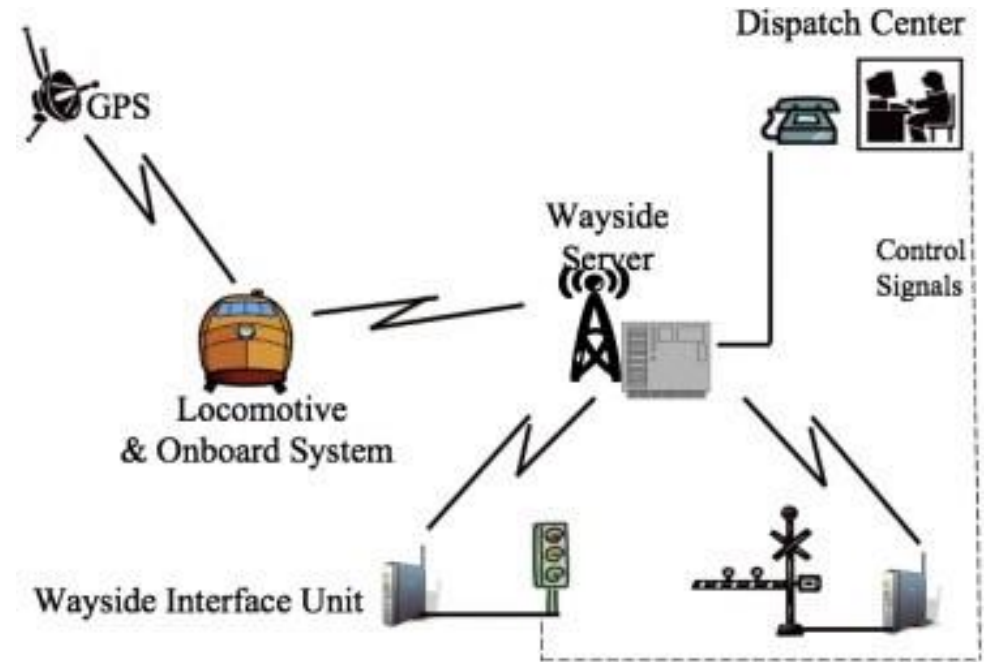
Rolling Stock Evolution

- Invented in the 1800s
- A reflection of the industrial revolutions
- In the 3rd revolution, IT was added to trains, in the form of computers and buses
- In the 4th industrial revolutions, information is collected by hundreds of sensors

