



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



Q3S

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

Q3S

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



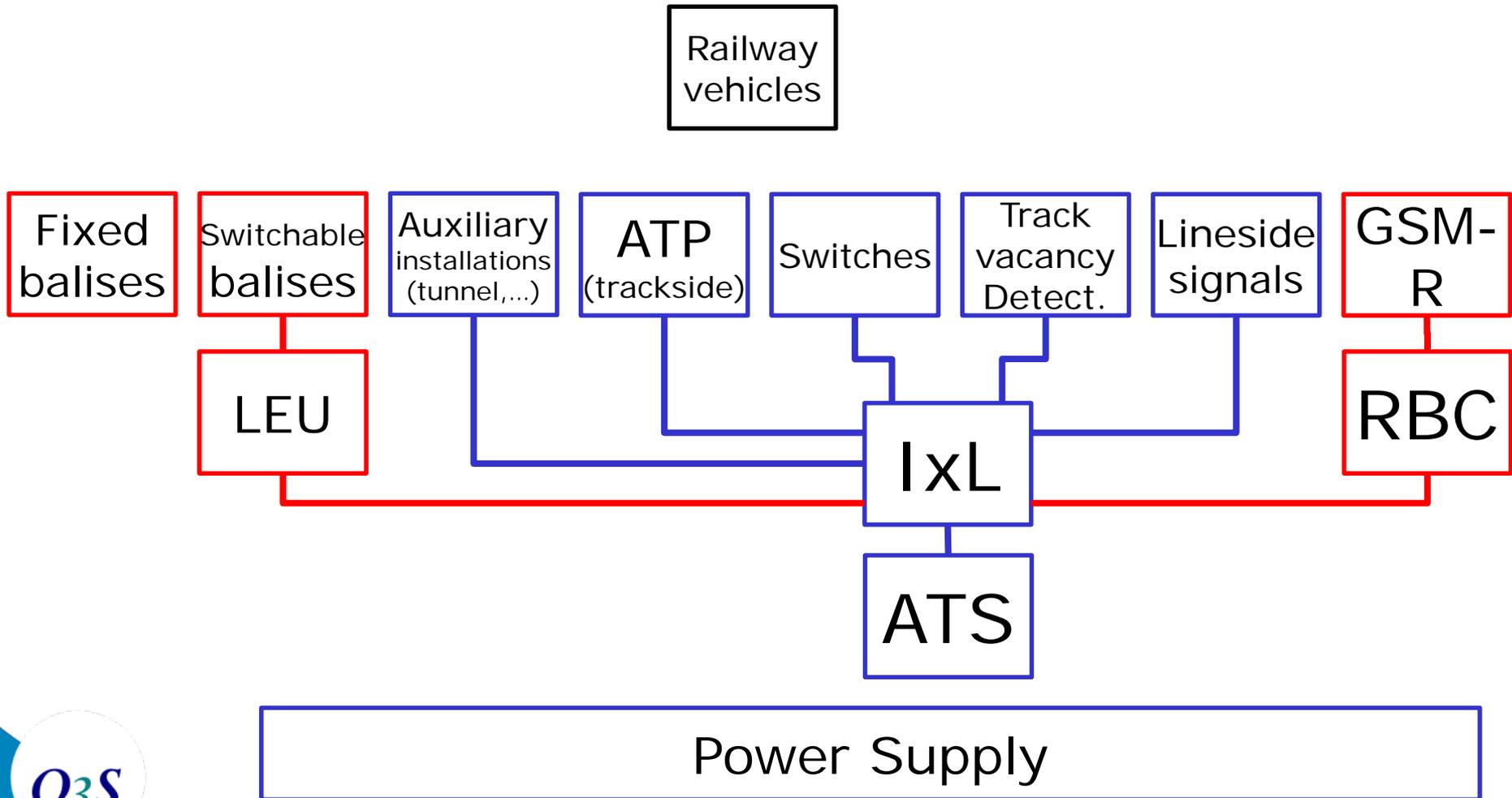
- Classical Signalling subsystem is made of following equipments:
 - Line side or cab signalling
 - Train detection device (Track circuits or axle counters)
 - Interlocking
 - Automatic Train Supervision (ATS)
 - On Board AWS or ATP
 - Trackside-related AWS or ATP equipment
 - Miscellaneous detectors

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)
 - ...

