Start-up activities for Advanced Signalling and Automation Systems

Compendium Safety & Interoperability

Target system & related processes

WHY THIS COMPENDIUM?

- Not all experts involved in Shift2Rail projects have the same level of information about the legal framework and established processes in the CCS domain (they may also lack a clear view on the strategic vision which is addressed in the S2R Master Plan and MAAP)

- That is needed to converge research activities towards the next evolution of the digital railway system in Europe

- This compendium provides guidance by basic information and strategic targets thus helping to overcome silo-approaches and integrating into a coherent future railway target system of IP2

TABLE OF CONTENTS

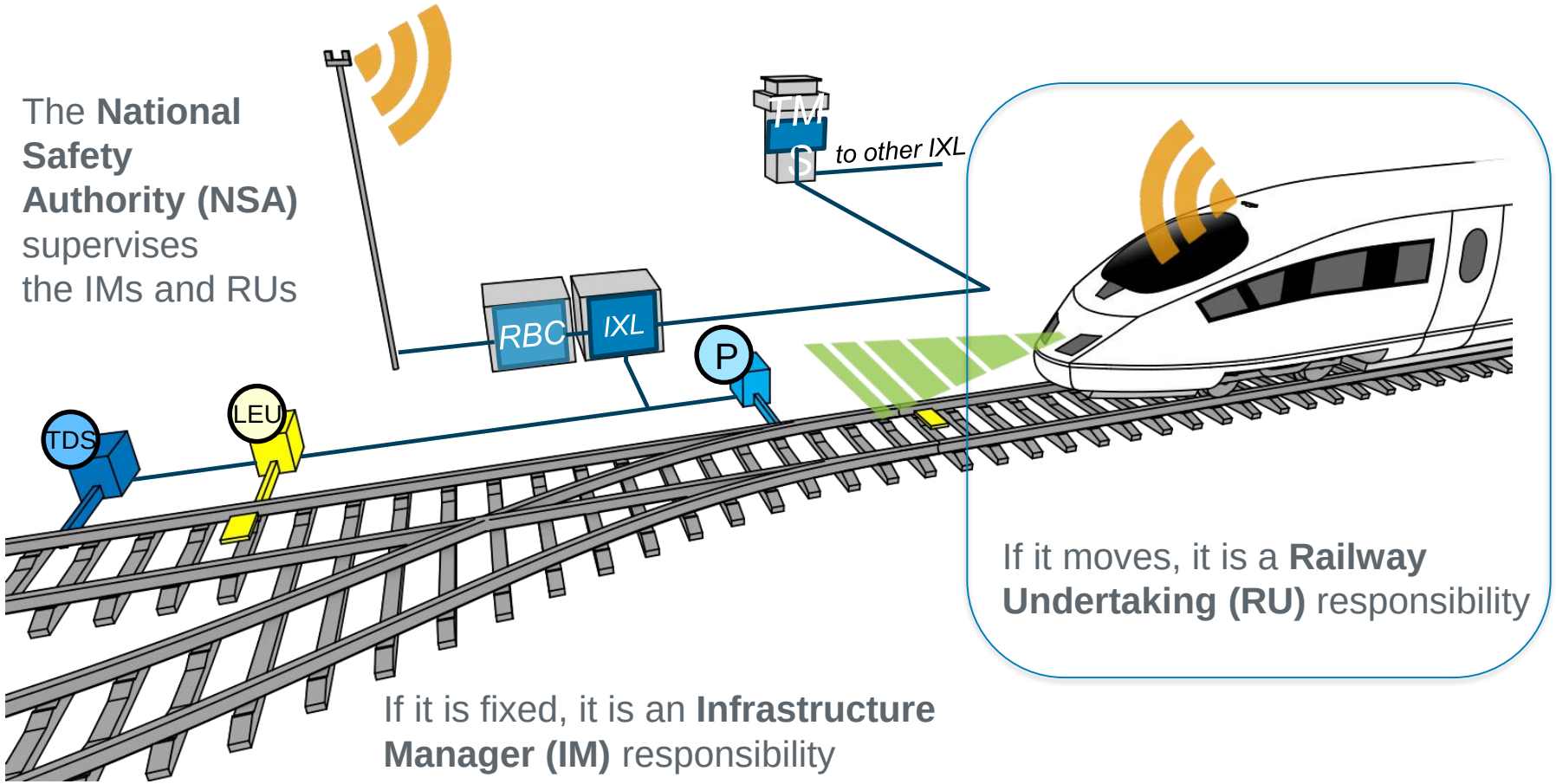
Chapter

Overview: Key concepts for managing the shared railway system

Roles and responsibilities

ROLES AND RESPONSIBILITIES
REGULATORY FRAMEWORK – THE SHARED RAILWAY SYSTEM

The **National Safety Authority (NSA)** supervises the IMs and RUs



If it moves, it is a **Railway Undertaking (RU)** responsibility

If it is fixed, it is an **Infrastructure Manager (IM)** responsibility

ROLES AND RESPONSIBILITIES

Each RU and IM has a Safety Management System (SMS). It must ensure that its part of the system is operated in a safe manner.

For all the sub-systems they operate, the RUs and IMs must ensure that they always meets the essential requirements for:

- Safety
- Environmental protection
- Technical Compatibility
- Reliability and Availability
- Health
- Access (for people of reduced mobility)

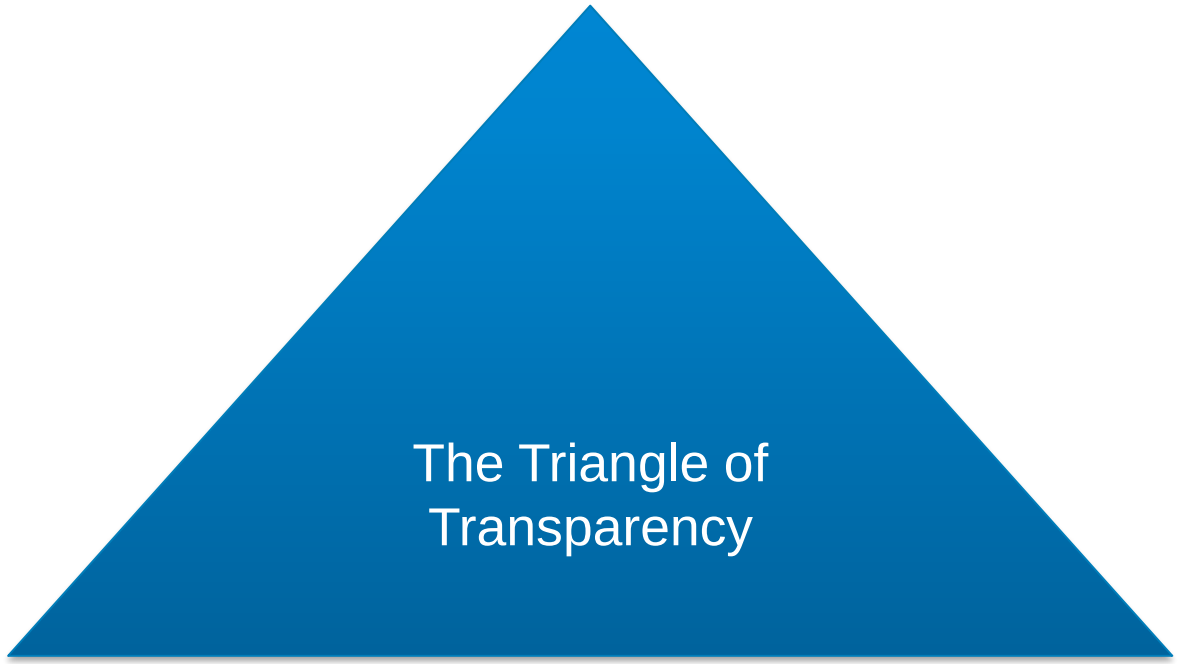
conforms to the rules:

- CSM on SMS
- TSIs
- National rules

Other actors (e.g. manufacturers, keepers, maintainers, loaders, etc) contribute to the safety of the system but the primary responsibility rests with the **RU** or **IM**. The **SMS** of RU or IM must ensure the efforts of these suppliers **deliver** the above. Entities in charge of maintenance (ECM) of Freight Wagons are certified.

