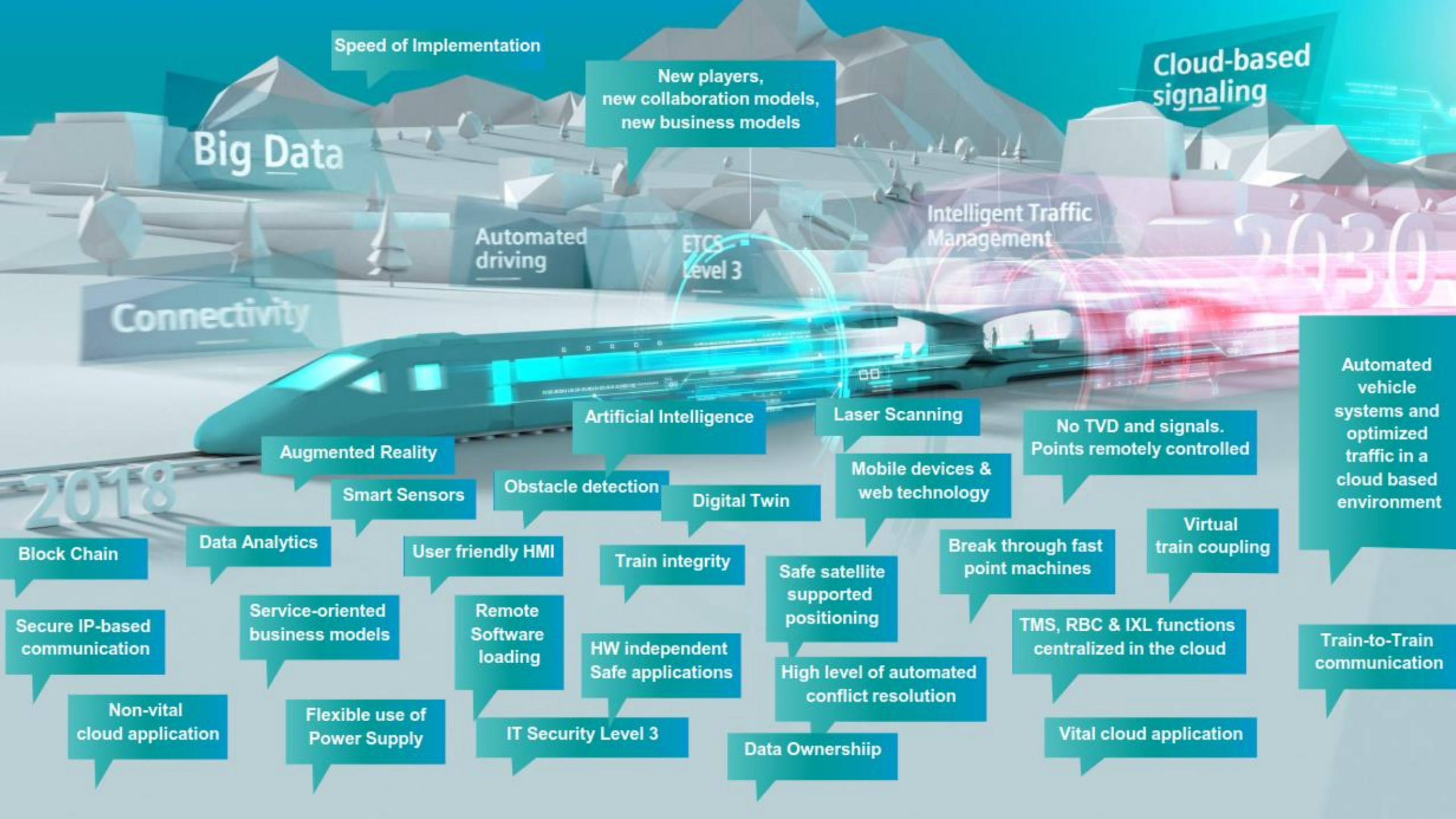
SIEMENS
Ingenuity for life

System Safety and Security for the digital railway

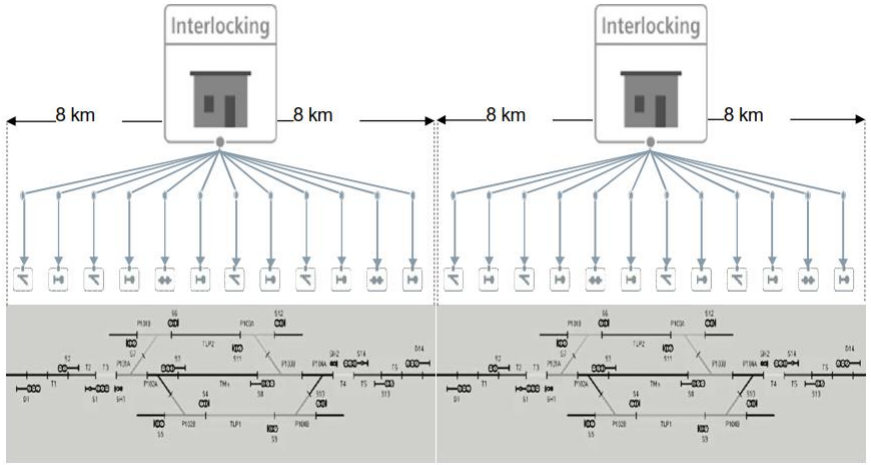
Dr Luke Wildman RAMSS


Speed of Implementation
New players, new collaboration models, new business models
Cloud-based signaling
Big Data
Automated driving
ETCS Level 3
Intelligent Traffic Management
2030
Connectivity
2018
Automated vehicle systems and optimized traffic in a cloud based environment
Artificial Intelligence
Laser Scanning
No TVD and signals. Points remotely controlled
Augmented Reality
Smart Sensors
Obstacle detection
Digital Twin
Mobile devices & web technology
