Univerzita Pardubice

RTCM Paper 093-2018-SC134-012

Certification and safety acceptance process for GNSS-based ERTMS/ ETCS and other railway high-safety integrity systems

by

Aleš Filip

University of Pardubice, Czech Republic

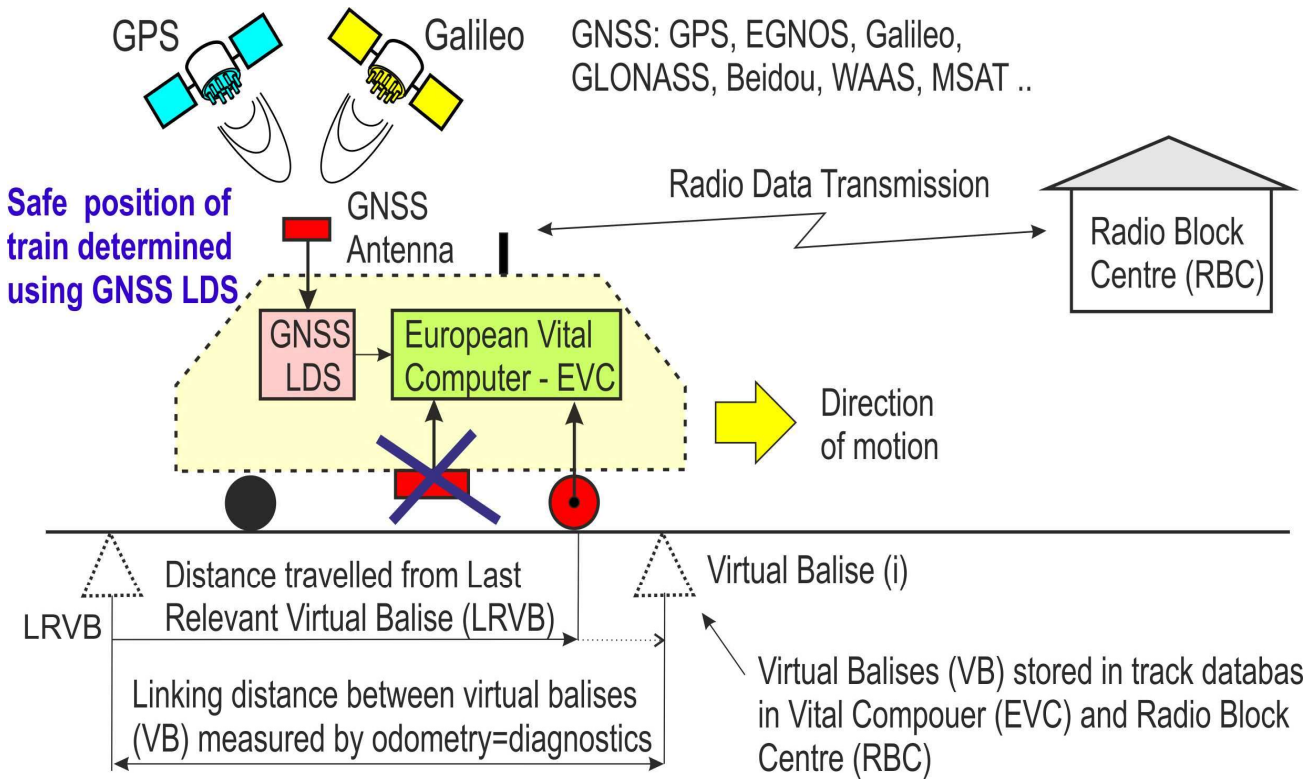
Plenary meeting of RTCM SC 134, SOGEI, Rome, 20-21 June 2018

Contents

1. Certification and safety approval process for interoperable railway signalling and train control systems;
2. Elements of the process, actors and results;
3. Safety approval process for GNSS integration with ERTMS … how to start the process … and what shall be done.

Motivation - GNSS for ERTMS/ ETCS

- European Railway Traffic Management System (ERTMS) was developed for railway signalling and traffic management in Europe;
- European Train Control System (ETCS), which is a part of ERTMS, employs track mounted balises for safe train position determination;



- It is intended to replace costly track balises with virtual ones detected by GNSS;
- This change must pass through certification and approval process.

