Safety integration for Authorization of Vehicles

Hervé GUILBERT - Giuseppe LEONE

29/06/2017 – BUDAPEST ERA TRAINING

ALSTOM
Designing fluidity

VOCABULARY

AUTHORIZATION TO PLACE IN SERVICE

VALIDATION

ERA

ACCEPTANCE

CERTIFICATION

ERATV

ASSESSOR

HOMOLOGATION

NNTR

DEBO

TSI

EBA

VIS

STI

NSA

NOBO

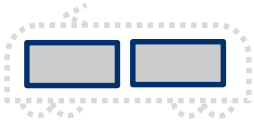
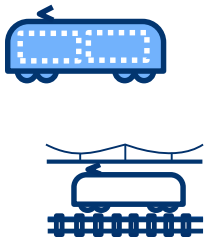
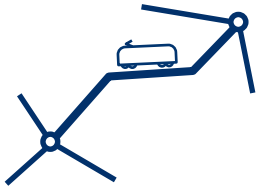
ANSF

INTEROPERABILITY CONSTITUENTS

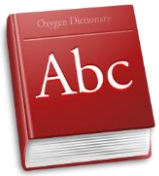
Authorization to place railway vehicles in service

- The Interoperability Directive: defines the process by which a subsystem or a vehicle is authorized to be placed in service.
- Authorization is granted by the National Safety Authority of the Member State where the sub-system is intended to be operated, based on evidences that the sub-system or vehicle complies with essential requirements of Interoperability Directive, in particular :
  - The subsystem/vehicle is compatible with the rest of the railway system,
  - The subsystem/vehicle can be safely integrated in this railway system
- These two objectives are achieved by means of compliance with technical rules and, when no technical rule exist, relevant risks analyses. The technical rules are the TSIs and the complementary national technical rules (NTR).
- The authorization is the recognition by the member-state that the sub-system/vehicle is compliant with the essential requirements.

Roles & Responsibilities as per EC

	>1 MS	Only 1 MS
1 PLACING ON THE MARKET OF MOBILE SUBSYSTEMS — Essential Requirements; No need for being "authorised" 	Applicant	
2 VEHICLE AUTHORISATION for PLACING ON THE MARKET in AREA of USE — 1. Placing on the market 2. Technical compatibility of SSYS within the vehicle 3. Safe integration of SSYS within the vehicle 4. Technical compatibility in the area of use 	ERA and NSAs	ERA or NSA (Applicant's choice)
3 CHECK BEFORE the USE OF authorised VEHICLE — Route compatibility on the basis of RINF and national rules 	Railway Undertaking	
4 Revocation — In case of **non-compliance to essential requirements** noticed during operation by Railway undertakings or ultimately by NSA and inducing **safety risks** (e.g. during supervision activities) authorisation can be revoked	Railway Undertaking & NSA	

Reference Framework for Authorization



- **Common Safety Methods**: to ensure Safe Integration
  - Gives a **Method** to define the **safety requirements** to be met

- **Technical Specifications**: to ensure product **Conformity**
  - **TSI** : **requirements** for integration within European rail network
  - **NTR** : **requirements** for integration at National level

Vehicle meets all applicable Requirements ⇨ Authorization

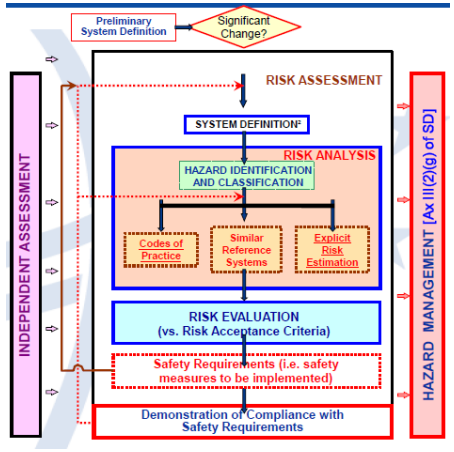
ALSTOM

Project Safety Plan

Safety Plan : initiate Safety Process

[Extract of a RS Safety Plan Summary]

- **Systems Description / Safety Requirements**
  - ***Description, Gaps, Targets & Requirements***
- **Safety Management System**
  - ***Organization, Risk Acceptance***
- **Safety Studies**
  - ***PHA, HLOG, FTA, SRIL, Safety Case***



CSM, 3 fundamental steps:

1. Hazard Identification ;
2. Risk assessment ;
3. Safety Demonstration.

Nota: this training is on CSM implementation, on a basis that it is applicable (eg.: significant change or new vehicle).

Project Safety Plan is a classical activity in Railways.

