RailTech® INTELLIGENT RAIL SUMMIT

Signalling and Cyber Security

Closing the gaps that prevent comprehensive security solutions

John Boss

BE(elec), MBA, FIRSE, MSc(cyber security)…*almost*

Objectives

- Take some hype out of cyber security
- Put things into context
- Help the decision makers

Conclusions from the research project

1. Cyber security must be addressed in relation to the whole business
2. A risk based cyber security management system is required
3. The signalling system remains the responsibility of the signalling engineer
4. A portfolio of measures is required.
5. Security must be driven from the top down

Cyber - concepts

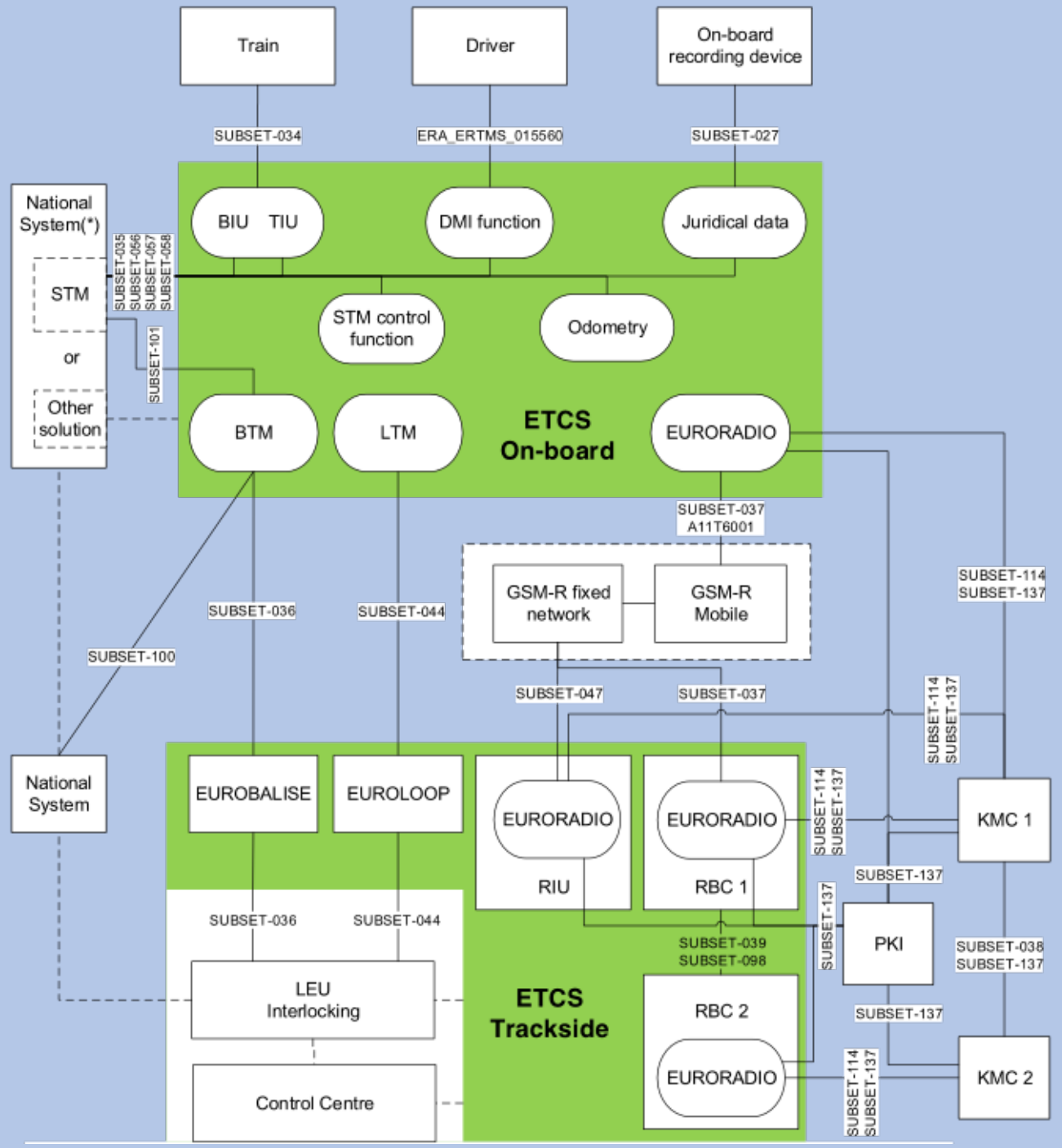
- Vulnerabilities: It works - but not in the way you expect…
- Anatomy of a cyber attack: the kill chain…