RTCM Paper 093-2018-SC134-012

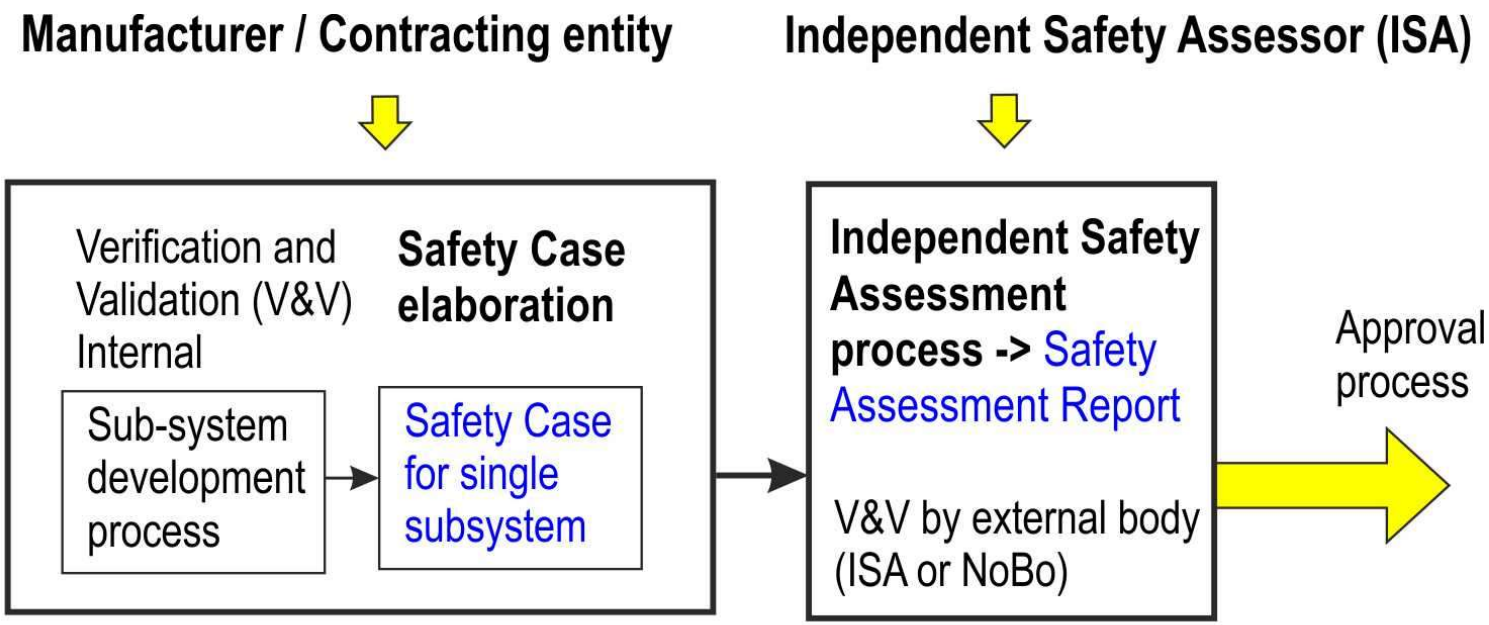
Motivation – Certification and authorization process

- ERTMS/ ETCS consists of numerous on-board and track-side equipment geographically distributed in different MSs and connected via optical, metal and radio (GSM-R and satellite) communication links;
- It is required to ensure the required interoperability among on-board and track-side subsystems shared between different actors, mainly Infrastructure Managers (IM) and Railway Undertakings (RU);
- High safety and dependability requirements for ERTMS must be met - also in cases when Track Balises are replaced with Virtual Balises and detected by GNSS;
- Therefore it is necessary to pass certification and approval process that guarantees that all requirements for ERTMS/ ETCS are met;

Directive (EU) 2016/797 extends authorization process of CCS (Control Command System) to entire railway system - it supports concept of “Cross Acceptance“ as a stepping stone to the interoperability within the Trans European Network.

