Quality & Safety for Systems & Software
Railway Engineering

Assurance provided by a second pair eyes (RASBO) of the correct Safe integration by the proposer of the ETCS into the infrastructure

Ir. Marc Bronchart
AsBo & Independent Safety Assessor

Quality & Safety for Systems & Software

Railway Engineering

Independent Assessment of the safe integration of an ETCS on an existing infrastructure

Ir. Marc Bronchart

AsBo & Independent Safety Assessor

Presentation structure

- Part I
  Safety impacts of the integration of ETCS within an existing Railway infrastructure

- Part II
  Regulatory framework

- Part III
  Independent Safety Assessment by the CSM Assessment Body

PART I

SAFETY IMPACTS OF THE INTEGRATION OF ETCS WITHIN AN EXISTING RAILWAY INFRASTRUCTURE

Safety Impact of ETCS Integration

- Railway infrastructure consists of following subsystems:
  - Track
  - Energy
  - Signalling
  - Rolling-stock
  - Civil work
  - Tunnel equipments
  - …..

Safety Impact of ETCS Integration

- All these subsystems are interfacing and interacting between them and with:
  - passengers
  - train drivers
  - maintenance staff
  - emergency services
  - ...

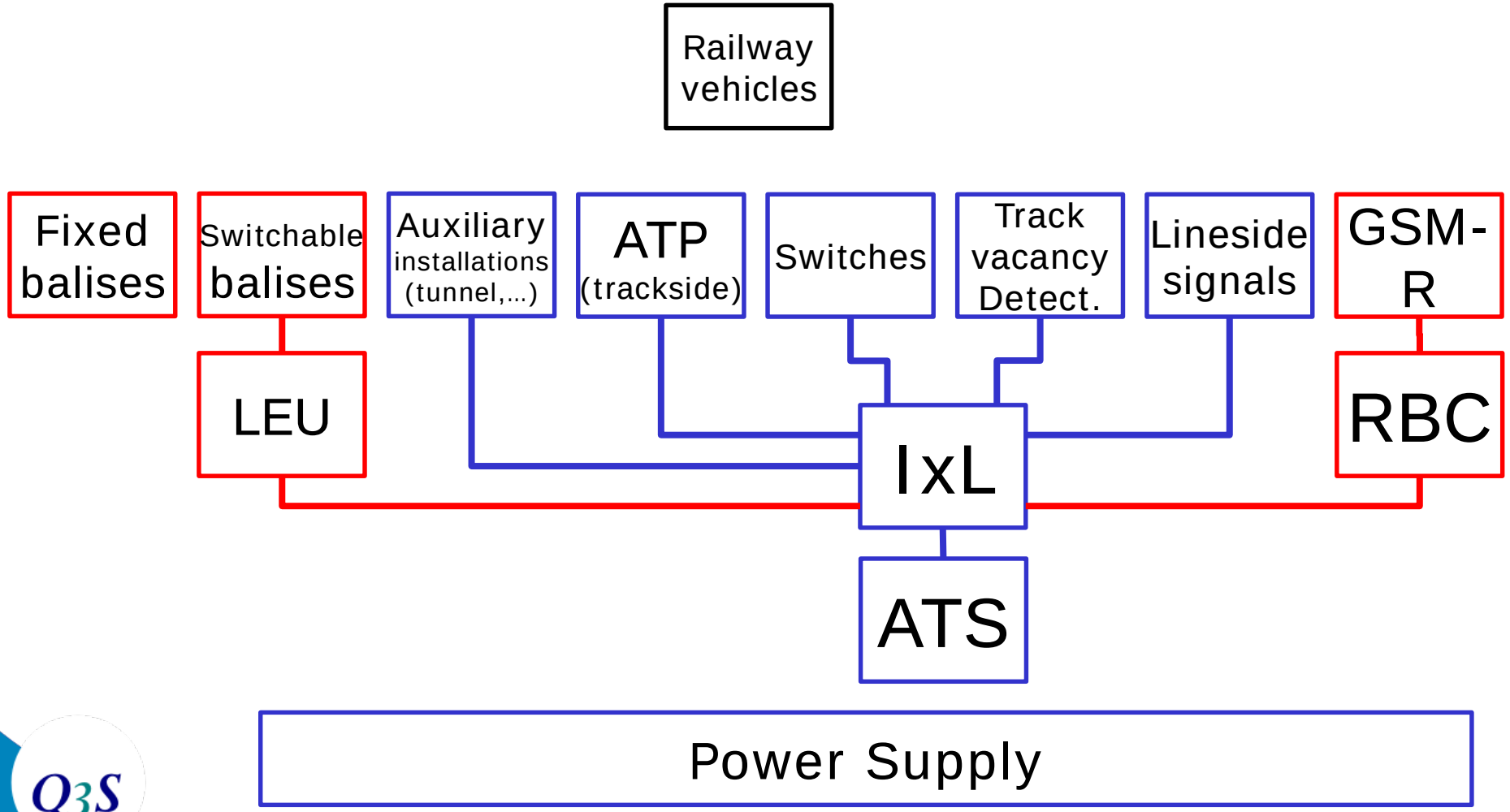
Safety Impact of ETCS Integration

- Classical Signalling subsystem is made of following equipments:
  - Line side or cab signalling
  - Train detection device (Track circuits or axle counters)
  - Interlocking
  - Automatic Train Supervision (ATS)
  - On Board AWS or ATP
  - Trackside-related AWS or ATP equipment
  - Miscellaneous detectors