ROLES AND RESPONSIBILITIES – REGULATORY FRAMEWORK AUTHORISATION OF VEHICLES AND NETWORK PROJECTS

Rule setter
EC + Member States



Authorising Entity
ERA or National Safety Authority

Assessment Body
NoBo
DeBo
CSM AsBo

Source: European Union Agency for Railways

WHAT IS INTEROPERABILITY?

Objectives from the Interoperability Directive

- to define an optimal level of **technical harmonisation**;
- to make it possible to facilitate**, improve and develop rail transport services** within the Union and with third countries;
- to contribute to the completion of the **single European railway area** and
- to contribute to the progressive achievement of **the internal market**.

Source: European Union Agency for Railways – Interoperability Directive

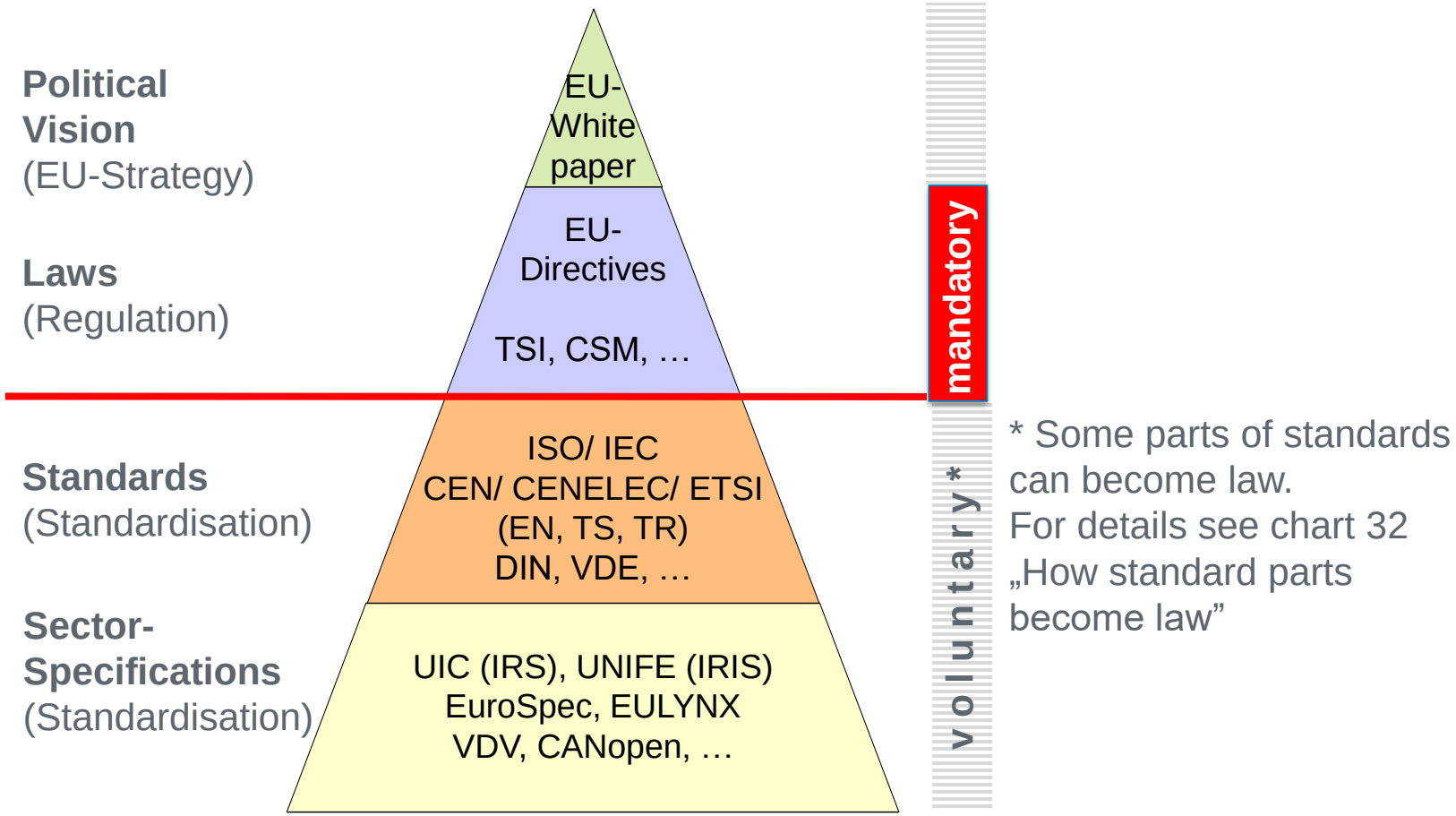
MANAGING A SHARED SYSTEM

- It follows that where it is necessary for all actors to “do the same thing“, **for meeting:**
  - **the objectives of the directive**
  - **the essential requirements for the system as a whole**
  - **the essential requirements for their part of the system**

- Then the things that everybody “must do the same” must be laid down in rules
  - the TSIs for the target system specifications and
  - national rules for legacy system specifications

- For all other elements of system specification the actors may choose their own method of meeting the essential requirements
  - below the red line in slide 10

REQUIREMENTS NEED STRUCTURE



Human and organisational components need to be integrated in all the requirements (both mandatory and voluntary)