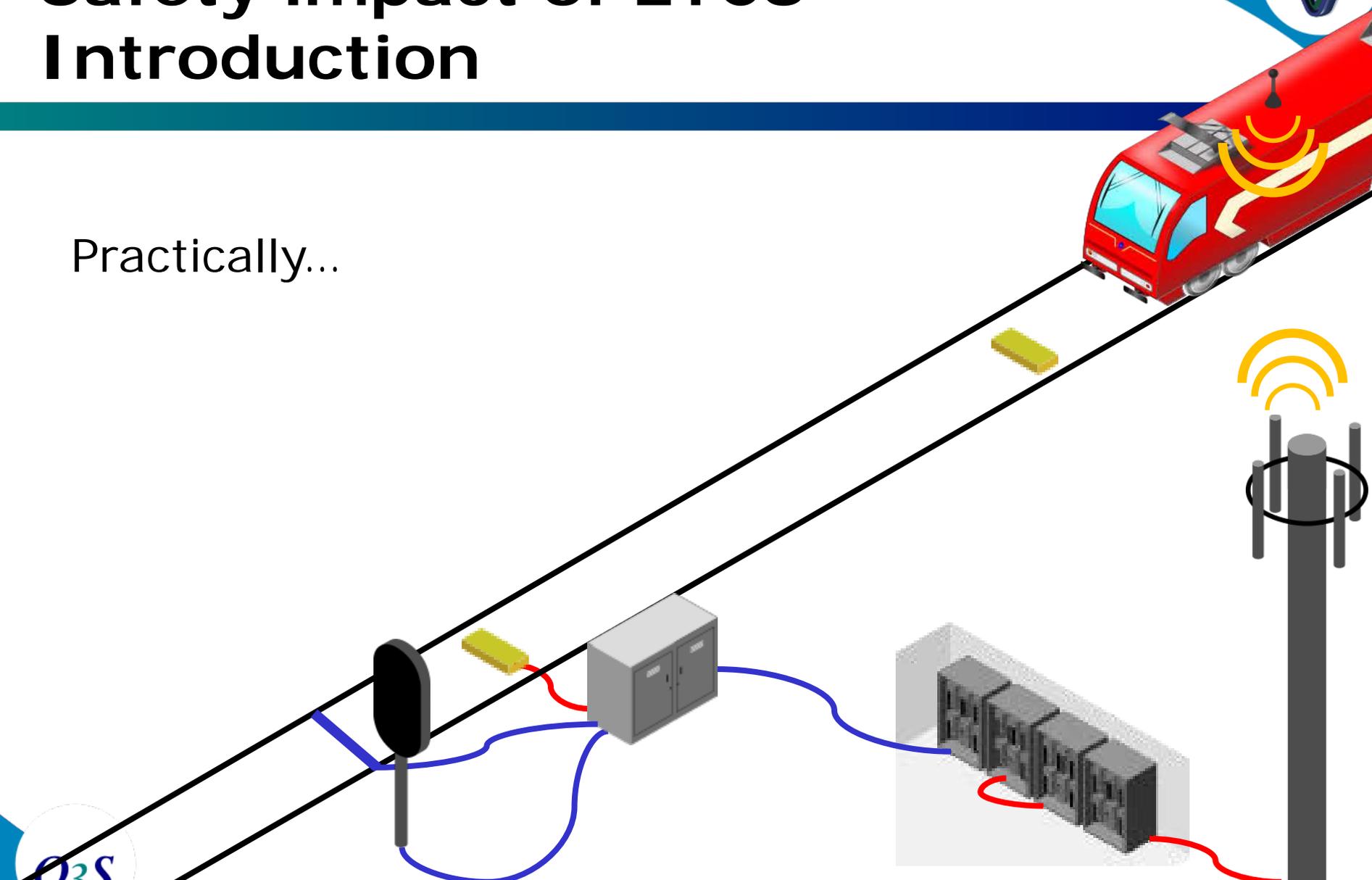
Safety Impact of ETCS Introduction



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

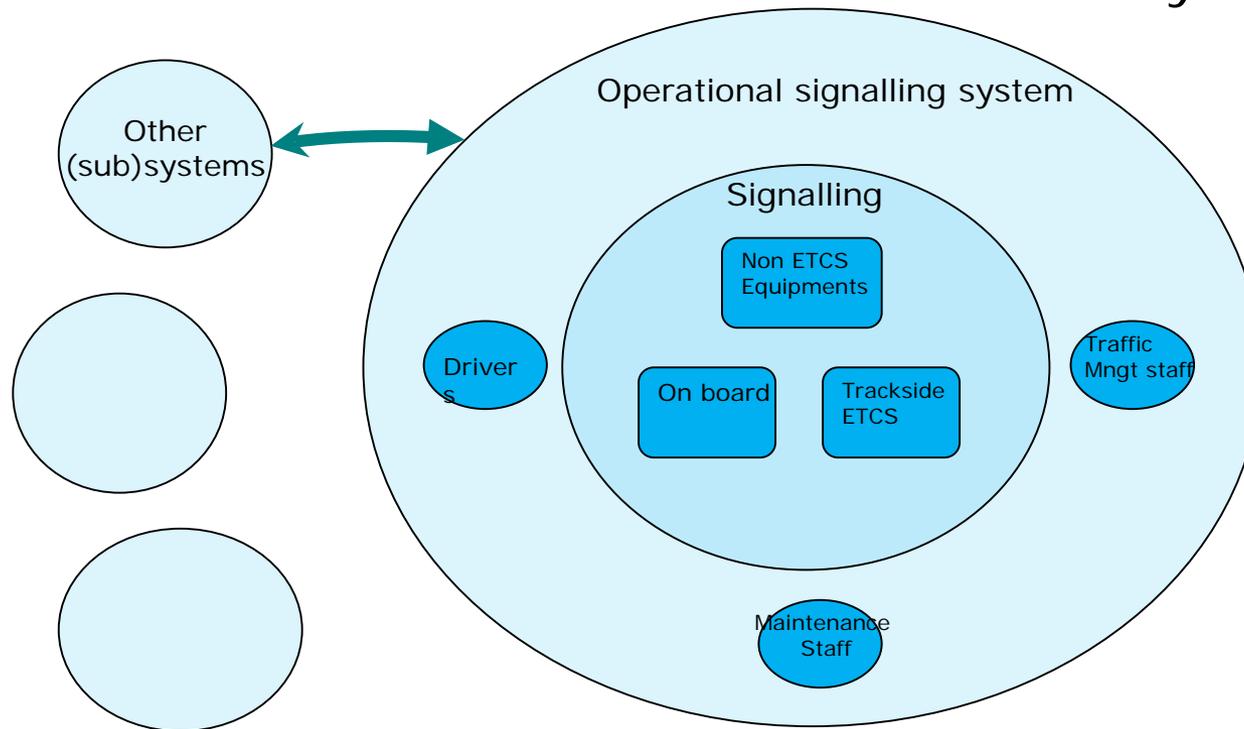


- Safety of the modified system needs to be demonstrated knowing that:
 - TSI CCS are requiring CENELEC application but limited to ETCS functionalities and equipments (constituents)
 - ETCS implementation is subjected to several design & operational choices by the Infrastructure owner.
ETCS is an configurable 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



Railway infrastructure



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
 - National Rules
 - Safety Directive
 - CSM RA
- NoBo
DeBo
National Safety Auth.
Assessment Body