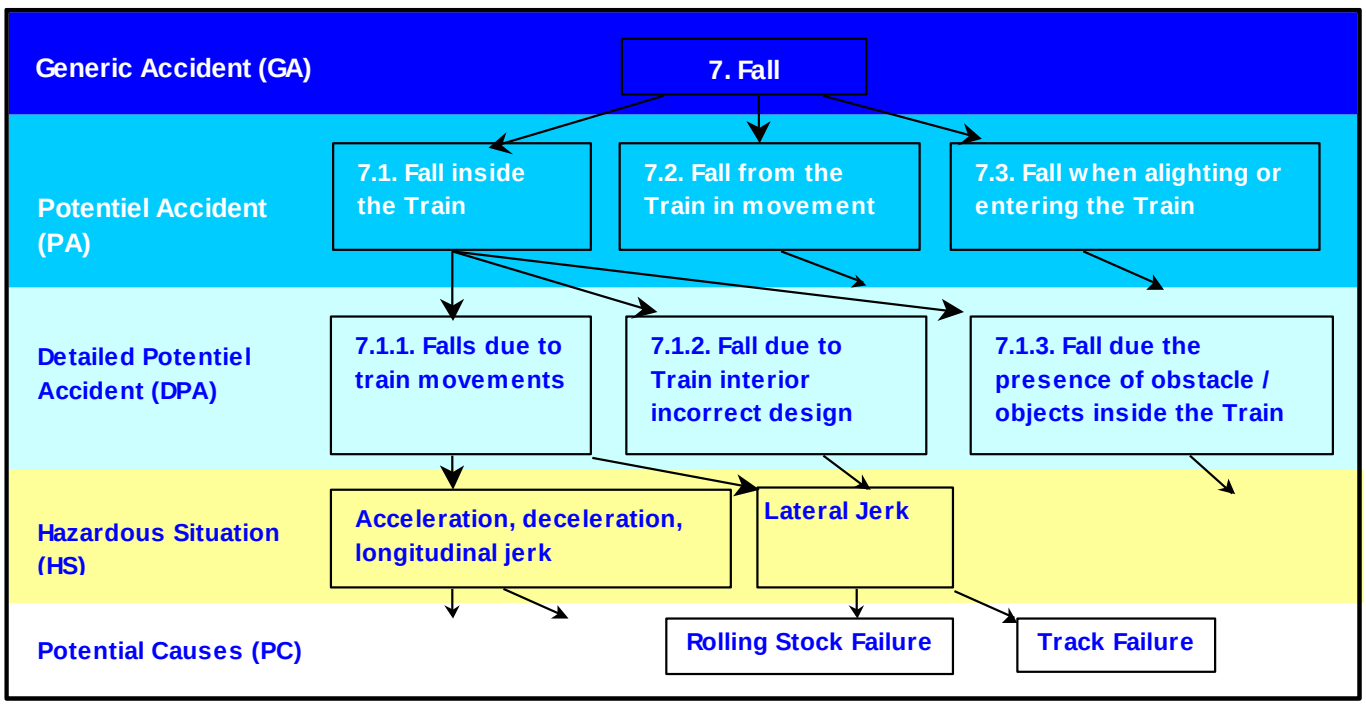
Application of CSM mainly consists in including Risk Acceptance Principles & Risk Declaration. Safety Assessment becomes mandatory.

No other major difference vs CENELEC, safety classical approach.

Hazard Identification

Hazard Identification: use of a Standard Hazard Breakdown Structure:

N°	ACCIDENTS GA	PA	DPA	Hazardous Situation	Potential Cause (PC)
1	Collision				
2	Derailment				
3	Asphyxia - suffocation				



Risk Analysis & Evaluation

Risk acceptation is done according **CENELEC recommendations**:

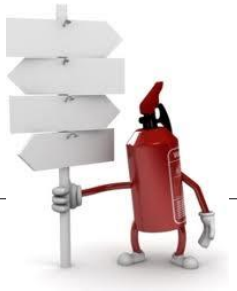
Freq occ of hazards	Severity Levels of Hazard Consequence			
	4: Insignificant	3: Marginal	2: Critical	1: Catastrophic
A: Frequent	Undesirable	Intolerable	Intolerable	Intolerable
B: Probable	Tolerable	Undesirable	Intolerable	Intolerable
C: Occasional	Tolerable	Undesirable	Undesirable	Intolerable
D: Remote	Negligible	Tolerable	Undesirable	Undesirable
E: Improbable	Negligible	Negligible	Tolerable	Tolerable
F: Incredible	Negligible	Negligible	Negligible	Negligible