Safety Impact of ETCS Introduction

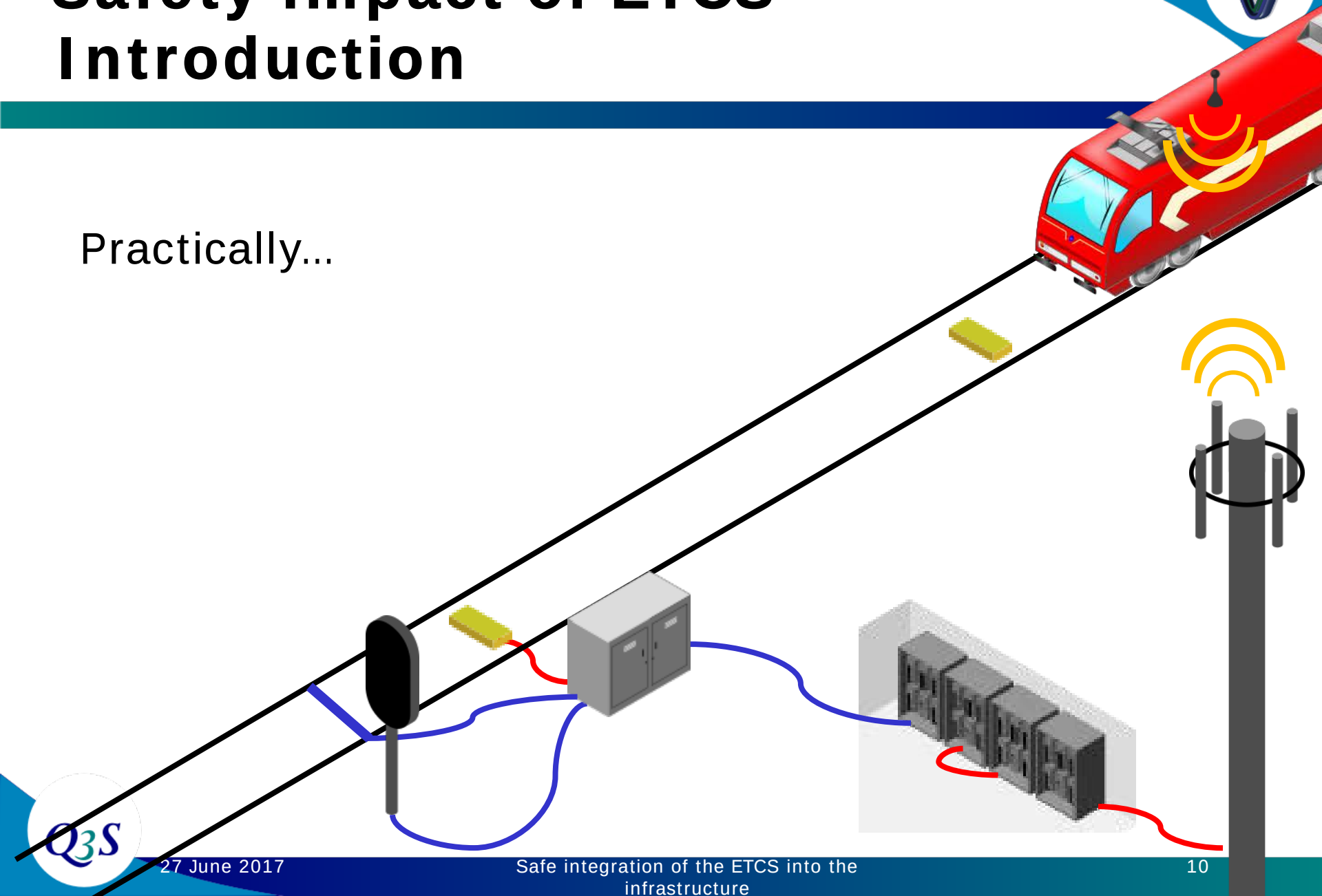
- Integration of ETCS within the existing infrastructure can lead to different situations:
  - Existing signalling system update leading to ETCS compatible signalling system
  - Existing Signalling system update leading to a dual signalling (Existing class B system + ETCS)
  - …

Safety Impact of ETCS Introduction



Safety impact of ETCS Introduction

Practically...



