EUG ERTMS Security Core Group

ENISA-ERA Conference
CYBERSECURITY in RAILWAYS

01.12.2022 | Lille

Topics

1. Main Challenges ERTMS Security
2. ESCG Top Goals
3. The ESCG set-up and deliveries
4. Synchronisation with other EU CCS and Cyber Security initiatives
5. Wrap up and Next steps

TSI Subsets contain basic Security thoughts – However, Operators face the need to implement state-of-the-art Security

The main challenges are:

1. Current subsets focus on cross border interoperability (RBC-Euroradio) only, while **Security requires a holistic approach**
2. Commonly agreed cyber **security standards require a higher level of security** than requested by current TSI subsets
3. Current installations must be seen as “legacy systems” with the **need for compensating measures** – Some operators now are defining cyber security measures, which lead to specific solutions per operator
4. **Future installations** should be **based on commonly agreed cyber security requirements** specifications

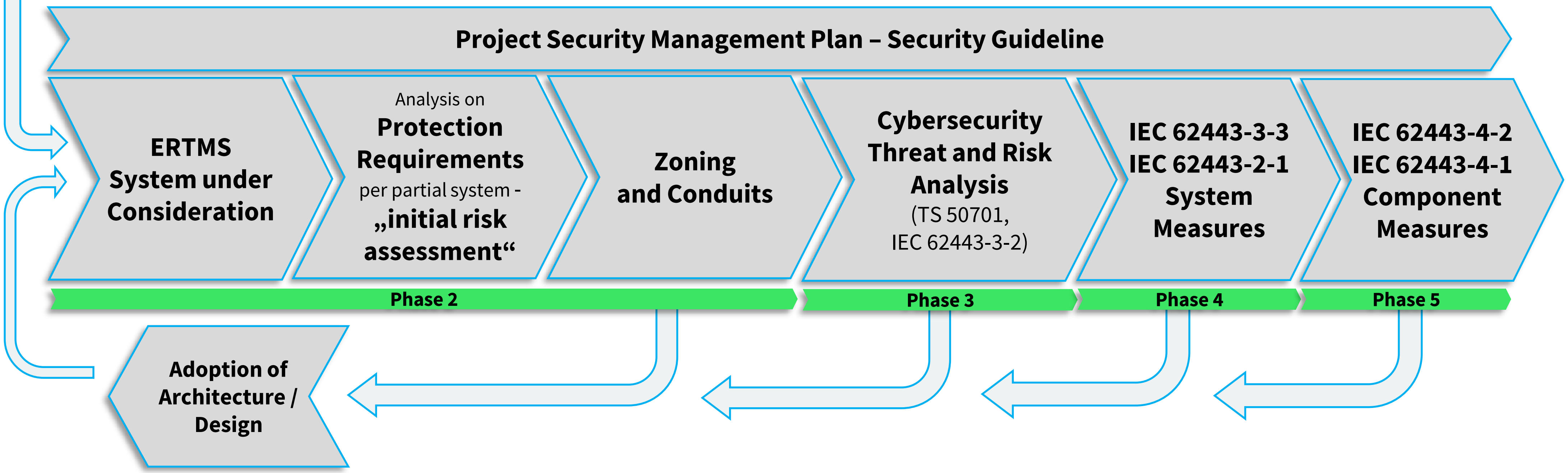
The ERTMS Security Core Group helps to solve these challenges by providing Guidance on

1. **Best practice** ERTMS implementation, based on TSI 2016(2019) to achieve common understanding and security level
2. **Future** ERTMS **requirements** to support next TSI (recast) and to guide “standard” implementation for the suppliers and infra managers
3. Provision of a norm and regulation compliant **risk analysis**
4. Provision of **security measure definition** documentation to support efficient and unified implementation
5. Ensuring **Synchronisation** with ERJU System Pillar, CER, EIM, ENISA, EULYNX, OCORA and further European organisations and representative bodies

The Management is compliant to IEC 62443 and TS 50701

Guidelines + Best practices + Standards

- IEC 62443, TS 50701
- EN 50159
- ERTMS Scope
- EULYNX/RCA Security Cluster
- OCORA Security Working Group
- Shift2Rail X2Rail 3