Paradigm 1: System Definition

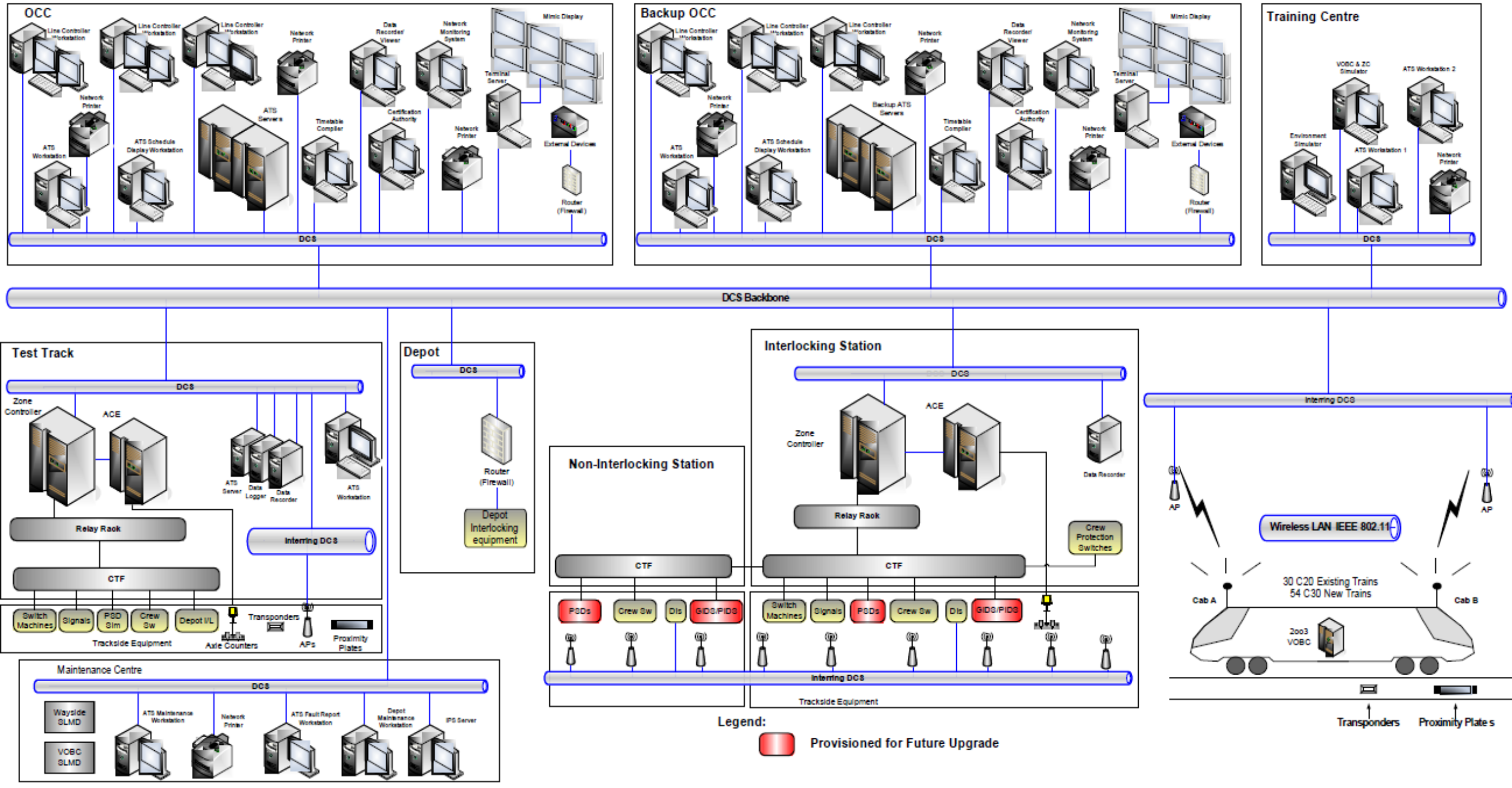
- IACS IEC 62443-1-1:
  "Collection of personnel, hardware and software…"