Steps in certification and authorization process

STEP_1: Simple generic safety-related system



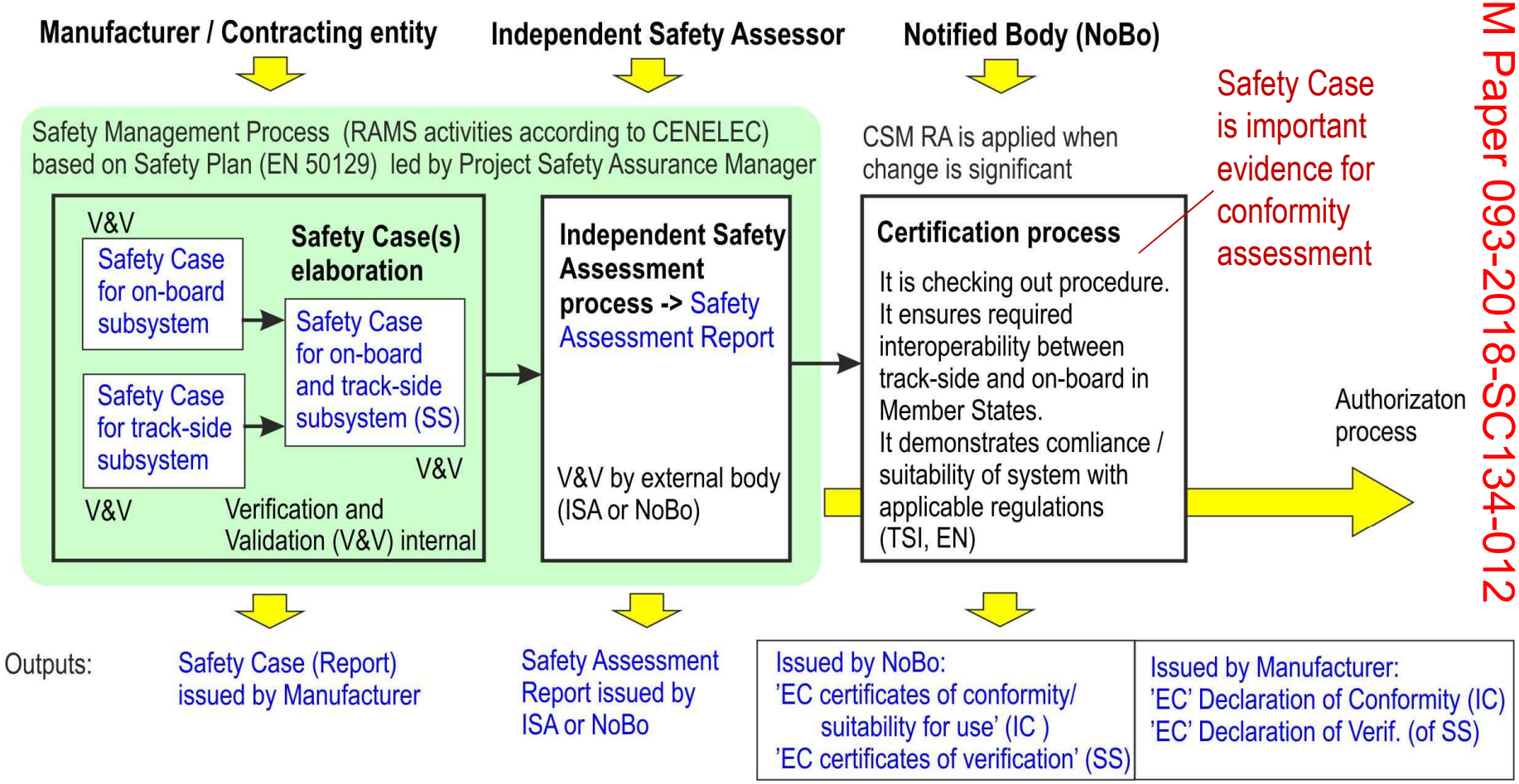
Safety Management Process (RAMS activities according to CENELEC) based on Safety Plan (EN 50129) led by Project Safety Assurance Manager

RTCM Paper 093-2018-SC134-012

- Approval process requires at least Safety Case and Assessment Report
- Verification , Validation (V&V) and Safety Case elaboration according to CENELEC safety standards EN 5012x, etc.
- It is not sufficient to apply CELENEC only for certification

