Speed of Implementation
New players, new collaboration models, new business models
Big Data
Automated driving
ETCS Level 3
Intelligent Traffic Management
2030
Connectivity
Artificial Intelligence
Laser Scanning
Augmented Reality
No TVD and signals. Points remotely controlled
Automated vehicle systems and optimized traffic in a cloud based environment
Mobile devices & web technology
Obstacle detection
Smart Sensors
Data Analytics
User friendly HMI
Train integrity
Block Chain
Safe satellite supported positioning
Break through fast point machines
Virtual train coupling
Secure IP-based communication
Service-oriented business models
Remote Software loading
HW independent Safe applications
High level of automated conflict resolution
TMS, RBC & IXL functions centralized in the cloud
Train-to-Train communication
Non-vital cloud application
Flexible use of Power Supply
IT Security Level 3
Data Ownership
Vital cloud application

SIEMENS

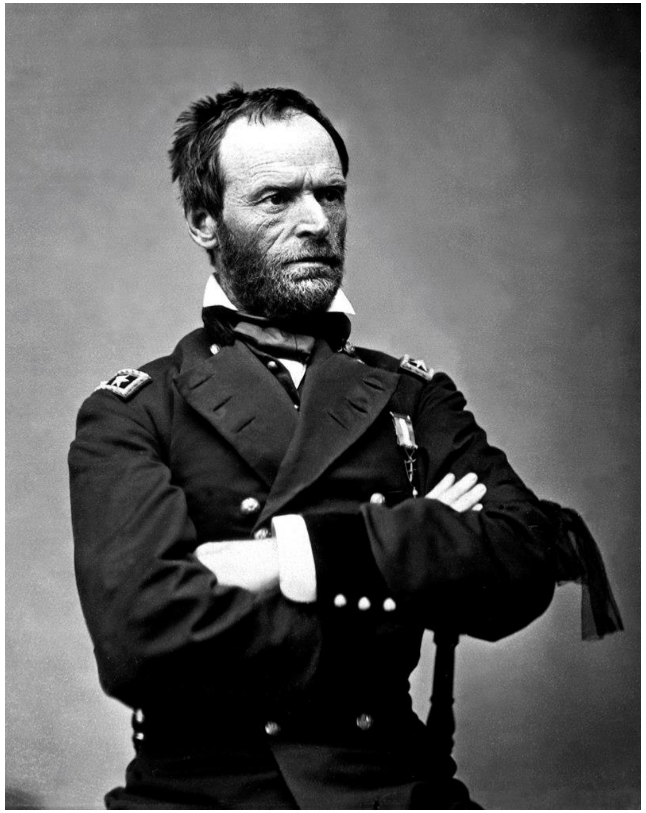
Ingenuity for life

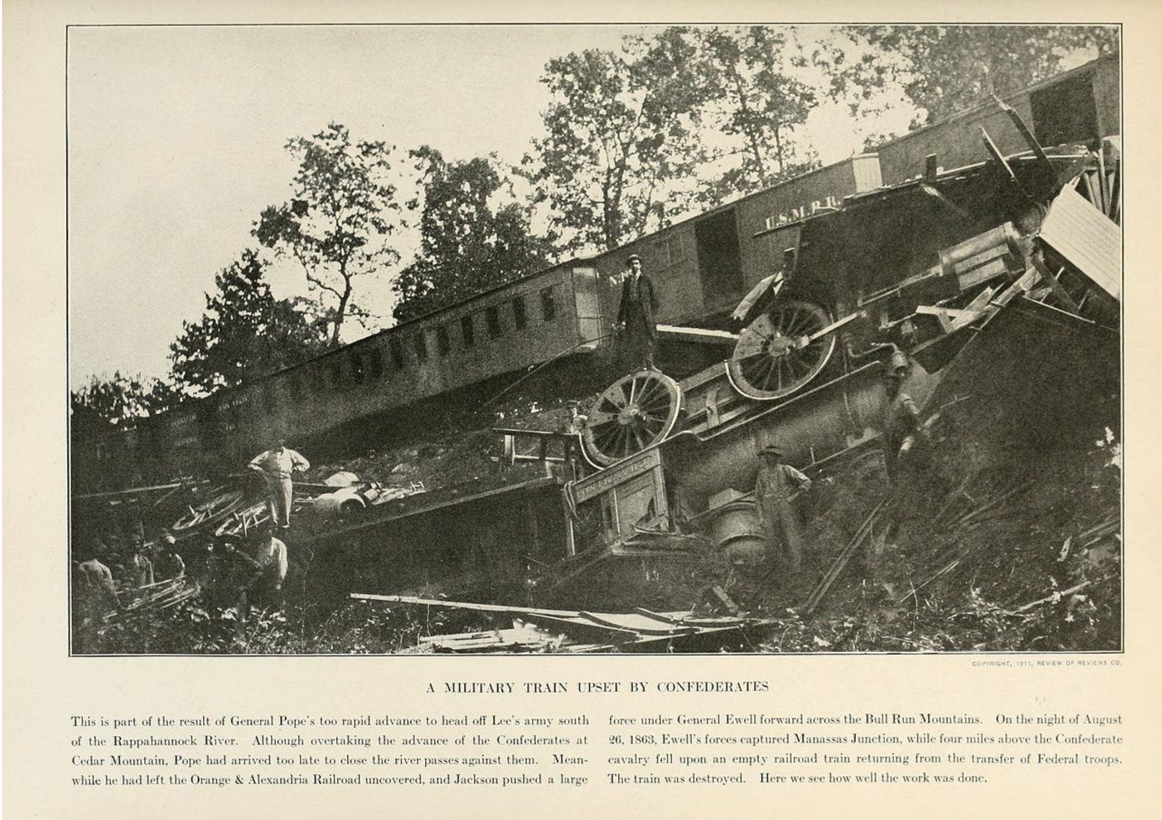
A Survey of Cybersecurity in Railway Signaling

Jens Braband

siemens.com/mobility

Railways and Security: how it began…





COPYRIGHT, 1911, REVIEW OF REVIEWS CO.