: compatible with **CSM**

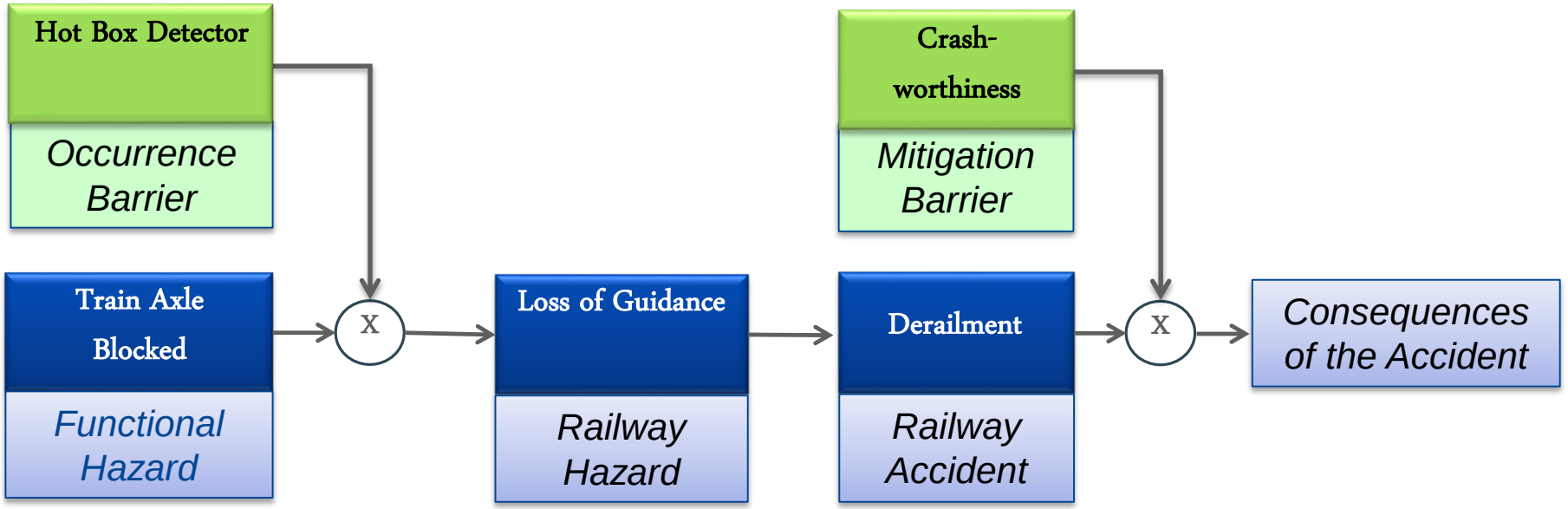
Risk Category	Action to be applied against each category
Intolerable	Shall be eliminated
Undesirable	Shall only be accepted when risk reduction is impracticable and with Safety Authority
Tolerable	Acceptable with adequate control and with the agreement of the Safety Auhtority
Negligible	Acceptable without the agreement of the Safety Authority (Internal or External).

Stakeholders can define their own standard Risk Acceptance Matrix

Safety Requirements



Occurrence and Mitigation Barriers:



Safety Requirements are defined during Hazard analyses, in order to REDUCE occurrence of Hazards or MITIGATE their effects.

Hazard Management: the Hazard Log

- Two main parts
  1. Hazard and related requirements presentation
  2. Evidences for hazard and requirements closure

Hazard Id	Hazard Description	Potential Accident	Hazard Classification			Safety Document (source)	Rq. Ref	Rq. Description	Resp.	Sub-system	Justification					Status of RQ	Status of HZ
			F	S	C						Implementation reference	Test Plan / Installation or Maintenance plan	Safety Case Certification	Related Safety and Verification references	Validation Conclusion		

