



Quality & Safety for Systems & Software *Railway Engineering*

Assurance provided by a second pair eyes (RASBO) of the correct Safe integration by the proposer of a new or modified Rolling Stock

Q3S

Ir. Marc Bronchart
AsBo & independent Safety Assessor



Presentation structure

- Part I
Safe integration
- Part II
Regulatory framework
- Part III
Independent assessment





PART I

SAFE INTEGRATION

Safe integration Railway vehicles



- Railway vehicles (“rolling stocks”) consist of following subsystems:
 - Rolling stock itself, including (not exhaustive list)
 - Braking devices
 - Traction cut-off
 - Coupling devices
 - Doors
 - Energy
 - Signalling
 - Particular fittings

Safe integration Interfaces to consider



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



PART II

REGULATORY FRAMEWORK



Regulatory framework

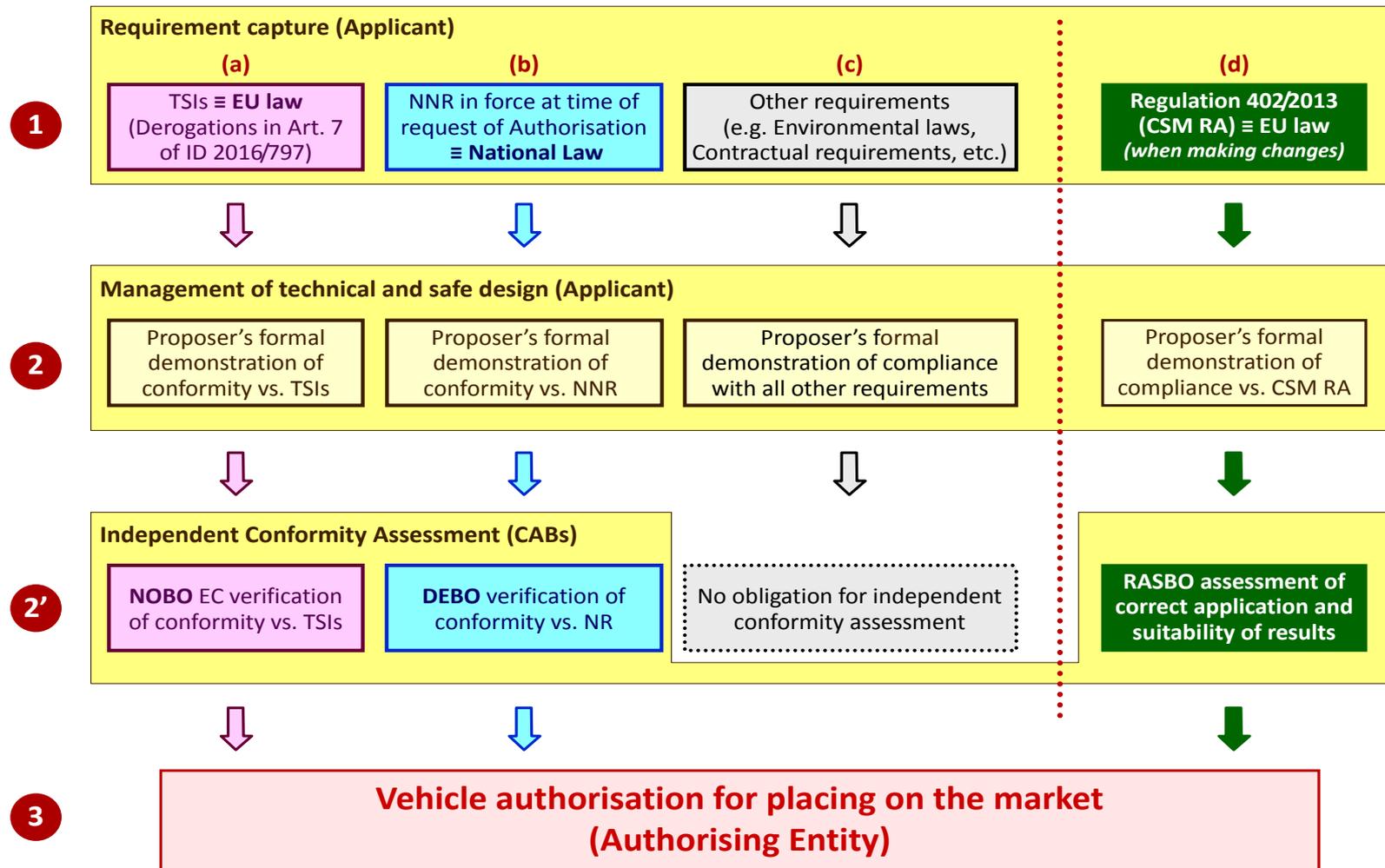
- TSIs per Subsystem
 - National Rules
 - Safety Directive
 - CSM REA
- NoBo
DeBo
National Safety Auth.
Assessment Body