Regulatory framework

TSIs
≡ EU law

National Rules
≡ National Law

CSM RA
≡ EU Law

Independent
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

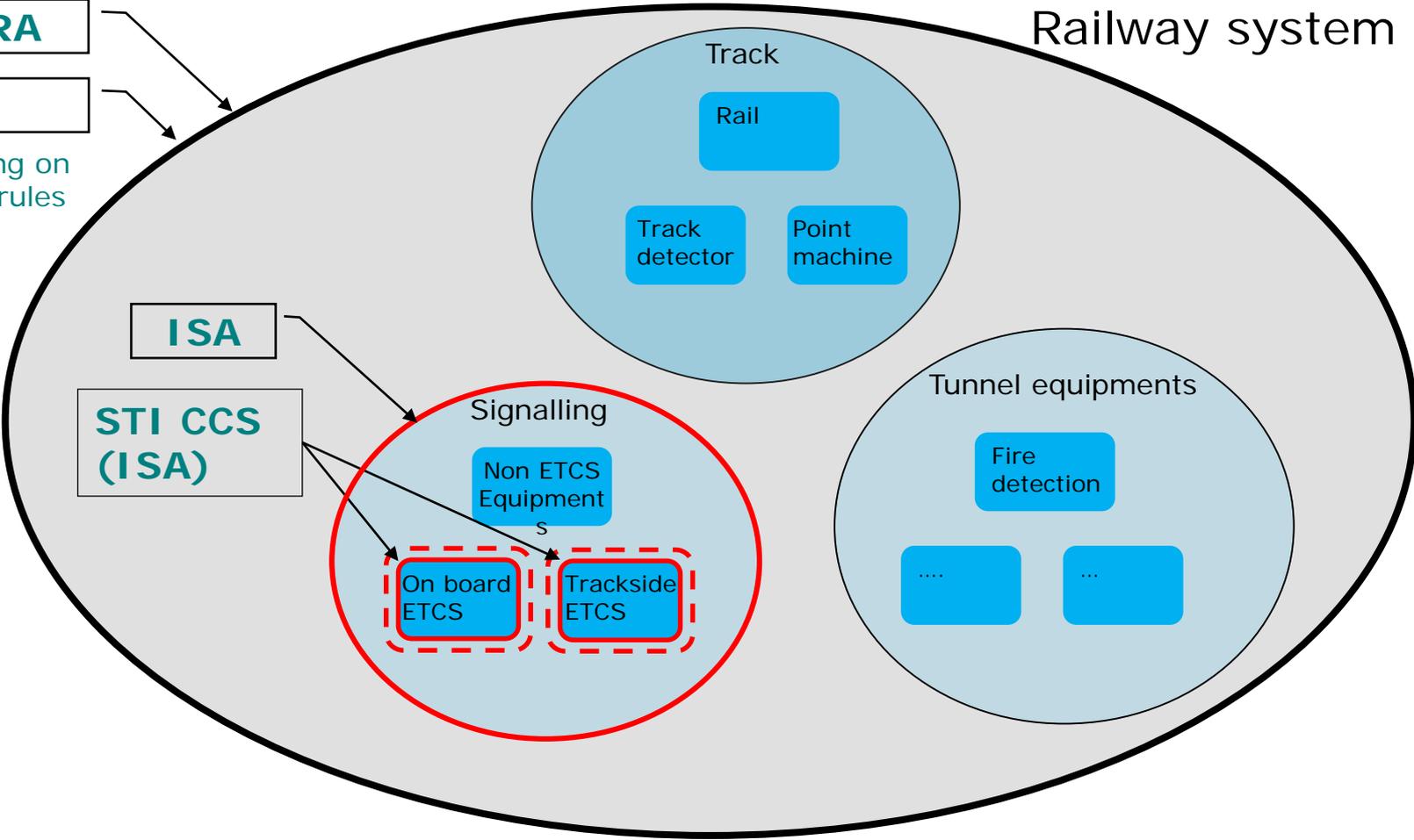


Regulatory framework

CSM RA

DeBo

Depending on national rules





Regulatory framework

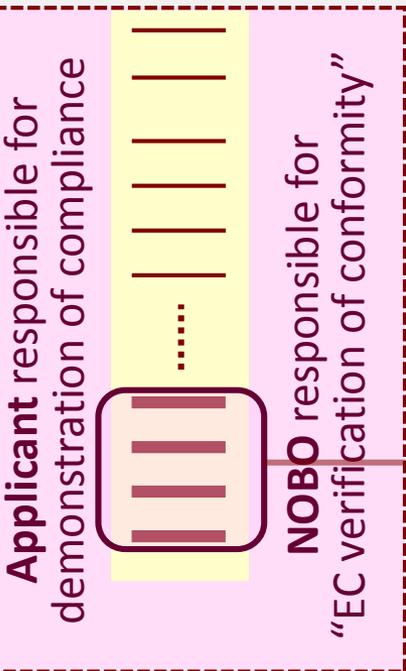
- **Duplication** of independent assessment work between different Conformity Assessment Bodies involved in a project **shall be avoided**
- Compliance with TSIs – Compliance with CSM Risk Assessment: **WHAT** is the interaction of (R)AsBo with other Conformity Assessment Bodies (CABs)



Regulatory framework

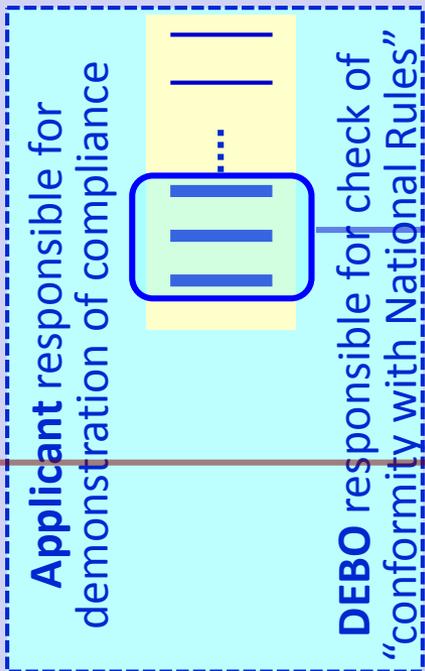
Compliance with TSIs and NR

TSIs
NoBo

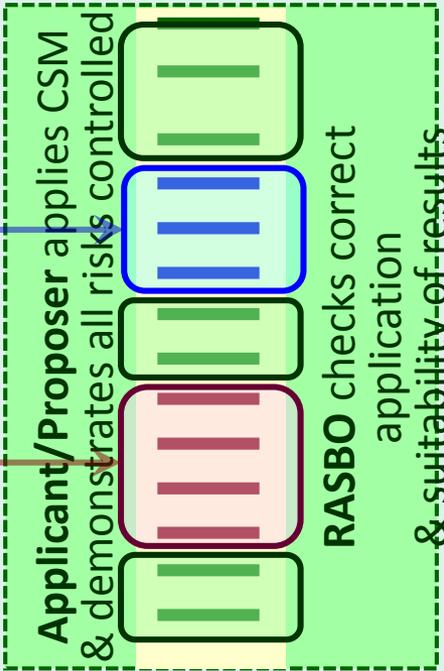


Compliance with CSM RA

National Rules
Debo



CSM RA
RASBo



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

STEP 1

Responsibilities of Applicant

Design, construct, install, test & demonstrate **Safe Integration** of components **within the sub-system**

Technical File containing all Operational & Maintenance Requirements linked to the design

Technical compatibility and safe integration of components within the sub-system (Use of CSM for RA)

Conformity with TSI(s)

Conformity with NNR

RA according to CSM RA

Check by NoBo

Check by DeBo

Check by CSM AsBo

(*) Agency checks ERTMS interoper compliance

(*) Applicant's "EC" Declaration of verification of sub-system

STEP 2

Responsibilities of Infrastructure Manager (IM)

Check technical compatibility and demonstrate **Safe Integration** of components and sub-systems **within the railway system**

Technical compatibility and safe integration of components and sub-systems into the railway system (Use of CSM for RA)

Conformity with TSIs (CCS, Energy, Infra) & registers (RINF)