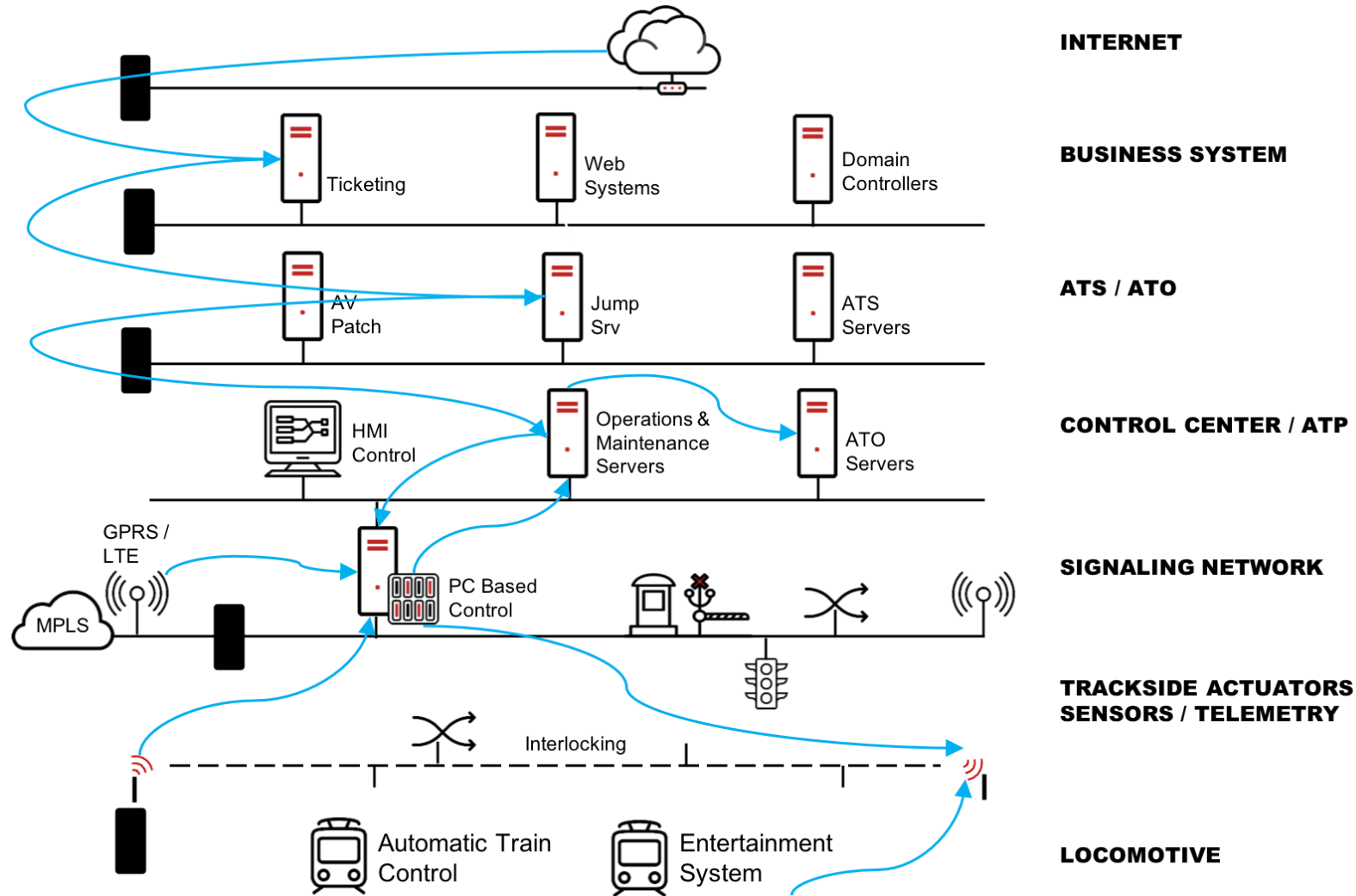


Example Application

- **Positive Train Control (PTC)** is designed to automatically stop a train before certain accidents occur.
- In 2008 a collision between two trains resulted in the deaths of 25 and injuries to more than 135 passengers.
- The US congress passed a law to implement PTC by 2015 later extended to 2018
- Complex system with no cybersecurity bolted in