A MILITARY TRAIN UPSET BY CONFEDERATES

This is part of the result of General Pope's too rapid advance to head off Lee's army south of the Rappahannock River. Although overtaking the advance of the Confederates at Cedar Mountain, Pope had arrived too late to close the river passes against them. Meanwhile he had left the Orange & Alexandria Railroad uncovered, and Jackson pushed a large force under General Ewell forward across the Bull Run Mountains. On the night of August 26, 1863, Ewell's forces captured Manassas Junction, while four miles above the Confederate cavalry fell upon an empty railroad train returning from the transfer of Federal troops. The train was destroyed. Here we see how well the work was done.

Railroads are the weakest things in war: a single man with a match can destroy and cut off communications.

William Tecumseh Sherman

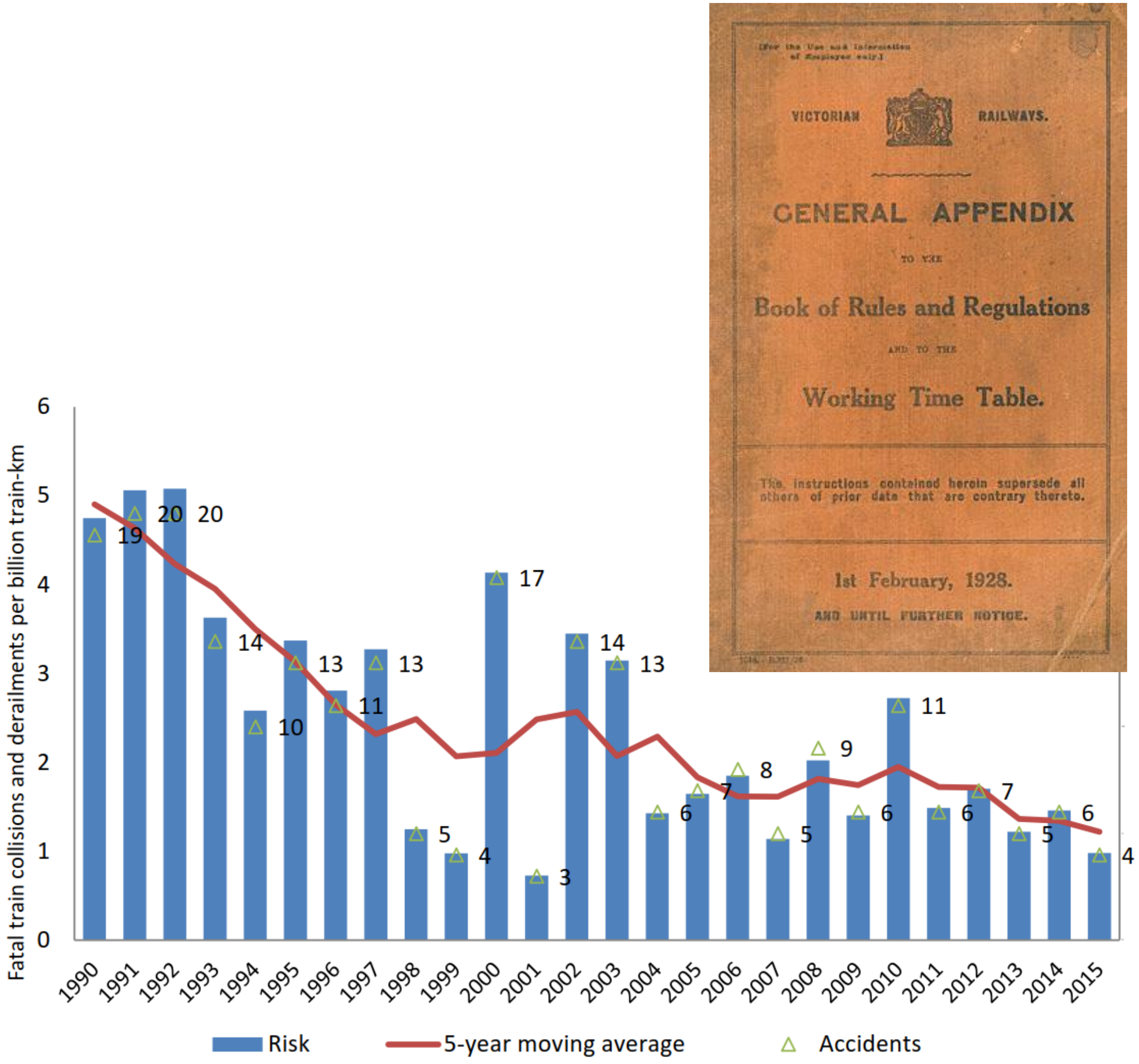
Traditional safety approach in railways

- Railways are traditionally operated by rules

- It is generally assumed that railways are safe, unless
  - a significant change is introduced
  - a safety-related incident has occurred

- This concept was formally also introduced into European law (CSM regulation)

- EU statistics show a slight steady downward trend



[For the Use and Information of Employes only.]

VICTORIAN RAILWAYS.

GENERAL APPENDIX

TO THE

Book of Rules and Regulations

AND TO THE

Working Time Table.

The instructions contained herein supersede all others of prior date that are contrary thereto.

1st February, 1928.

AND UNTIL FURTHER NOTICE.