- To a hammer the world is a nail

ERTMS

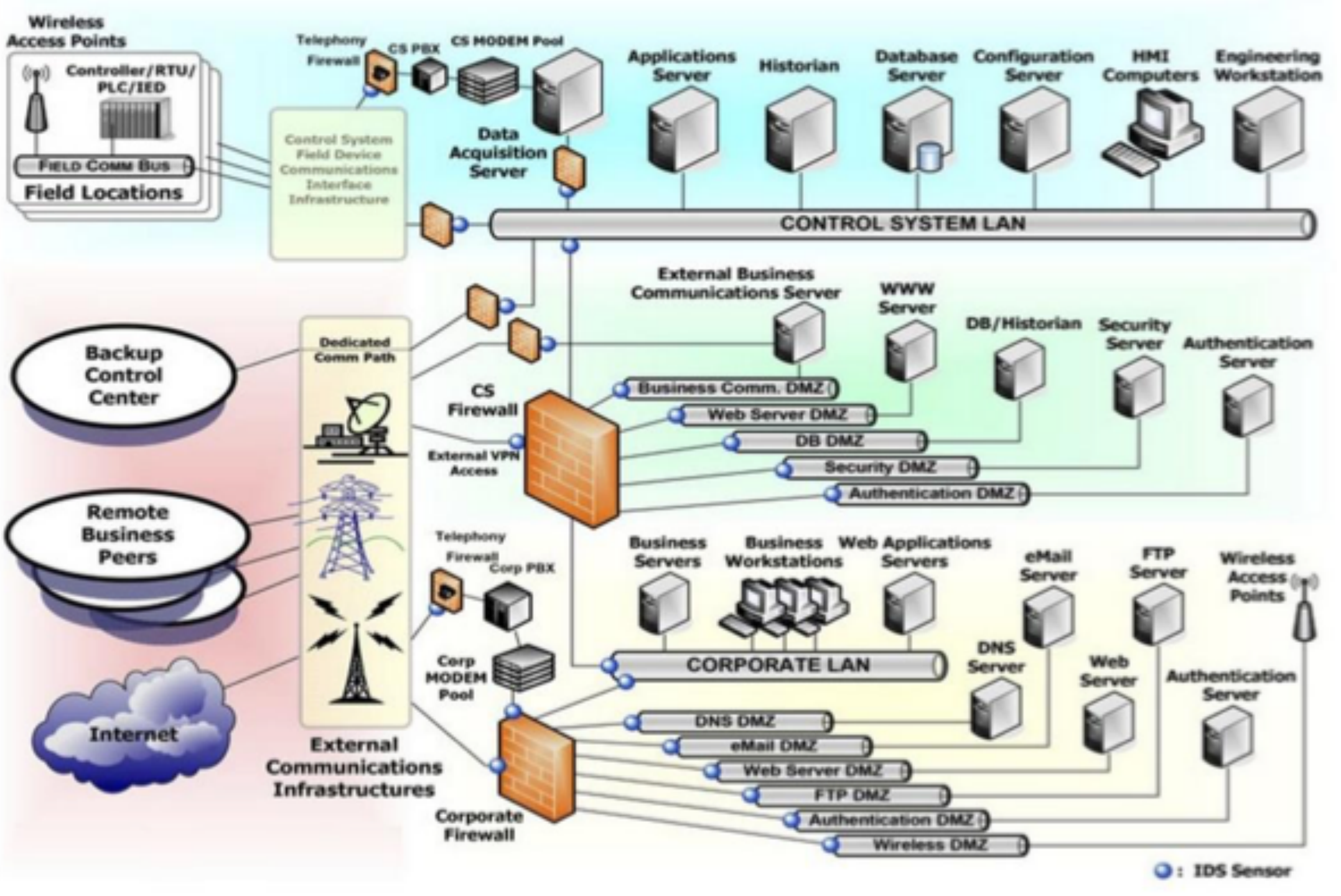


Bron: Subset-026-2 v360

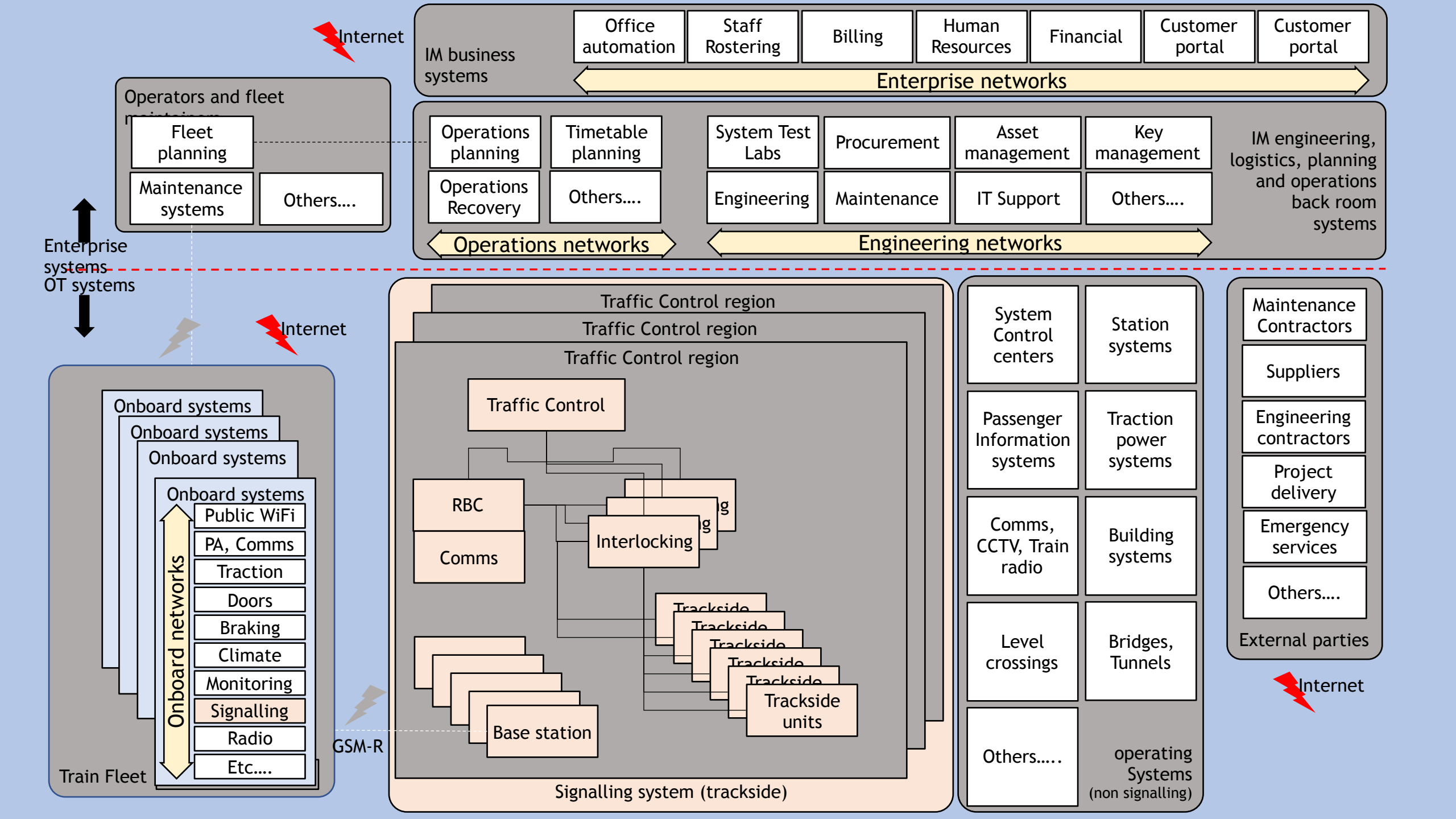


Bron: www.railengdigest.com: "Beginners Guide: Railway signalling till ATC", Sujay Sujatharen; 21 Aug 2018. accessed 26 Sept 2019

NIST
(with IDS)



Bron: NIST SP 800-82 Rev 2, Guide to Industrial Control Systems (ICS) Security


Internet
IM business systems
Office automation
Staff Rostering
Billing
Human Resources
Financial
Customer portal
Customer portal
Enterprise networks
Operators and fleet
Fleet planning
Maintenance systems
Others....
Operations planning
Timetable planning
Operations Recovery
Others....
Operations networks
System Test Labs
Procurement
Asset management
Key management
Engineering
Maintenance
IT Support
Others....
Engineering networks
IM engineering, logistics, planning and operations back room systems
Enterprise systems
OT systems
Internet
Onboard systems
Onboard systems
Onboard systems
Onboard systems
Public WiFi
PA, Comms
Traction
Doors
Braking
Climate
Monitoring
Signalling
Radio
Etc....
Onboard networks
Train Fleet
GSM-R
Traffic Control region
Traffic Control region
Traffic Control region
Traffic Control
RBC
Comms
Interlocking
Trackside
Trackside
Trackside
Trackside
Trackside
Trackside units
Base station
Signalling system (trackside)
System Control centers
Station systems