Chapter

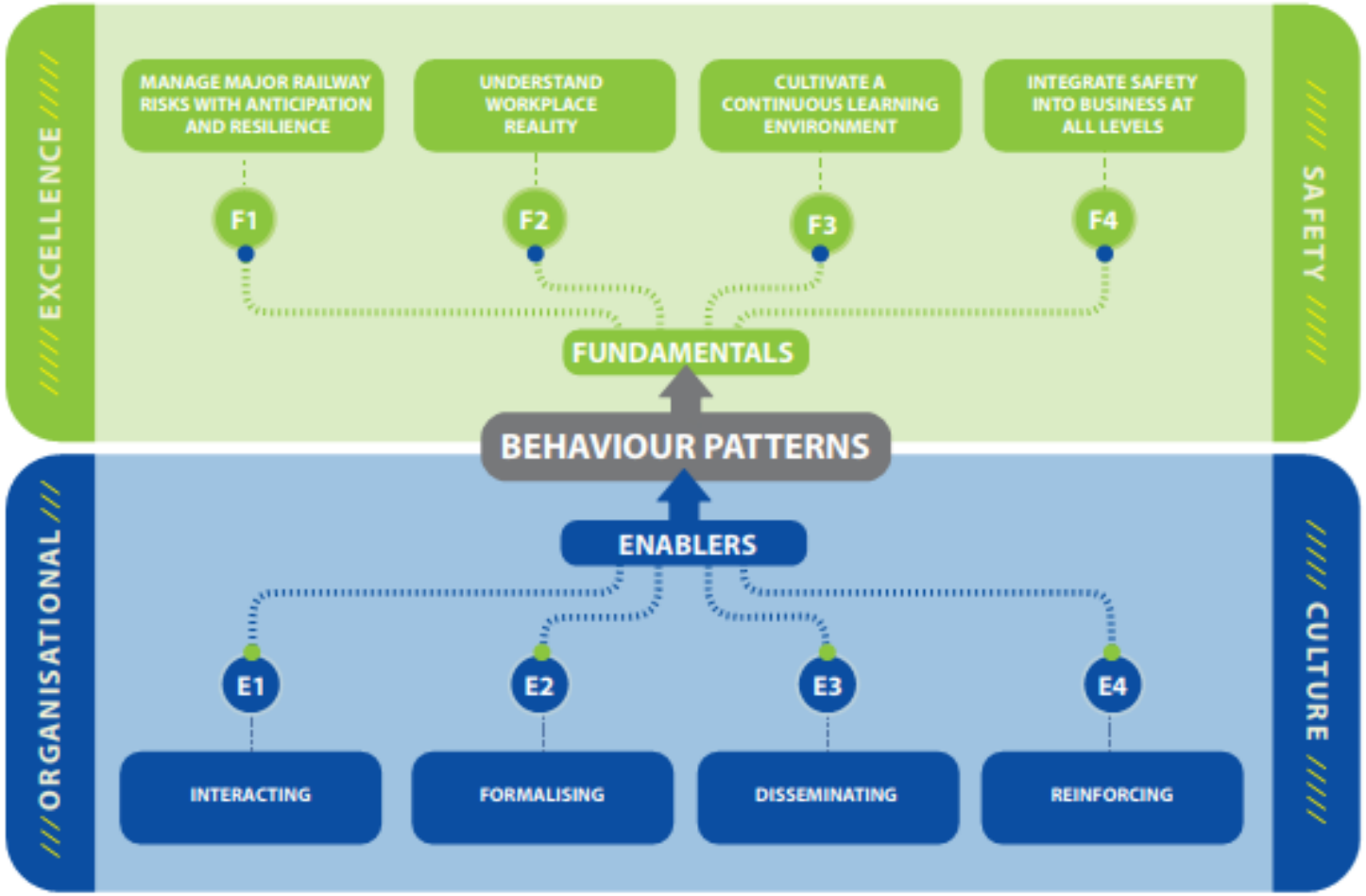
Overview: Key concepts for managing the shared railway systems

SAFETY

SAFETY CULTURE

Source: European Union Agency for Railways

STRONG REGULATORY SAFETY CULTURE



EUROPEAN RAILWAY SAFETY CULTURE MODEL

Source: European Union Agency for Railways

SAFETY STRUCTURES

- Permissioning scheme for equipment
- Permissioning scheme for safety management systems
- Maintenance scheme for rolling stock (incl. ECMs)
- Independent Supervision (NSAs)
- Independent Accident Investigation (NIBs)
- Independent Assessment Bodies (CSM Risk Assessment)
- Defined responsibilities in law (cannot subcontract responsibility)
- Where there is a need for a Common Approach – “Common Safety Methods”
- Monitoring at a European Level (Commission & Agency) including CSIs and CSTs (NRVs)

THE RISE OF SAFETY MANAGEMENT SYSTEMS

- 6th July 1988 – Piper Alpha oil production platform explosion
- 167 lost, only 62 survivors
- Lord Cullen's recommendations (106) move away from prescription to safety cases as a more effective system

SAFETY MANAGEMENT SYSTEMS IN RAIL
RAILWAY SAFETY DIRECTIVE (EU) 2016/798– ARTICLE 9.2

The SMS must:

- be **documented** in all relevant parts
- describe the **distribution of responsibilities** within the organisation of IM or RU
- show how control by the **management** on different levels is secured
- show how **staff** and their representatives on all levels are involved
- show how **continuous improvement** of the safety management system is ensured

All these requirements shall be included in the SMS

SAFETY MANAGEMENT SYSTEMS IN RAIL
RAILWAY SAFETY DIRECTIVE (EU) 2016/798 – ARTICLE 9.3

The requirement of the SMS shall be fulfilled through:

- **safety policy** and corporate **safety targets**
- **compliance** with standards or other prescriptive conditions
- change management
- risk management
- operational and front-line **staff competence management**
- **communication** and info exchange, **document** management
- **emergency** management
- reporting of unexpected outcomes
- internal **auditing** of the SMS

All these elements shall be defined in the organisation of the company and shall be DOCUMENTED