Remember the early 90‘s? Not so long ago…

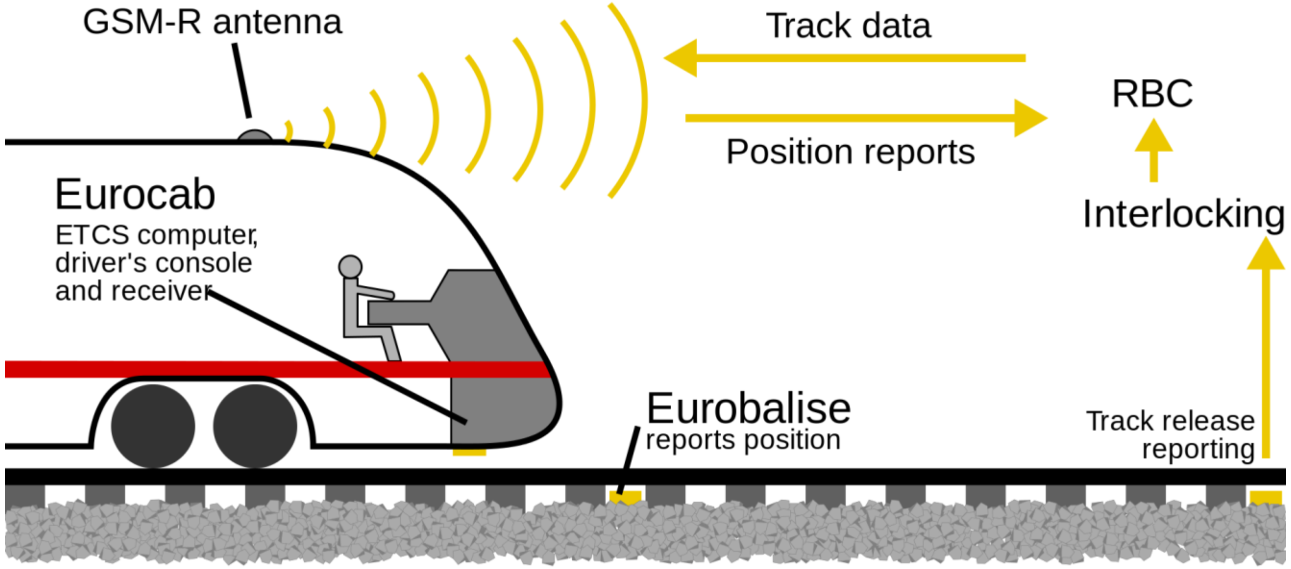
- First high-speed trains in operation in Germany
- First computer-based interlockings deployed
- First driverless metros in France
- Mainly proprietary technology
- Already some research projects in radio-based train control
- Rollout of GSM, GPS etc
- No harmonised standards
- No cross-border interoperability
- No European agency for railways
- In many countries privatization about to begin
- …

And then came ETCS…

Changes in ETCS w. r. t. conventional signalling:

- Public Radio System (new)
- Balise System (updated)
- Moving Block (L3 only)
- Train Integrity (L3 only)
- ….

So Security analysis focused mainly on the radio link.



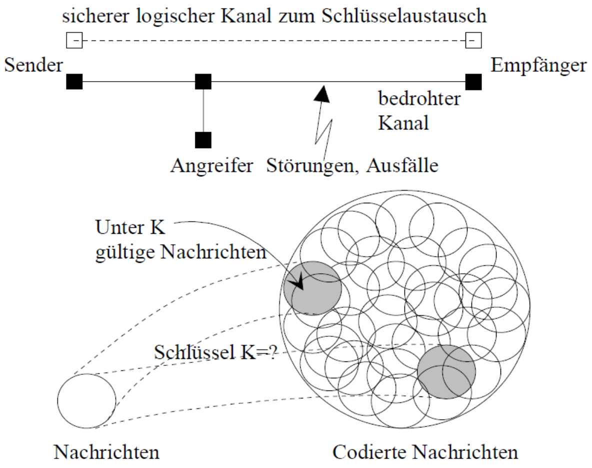
… and extensive security analysis was performed for the radio link

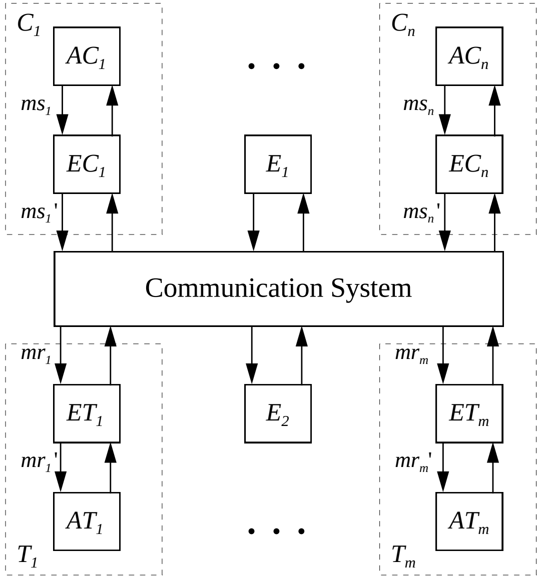
However trade-offs between safety and security had to be made e. g.

- cryptographic security mechanisms introduce an additional delay
- fortunately many safety-related messages are not time-critical e. g. movement authorities
- but emergency stop messages are…

Safety would require that emergency stops are executed as quick as possible
Availability (security) would require that only authenticated messages are processed

For ETCS it was decided that emergency stop messages are not authenticated.





C_i: trackside entity (RBC)