Block Chain
Data Analytics
User friendly HMI
Train integrity
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
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
High level of automated conflict resolution
Data Ownershiip
Vital cloud application

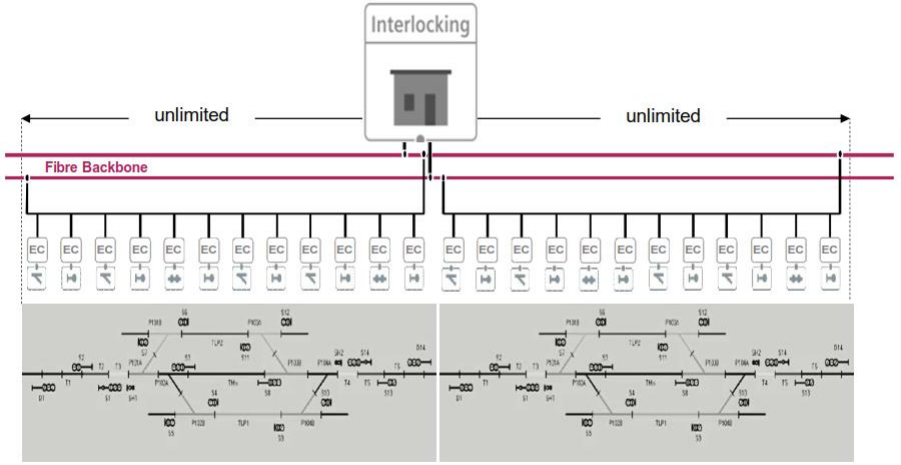
Wayside architectural Change - in the Age of Digitalization

SIEMENS
Ingenuity for life

- Conventional radial cabling to field elements
- Decentralised Interlocking in location cases, Signalling equipment rooms, and stations
- Specialized proprietary hardware
- Control distance up to 8 km
- Proprietary interfaces to field elements and between stations