Safety Impact of ETCS Introduction

- Following topics need also to be taken into account:
- Co-existence of different signalling systems on the network and associated transition zones
- Temporary configurations due to migration strategy leading to increased complexity

Safety Impact of ETCS Introduction

- Introduction of the ETCS equipment leads to equipments changes, even outside the signalling s/s:
  - New ETCS equipments
  - New interfaces between equipments and new interfaces with humans
  - Modifications or replacement of existing equipments (opportunity)
  - Removal of equipments

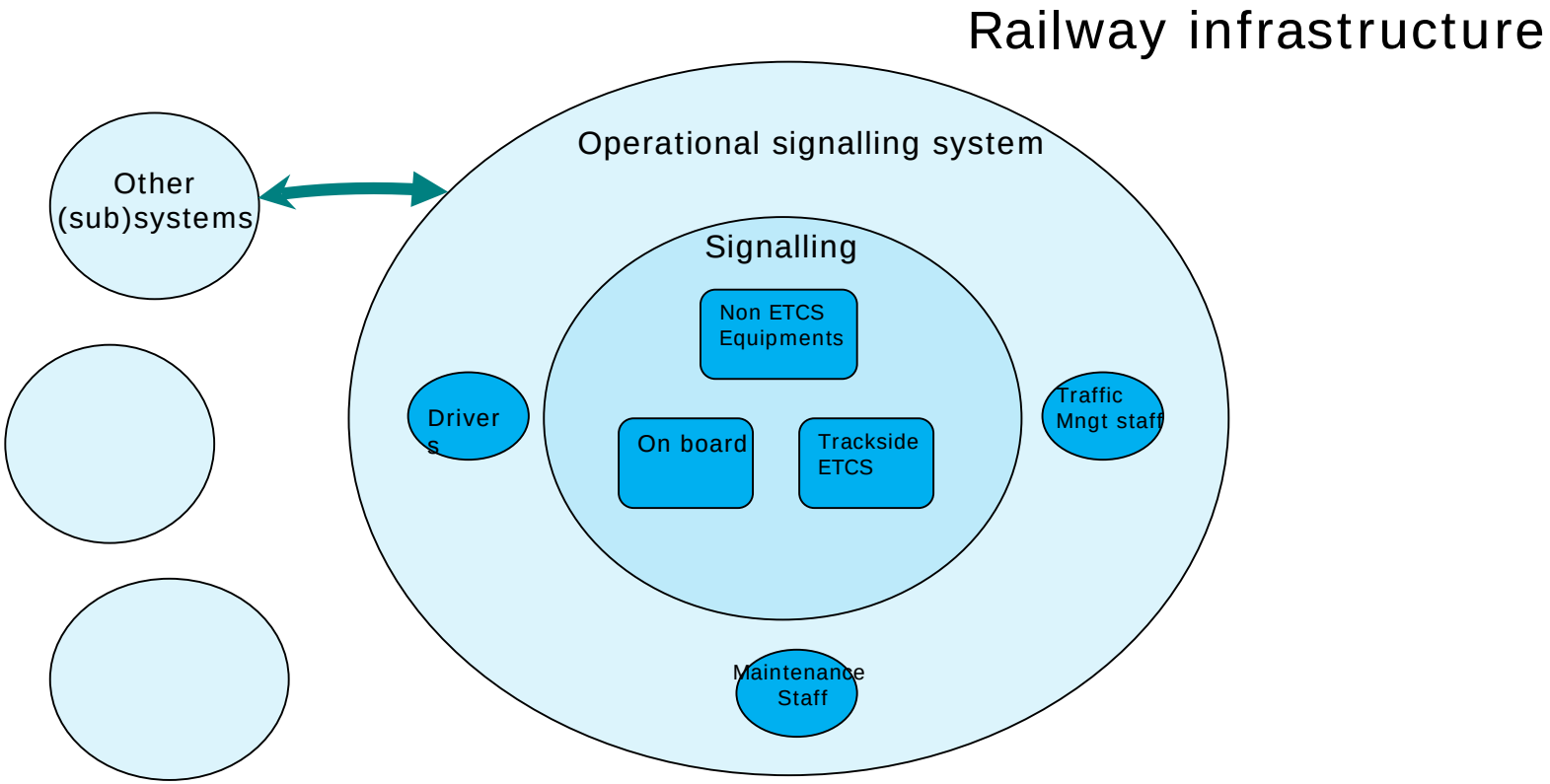
Safety Impact of ETCS Introduction

- Introduction of the ETCS lead also to:
  - Functional changes at the signalling system (obvious)
  - Operational & maintenance changes
  - Functional changes at the global system level (opportunity for new functions, different functional implementation)

Safety Impact of ETCS Integration

- Safety of the modified system needs to be demonstrated knowing that:
  - TSI CCS are requiring CENELEC application but limited to ETCS functionalities and equipments (constituents)
  - ETCS implementation is subjected to several design & operational choices by the Infrastructure owner. **ETCS is an configurable system that need to be further designed**
  - Not all equipments are subjected to Interoperable requirements
  - Existence of / need for specific functionalities are particular for the considered infrastructure

Safety impact of ETCS Integration



Safety Impact of ETCS Integration

⇨ TSI requirements are not sufficient for ensuring the safety of the modified system

Safety Impact of ETCS Integration

- Simple question:

How can ensure safety of the modified infrastructure taking all these elements into account?