Regulatory framework

CSM REA as support for the APoM



Regulatory framework

Placing On the Market



- *"placing on the market" means the first making available on the Union's market of an interoperability constituent, subsystem or vehicle ready to function in its design operating state*

Article 2 (35) of
Interoperability Directive
2016/797/EU



Regulatory framework

- STI LOC&PAS (locomotives & passengers)
- STI WAG (wagons)
- STI NOI (noise).
- Others transverse
 - Tunnel
 - PRM
 - CCS)

Or Functionnal

OPE

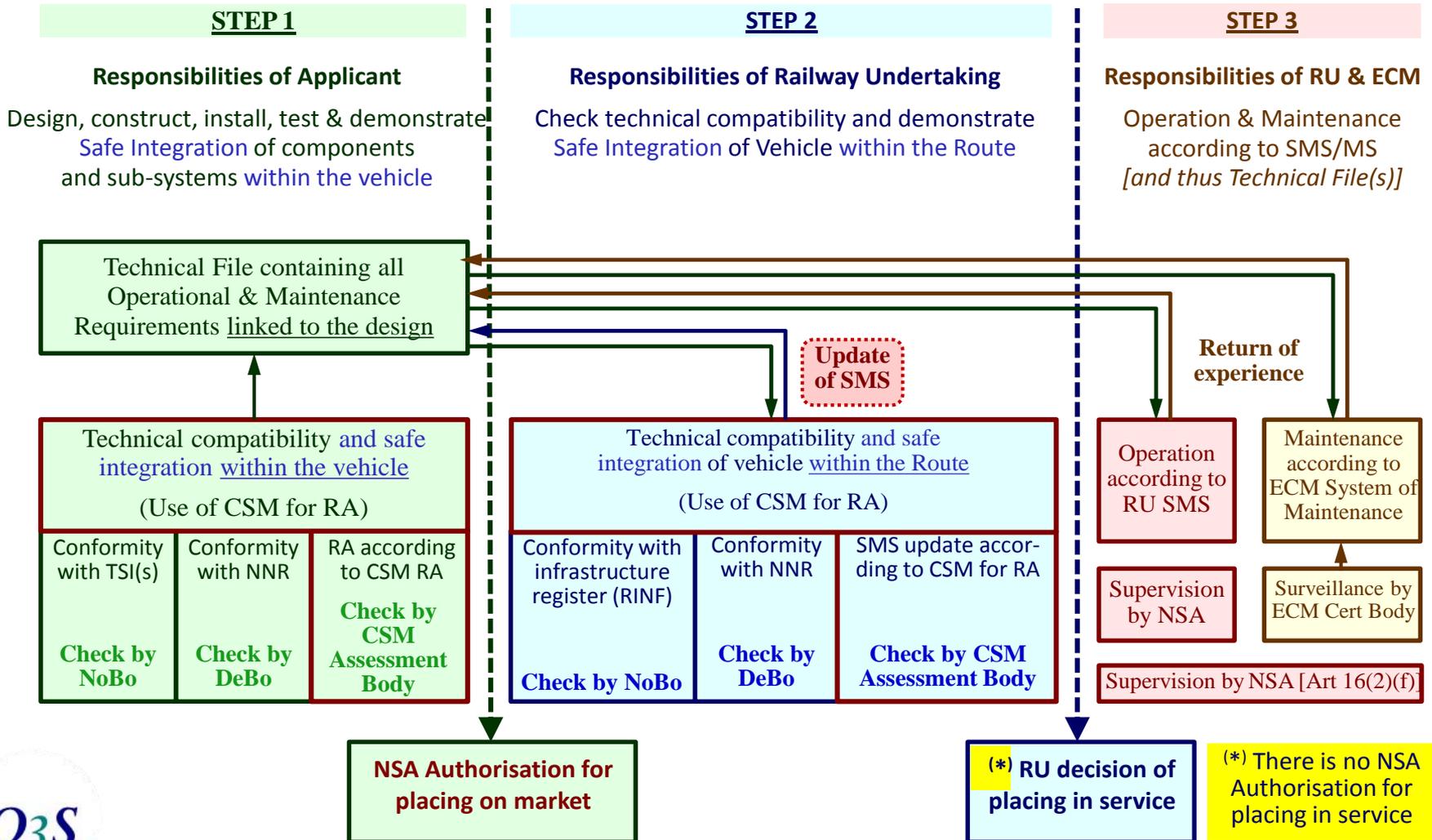
TAF

AP). TSIs per Subsystem



Regulatory framework

Roles and responsibilities for safe integrations





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)