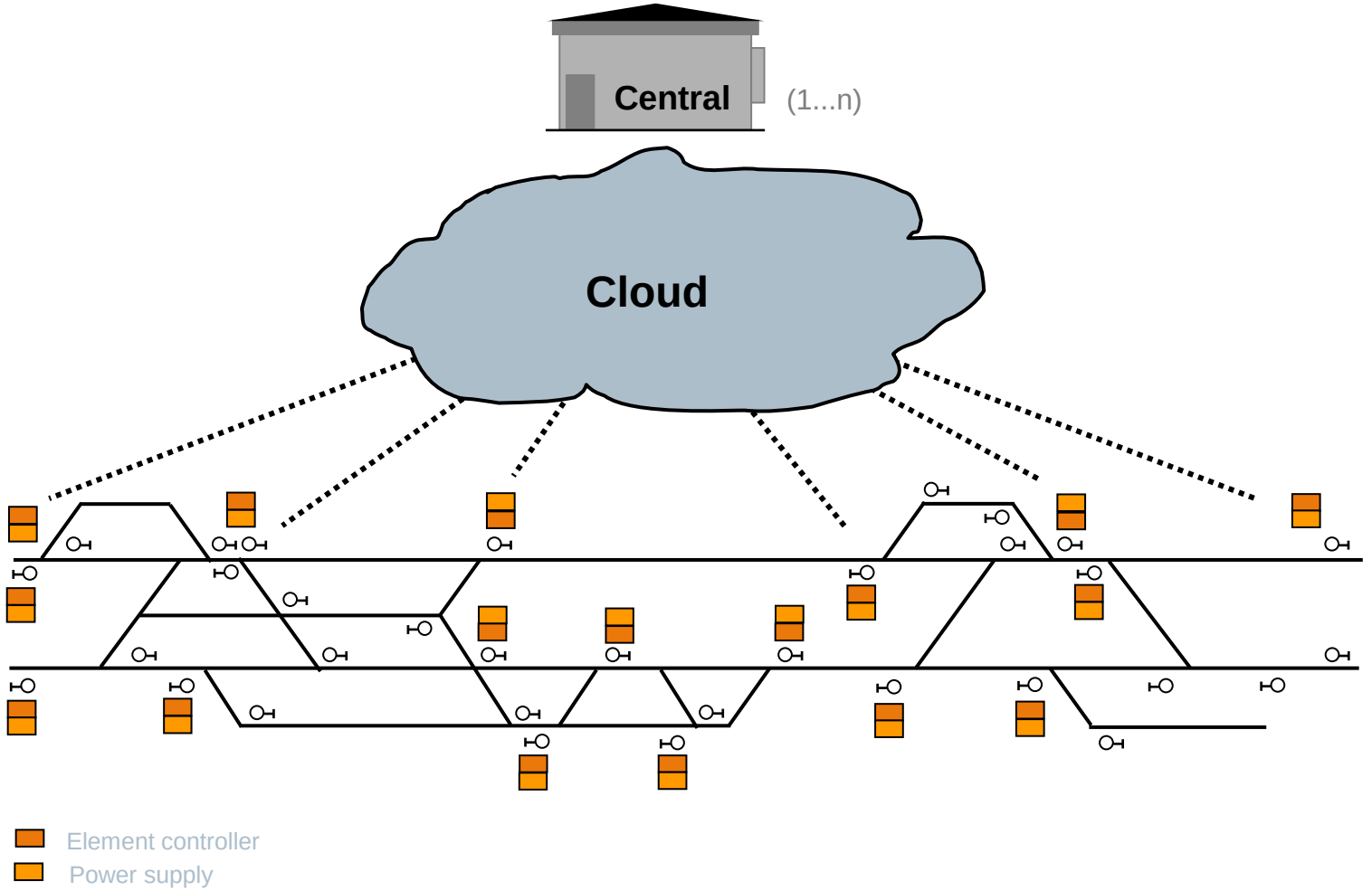
- Secure IP based system architecture
- Centralised Interlocking cabinets
- Specialized proprietary hardware
- Unlimited control distance
- Standardized interfaces to element controllers and between stations



Vision - Centralised Wayside Architecture

SIEMENS
Ingenuity for life

COTS Hardware
Remote Hosting



Benefits of digitalisation

SIEMENS
Ingenuity for life

Highest Safety Standards :
Automated protection for train separation and speed and maintenance workers