T_i: trainside entity

AC_i : application layer trackside

EC_i : EuroRadio layer trackside

AT_i : application layer trainside

ET_i : EuroRadio layer trainside

E_i : other communicating entities

ms_i, ms_i': message stream sender

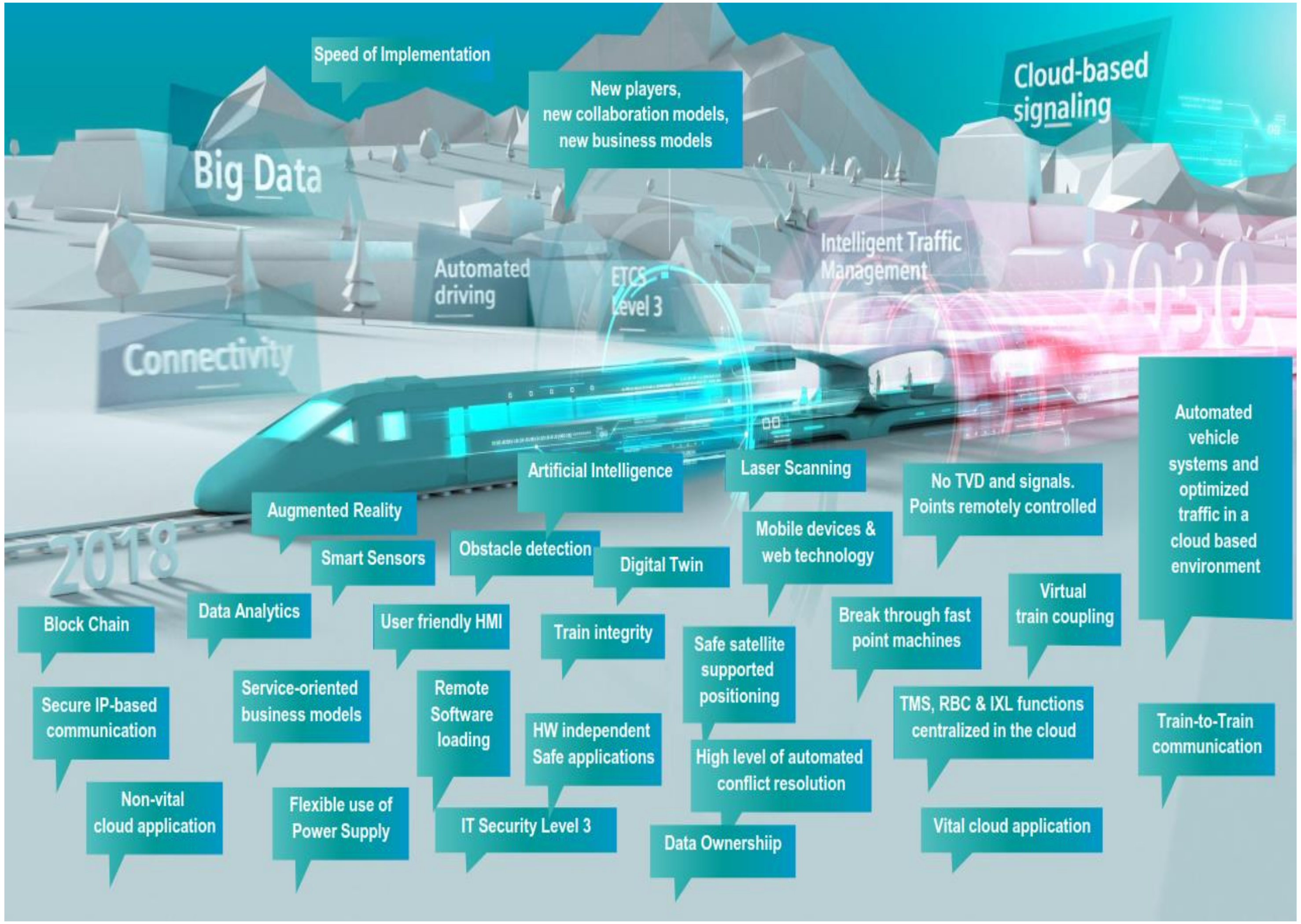
mr_j, mr_j': message stream receiver

… and many other security-related applications were introduced

SIEMENS

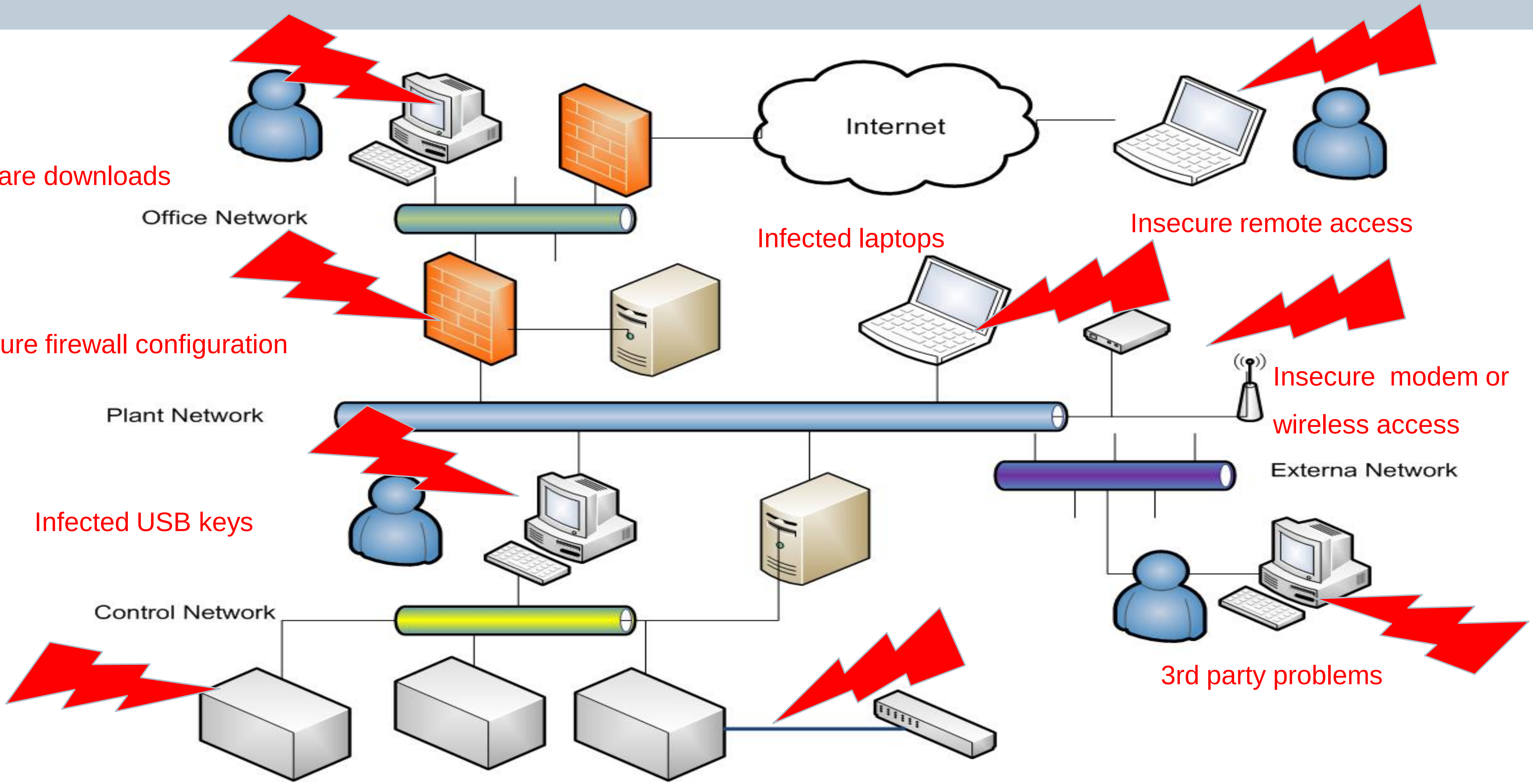
- Remote operation of interlockings
- Remote maintenance including SW update
- Automated driving
- Use of COTS HW and SW
- IP based interlockings
- Interlocking in the cloud
- …