Train Kill Chain

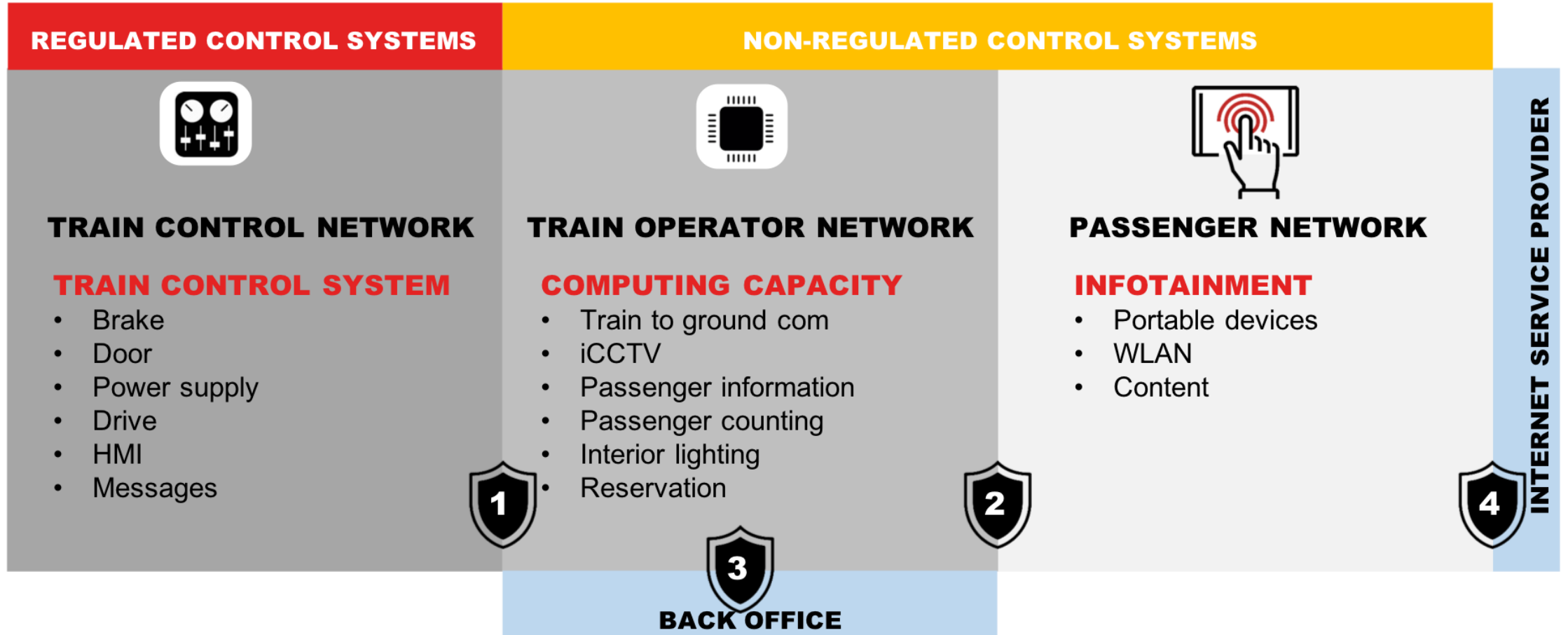


How much does it cost to hack a train?