Reduced infrastructure costs :
Less trackside equipment, centralised, non- proprietary

Capacity Increases:
Driving with continuous electronic lookahead; Trains can run closer together

Increased availability :
Less equipment, more monitoring

Increased Security:
Security architectures, defence in depth, Authentication, monitoring, encryption, patch management, mature security culture

Energy Efficiency:
Automated Train Regulation (speed, brake)

A few of the Challenges encountered so far

SIEMENS
Ingenuity for life

- Systems (Trackside, TMS, Onboard, Comms, …) to be integrated with performance
- New products to be integrated
- Diverse User requirements
- New Ways of Working (Operations) and Products (Maintenance)
- Speed of Implementation: Challenging time frames, Resourcing
- Cyber-Security : If it is not Secure it is unlikely to be Safe (ONRSR)
- Complex Supply Chains

Systems Engineering

SIEMENS
Ingenuity for life

Challenges

- Differing requirements across customers
- Non-standard technical requirements and changes
- Extended time required for requirements clarification

Innovation

- Identifying Standard requirements and solutions
- Safety-Related Application Conditions included

Benefits

- Provides some reuse over related series of projects
- Baseline for generic assurance cases

Better

- Standardised solutions and requirements e.g. UNISIG European Rail Traffic Management System
- Shared processes and tools : Requirements, Configuration EULYNX is standardising processes, architectures and requirements over several European projects.

ertms

EULYNX

EULYNX Initiative

EULYNX Partners:
Bane NOR
Société Nationale des Chemins de Fer Luxembourgeois (CFL)
DB Netz AG (DB)
S.A. Infrabel
Liikennevirasto (FTA)
Network Rail
ProRail B.V.
Rete Ferroviaria Italiano (RFI)
SBB AG
Société Nationale des Chemins de Fer Français (SNCF)
SŽ-Infrastruktura, d.o.o. (SŽ)
Trafikverket

System engineering process

Document number: Eu.Doc.27
Baseline: 2.0 (0.A)
EULYNX Baseline Set: 2

BANE NOR · CFL · DB NETZE · INFRABEL · NetworkRail · ProRail · Liikennevirasto · RFI · SBB CFF FFS · SNCF · Slovenske železnice · TRAFIKVERKET

© EULYNX Partners

Modular Safety Cases

SIEMENS
Ingenuity for life

Challenges

- Larger projects introduce new products and technologies: Wireless, Cloud, ..
- Specific Application needs novel configuration
- Product application design may be new to engineers

Innovation

Product Application Safety Cases (PASC) binding :

Product Safety Related Application Conditions,
Product related testing and Integration activities
Product-specific risk assessments, Template Validation
Product related Operations and Maintenance
Supporting Product Safety Cases

Benefits

- Manages new product risk, novel application risk, re-usable sometimes/partly

Better

- Modular Safety Cases by Function (e.g. LX Object Controller)
- Potential to support cross-acceptance

Design Assurance

SIEMENS
Ingenuity for life

Challenges

- Novel Principles
- Complex Logic and failure modes.