Project Security Management Plan – Security Guideline

ERTMS System under Consideration

Analysis on **Protection Requirements** per partial system - **„initial risk assessment“**

Zoning and Conduits

Cybersecurity Threat and Risk Analysis (TS 50701, IEC 62443-3-2)

IEC 62443-3-3 IEC 62443-2-1 System Measures

IEC 62443-4-2 IEC 62443-4-1 Component Measures

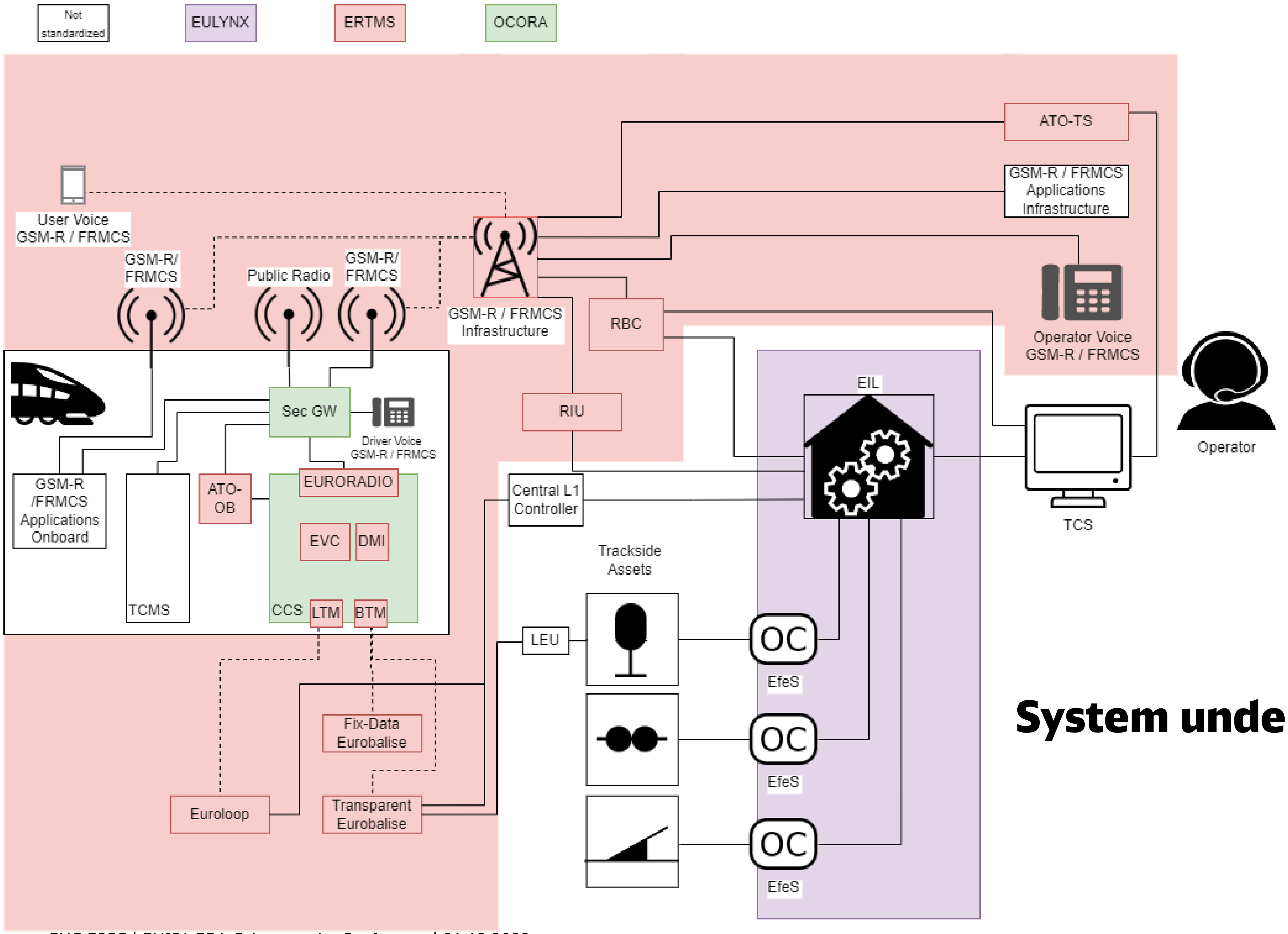
Phase 2

Phase 3

Phase 4

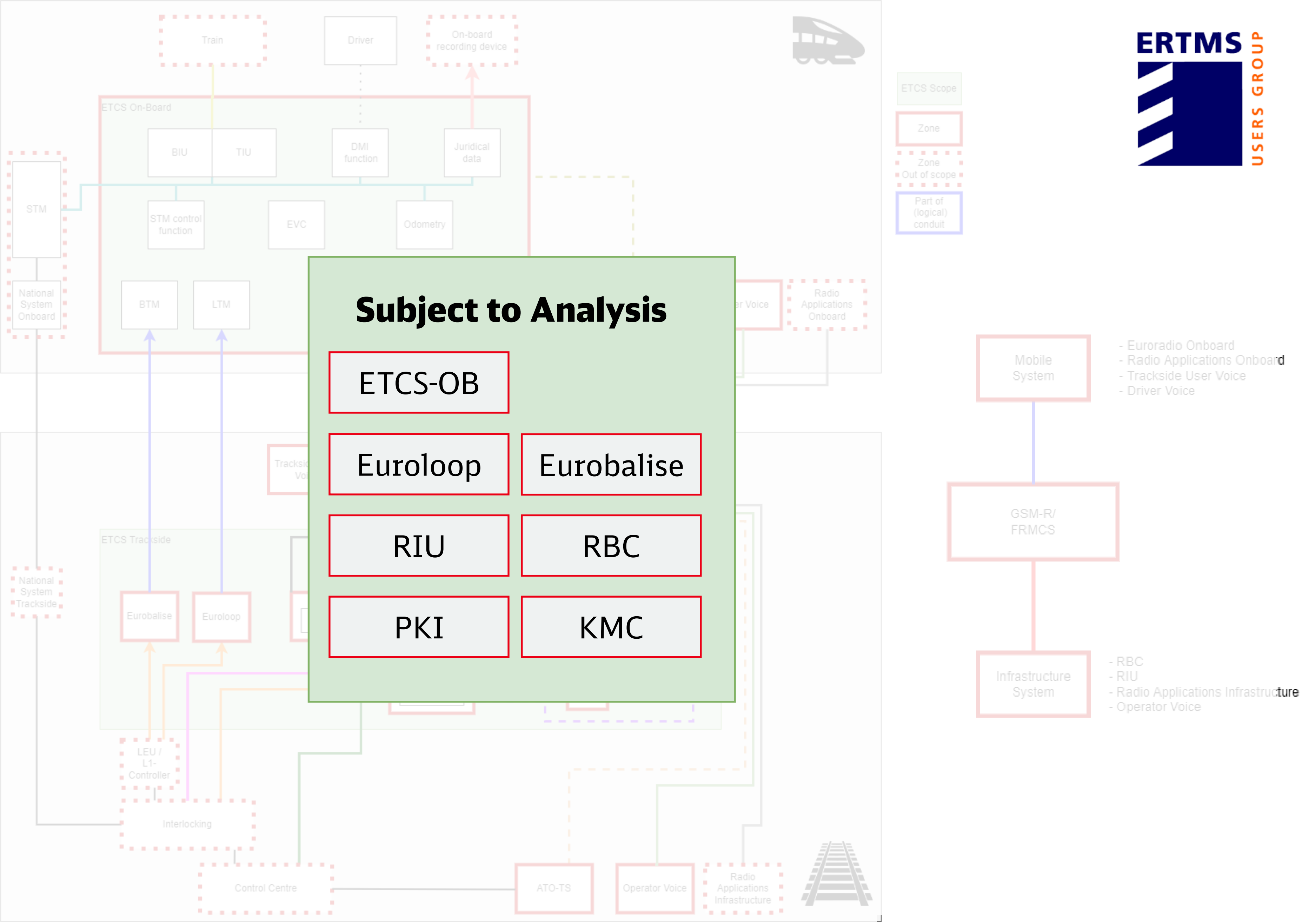
Phase 5

Adoption of Architecture / Design



System under Consideration

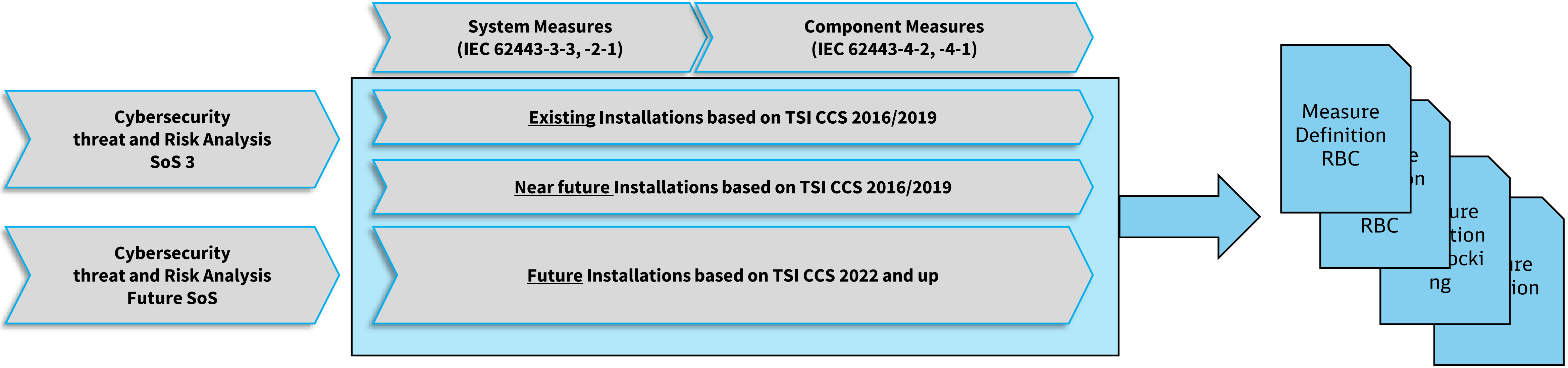
Zone and Conduit Model



Subject to Analysis

- ETCS-OB
- Euroloop
- Eurobalise
- RIU
- RBC
- PKI
- KMC

The risk analysis is performed for different application phases



System Measures
(IEC 62443-3-3, -2-1)

Component Measures
(IEC 62443-4-2, -4-1)

Cybersecurity
threat and Risk Analysis
SoS 3

Cybersecurity