Steps in certification and authorization process

STEP_2: Complex safety-related system for ERTMS/ETCS

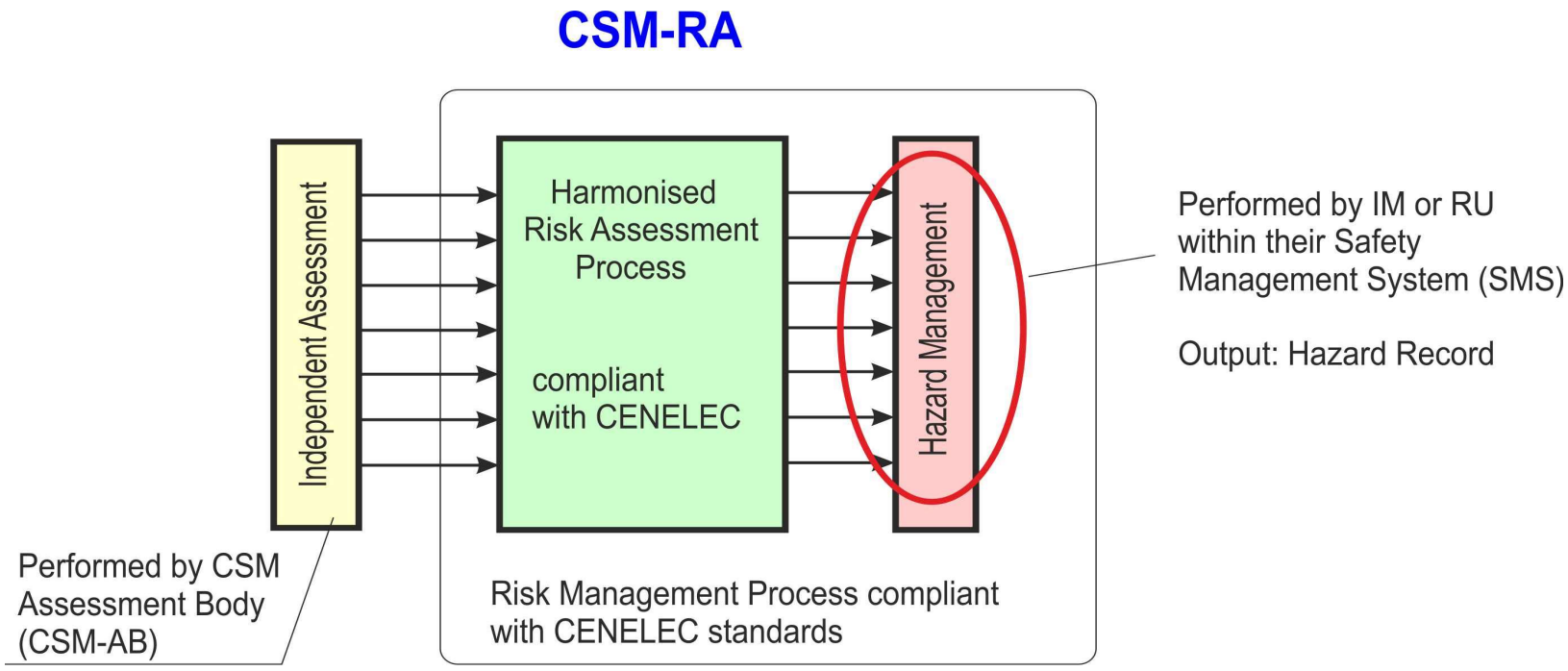


RTCM Paper 093-2018-SC134-012

- Excepting V&V and Safety Case, system compliance with ERTMS/ETCS Technical Specifications for Interoperability (TSIs) should be checked …

Steps in certification and authorization process

- Railway actors have to manage safely changes of the European railway system – including GNSS integration with ERTMS.
- Common Safety Method for Risk evaluation and Assessment (CSM-RA) must be used if system change (safety related) is significant
- CSM-RA harmonizes Risk Management Process, enables to introduce Cross-acceptance of Risk Assessment Process



RTCM Paper 093-2018-SC134-012

Steps in certification and authorization process

- Activities such as V&V, Safety Case elaboration, its independent Risk Assessment and Conformity Assessment with respect to TSI‘s (i.e. certification) cover only part of V-Cycle (Life-cycle) according to CENELEC EN 50126;

- Safety monitoring during real system operations is not covered by the activities above;

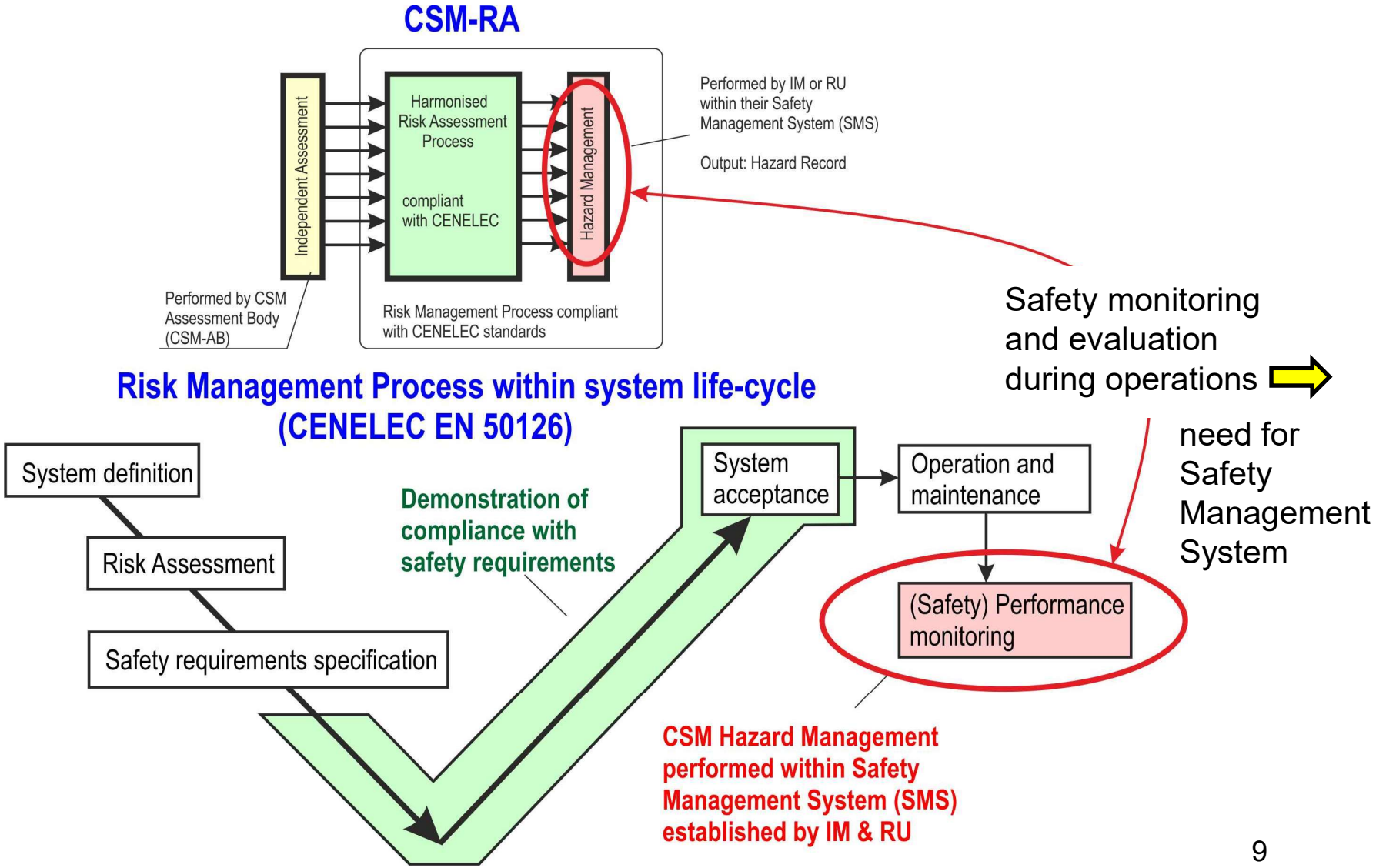
- However, CSM-RA shall cover the whole CENELEC lifecycle, including safety evaluation during system operations …