Step 1.a
Hazard description

Step 1.b
Mitigation description

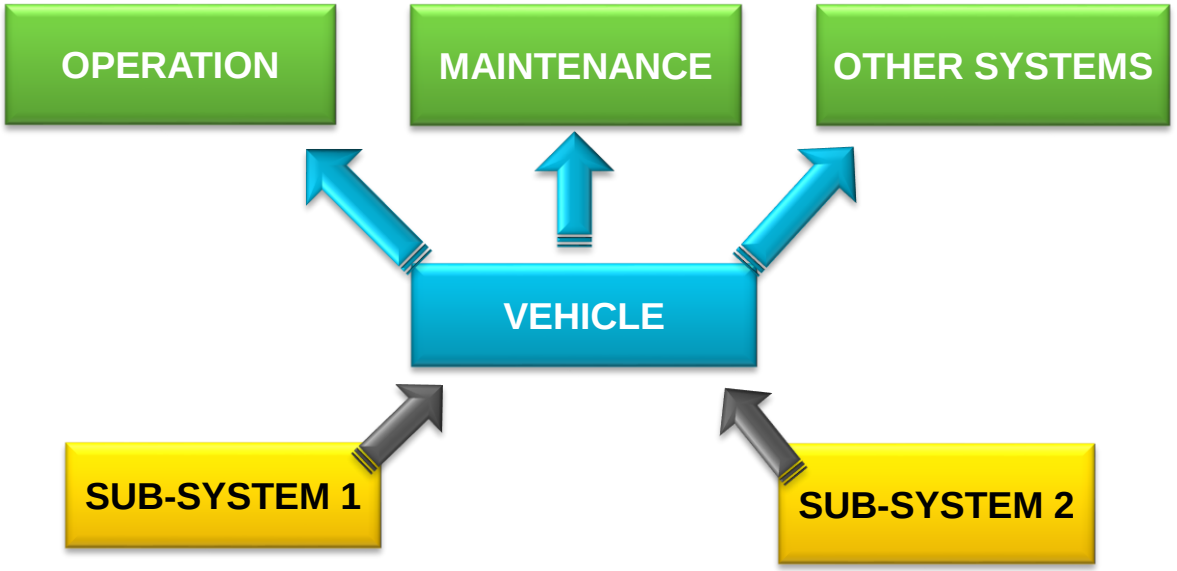
Step 2.a
evidences of closure

Step 2.b
Status of RQ and HL

Hazard Log is the **central mechanism** for the Project Safety Manager to monitor implementation of all **Safety Requirements.** Post evaluation of hazards can be done in the Hazard Log.

Exported safety requirements

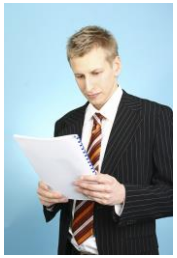
- Exported requirements are often linked to interfaces between sub-systems of a Railway project :
  - ✓Exchanged data
  - ✓Mechanical interfaces
- Requirements are exported:
  - ✓From Sub-systems to System
  - ✓From System to External (out of the Contract scope)



Risk Acceptance Principles

1- Codes of Practice (CoP)

This principle allow to analyse if one or several hazards can be covered by application of relevant codes of practice:



- ✓ **Check that relevant part of the system is within the scope of related CoP**
- ✓ **Comparison of vehicle design parameters with requirements of CoP**
- ✓ **If the design parameters fulfil the requirements of CoP, the associated risk(s) can be deemed acceptable**

Standards / Codes of Practice	Reference
Railway applications Fire protection on railway vehicles	EN 45545
Technical Specifications for Interoperability - Persons with Reduced Mobility *(e.g: gives gap between train and platform to avoid fall of PRM)*	2008/164/EC
Railway applications – Rolling stock equipment – Shock and vibration tests	IEC 61373

Risk Acceptance Principles

2- Use of reference system

Allows to control of one or several hazards by comparison with similar reference systems:

- ✓ **Check that reference system is suitable (acceptable safety level, same operating and environmental conditions)**
- ✓ **Use the Safety Requirements defined for the Reference System, or**
- ✓ **Perform a Gap analysis in order to demonstrate the Safety No Regression**

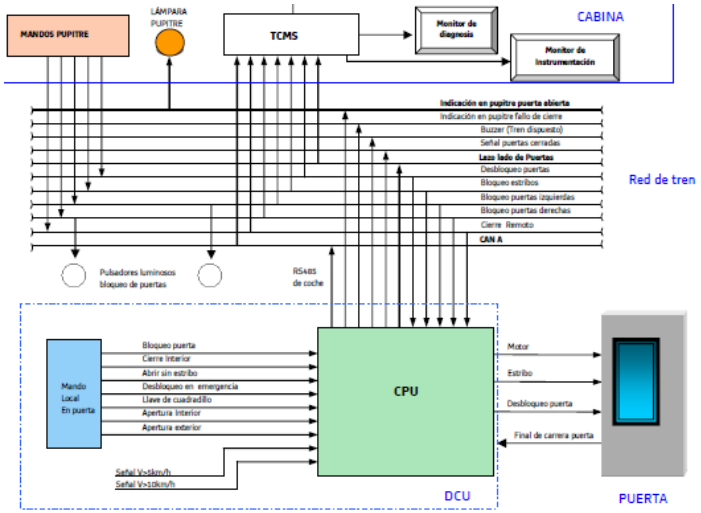
➢ **Conclusion: Safety No Regression**

Modification description	Documentation	Gap Analysis	No Regression
Axle mounting	SPA 123456-1 A0	Same mounting device	OK
Fixation structure	SPA 123456-2 A0	Similar solution	OK
Fixing device	SPA 123456-3 A0	Identical	OK
Global modification			OK