Conformity with NNR

SMS update according to CSM for RA

Check by NoBo

Check by DeBo

Check by CSM Assessment Body

Update of SMS

STEP 3

Responsibilities of IM

Operation & Maintenance according to SMS [and thus Technical File(s)]

Operation, Maintenance and Monring according to IM SMS

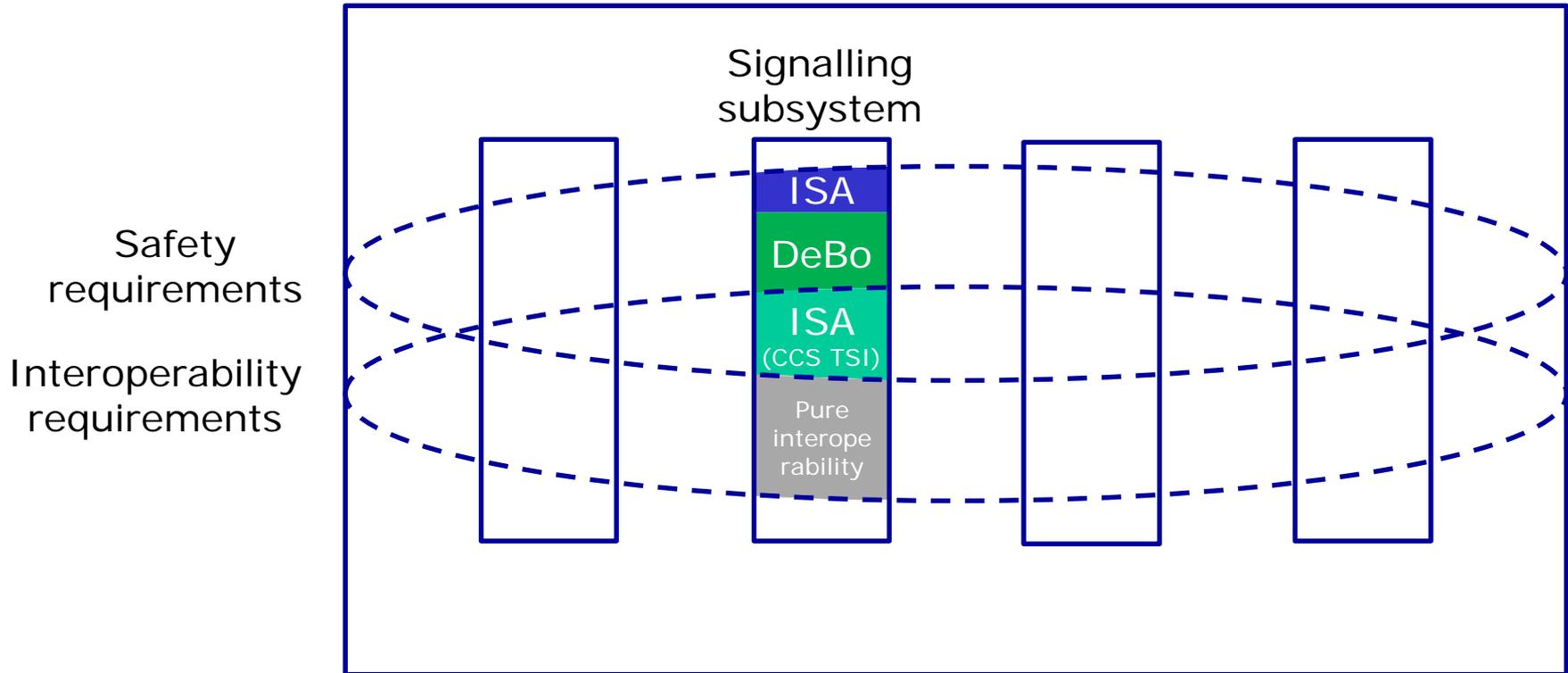
Supervision by NSA [Art 16(2)(f)]