- Therefore CSM-RA requires Safety Management System (SMS) to be performed with RU (Railway Undertaking) and IM (Infrastructure Manager) to fill in the gap mentioned above;

- European common Safety Targets (for the whole railway systems) are used for safety evaluation within Safety Management System .

Steps in certification and authorization process

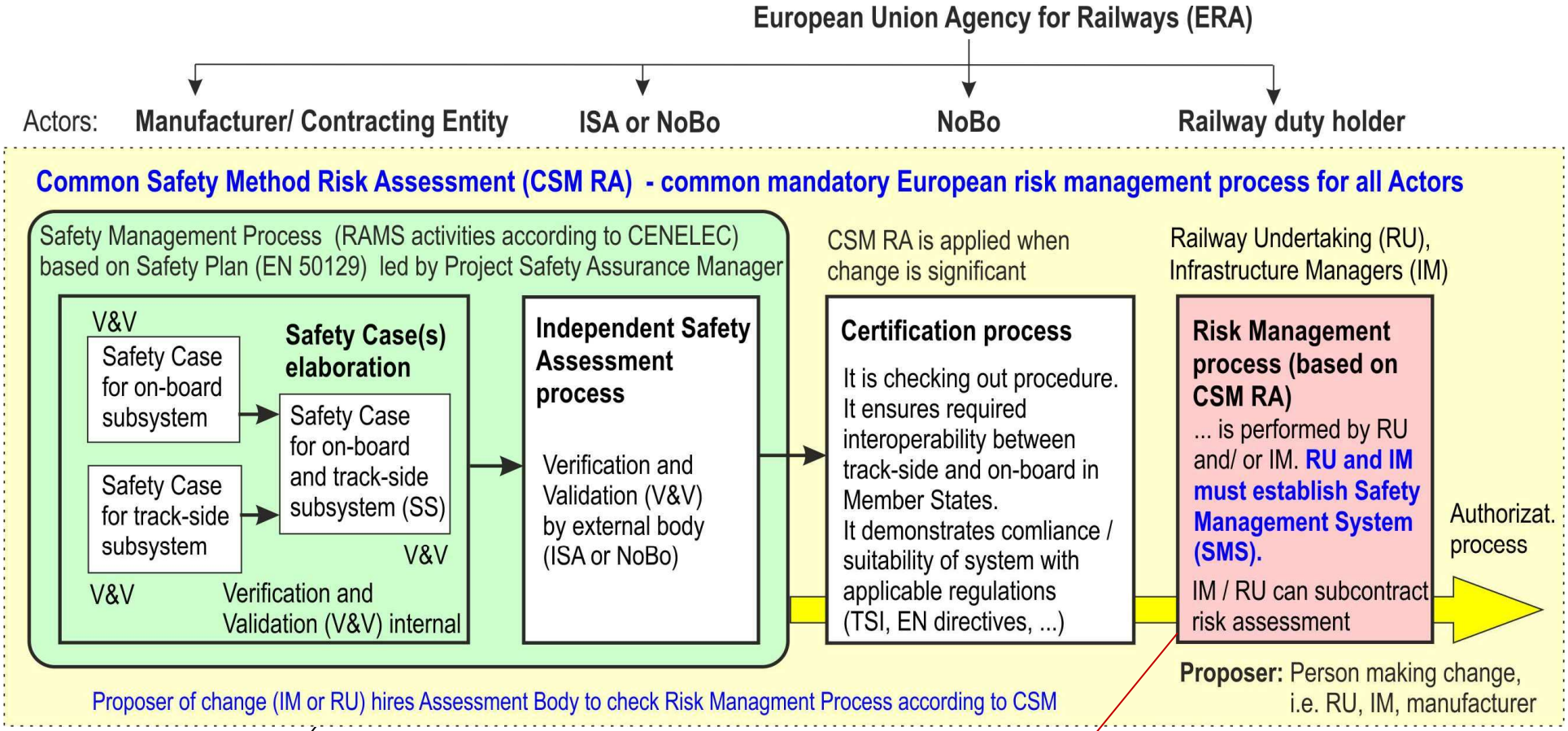
- Compliance of CSM-RA with CENELEC V-cycle (EN 50126)



RTCM Paper 093-2018-SC134-012

Steps in certification and authorization process

STEP_3: Complex safety-related system for ERTMS … continuation



CENELEC + CSM-RA + TSIs + EU regulations =
Framework for certification and safety approval
(of significant safety relevant change)