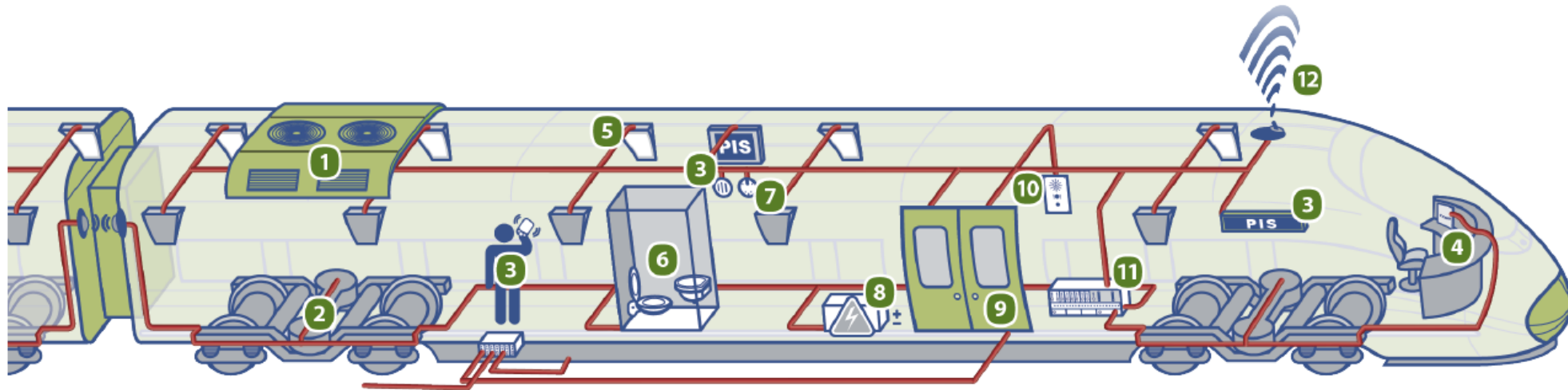


**What will
evil Jesus
do?**

First: Pick a Method



Second: Pick a Target

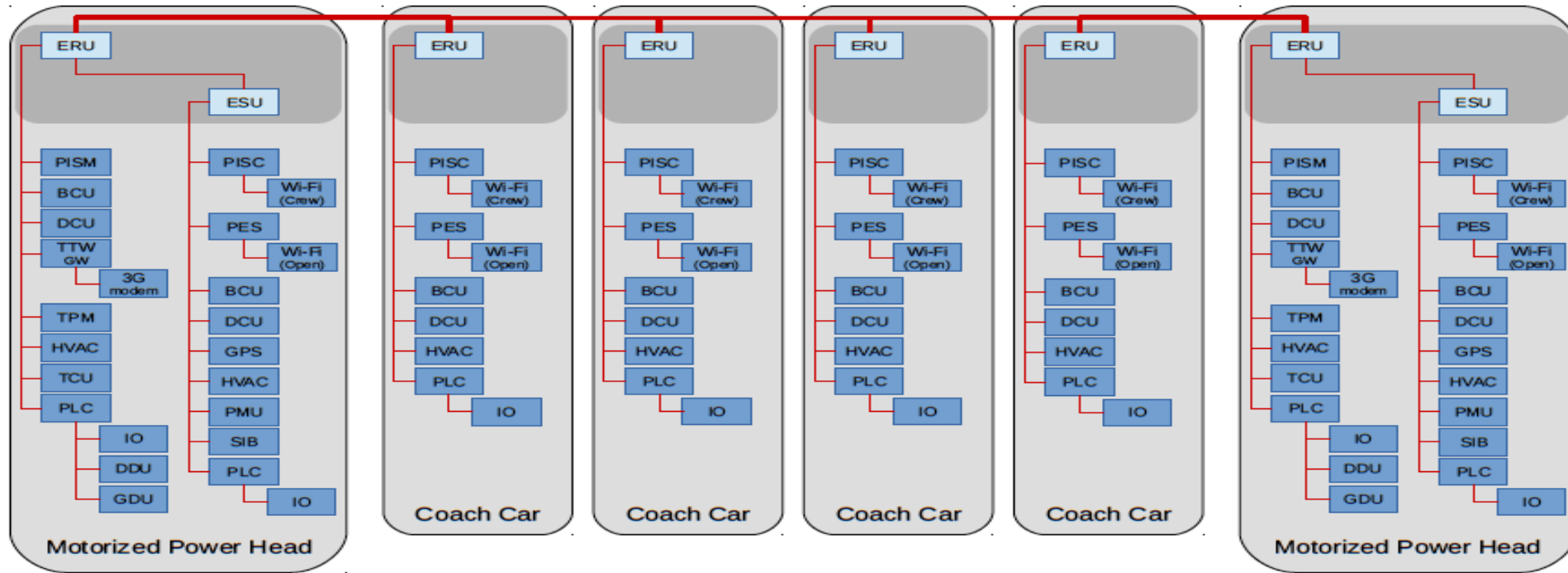


TCMS, FOR THE MONITORING, CONTROL AND AUTOMATION OF:

- | | | | |
|-----------------------|-------------------|------------------------|------------------------------------|
| 1 HVAC | 2 Brakes | 5 Lights | 9 Doors |
| 2 Bearing temperature | 2 Traction | 6 Water tanks | 10 Emergency communications |
| 2 Speed measurement | 3 PIS | 7 Surveillance Cameras | 11 Vehicle Control Unit |
| 2 Lateral vibration | 4 Driver Controls | 8 Batteries | 12 Train-To-Wayside communications |

From: Threat Modeling for Train Control and Management Systems based on the Ethernet Train Backbone

Third: Find a Flaw



- | | | | |
|------|--|------|--------------------------------------|
| BCU | Brake Controller Unit | PES | Passenger Entertainment System |
| DCU | Door Controller Unit | PISC | Passenger Information System Client |
| DDU | Driver Display Unit | PISM | Passenger Information System Manager |
| ERU | Ethernet Routing Unit | PLC | Programmable Logic Controller (Unit) |
| ESU | Ethernet Switching Unit | PMU | Power Management Unit |
| GPS | Global Positioning System (Unit) | SIB | Station Identification Beacon |
| GDU | Guard Display Unit | TCU | Traction Controller Unit |
| HVAC | Heating, Ventilation and Air Conditioning (Controller) | TPM | Time and Position Manager |
| IO | Input Output (Unit) (Digital or Analog) | TTW | Train To Wayside (Gateway) |