Innovation

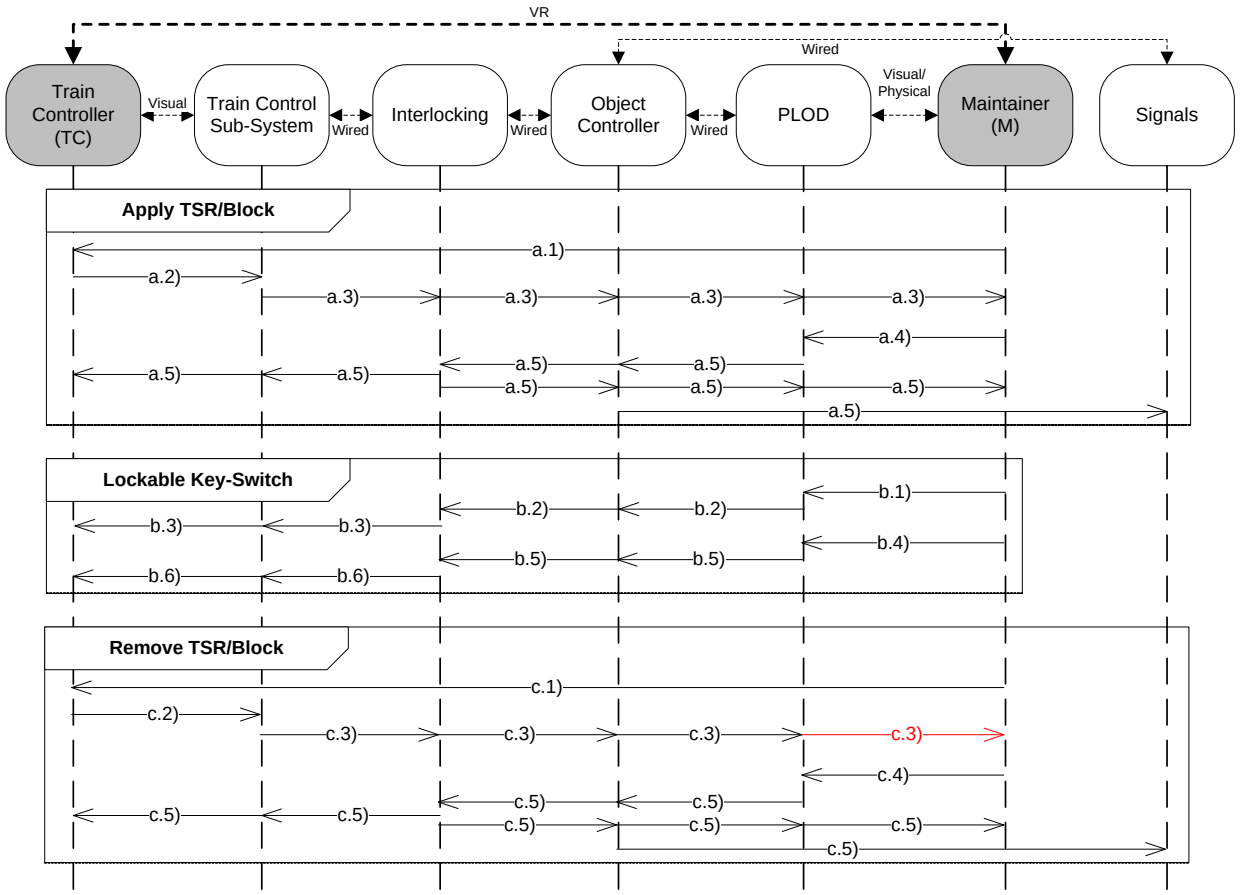
- Model-based Safety Analysis for Interlocking Logic
- E.g. Message-sequence Charts
- State Machines
- Transition-based structure for Failure Analysis

Benefits

- Better shared understanding of detailed design
- Analysis traceable to design
- Basis for SFAIRP demonstration