Safety Management System (SMS)

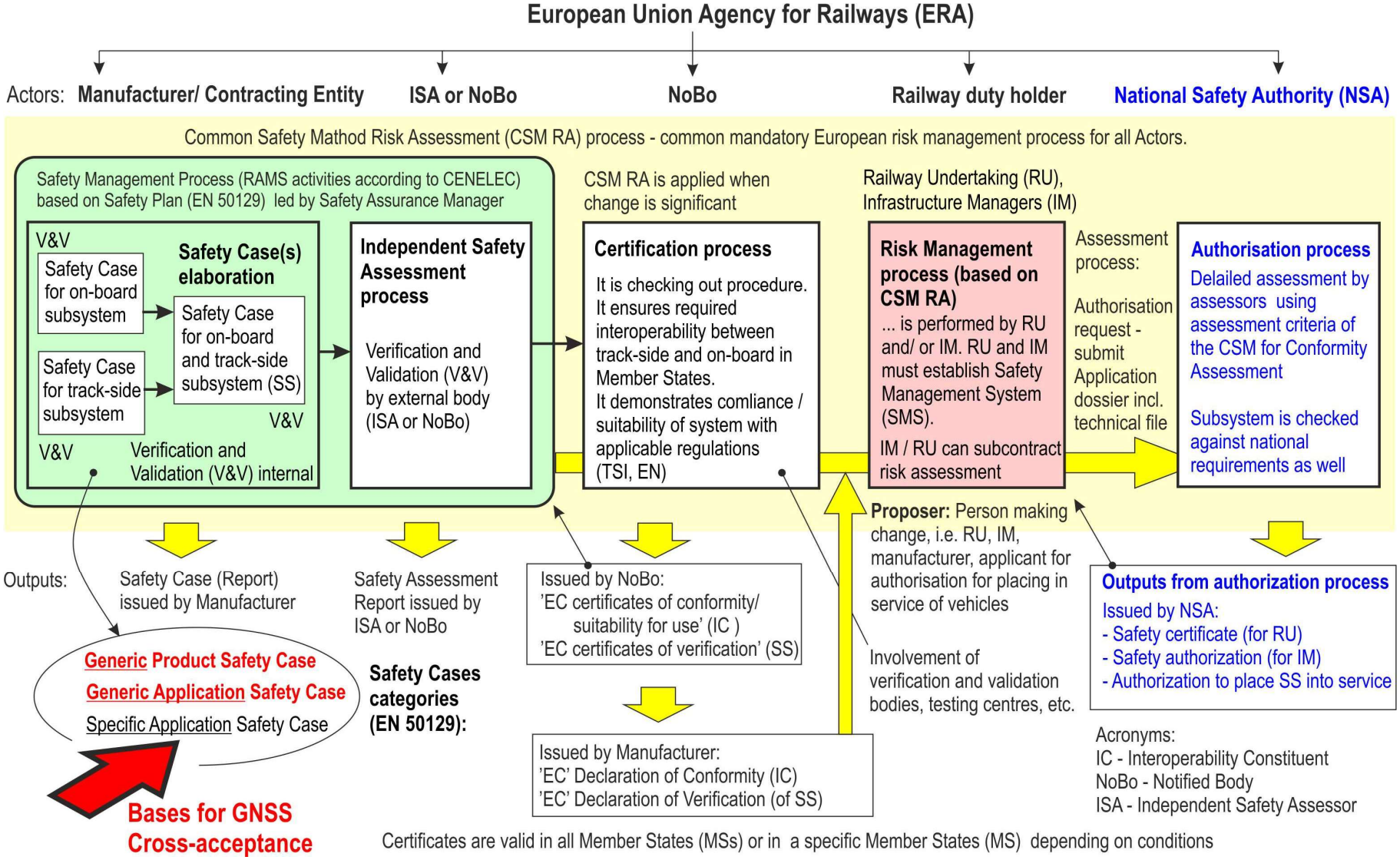
RTCM Paper 093-2018-SC134-012

Safety approval process for integration of GNSS with ERTMS

- The aim of European railway authorities and European railway industry is to develop interoperable railway systems based on common regulations;
- Cross-acceptance of Safety Approvals for sub-systems and equipment by the different national railway authorities is essential;
- Cross-acceptance is also critical for exploitation of (aviation) GNSS SoL service for ERTMS;
- Safety Case is very important part of the conformity assessment documenting the achieved safety levels, even though there are replaced by higher level certificates during certification and safety approval process.
- The Cross-acceptance of GNSS SoL service can be achieved via two Generic Safety Cases from the following EN 50129 safety cases family:
  - Generic Product Safety Case *(independent of railway application);*
  - Generic Application Safety Case *(for a class of applications).*

Steps in certification and authorization process

STEP_4: Framework for the whole certification and safety approval process



RTCM Paper 093-2018-SC134-012

Safety approval process for integration of GNSS with ERTMS

- **Generic Product Safety Case** = Generic Safety Case for a Product (i.e. SBAS), *independent of ERTMS/ETCS solution*

It should include:

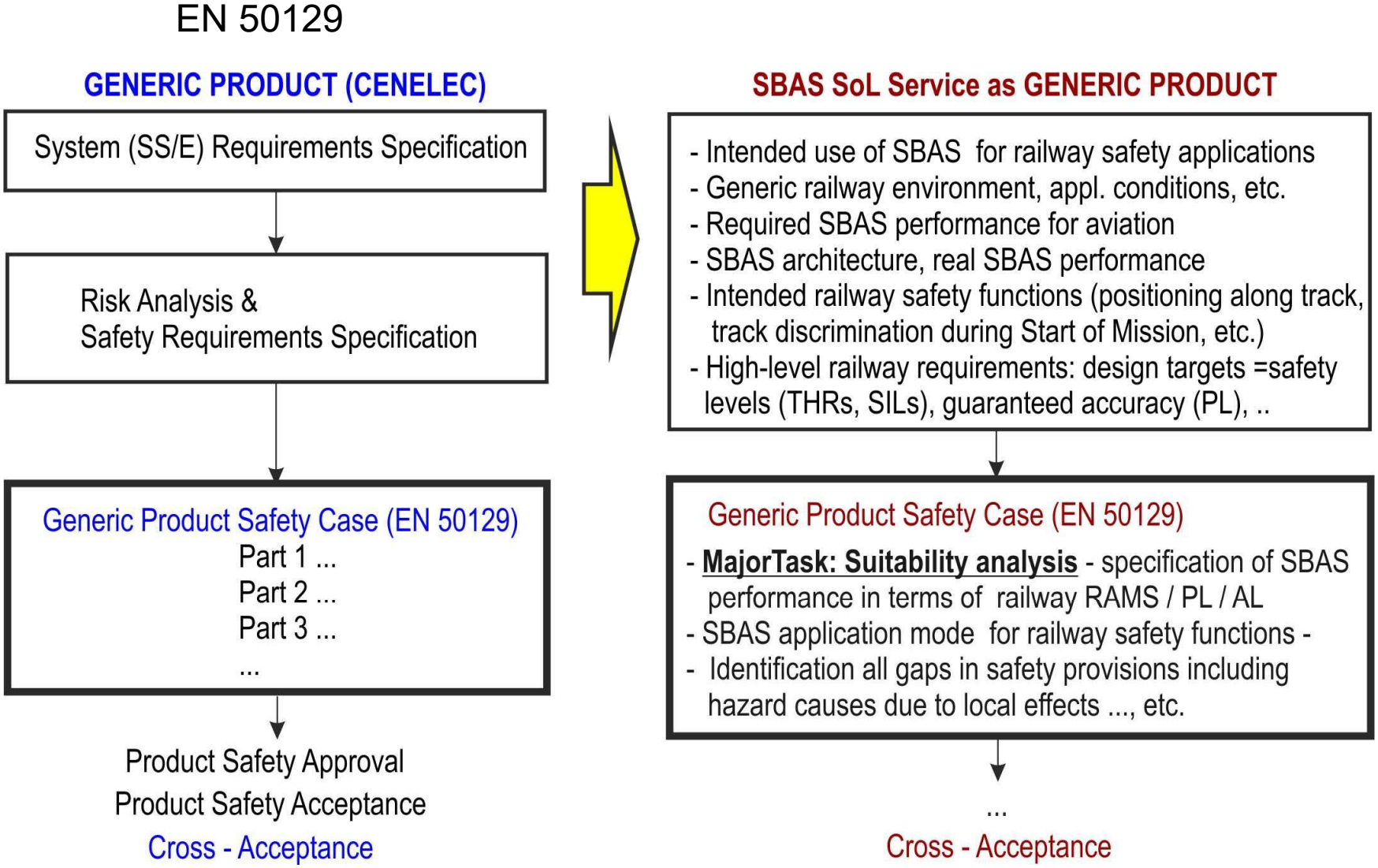
(a) *Genetic description of railway SBAS safety applications*, railway safety concepts, required safety levels / design targets, functions to be performed – determination of train position along track, track determination function during SOM (Start of Mission), etc.

(b) *SBAS suitability analysis* – i.e. the determination of real SBAS performance in terms of railway RAMS (EN 50126) and guaranteed accuracy (Protection Level) … what railway can expect from SBAS

(c) *The identification all gaps in safety provisions* due to SBAS imperfections, railway environmental effects (multipath, EMI), potential intentional attacks e.g. spoofing (security gaps) – from viewpoint of railway high-safety integrity requirements.