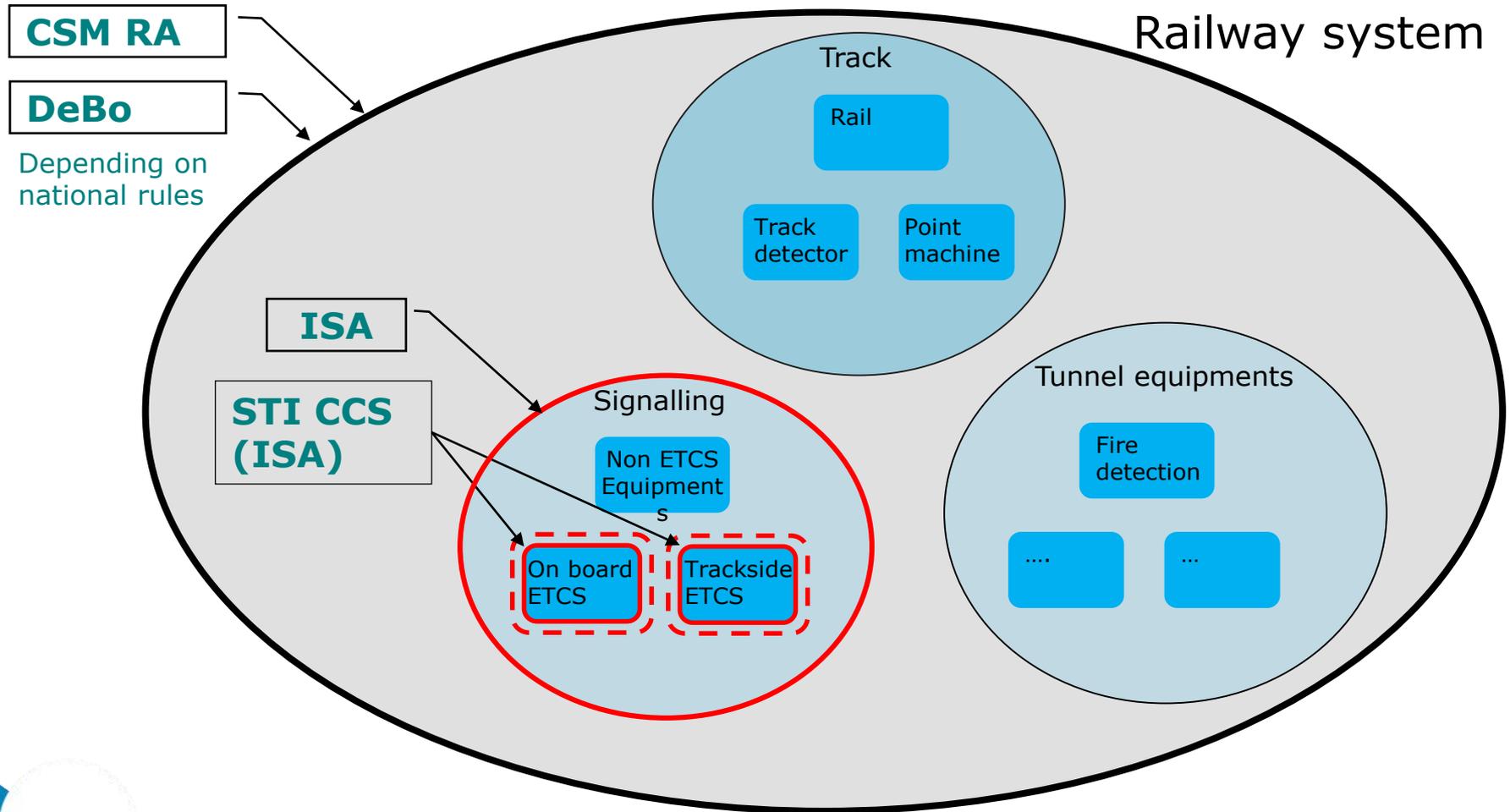
Safety Impact of ETCS Integration



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



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)