- Need to define an approach ensuring global consistency from a safety point of view

Safety Impact of ETCS Integration

- Safety integration needs a global approach not sub-system per sub-system) and even in one sub-system TSI not ensuring safety

PART II

REGULATORY SAFETY FRAMEWORK

Regulatory framework

- TSIs per Subsystem — NoBo
- National Rules — DeBo
- Safety Directive — National Safety Auth.
- CSM RA — Assessment Body

Regulatory framework

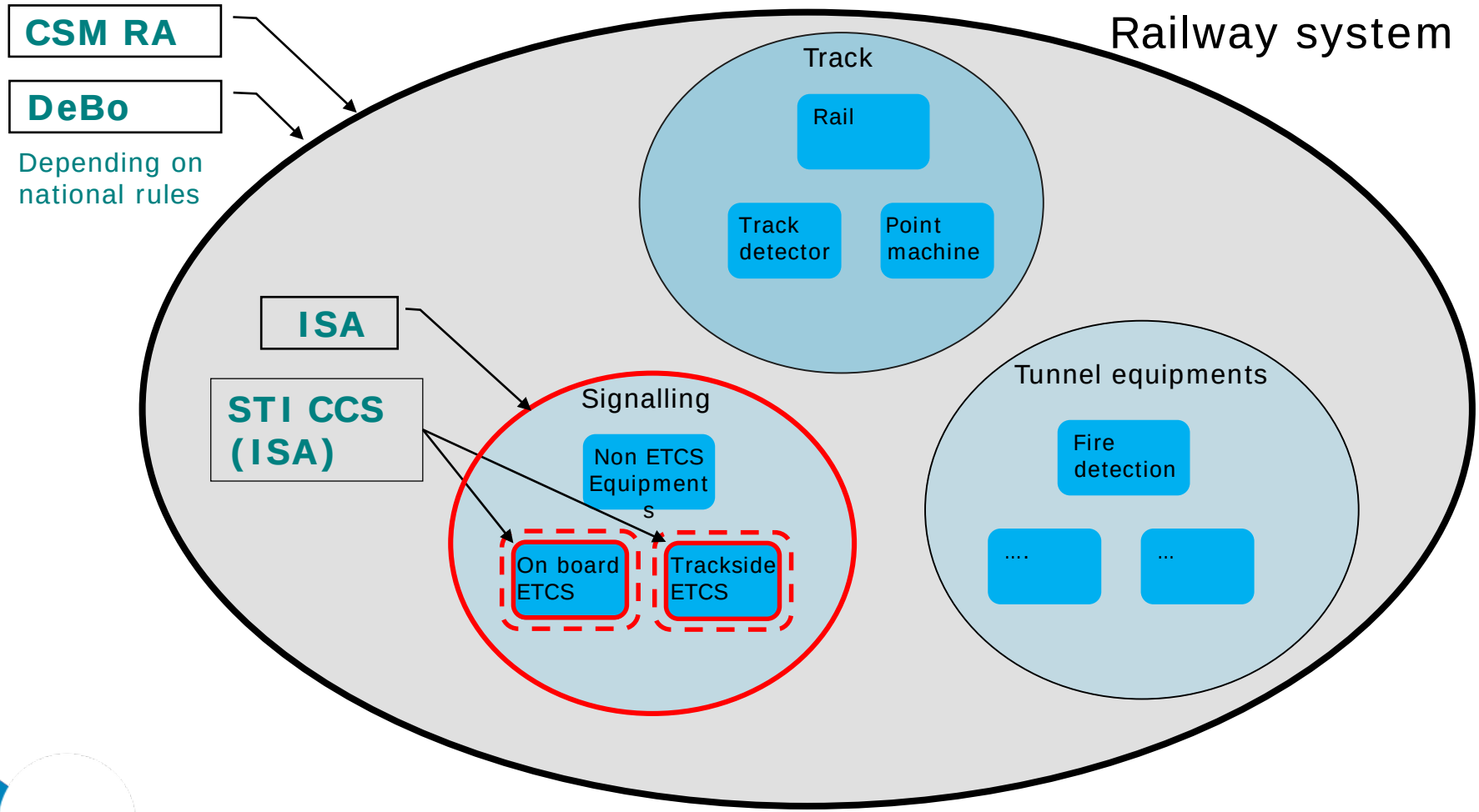
TSIs ≡ EU law	National Rules ≡ National Law	CSM RA ≡ EU Law
Independant Conformity Assessment by	NOBO	DEBO	ASBO

- TSIs contain essential requirements related to safety **as far as they are necessary for interoperability**
- Sole compliance with TSIs does not ensure safety is fully covered → additional risk assessment necessary
- Only where necessary for interoperability purposes, TSIs request application of specific part(s) of CSM RA
- TSIs do not question necessity to apply CSM RA for safe management of changes -> CSM RA must also be applied to demonstrate safety is fully controlled

BUT

Application of CSM RA shall not lead to requirements contrary to a TSI otherwise
TSIs need to be revised or MS shall ask for a derogation