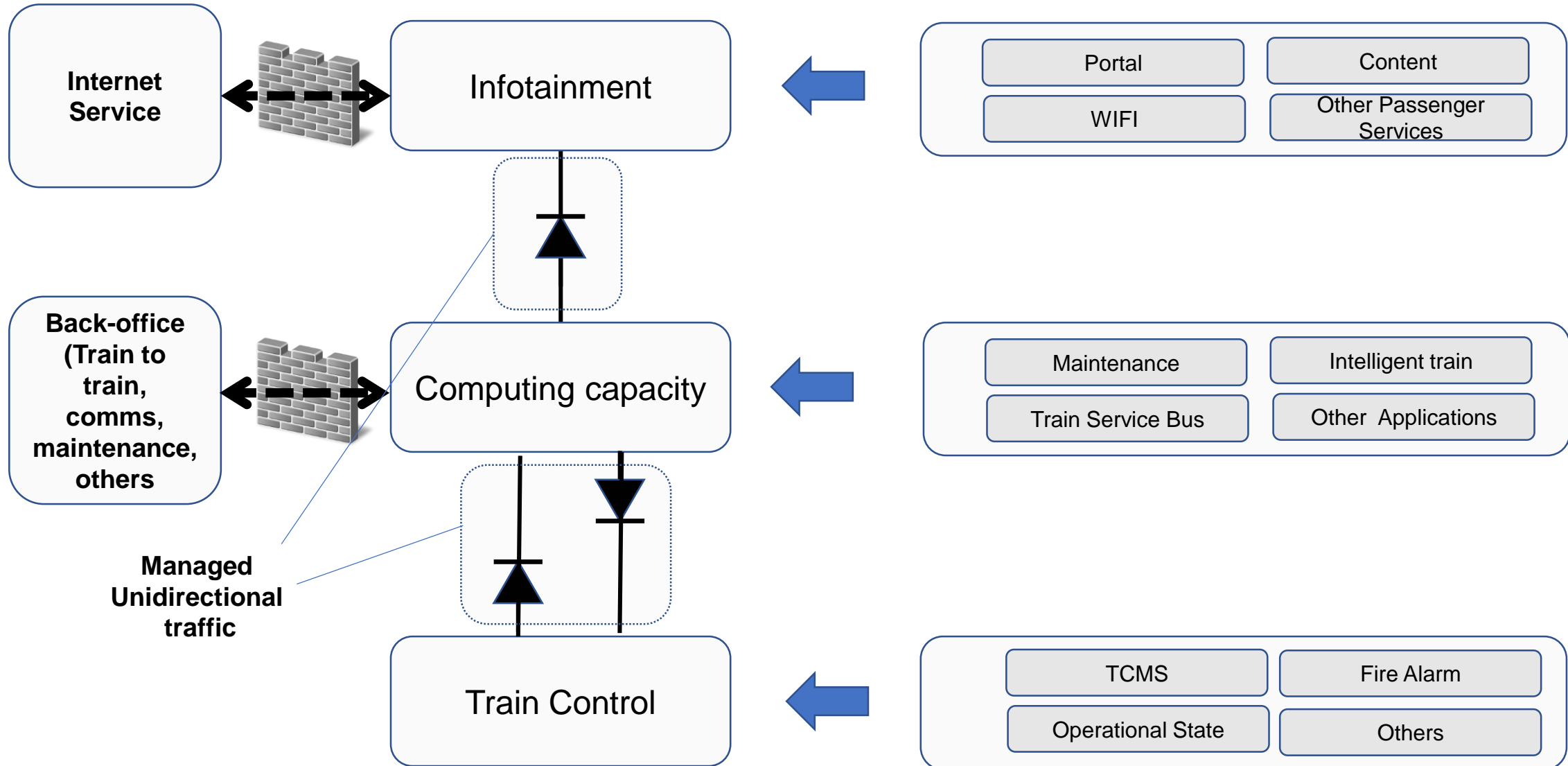
From: Threat Modeling for Train Control and Management Systems based on the Ethernet Train Backbone

Challenges protecting trains

- Train control is a critical network, lose of life is possible
 - Highest level of security required
- Reduced space
 - Requires a compact solution
- Regulations and Standards
 - EN 5012, EN5015
- Unmanned security
 - Configuration based tools (Firewall, AV) not suitable
- Flexible configuration for different trains
- Able to work with existing software/hardware configuration and protocols



Segmentation on rolling stock



Takeaways

- Today's cyberattacks aim to disrupt production, damage equipment, harm a company's brand or demand ransom in rail networks.
- Rolling stocks contain complex networks with very little security
- IT-class security fails to maintain a secure perimeter, and should not be applied to rolling stock.
- Hardware segmentation minimizes the risk in rolling stock





Thank you

Questions?

@verifythetrust