threat and Risk Analysis
Future SoS

Existing Installations based on TSI CCS 2016/2019

Near future Installations based on TSI CCS 2016/2019

Future Installations based on TSI CCS 2022 and up

Measure
Definition
RBC

- Measure Definition and Application **Guideline per System/Component**
- **Respect** of **application status**
- Base for **migration plan**
- **Proposal** for **future TSI Subsets**

European Collaboration allows for efficient and harmonized standards

Initiatives already started:

1. Representative bodies (technical and policy) process synchronisation
2. EUG exchange on KMS,KMC,PKI Set-up
3. Synchronisation with EULYNX/RCA and OCORA on Security Process and Shared Security Services
4. Shift2Rail X2Rail3 Synchronisation on Shared Security Services

- System Pillar Security Group will make use of the already performed analysis and definitions
- The ESCG will finish its current task until 03/2023

Conclusions and future challenges

What we achieved:

- Common understanding on status and **Need for security**
- **Practical guidance** on improving ERTMS Security for **existing installations**
- **Practical method** for **improving future ERTMS/CCS Security**
- **Active team** with knowledge on **Security** for **on-board** and **trackside ERTMS**

EUG ERTMS Security Core Group webpage:
https://ertms.be/workgroups/cyber security

To be addressed:

- Development of ERTMS security **migration roadmap**
- Include Guideline to **TSI CCS application guide**
- Transfer guideline requirements into **TSI CCS subsets**
- **Possible** expansion to **ATO-OB** and **ATO-TS**

- ESCG expert group **can be used** as
  - **extended work bench** and
  - **mirror group**

  to review and delivery content **to System Pillar** Security group

Thank you for your attention!

(www.ertms.be)