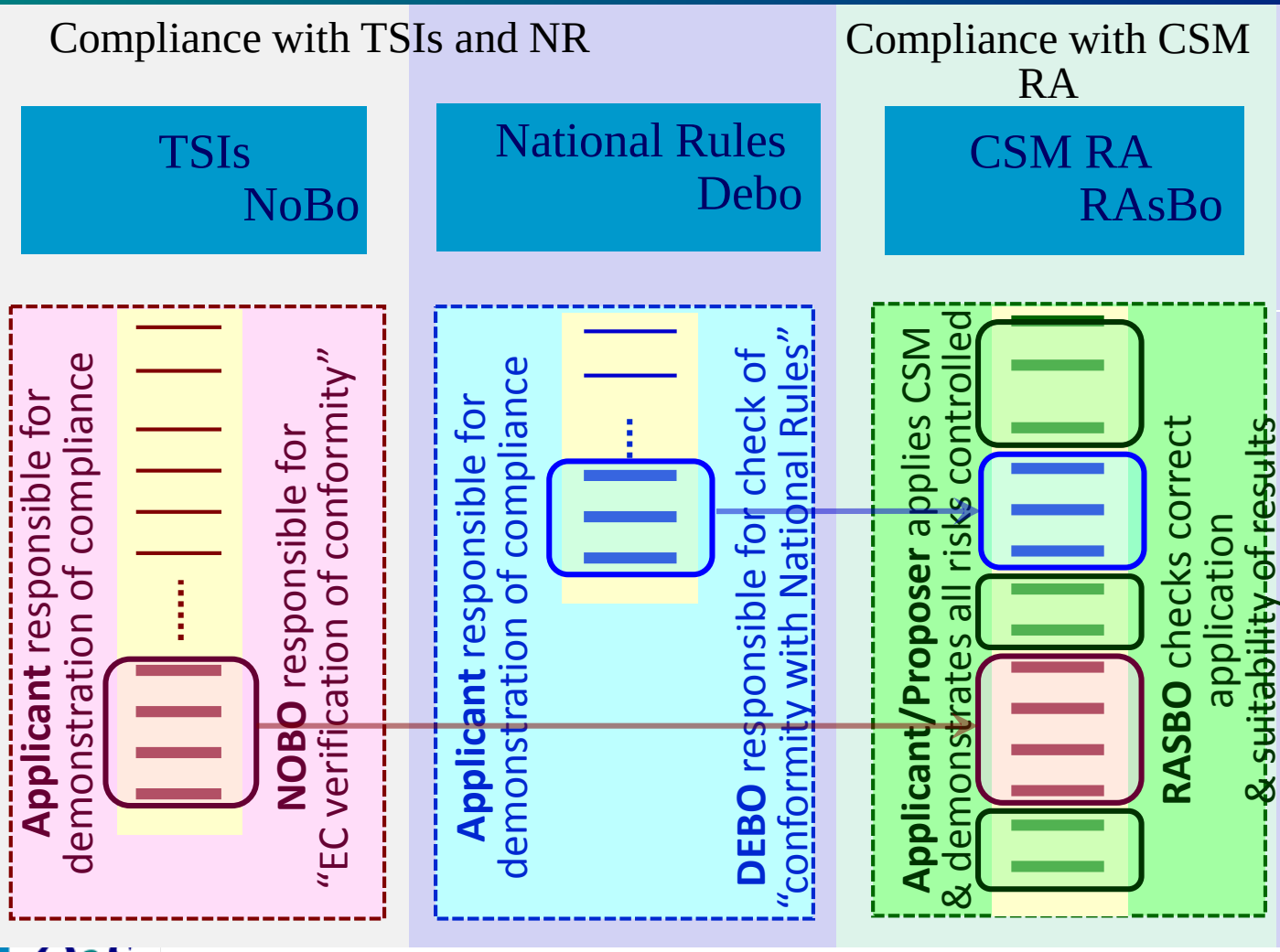
Regulatory framework



Regulatory framework

- Duplication of independent assessment work between different Conformity Assessment Bodies involved in a project shall be avoided
- Compliance with TSIs – Compliance with CSM Risk Assessment: WHAT is the interaction of (R)AsBo with other Conformity Assessment Bodies (CABs)