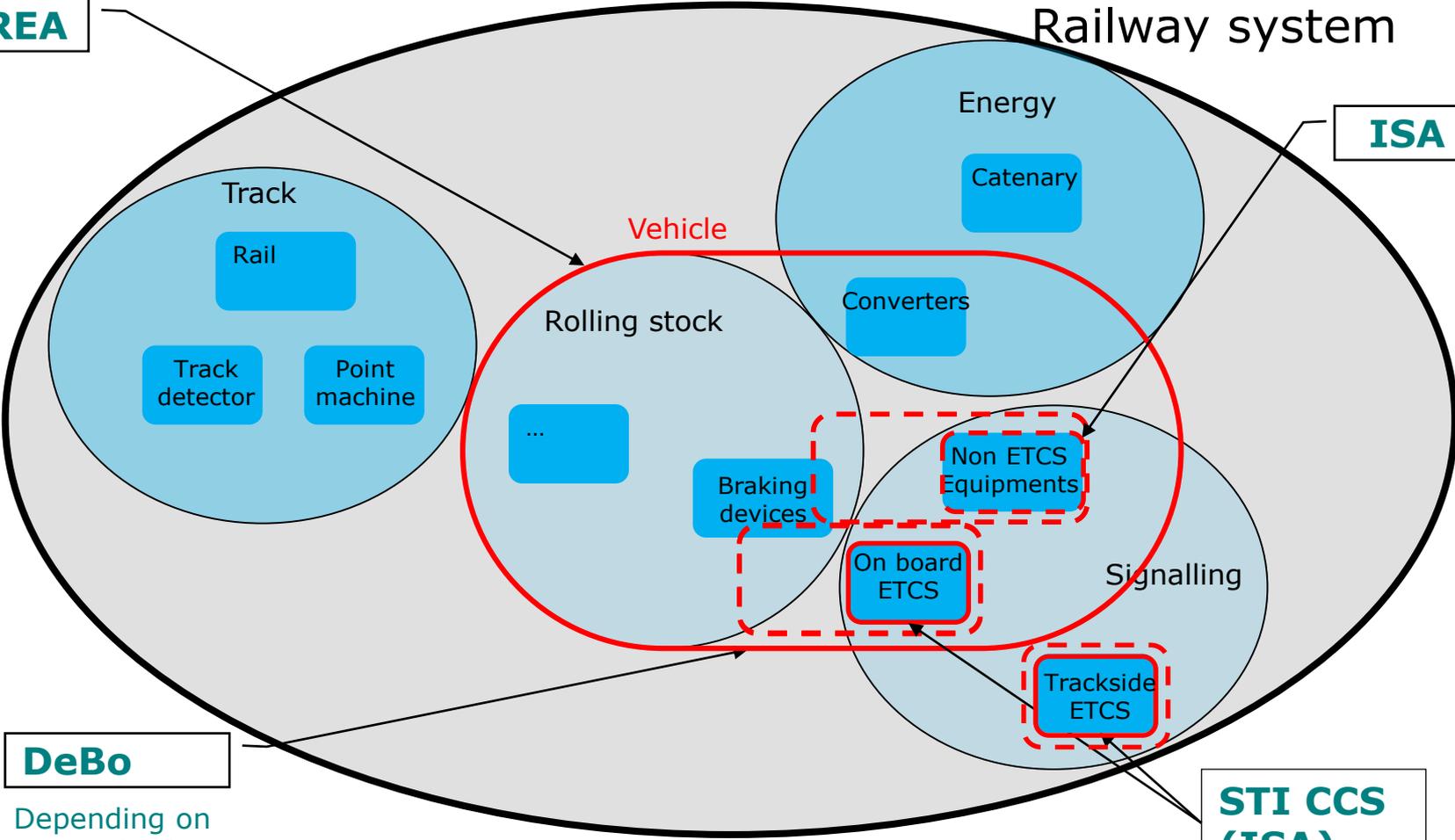


Regulatory framework

CSM REA

Railway system

ISA



DeBo

Depending on national rules

STI CCS (ISA)



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

Regulatory framework

New or modified vehicle



- New or modified vehicle?
 - Currently not clear (enough) if independent assessment is required from safety perspective
(more information available about interoperability)
 - Does it mean new or modified **type** of vehicle?

Regulatory framework

New or modified vehicle



- New or modified vehicle?
 - Is it linked with potential impact of railway undertaking certificate?
 - But certificate means “is able to”
(Railway Safety Directive, Article 10 § 1)
 - What about actual safety level?
Is the Safety Management System really applied?

Regulatory framework

New or modified vehicle



"By 16 June 2018, the Commission shall adopt, by means of implementing acts, practical arrangements specifying:

(a) how the requirements for the single safety certificate laid down in this Article shall be fulfilled by the applicant and listing the documents required;

(b) the details of the certification process, such as procedural stages and timeframes for each stage of the process;

[...]"

Railway Safety Directive 2016/798/EU
Article 10, §10

Regulatory framework

New or modified vehicle



- Assessment can vary from “no assessment” (no significant change) to “full assessment”


Possibility of a “slide” in
the principles by abusing
CSM REA regulation

- In case of assessment
 - same kind of assessment activities
 - “1 + Δ ” approach is often used
 - Assessment not only on the “ Δ ”, but also potential influence on the “1”