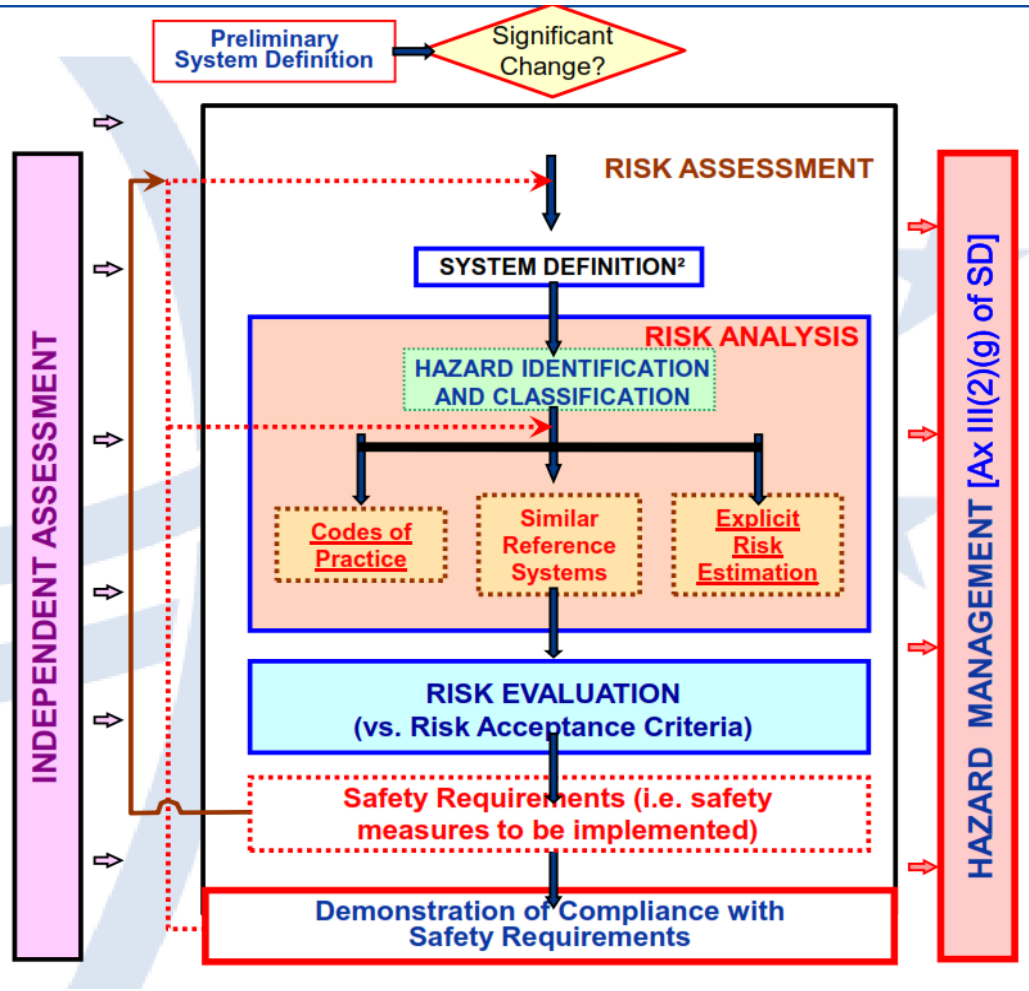
SAFETY MANAGEMENT SYSTEMS

- Check whether SMS is sufficient to allow operation to begin (Certification: CSM for Conformity Assessment (*) / CSM on SMS requirements (EU) 2018/762 – maximum validity 5 years)
- Supervision of the functioning of the SMS by National Safety Authorities during operation (CSM Supervision)
- Railway Undertakings checking for themselves that their systems are functioning correctly during operation (CSM Monitoring)

(*) The CSM for Conformity Assessment will be definitively repealed in 2025

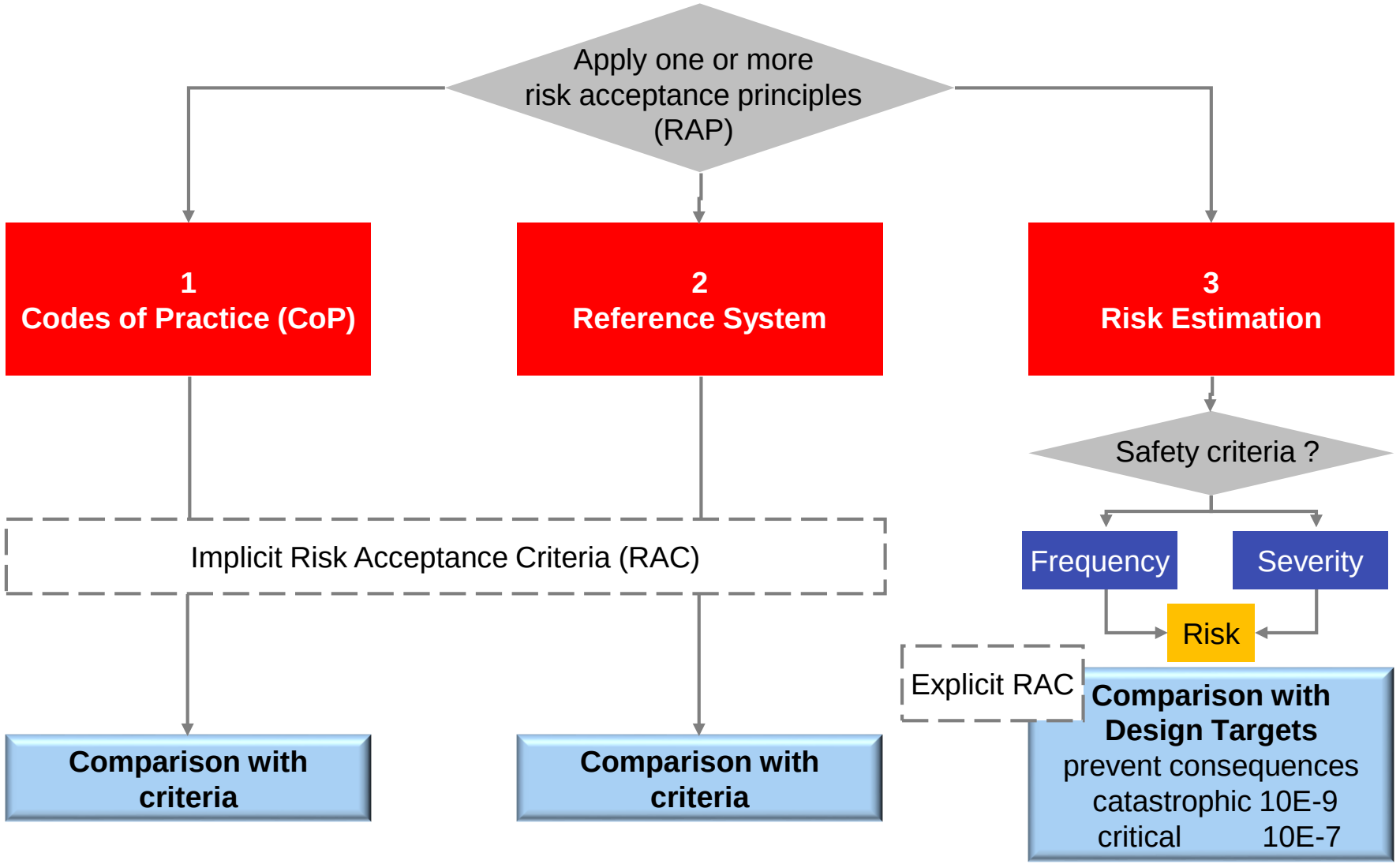
COMMON APPROACH TO RISK ASSESSMENT

- Basically CSM is an iterative process made of 3 steps:
  - (a) Identification of hazards, associated safety measures and resulting safety requirements
  - (b) Risk analysis and risk evaluation based on exiting risk acceptance principles
  - (c) Demonstration of the system compliance with the identified safety requirements
- Additional requirements for mutual recognition:
  - (a) Hazard Management
  - (b) Independent Assessment (Assessment Body)



Source: European Union Agency for Railways

THE 3 RISK ACCEPTANCE PRINCIPLES



INDEPENDENT ACCIDENT INVESTIGATION BODY

- The objective is **prevention of accidents and possible improvement of railway safety**
- The investigation body shall investigate serious accidents and might investigate in addition also those accidents and incidents which under slightly different conditions might have let to serious accidents.
- The investigation body shall, at its discretion, decide whether or not to investigate such an accident or incident. In its decision it shall take into account:
  - (a) the seriousness of the accident or incident
  - (b) whether it forms part of a series of accidents or incidents relevant to the system as a whole;
  - (c) its impact on railway safety and
  - (d) requests from IM, RU and NSA

INTEROPERABILITY DIRECTIVE VS SAFETY DIRECTIVE

- The **Interoperability Directive** covers all things the actors **must do the same to make the shared system work**

- The **Safety Directive** contains the requirements to ensure that the actors **manage their part of the shared system safely**

- Sometimes the Interoperability Directive “imports” concepts from the Safety Directive (e.g. the use of the CSM RA for requirements capture for vehicle type design)

Chapter

Overview: Key concepts for managing the shared railway system

VEHICLE AUTHORISATION

WHAT IS VEHICLE AUTHORISATION?

Why is it required?