- .. and many more are in the pipeline



Speed of Implementation
New players, new collaboration models, new business models
Cloud-based signaling
Big Data
Intelligent Traffic Management
2030
Automated driving
ETCS Level 3
Connectivity
Automated vehicle systems and optimized traffic in a cloud based environment
Artificial Intelligence
Laser Scanning
No TVD and signals. Points remotely controlled
Augmented Reality
2018
Mobile devices & web technology
Smart Sensors
Obstacle detection
Digital Twin
Virtual train coupling
Block Chain
Data Analytics
User friendly HMI
Train integrity
Safe satellite supported positioning
Break through fast point machines
Secure IP-based communication
Service-oriented business models
Remote Software loading
HW independent Safe applications
TMS, RBC & IXL functions centralized in the cloud
Train-to-Train communication
High level of automated conflict resolution
Non-vital cloud application
Flexible use of Power Supply
IT Security Level 3
Data Ownershiip
Vital cloud application

But what about closed networks and air gaps?



Malware downloads

Insecure firewall configuration

Infected USB keys

Incorrect application logic

Infected laptops

Insecure links

Insecure remote access

Insecure modem or wireless access

3rd party problems

What’s the problem with safety and security?

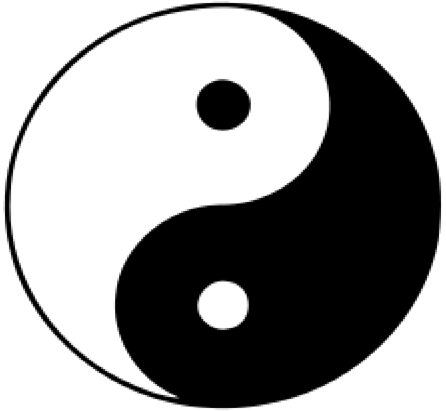
SIEMENS

“If it’s not secure, it’s unlikely to be safe!”

Department for Transport

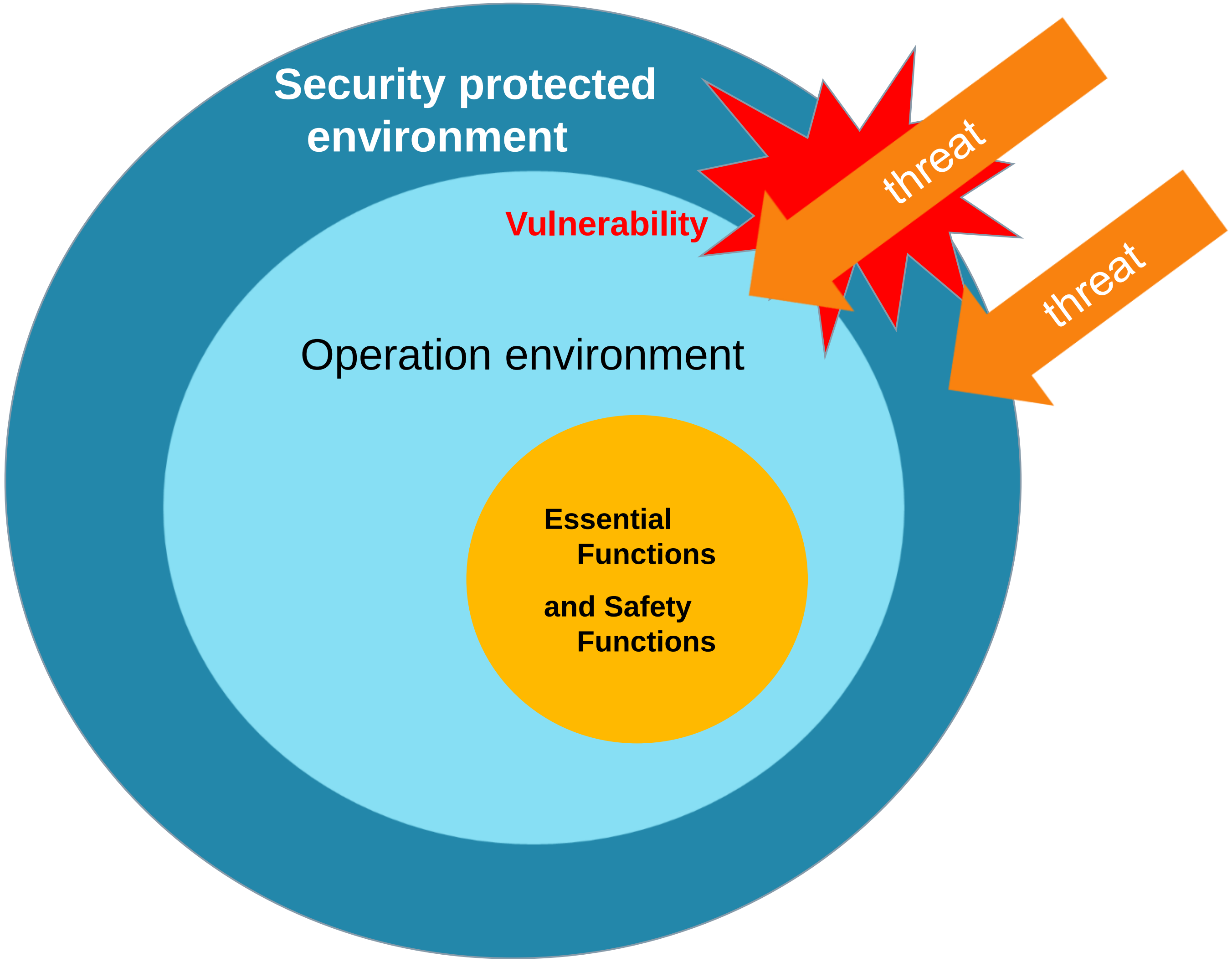
Safety and Security have

- complementary goals
- different regulatory authorities
- different terminology
- different communities
- different standards
- ….