Passenger Information systems
Traction power systems
Comms, CCTV, Train radio
Building systems
Level crossings
Bridges, Tunnels
Others.....
operating Systems
(non signalling)
Maintenance Contractors
Suppliers
Engineering contractors
Project delivery
Emergency services
Others....
External parties
Internet

Paradigm 2: Risk Assessment

- To a hammer…..

Two definitions of the risk assessment process

safety

Hazard with probability of occurrence	causing consequences	producing safety risk

security

Likelihood of threat actor exploiting a vulnerability	causing impact	producing security risk

Security for safety or Security for security

A Portfolio of Measures – guided by risk

Network Security

Architecture
Firewalls
Gateways
DPI
IDS
IPS
DMZ
Segmentation
encryption
VPN
Security by design
…..

Intelligence & Incident management

CERT
ISAC
SOC
Intelligence
SIEM
TIP
notification

Governance and support

Budget
Resource
Mgt Commitment

CSMS

Threat Risk Analysis
Security program
Organisation
Budget forecast
Policies
Training
Doc management

Conclusions

1. Cyber security must be addressed in relation to the whole business
2. A risk based cyber security management system is required
3. The signalling system remains the responsibility of the signalling engineer
4. A portfolio of measures is required.
5. Security must be driven from the top down

Thank you