- Public interest
- Special check at a safety relevant event (new or upgraded vehicle design)
- To ensure compatibility of networks and vehicles managed by different entities
- IMs and RUs can not always be relied upon spontaneously to deliver full interoperability
- For interoperability, it is necessary to deliver technical compatibility: *“The technical characteristics of the infra and fixed installations must be compatible with each other and with those of the trains to be used on the system”.*
- Legal certainty for applicants
- Equality of treatment for manufacturers in all Member States

Source: European Union Agency for Railways

WHAT IS VEHICLE AUTHORISATION?

Vehicle Type Authorisation is:

- Legal act issued by an authorising entity based on reasonable assurance that the applicant and the actors supporting the applicant have fulfilled their responsibilities (full definition in Art. 2 (16) of Regulation 2018/545)

Its Purpose is:

- To ensure conformity with the essential requirements of the applicable legislation
- To enable individual vehicles manufactured according to the design type to be placed on the market based on an applicant's declaration of conformity to the type

Source: European Union Agency for Railways

WHAT IS VEHICLE AUTHORISATION?

The Authorising Entity

SHOULD: ☑

- satisfy itself of the efficacy of the process
- satisfy itself of consistency, completeness and plausibility of the documentation

SHOULD NOT: ☒

- repeat or duplicate work carried out by other checking bodies
- use the authorisation process to check or evaluate the competence of checking bodies

Source: European Union Agency for Railways

WHAT IS VEHICLE AUTHORISATION?

Is vehicle authorisation time limited?

To give applicants legal certainty a vehicle type authorisation/Vehicle authorisation for placing on the market is generally not time limited.

When a vehicle/vehicle type authorisation may be rendered invalid?

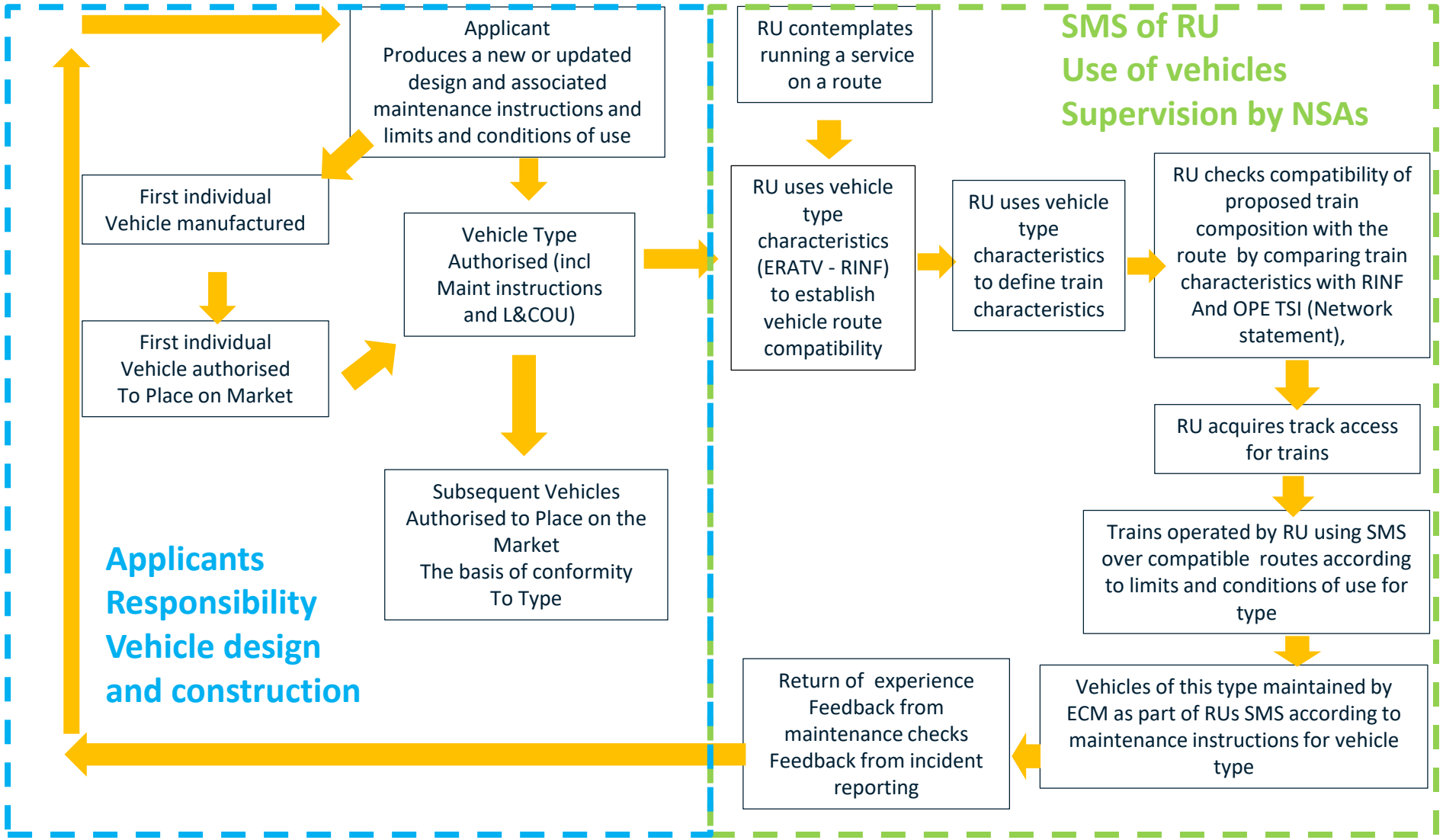
Only under two cases:

- Rules change (TSIs and/or NTRs) – Renewed authorisation required
- Subsequent discovery that the essential requirements were not met at authorisation (defective design or manufacture) – Amendment – Suspension or Revocation of authorisation

Not to be used in case of failure to meet the essential requirements due to actions or inactions of RUs or ECMs in the operation of their SMS (e.g. poor maintenance)

Source: European Union Agency for Railways

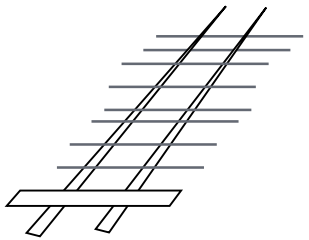
IMPLEMENT & IMPROVE



COMPATIBILITY OF TRAINS WITH ROUTES

ERATV:
EU register of authorised type of vehicles

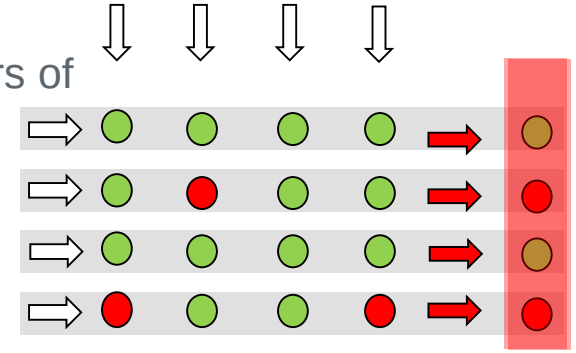
RINF:
Register of Infrastructure



Technical parameters of rolling stock

Technical parameters of

- route A
- route B
- route C
- route D



compatibility of **rolling stock** with **route**

Technical parameters of routes and rolling stock derive from various TSIs, e.g. TSI CCS, INF, RST, SRT, PRM, Noise - and also still from National Technical Rules

Chapter

Change Management: How to introduce innovation into the shared system

HOW STANDARD PARTS BECOME LAW

Interoperability Directive

Annex III: **Essential Requirements**

"1.1.4. The design of fixed installations and rolling stock and the choice of the materials used must be aimed at limiting the generation, propagation and effects of fire and smoke in the event of a fire."