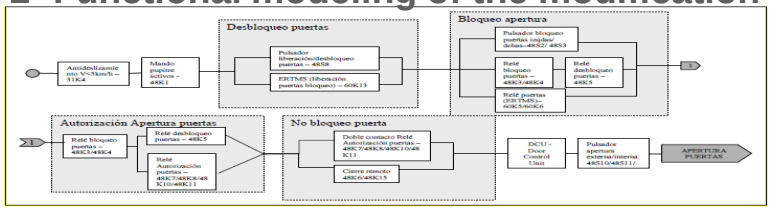
Risk Acceptance Principles

3 – Explicit Risk Estimation

1- Definition of the modification



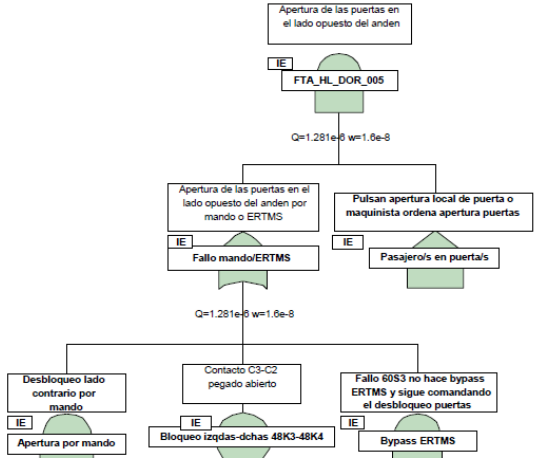
2- Functional modeling of the modification



EU2015/1136 defines design targets for technical functions that can in case of failure, directly lead to catastrophic or critical consequences

- Catastrophic: 10-9/h
- Critical: 10-7/h

3- Logical & Mathematical modeling (FTA)



4- Conclusion: Safety Target

- **Severity** = Critical
- **THR Target** (RS): $10^{-8} \leq \lambda < 10^{-7}$ /h
- **Result :** $\lambda = 1,5\ 10^{-8}$

Modification **OK**

Safety Demonstration

Safety Demonstration

Safety Demonstration is performed though formal **verification and validation** of correct integration of the **Safety Requirements** (issued from the Hazard Analyses),during all the necessary project activities (spec., design, manufacturing, testing...).

The Safety demonstration is documented and synthesized with the closure of Hazard Log and **Safety Report** (Safety Case).

Monitoring of Safety Requirements until closure of the **Hazard Log**, with adequate records, is a key input of Safety Demonstration

Safety Assessment process

AssBo

Safety Assessment Report

Supplier (Alstom)