How do we cope with this situation?

Safety and Security: United or Seperated?



Security can be viewed as an external influence similar to temperature, humidity, EMC etc. This view was already in Mü8004 and has been extended in the CENELEC standards.

Security provides an environment in which essential functions (incl. safety) are not adversely affected

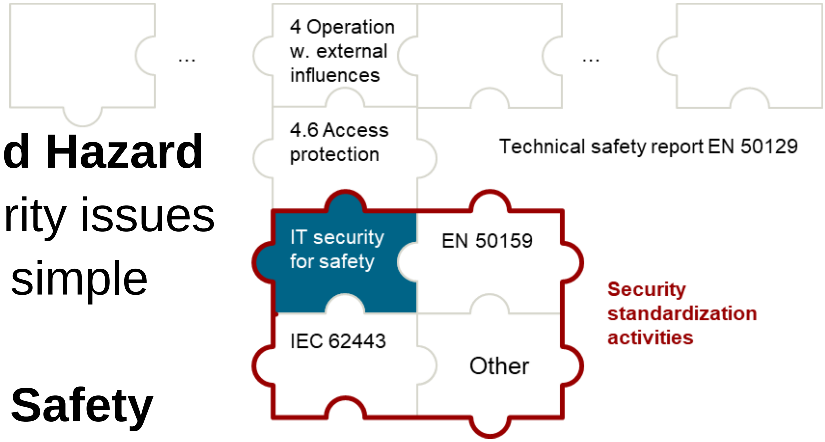
Security and safety issues should be separated as far as possible, also with respect to certification.

This calls for a “security-informed safety case”

EN 50129:2018 introduced the basics

The **safety management process** aims at minimizing the residual risk of safety-related systematic faults and **security threats (including IT-Security threats) so far as safety is concerned….**

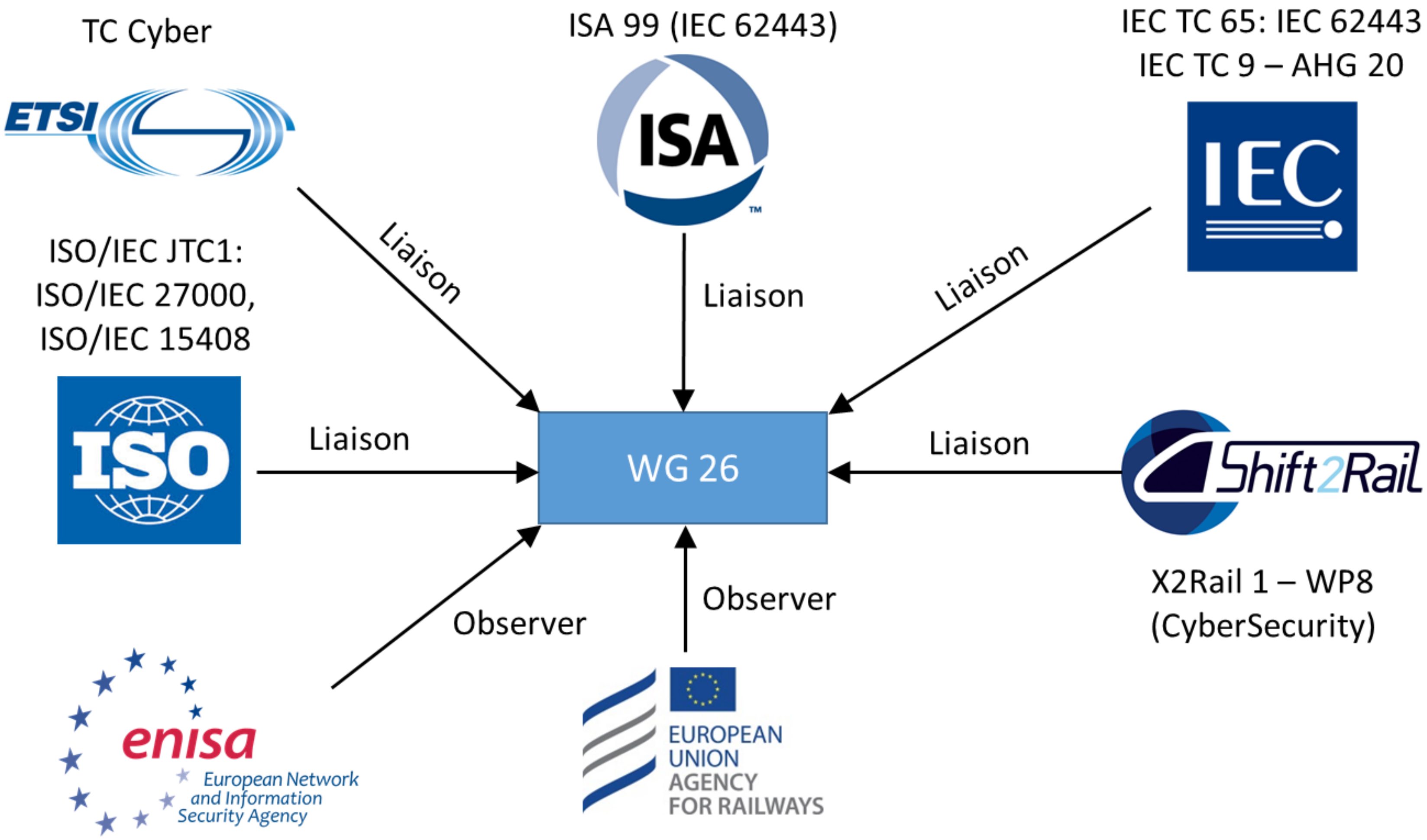
IT-Security threats shall be managed during the Risk Assessment and Hazard Control (or existing analyses shall be referenced), if an impact of IT-Security issues on functional safety is reasonably foreseeable and cannot be excluded by simple arguments (e.g. a system having no connection to untrusted networks). **Measures addressing security shall be recorded or referenced in the Safety Case** (section 4.5 of the Technical Safety Report, as described in 7.2)….