TSIs specify requirements to **ensure the 4 objectives of the Directive**

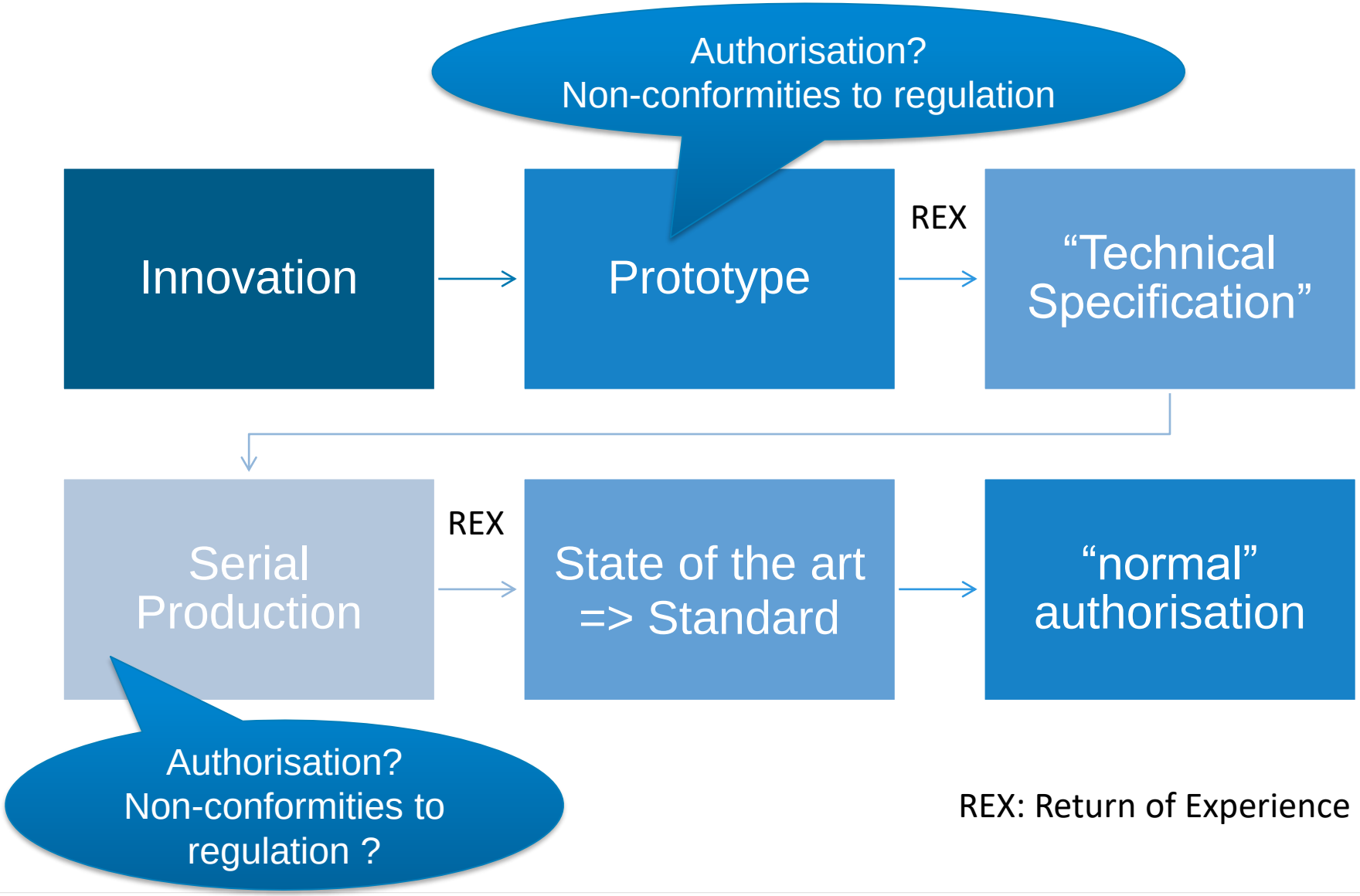
TSI LOCPAS, ch. 3.1: Elements of the rolling stock subsystem corresponding to the **essential requirements**

Ref. Point	Element of the rolling stock sub-system	Safety	Reliability-Availability	Health	Environmental protection	Technical compatibility
4.2.10.2	Fire safety – Measures to prevent fire	1.1.4		1.3.2	1.4.2	

Harmonised" EU standards specify **one way that the essential requirements may be met in accordance with the TSIs**

Index N°	Characteristics to be assessed	Point	Document N°	Mandatory points
58	Measures to prevent fire – material requirements	4.2.10.2.1	EN 45545-2:2013	relevant cl. [6]

AGILE V-CYCLE FOR EACH STAGE: FROM INNOVATION TO STANDARD PRODUCT



REX: Return of Experience

TECHNICAL REGULATION (TSI)

What should a TSI cover?

- TSIs must specify **The Optimal Level of Harmonisation**

- If a common specification is necessary for:
  - Network-Vehicle Compatibility
  - Market opening
  - Avoiding Member States creating their own rules for the essential requirements

Then it should be within a TSI

BUT only if a railway specific specification is necessary

RESEARCH & INNOVATION, STANDARDS, REGULATION

Research & Innovation (S2R +EC (MOVE+RI))