Safety Report

Safety Req. Specification

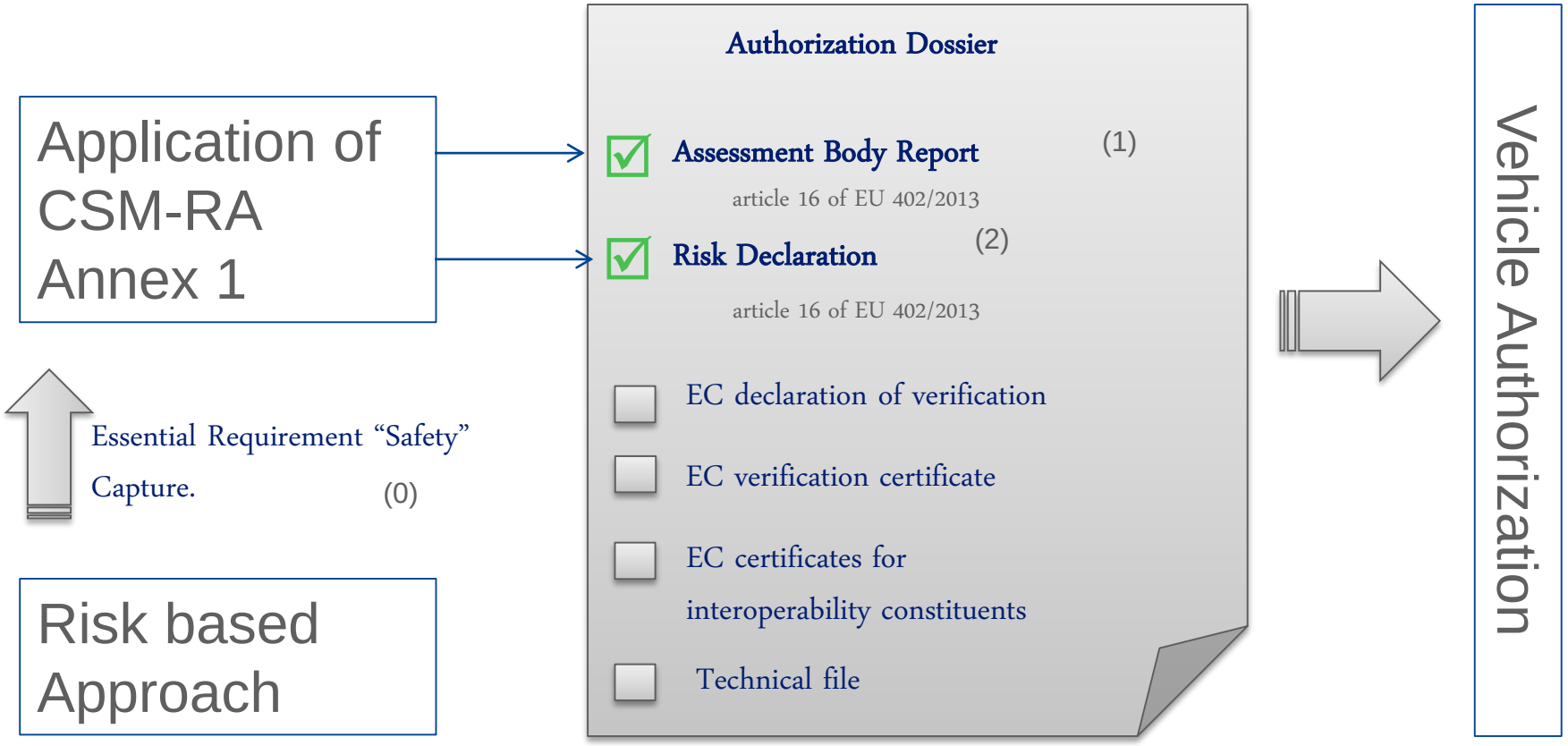
System Req. Specification

National Safety Authority

Authorization Dossier

- [x] Assessment report
- [x] Risk declaration
- [ ] EC declaration of verification
- [ ] EC verification certificate
- [ ] EC certificates for interoperability constituents
- [ ] Technical file