Regulatory framework



Applicant/Proposer must

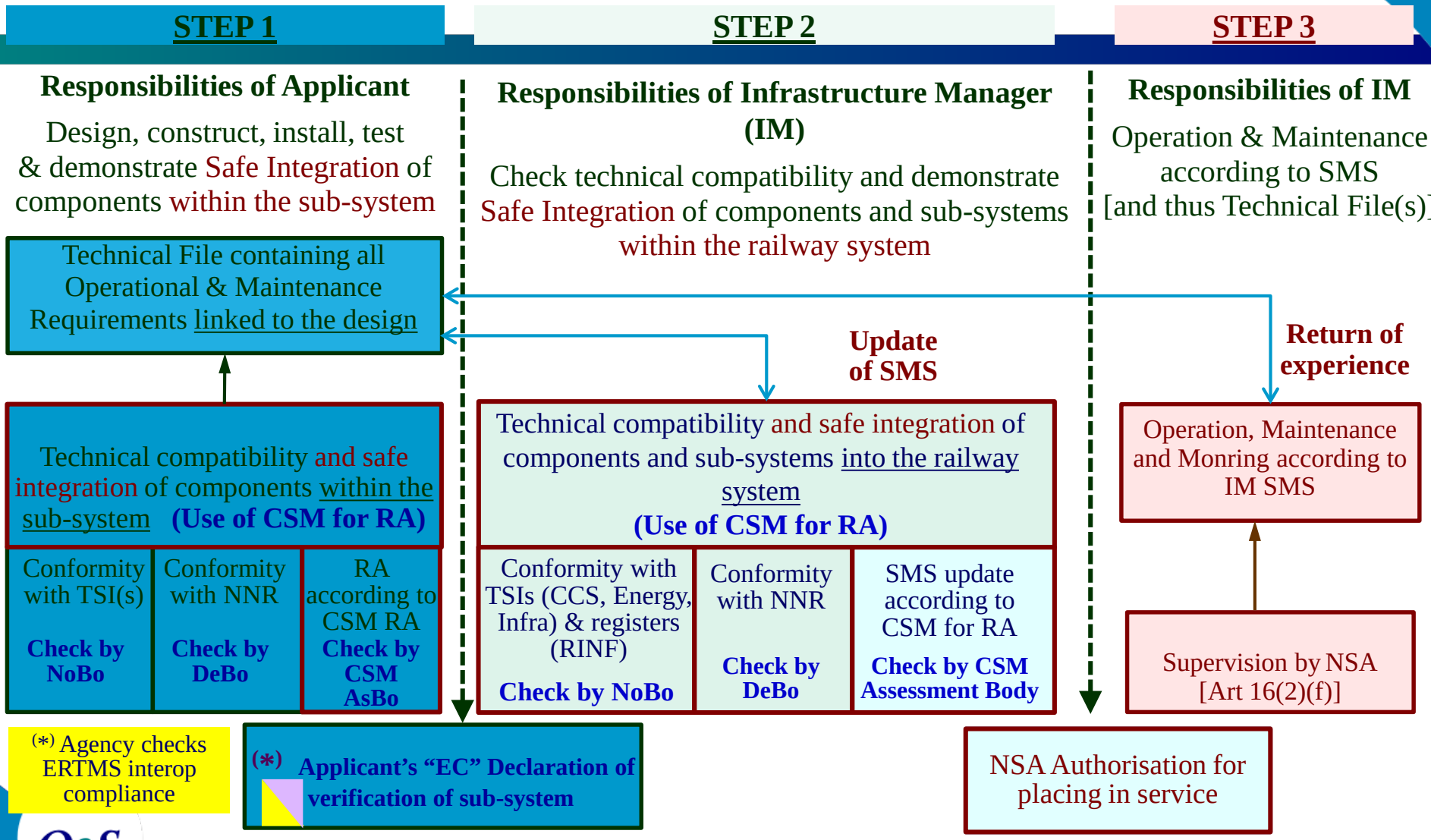
- Apply TSIs, NR & CSM RA
- Demonstrate that all risks are controlled at an acceptable level

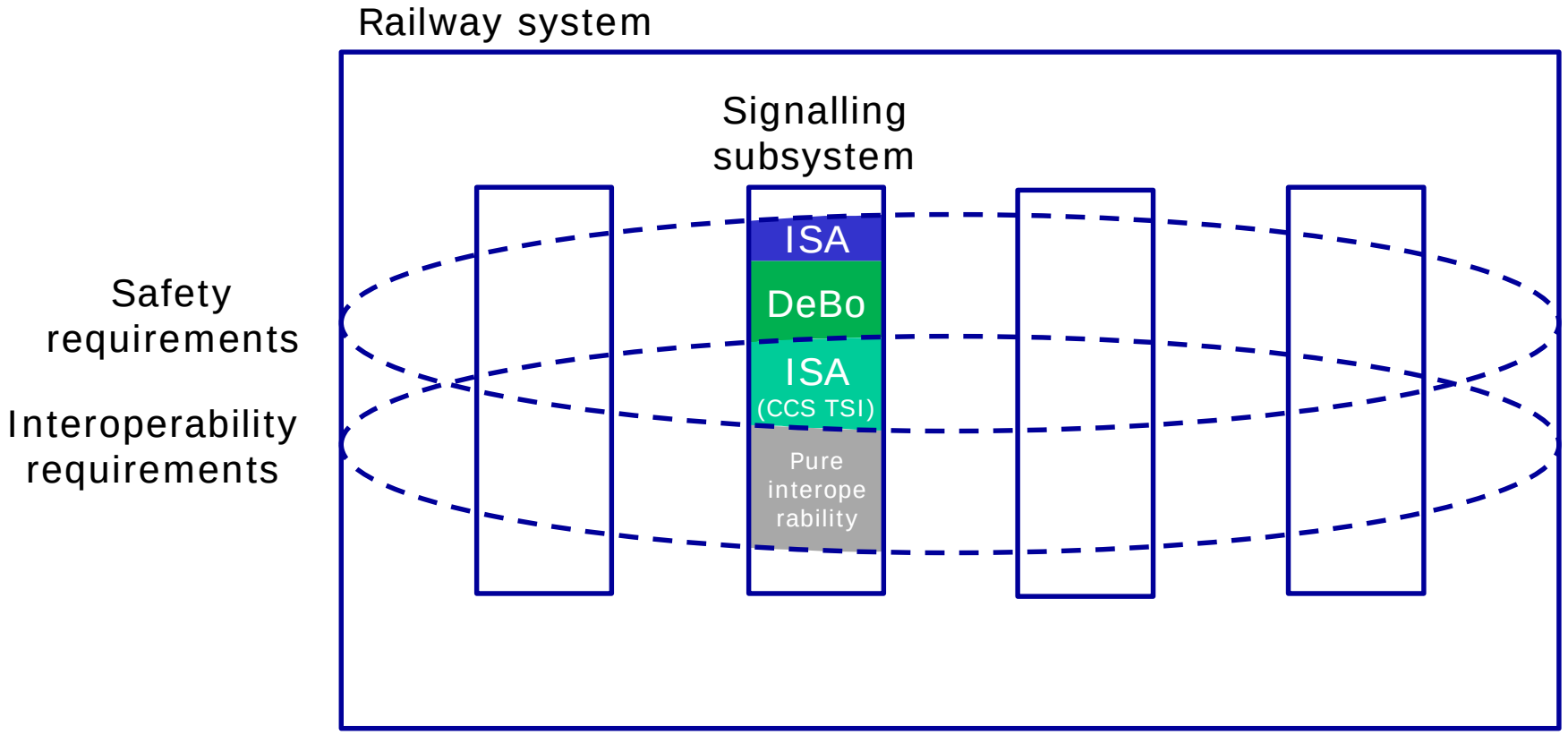
Authorising Entity (e.g. NSA) issues authorisation based on evidences of:

- Proposer's risk assessment & Safe Integration + **RASBO's** assessment
- Conformity with TSI's checked by **NoBo** & with National Rules by **DeBo**

Regulatory framework

Authorisation for placing in service of fixed installations




Railway system
Signalling subsystem
ISA
DeBo
ISA (CCS TSI)
Pure interope rability
Safety requirements
Interoperability requirements

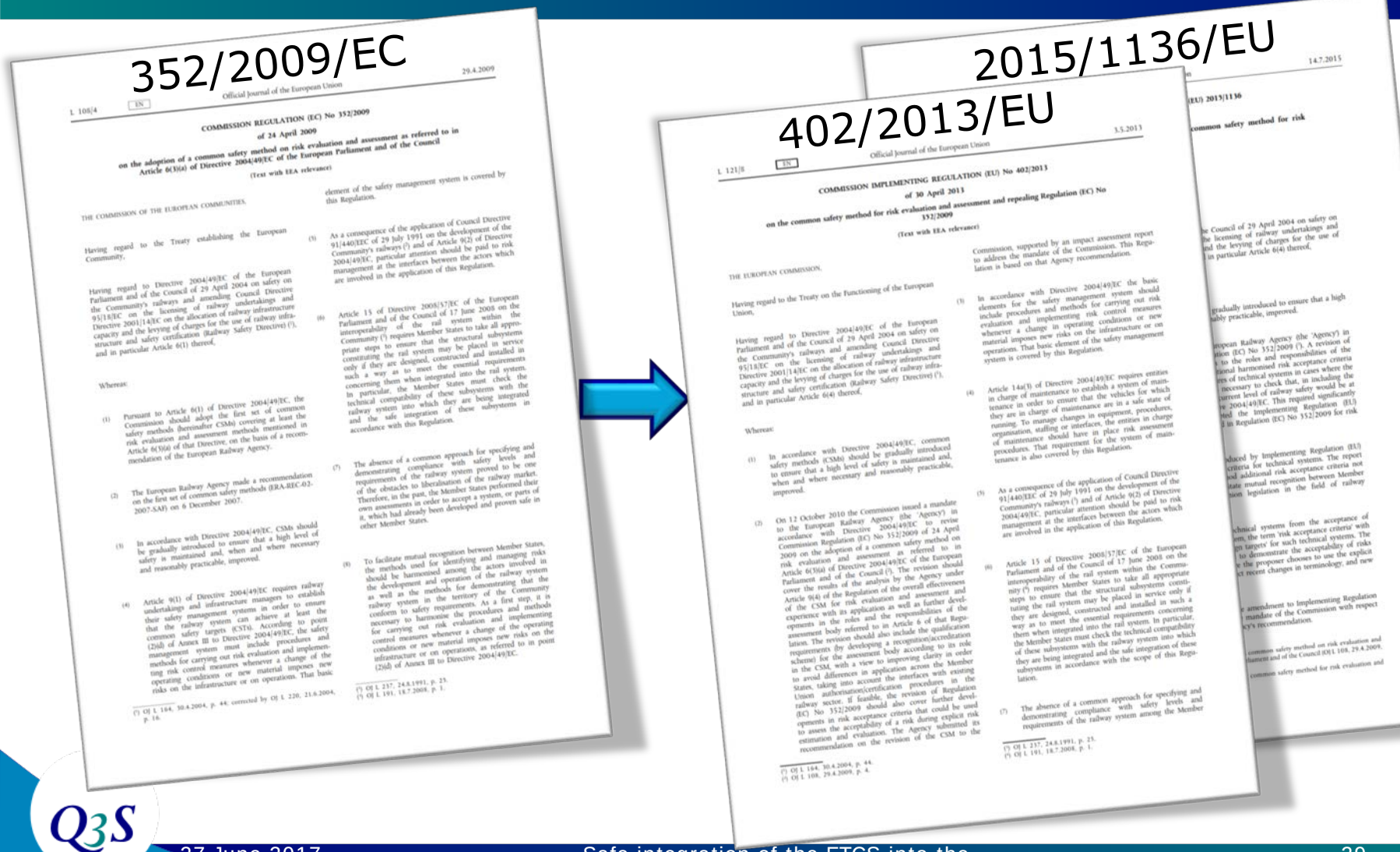
Regulatory framework
When is an ISA needed?