Responsibility: This Generic Safety Case for Product shall be delivered from the Product/ service supplier to System supplier/ configurator)

Safety approval and acceptance process for Generic Product Safety Case (CENELEC)… e.g. for Generic Safety Case for SBAS



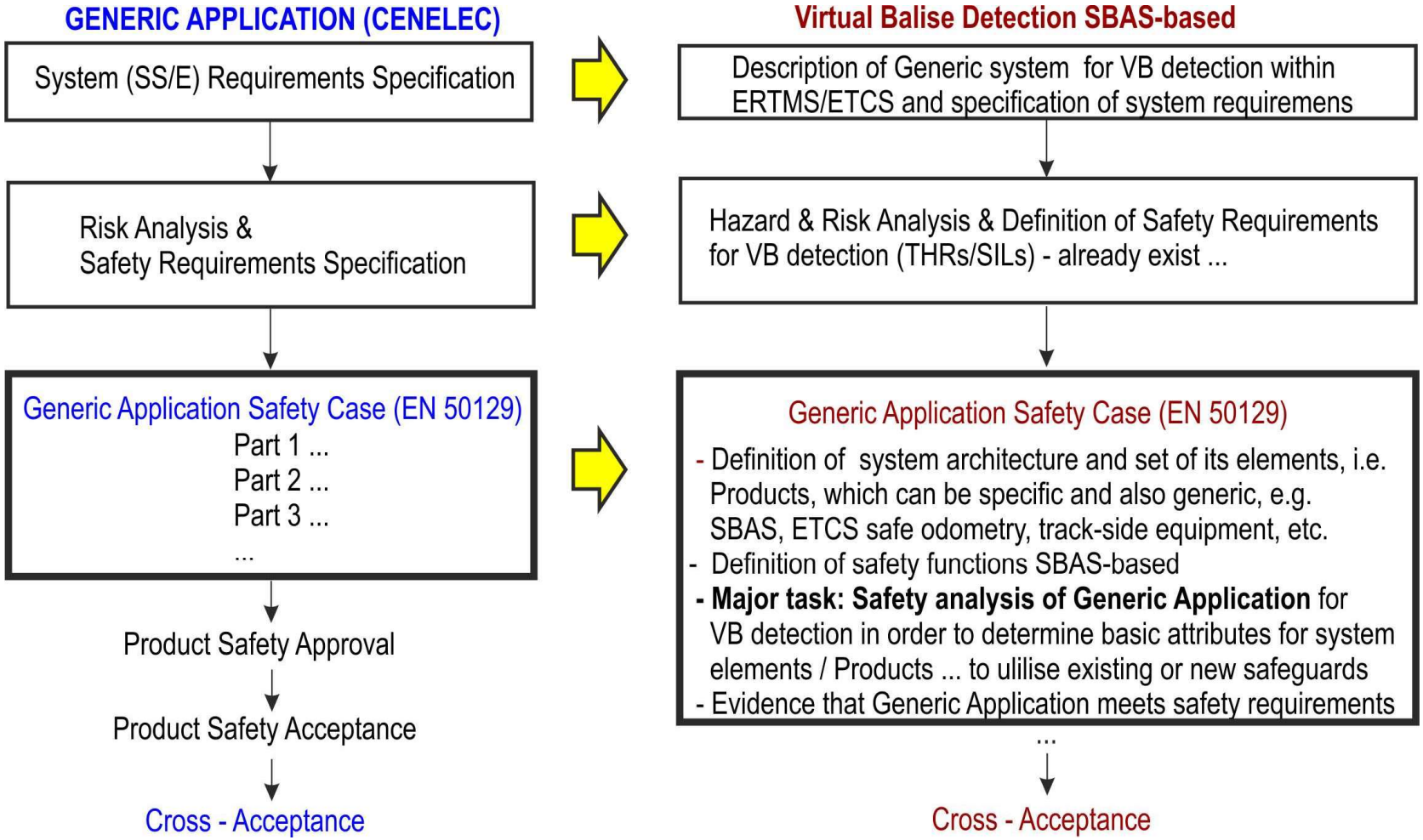
RTCM Paper 093-2018-SC134-012

Safety approval process for integration of GNSS with ERTMS

- **Generic application Safety Case** = Safety Case for a Generic Application, i.e. *for a class of ERTMS applications* –

  Example: use of SBAS within ERTMS for virtual balise detection taking into account all existing ETCS and newly introduced safety barriers;

Safety acceptance and approval process for Generic Application Safety Case (CENELEC) e.g. for SBAS-based ERTMS/ETCS



Generic safety cases shall be mutually recognized in all EU MSs.

RTCM Paper 093-2018-SC134-012

Conclusions

1. Certification and safety approval process applied on European railways enables to achieve the required interoperability and very high safety levels (SIL 4);
2. Basic element in this process is a Safety Case;
3. The process must be also applied for introduction of GNSS into ERTMS/ETCS;
4. The required cross-acceptance of Safety Cases for application of GNSS SoL service in railway signalling and train Control can be achieved by means of two Generic Safety Cases (EN 50129): (a) General Product Safety Case, and (b) Generic Application Safety Case
5. Generic Product Safety Case for SBAS is a key element for introduction of SBAS/EGNOS into ERTMS/ETCS.

Univerzita Pardubice

Acknowledgement

This work was supported from the project PosiTrans (2018-2020) performed within the Czech MŠMT OP VVV programme.

Reference:

Filip, A., Sabina, S. and Rispoli, F.: A Framework for Certification of Train Location Determination System Based on GNSS for ERTMS/ ETCS. COMPRAIL 2018, Lisbon, 2-4 July 2018, 14 pages.