Better

- Model-based design and analysis (e.g SysML)
- Automatic verification



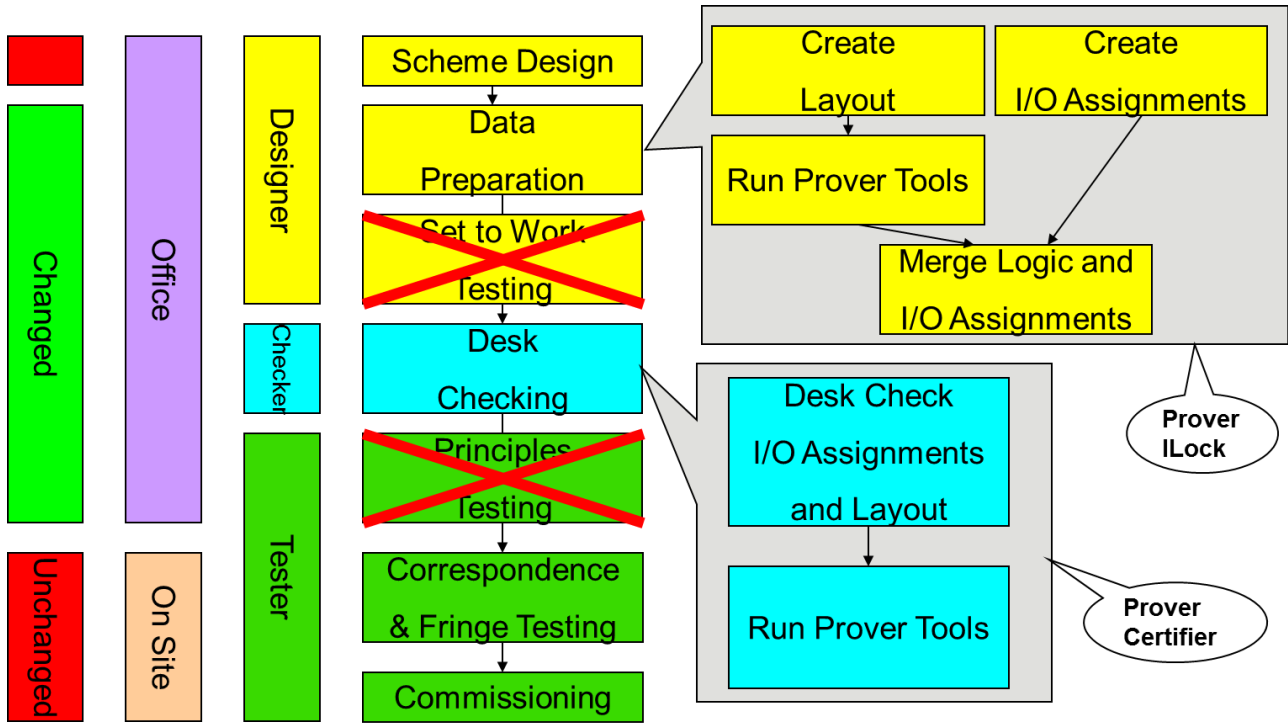
Interlocking Data – Automation : Prover Technology iLock/Certifier

SIEMENS
Ingenuity for life

- Prover iLock and Prover Certifier (certified SIL4)
- Automated solution for Interlocking data :
  - Create interlocking data automatically from railway layout data
  - Run functional testing of interlocking data automatically
  - Prove interlocking data against safety principles automatically

- This fundamentally changes activities of Designer, Checker and expectations of the customer

- Extends naturally to other Safety and non-safety functions as Digitalisation continues i.e Automated train control systems (CBTC/ETCS)