Safe Integration: use of CSM-RA in Vehicle Authorization

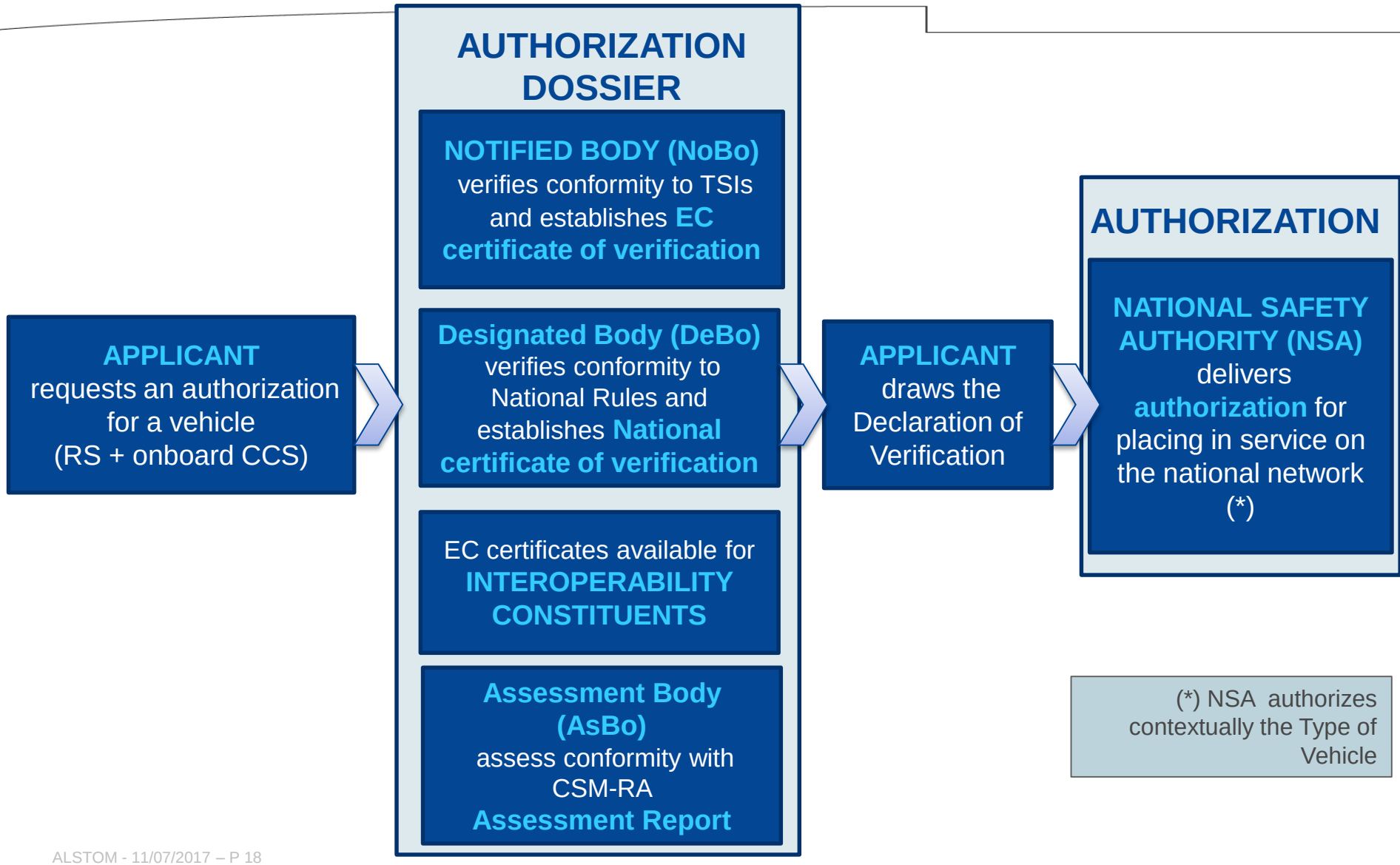


(0) Not to cover essential requirements other than safety

(1) Need for an AssBo

(2) No need to provide all the safety demonstration

Vehicle authorization process and stakeholders



Interoperability constituents

Certification at component level: Interoperability constituents

- Interoperability constituents are defined as '*any elementary component, group of components, subassembly or complete assembly of equipment incorporated or intended to be incorporated into a subsystem upon which the interoperability of the trans-European conventional rail system depends on directly or indirectly*".
- Interoperability constituents (IC) are listed and specified in Section 5 of the relevant TSI
  - 15 ICs listed in 2015 LOC&PAS TSI including toilet discharge connection, contact strips ....
- An EC declaration of conformity or suitability for use is drawn up by the manufacturer or his authorized representative established in the European Union before placing an interoperability constituent on the market. Therefore ICs are delivered with an EC certificate.

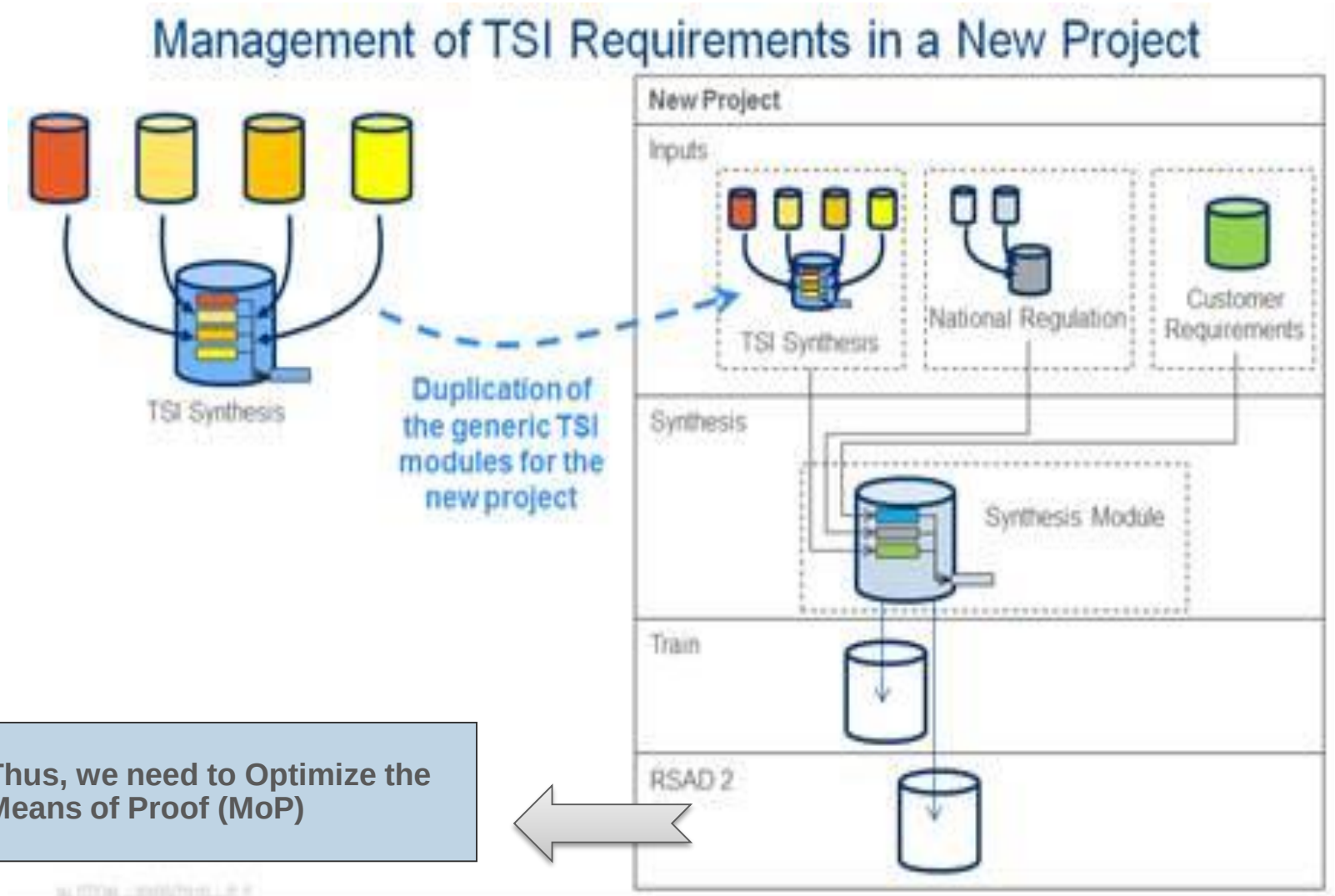
Certification at sub-system level

- Conformity assessment against applicable TSIs
  - by a Notified Body.
  - Validity in the entire EU
- Conformity assessment against complementary national technical rules
  - by a Designated Body.
  - Validity in the member state only.