- When are CENELEC 50129, 50126 & 50127, standards applicable?
  - By application of the commission regulation 2016/919/EU (TSI relating to Control-Command and Signalling).
  - Contractual obligation
  - Application of national legislation
  - On a Volunteer basis

PART III

INDEPENDENT SAFETY ASSESSMENT BY THE CSM ASSESSMENT BODY

Independent Assessment CSM REA



Independent Assessment
Role of the AsBo

*"An assessment body shall carry out an independent assessment of the **suitability** of both the **application** of the risk management **process** as set out in Annex I and of its **results**".*

Article 6 (1) of the CSM REA about Independent Assessment

Independent Assessment
Role of the AsBo

*"Assessment body" means the independent and competent external or internal individual, organisation or entity which undertakes investigation to provide a **judgement**, based on **evidence**, of the **suitability** of a system to fulfil its safety requirements*

Article 3 (14) of the CSM REA about assessment body

Independent Assessment Conditions for AsBo's

*"This assessment body shall meet the criteria listed in **Annex II**. Where the assessment body is not already designated by existing Union or national legislation, the proposer shall appoint its own assessment body **at the earliest appropriate stage** of the risk assessment process"*.

Article 6 (1) of the CSM REA about Independent assessment

Independent Assessment Conditions for AsBo's (continued)

- Annex II: criteria for accreditation **or** recognition following ISO17020:2012
  - Competence
    - In risk management
    - In **the parts** of the **railway system** (different areas of competence, technical as well as functional subsystems)
    - In the correct application of safety and quality management systems or in auditing management systems
  - Independence (types A, B, C)

Independent Assessment Conditions for AsBo's (continued)

- An AsBo has to take into account
  - organisation put in place to ensure coordinated approach to achieving system safety
  - Methodology put in place
  - Technical aspects for assessing relevance and completeness

Independent Assessment Methodology

- Use of combined types of activities:
  - Audit, visit, interview
  - Document review
  - Test witnessing
  - Specific analyses (or request)
- Focus on vertical and horizontal project life-cycle cross-section
- Assessor **IS NOT** performing design, verification or test activities

Independent Assessment Methodology

- Assessor must accept alternative ways, different from what he would have expected/done

Independent Assessment Result

- Safety Assessment report
  - Identification of the AsBo
  - Independent Assessment plan
  - Definition of the scope & limitations
  - Results of the independent assessment
    - Carried out activities
    - Non-compliances
    - Recommendations
  - Conclusions

Independent Assessment Key points

- Risk study is only the tip of the iceberg
- Structured system approach (engineering)
- Effective application of appropriate quality procedures
- Iterative approach (not only a high level risk analysis but a real safety approach in relation with the design and the implementation)

Independent Assessment Key points

- Assessment is related to a system, sub-system, item or product not to a documentation set or a safety case only

- A document cannot be assessed !

Independent Assessment

“Assessment” vs. “Independent Assessment”

- “(Risk) Assessment” remains under the responsibility of the proposer
  - “Overall process comprising a risk analysis and a risk evaluation”
- “Independent Assessment” falls under the responsibility of the assessment body

Independent Assessment Practical use

- Title of the CSM REA and the major part of the text speaks about “risks”.
  This is **often understood** that:
  - The requirements of the CSM REA are **limited** to the analysis **only**!
  - Worthwhile to reword it? “safety” instead of “risk”

Independent Assessment Particular issues

- Follow up of mitigation measures until resolution/closure and associated evidences
- Efforts for risk analyses are minor regarding to the rest

Independent Assessment Particular issues

- Need for a Risk Analysis even to confirm no impact of changes !!!
- Need for both a technical expert and global risk approach based on processes.
- Need to consider the global infrastructure, not restricted to the subsystem it belongs to

Independent Assessment Current difficulties

- Safety is a matter of “grey” (no “black & white”).
  AsBo judgement cannot be summarised as “a tick in the box”.
- AsBo contracts are subject to the law of the market. The less expensive AsBo (the AsBo doing less than the other ones?) is the winner.
  It could oblige the most conscientious ones to lower their “judgement criteria”

Independent Assessment Current difficulties

- Synchronisation of appointment of assessment bodies
  - "*[…] the proposer shall appoint its own assessment body at the earliest appropriate stage of the risk assessment process*"

    CSM REA 402/2013/EU
    Article 6, § 1

  - What is the appropriate stage?
    For infrastructure project, civil works come first (years) before others, but coherency has to be achieved!

Q&A