Cyber Security

SIEMENS
Ingenuity for life

Challenges

- There is no air-gap
- Digitalisation increases the cyber-attack surface

Innovations

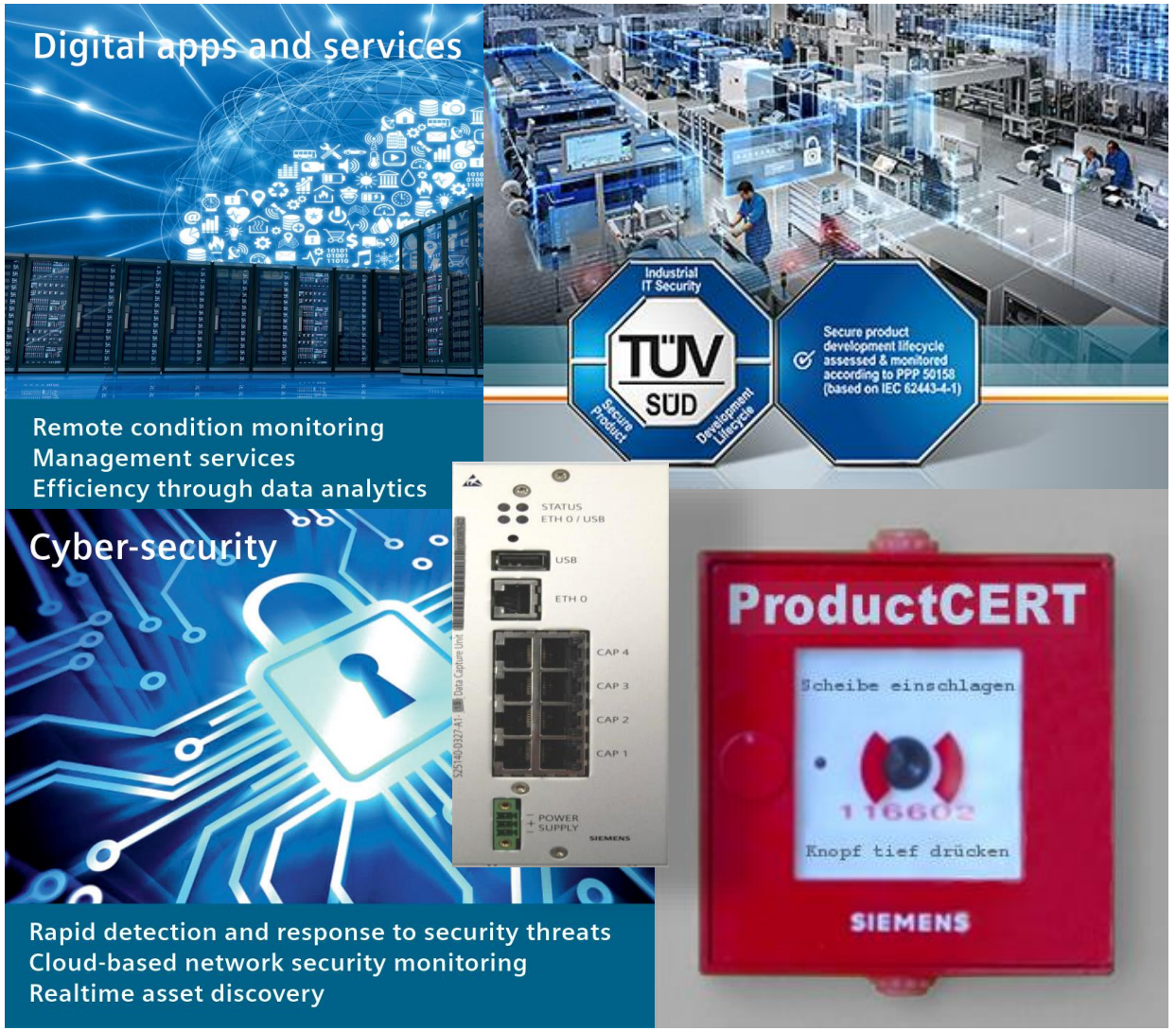
- Application of Industrial Control Systems standard (IEC. 62443) in product and solution lifecycle
- Introduction of rail-safety certified one-way gateways (data-diodes) to support export of data for maintenance and passenger information
- Encrypted channels, Security Incident Event monitoring, Endpoint protection, Patching,…

Benefits

- Certifiable achievement of levels of security SL2/3
- Reduction of Security Risk SFAIRP