- Assessment bodies(NoBos and DeBos) issue “certificates of verification” with a reference to examinated technical file.
- Applicant issues a “declaration of conformity”

- In most of MS the NSA is engaged to a max time for the answer (usually 4 months)

Management of Regulatory Requirements & MoP



Thus, we need to Optimize the Means of Proof (MoP)

Means of Proof (MoP) Optimization

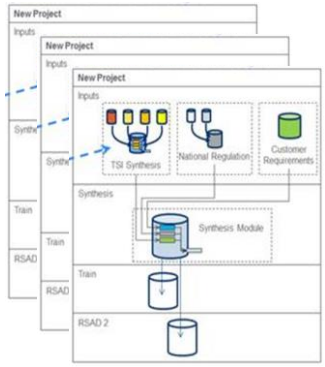
TSE / CERTIF
Central Eng Métiers

T & P

Definition of Generic « Good-Enough » Regulatory MoP

Europe Improved Certification Efficiency

Certification ADN for projects



Case study – Authorisation of PKP ED 250

- Multi country authorisation:

Country	NOBO	DEBO	AssBo
Poland	RINA	IK	IK
Czech Republic		VUZ	VUZ
Austria		Cross- Acceptance	Specific approach
Germany		Alstom SLZ	Included in DEBO

Case study – Authorisation of PKP ED 250

What difficulties did we identified …

- First high speed train in Poland
- Integration of project inside network upgrade
- Multi country authorization process

and how we addressed them

- We created a local Polish team in Warsaw (from 1 person up to 4 persons)
- We regularly involved our Customer on difficulties faced, asking for support
- We start the contact with the different stakeholder (DU, BMVIT, EBA, VUZ) during tender phase
- We have regular contact and meeting with all stakeholder during project evolution
- We take benefit of a similar train (ETR610) with authorization process on going during tender and first stage of the project

Best practices at tender stage

- ✓ Propose your own detailed interpretation of the hierarchy between possibly contradictory technical requirements (basically European rules higher that national ones and national rules higher than contractual specification or not mandatory standards)
- ✓ Identify from tender stage which derogations will have to be requested.
- ✓ Identify regulatory European and national technical rules (regulatory framework) applicable to the tender, mentioning the indices of publication of the reference documents.
- ✓ Prepare a clause-by-clause review of this regulatory framework.
- ✓ Attach to the tender preliminary safety & certification plans including provisional schedule with main steps, tests and document list which constitute the certification dossier, including safety assessment report.

Best practices - Project/ Product development

- ✓ Include a certification manager in the project organization, reporting to the validation manager, safety manager independent from project team
- ✓ Involve all Independent assessors (NoBo, DeBo, AssBo) and NSA as soon as possible. Identify the different entities and their respective role.
- ✓ Prepare a clause-by-clause review of the sections related to safety & certification.
- ✓ Include the safety & certification (type authorization) process in the platform development process
- ✓ Due to NTR, detailed content of the Authorization dossier depends on the Member State where the Authorization is required.
- ✓ Cross- acceptance agreements simplify the different national authorization dossiers, in particular for non TSI conform vehicles

Conclusion

Safety & Certification can support decision making during the project

Safety Assessment gives more confidence in Safety Demonstration, while TSI compliance focus more or nominal vehicle behavior, not on degraded modes.

CSM, TSI, NTR contributes to standardization of Safety & Certification activity between projects, with cost & time optimization

Conclusion

Authorization Process is strongly based upon Requirements Management: for Safety and Technical Compliance demonstration.

Authorization Process is a Project Management activity that relies on all internal and external stakeholders.

ALSTOM

Conclusion

Liberalization of railway activities

Directive 2012/34 establishing a single European railway area (replaces Directives 1991-440 and 2001-14)

Interoperability

- Interoperability Directive 2008/57/EC & Directive (EU) 2016/797

Railway Safety

- Safety Directive 2004/49/EC & Directive (UE) 2016/798

This set of regulations applies only on national networks, No EU regulation for urban ones

www.alstom.com

ALSTOM
Designing fluidity

Definitions

- **Validation**
  - confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled
- **Verification** (ISO 9000 definition)
  - confirmation, through the provision of objective evidence, that specified requirements have been fulfilled.
- **Certification**
  - Conformity Assessment of a product, usually performed by an independent body, based on a set of technical evidences presented by the applicant.

Definitions

- **Authorization**
  - Authorization to place in service:
    - Administrative Decision granted by a National Authority to authorize a railway product to be placed in service.
  - Type authorization
    - In case of rolling stock, a National Authority can deliver a " Type authorization". A type authorization is attached to a type of vehicle and allows any railway undertaking to place in service each individual vehicle of this type through its relevant Safety Certificate part B.