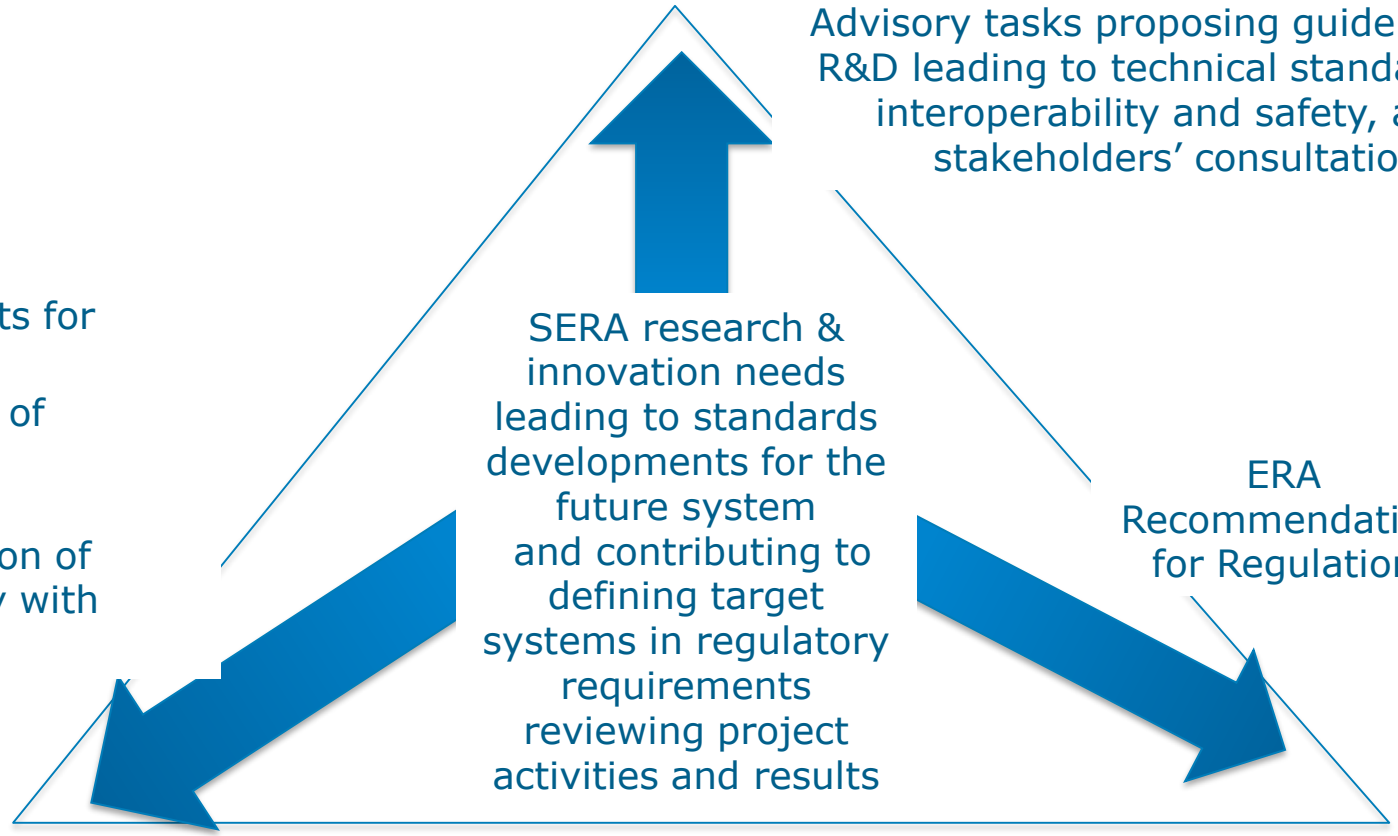
Advisory tasks proposing guidelines for R&D leading to technical standards for interoperability and safety, after stakeholders' consultation

ERA Requests for standards

- To be part of regulation
- To confer presumption of conformity with regulation

SERA research & innovation needs leading to standards developments for the future system and contributing to defining target systems in regulatory requirements reviewing project activities and results

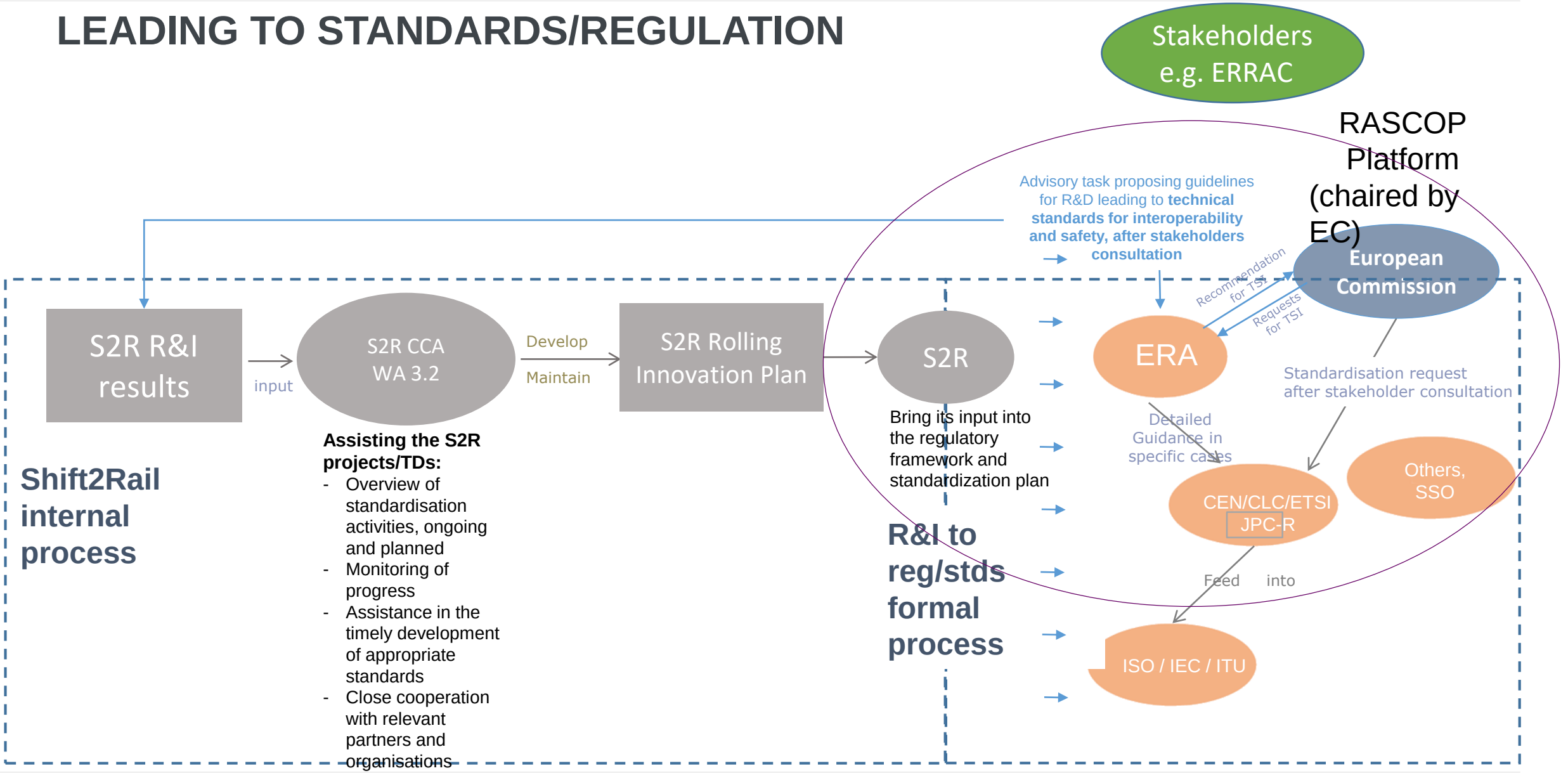
ERA Recommendation for Regulation



Standards (CEN/CENELEC/ETSI and others)

Technical Regulation (EC)
Technical Specifications for Interoperability
ERA Technical document
Common Safety Methods
Implementing Acts and others