Return of experience

NSA Authorisation for placing in service



Railway system





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



352/2009/EC
29.4.2009
Official Journal of the European Union

COMMISSION REGULATION (EC) No 352/2009
of 24 April 2009
on the adoption of a common safety method on risk evaluation and assessment as referred to in Article 6(3)(a) of Directive 2004/49/EC of the European Parliament and of the Council
(Text with EEA relevance)

THE COMMISSION OF THE EUROPEAN COMMUNITIES,

Having regard to the Treaty establishing the European Community,

Having regard to Directive 2004/49/EC of the European Parliament and of the Council of 29 April 2004 on safety on the Community's railways and amending Council Directive 95/18/EC on the licensing of railway infrastructure and Directive 2001/14/EC on the allocation of railway infrastructure capacity and the levying of charges for the use of railway infrastructure and safety certification (Railway Safety Directive⁽¹⁾), and in particular Article 6(1) thereof,

Whereas:

- Pursuant to Article 6(1) of Directive 2004/49/EC the Commission should adopt the first set of common safety methods (hereinafter CSMs) covering at least the evaluation and assessment methods mentioned in Article 6(3)(a) of that Directive, on the basis of a recommendation of the European Railway Agency;
- The European Railway Agency made a recommendation on the first set of common safety methods (RAA-REC-02-2007-SAF) on 6 December 2007;
- In accordance with Directive 2004/49/EC, CSMs should be gradually introduced to ensure that a high level of safety is maintained and, when and where necessary and reasonably practicable, improved;
- Article 9(1) of Directive 2004/49/EC requires railway undertakings and infrastructure managers to establish their safety management system in order to ensure that the railway system can achieve at least the common safety targets (CSTs). According to point (2)(b) of Annex III to Directive 2004/49/EC, the safety management system must include procedures and methods for carrying out risk evaluation and implementing risk control measures whenever a change of the operating conditions or new material imposes new risks on the infrastructure or on operations. That basic element of the safety management system is covered by this Regulation.
- As a consequence of the application of Council Directive 91/440/EEC of 29 July 1991 on the development of the Community's railways⁽²⁾ and of Article 9(2) of Directive 2004/49/EC, particular attention should be paid to risk management at the interfaces between the actors which are involved in the application of this Regulation.
- Article 15 of Directive 2008/17/EC of the European Parliament and of the Council of 17 June 2008 on the interoperability of the rail system within the Community⁽³⁾ requires Member States to take all appropriate steps to ensure that the structural subsystems constituting the rail system may be placed in service only if they are designed, constructed and installed in such a way as to meet the essential requirements concerning them when integrated into the rail system, such as a way as to ensure the technical compatibility of these subsystems with the rail system into which they are being integrated and the safe integration of these subsystems in accordance with this Regulation.
- The absence of a common approach for specifying and demonstrating compliance with safety levels and requirements of the railway system proved to be one of the obstacles to liberalisation of the railway market. Therefore, in the past, the Member States performed their own assessments in order to accept a system, or parts of it, which had already been developed and proven safe in other Member States.
- To facilitate mutual recognition between Member States, the methods used for identifying and managing risks should be harmonised among the actors involved in the development and operation of the railway system as well as the methods for demonstrating that the system is in conformity with safety requirements. As a first step, it is necessary to harmonise the procedures and methods necessary to harmonise the procedures and methods for carrying out risk evaluation and implementing risk control measures whenever a change of the operating conditions or new material imposes new risks on the infrastructure or on operations, as referred to in point (2)(b) of Annex III to Directive 2004/49/EC.

(¹) OJ L 164, 30.4.2004, p. 44, corrected by OJ L 226, 21.8.2004, p. 16.
(²) OJ L 237, 24.8.1991, p. 23.
(³) OJ L 191, 18.7.2008, p. 1.