…
4 Operation w. external influences
…
4.6 Access protection
Technical safety report EN 50129
IT security for safety
EN 50159
IEC 62443
Other
Security standardization activities

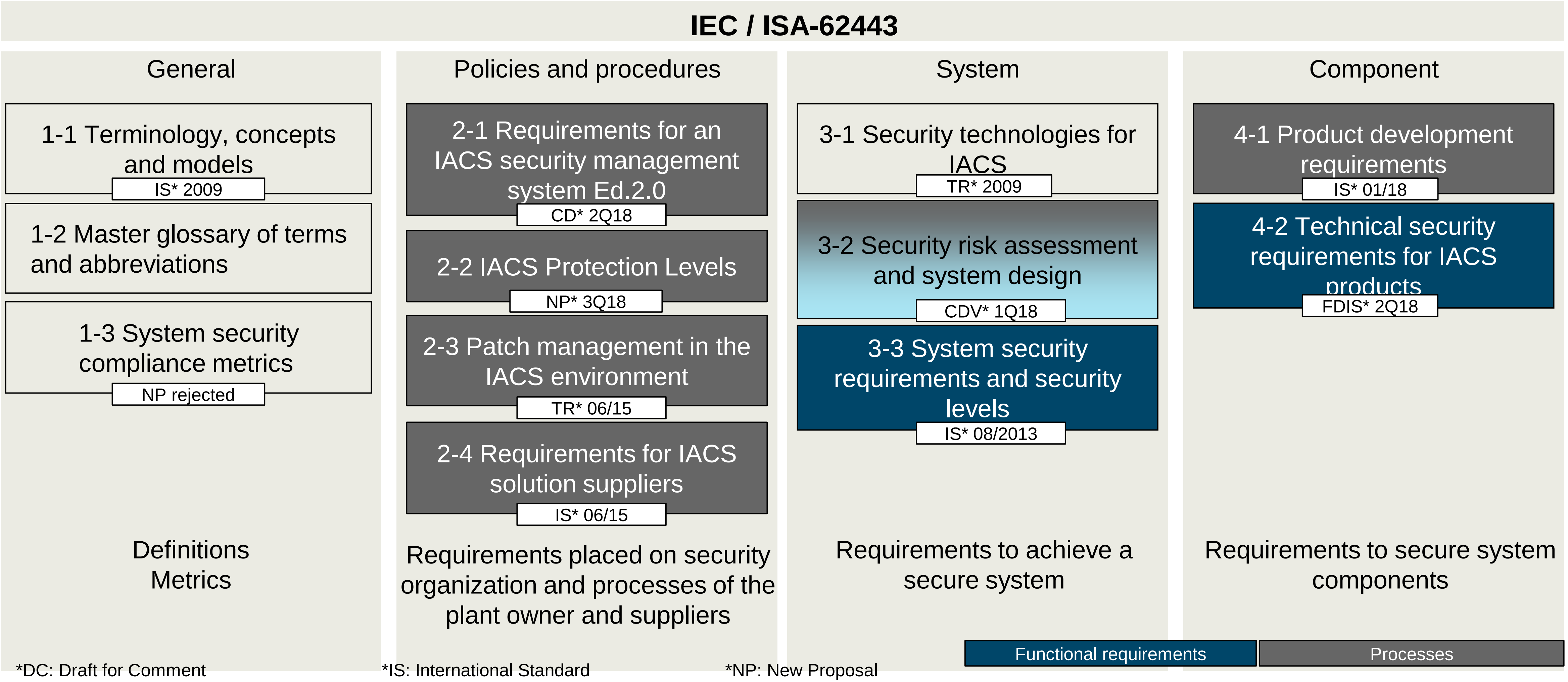
This section [of the technical safety report] shall describe how **IT-Security threats which have the potential to affect safety-related functions have been evaluated and how protection against them has been achieved.**

… and CENELEC WG26 focuses Security Standardisation for Railways

SIEMENS



IEC 62443 – A Global Standard for Industry Automation IT Security



IEC / ISA-62443

General

- 1-1 Terminology, concepts and models — IS* 2009
- 1-2 Master glossary of terms and abbreviations
- 1-3 System security compliance metrics — NP rejected

Definitions
Metrics

Policies and procedures

- 2-1 Requirements for an IACS security management system Ed.2.0 — CD* 2Q18
- 2-2 IACS Protection Levels — NP* 3Q18
- 2-3 Patch management in the IACS environment — TR* 06/15
- 2-4 Requirements for IACS solution suppliers — IS* 06/15

Requirements placed on security organization and processes of the plant owner and suppliers

System

- 3-1 Security technologies for IACS — TR* 2009
- 3-2 Security risk assessment and system design — CDV* 1Q18
- 3-3 System security requirements and security levels — IS* 08/2013

Requirements to achieve a secure system

Component

- 4-1 Product development requirements — IS* 01/18
- 4-2 Technical security requirements for IACS products — FDIS* 2Q18

Requirements to secure system components

Functional requirements | Processes

*DC: Draft for Comment
*CDV: Committee Draft for Vote

*IS: International Standard
*TR: Technical Report

*NP: New Proposal
*FDIS: Final Draft for IS

The way forward in Railway IT Security Standardisation

2001: EN 50159-2 published (communication security)

2011: Integration with EN 50159-1

May 2014 : SC9XA Survey group (SGA16)

Sep 2016 : SC9XA/SGA16 report

June 2016 : Creation of a TC9 X – SG24.