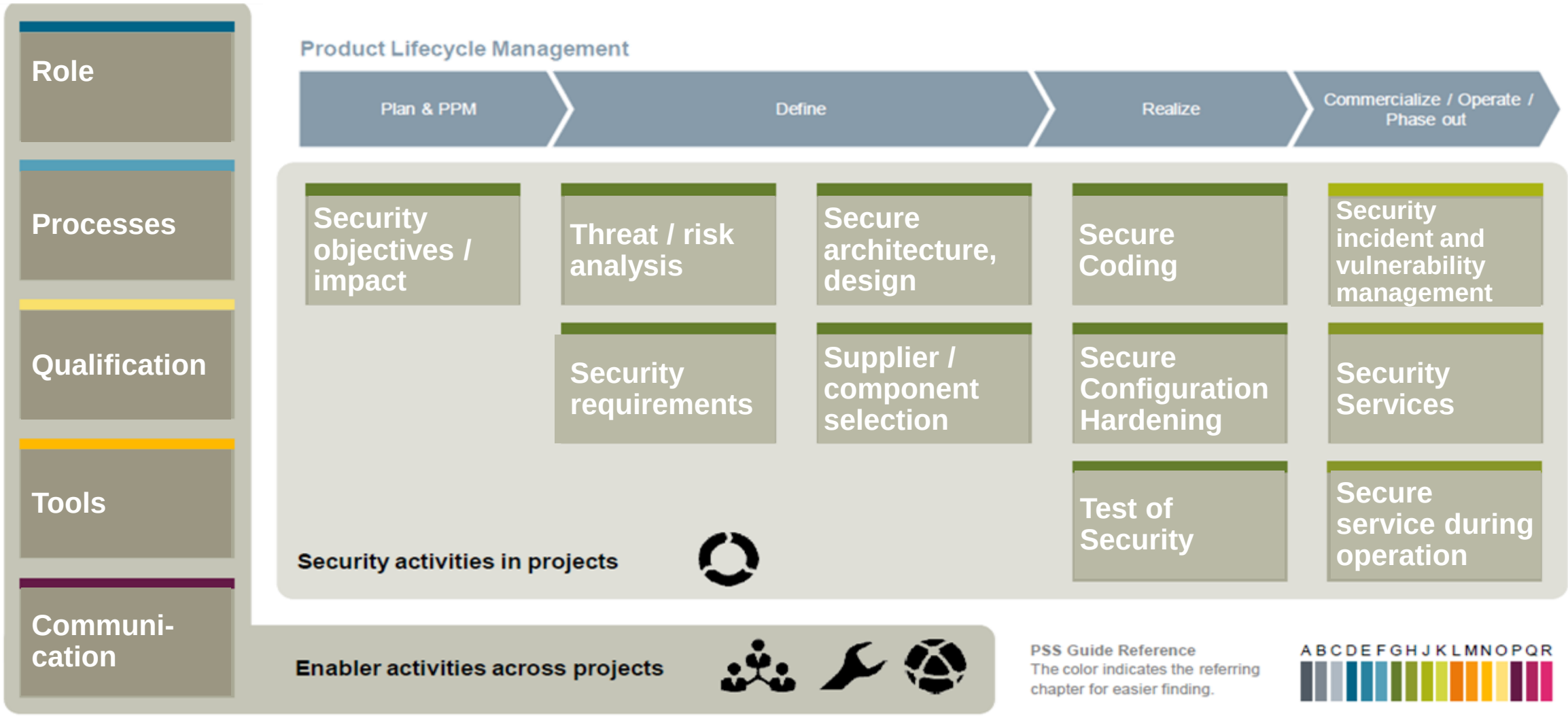
Better

- Mature resilient security organisations maintaining security controls and culture



Security activities in the product lifecycle and in projects

SIEMENS
Ingenuity for life



IT security is the task of all!
Training concept on four levels

SIEMENS
Ingenuity for life

Specialist Security

International cooperation in the field of IT security

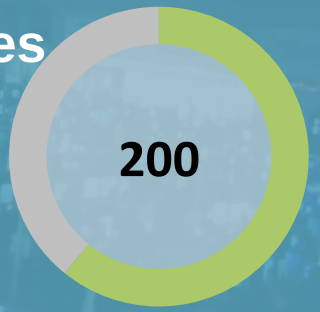
Corporate Technology, Universities, Shift2Rail, SG24

Roll-specific training

Product Solution Security roles

Curriculum for Experts

and Security Management



Security (e.g. in projects)

Project specific training for network, commissioning, maintenance, security testing

Awareness Programm

PSS Web Based Training by group (e.g. Management, Project

and Service Personal)

Charter of Trust
Munich Security Conference Feb 2018

SIEMENS
Ingenuity for life

Principles

1. **Ownership for cybersecurity**
2. **Responsibility throughout the digital supply chain:**
   Identity & access management, Encryption, Continuous protection
3. **Security-by-default**
4. **User-centricity**
5. **Innovation and co-creation**
6. **Education**
7. **Certification for critical infrastructure and solutions**
8. **Transparency and response**
9. **Regulatory framework**
10. **Joint initiatives**

SIEMENS AES AIRBUS Allianz Atos enel

DAIMLER IBM Munich Security Conference msc Münchner Sicherheitskonferenz NXP SGS T··