PART III

INDEPENDENT ASSESSMENT

Safe integration

Multiple aspects



- “Dynamic” safety
 - Control-command & signalling
- “Static” safety
 - Fire safety
 - Mechanical resistance

➔ It requires several competencies for assessment

Independent assessment

Vehicle particular topics



- Global approach is required
- Technical compatibility is not sufficient
- Safety objectives...
 - ... may depend on common targets (e.g.: ERTMS/ETCS on-board)
 - ... may be not commonly defined at Union level

Independent assessment

Current difficulties



- Safety objectives not commonly defined at Union level
 - Pure national rules
- Independent Assessment can rely on it (DeBo?)...
- Possible influence on international requirements has “only” to be assessed.

Independent assessment

Key items



- Safety objectives not commonly defined at Union level
 - How to make a “judgement”?
 - risk acceptance criteria defined in the Safety Management System of the Railway Undertaking could not match with safety requirements of all Member States
 - The CSM REA gives some quantitative objectives ($10^{-7}/h$ or $10^{-9}/h$) when detailing the criterion “explicit risk estimation”... without giving the scope of them



Independent assessment

Key items



- More and more software
- Formal approval and management of “imported” constraints from
 - “solution providers” (subcontractors)
 - Infrastructure managers
 - ...
- Formal issue of “exported” constraints towards relevant actors
 - Ultimately to the Railway Undertakings and Entities in Charge of Maintenance

Independent assessment

Key items



- EMC
 - One can hope that norms are sufficient for reaching appropriate safety level

Q&A