2015/1136/EU
14.7.2015
Official Journal of the European Union

COMMISSION IMPLEMENTING REGULATION (EU) No 1136/2015
of 30 April 2015
on the common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009
(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Directive 2004/49/EC of the European Parliament and of the Council of 29 April 2004 on safety on the Community's railways and amending Council Directive 95/18/EC on the licensing of railway infrastructure and Directive 2001/14/EC on the allocation of railway infrastructure capacity and the levying of charges for the use of railway infrastructure and safety certification (Railway Safety Directive⁽¹⁾), and in particular Article 6(4) thereof,

Whereas:

- In accordance with Directive 2004/49/EC, common safety methods (CSMs) should be gradually introduced, to ensure that a high level of safety is maintained and, when and where necessary and reasonably practicable, improved.
- On 12 October 2010 the Commission issued a mandate to the European Railway Agency (the 'Agency') in accordance with Directive 2004/49/EC to revise Commission Regulation (EC) No 352/2009 of 24 April 2009 on the adoption of a common safety method on risk evaluation and assessment as referred to in Article 6(3)(a) of Directive 2004/49/EC of the European Parliament and of the Council⁽²⁾. The revision should cover the results of the analysis by the Agency under Article 9(4) of the Regulation of the overall effectiveness of the CSM for risk evaluation and assessment and its application as well as further developments in the field of risk evaluation and assessment. The revision should also include the qualification of the assessment body referred to in Article 6 of that Regulation in the role and the responsibilities of the Member States when integrated into the rail system. In particular, the Member States must check the technical compatibility of these subsystems with the railway system into which they are being integrated and the safe integration of these subsystems in accordance with the scope of this Regulation.
- The absence of a common approach for specifying and demonstrating compliance with safety levels and requirements of the railway system among the Member States, taking into account the interfaces with existing Union authorities/certification procedures in the railway sector, if feasible, the revision of Regulation (EC) No 352/2009 should also cover further developments in risk acceptance criteria that could be used to assess the acceptability of a risk during explicit risk estimation and evaluation. The Agency submitted its recommendation on the revision of the CSM to the Commission, supported by an impact assessment report to address the mandate of the Commission. This Regulation is based on that Agency recommendation.
- In accordance with Directive 2004/49/EC the basic elements for the safety management system should include procedures and methods for carrying out risk evaluation and implementing risk control measures whenever a change in operating conditions or new material imposes new risks on the infrastructure or on operations. That basic element of the safety management system is covered by this Regulation.
- Article 14a(3) of Directive 2004/49/EC requires entities in charge of maintenance to establish a system of maintenance in order to ensure that the vehicles for which they are in charge of maintenance are in a safe state of operation. To manage changes in equipment, procedures, organisation, staffing or interfaces, the entities in charge of maintenance should have in place risk assessment procedures. That requirement for the system of maintenance is also covered by this Regulation.
- As a consequence of the application of Council Directive 91/440/EEC of 29 July 1991 on the development of the Community's railways⁽²⁾ and of Article 9(2) of Directive 2004/49/EC, particular attention should be paid to risk management at the interfaces between the actors which are involved in the application of this Regulation.
- Article 15 of Directive 2008/17/EC of the European Parliament and of the Council of 17 June 2008 on the interoperability of the rail system within the Community⁽³⁾ requires Member States to take all appropriate steps to ensure that the structural subsystems constituting the rail system may be placed in service only if they are designed, constructed and installed in such a way as to meet the essential requirements concerning them when integrated into the rail system. In particular, the Member States must check the technical compatibility of these subsystems with the railway system into which they are being integrated and the safe integration of these subsystems in accordance with the scope of this Regulation.
- The absence of a common approach for specifying and demonstrating compliance with safety levels and requirements of the railway system among the Member States, taking into account the interfaces with existing Union authorities/certification procedures in the railway sector, if feasible, the revision of Regulation (EC) No 352/2009 should also cover further developments in risk acceptance criteria that could be used to assess the acceptability of a risk during explicit risk estimation and evaluation. The Agency submitted its recommendation on the revision of the CSM to the Commission, supported by an impact assessment report to address the mandate of the Commission. This Regulation is based on that Agency recommendation.

(¹) OJ L 164, 30.4.2004, p. 44, corrected by OJ L 226, 21.8.2004, p. 16.
(²) OJ L 237, 24.8.1991, p. 23.
(³) OJ L 191, 18.7.2008, p. 1.



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