- investigate and identify the various, varying and intended approaches

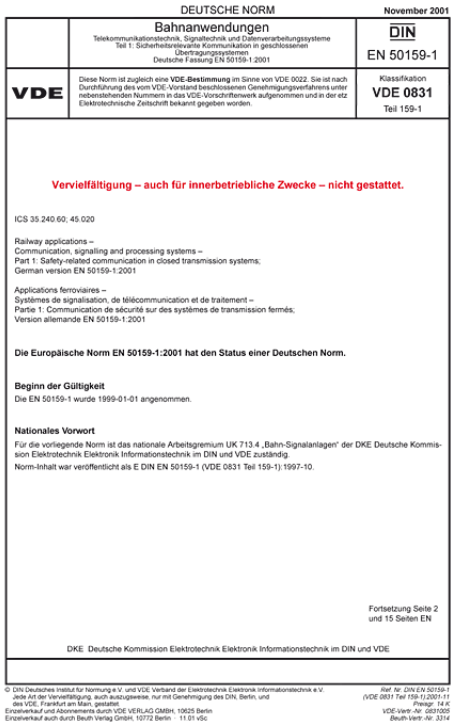
July 2017 : Creation of TC 9X – WG 26 to produce a Technical specification

- 68 experts registered,
- Approx. 30 people participating to F2F events
- Regular meetings and conference calls

June 2019: prTS 50701 published for commenting

October 2019: prTS 50701 published for voting

August 2020: publication TS 50701



DEUTSCHE NORM November 2001

	Bahnanwendungen Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme Teil 1: Sicherheitsrelevante Kommunikation in geschlossenen Übertragungssystemen Deutsche Fassung EN 50159-1:2001	DIN EN 50159-1
VDE	Diese Norm ist zugleich eine **VDE-Bestimmung** im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Vorstand beschlossenen Genehmigungsverfahrens unter nebenstehenden Nummern in das VDE-Vorschriftenwerk aufgenommen und in der etz Elektrotechnische Zeitschrift bekannt gegeben worden.	Klassifikation **VDE 0831** Teil 159-1

Vervielfältigung – auch für innerbetriebliche Zwecke – nicht gestattet.

ICS 35.240.60; 45.020

Railway applications –
Communication, signalling and processing systems –
Part 1: Safety-related communication in closed transmission systems;
German version EN 50159-1:2001

Applications ferroviaires –
Systèmes de signalisation, de télécommunication et de traitement –
Partie 1: Communication de sécurité sur des systèmes de transmission fermés;
Version allemande EN 50159-1:2001

Die Europäische Norm EN 50159-1:2001 hat den Status einer Deutschen Norm.

Beginn der Gültigkeit

Die EN 50159-1 wurde 1999-01-01 angenommen.

Nationales Vorwort

Für die vorliegende Norm ist das nationale Arbeitsgremium UK 713.4 „Bahn-Signalanlagen" der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE zuständig.

Norm-Inhalt war veröffentlicht als E DIN EN 50159-1 (VDE 0831 Teil 159-1):1997-10.

Fortsetzung Seite 2
und 15 Seiten EN

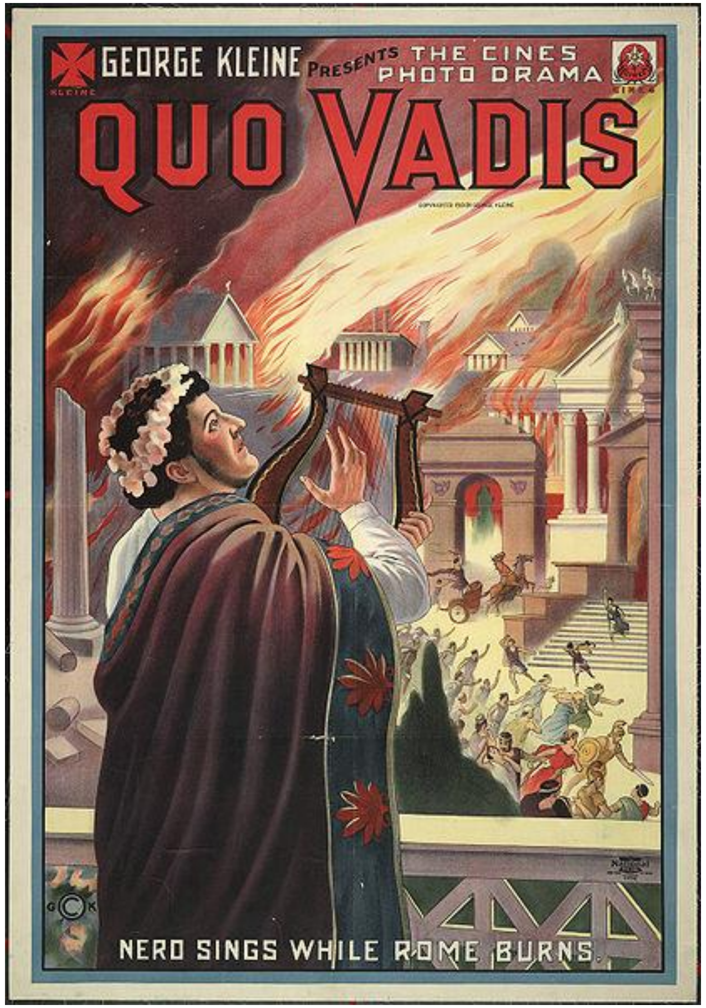
DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE

© DIN Deutsches Institut für Normung e.V. und VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V.
Jede Art der Vervielfältigung, auch auszugsweise, nur mit Genehmigung des DIN, Berlin, und des VDE, Frankfurt am Main, gestattet.
Einzelverkauf und Abonnements durch VDE VERLAG GMBH, 10625 Berlin
Einzelverkauf auch durch Beuth Verlag GmbH, 10772 Berlin · 11.01 vSc

Ref. Nr. DIN EN 50159-1
(VDE 0831 Teil 159-1):2001-11
Preisgr. 14 K
VDE-Vertr.-Nr. 0831005
Beuth-Vertr.-Nr. 3314

Conclusion: Security has to become part of our Digitalization DNA

- Safety and Security have to be separated as far as reasonable but need effective coordination
- Digitalization without proper consideration of security is infeasible
- IEC 62443 will become the backbone also for railways
- However some adaptations to the railway environment are necessary
- These will be introduced by TS 50701
- Last but not least security is a joint effort by all stakeholders


GEORGE KLEINE PRESENTS THE CINES PHOTO DRAMA
QUO VADIS
NERO SINGS WHILE ROME BURNS.

Source: Wikipedia (Public Domain)