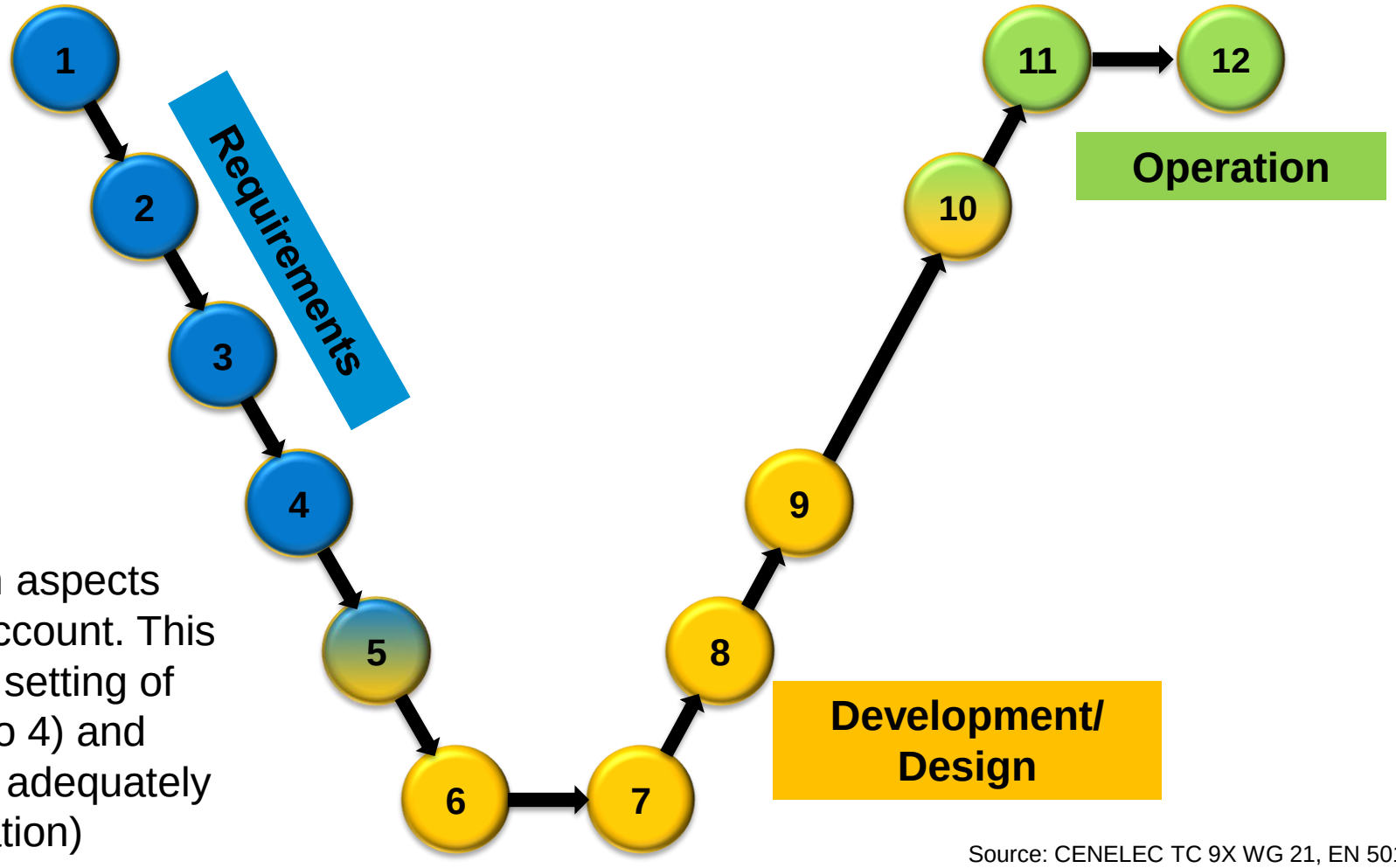
S2R R&I RESULTS AND PROCESS LEADING TO STANDARDS/REGULATION



Chapter

Design and production of vehicles, network projects, subsystems and components

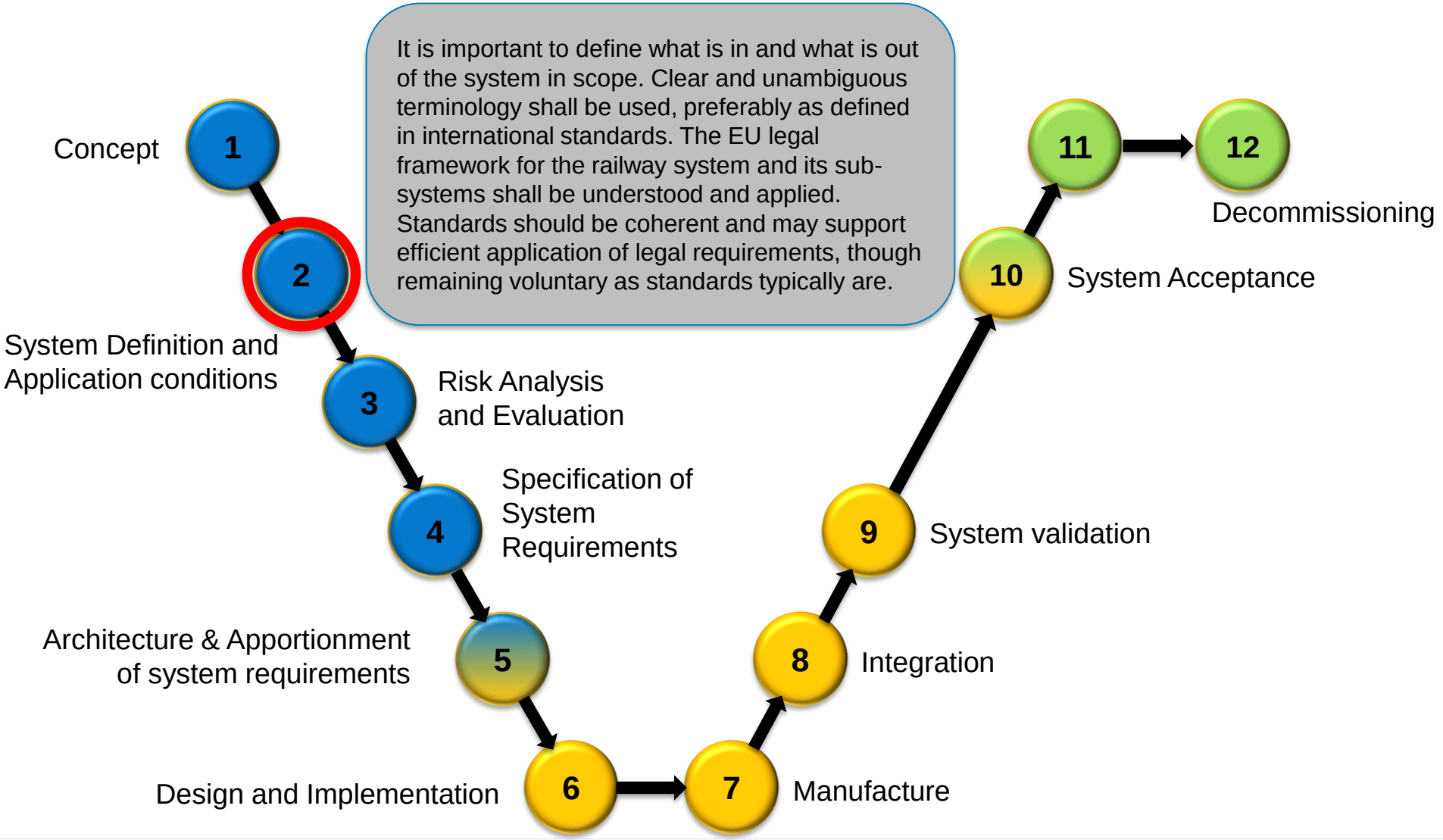
LIFE-CYCLE OF A TECHNICAL PRODUCT



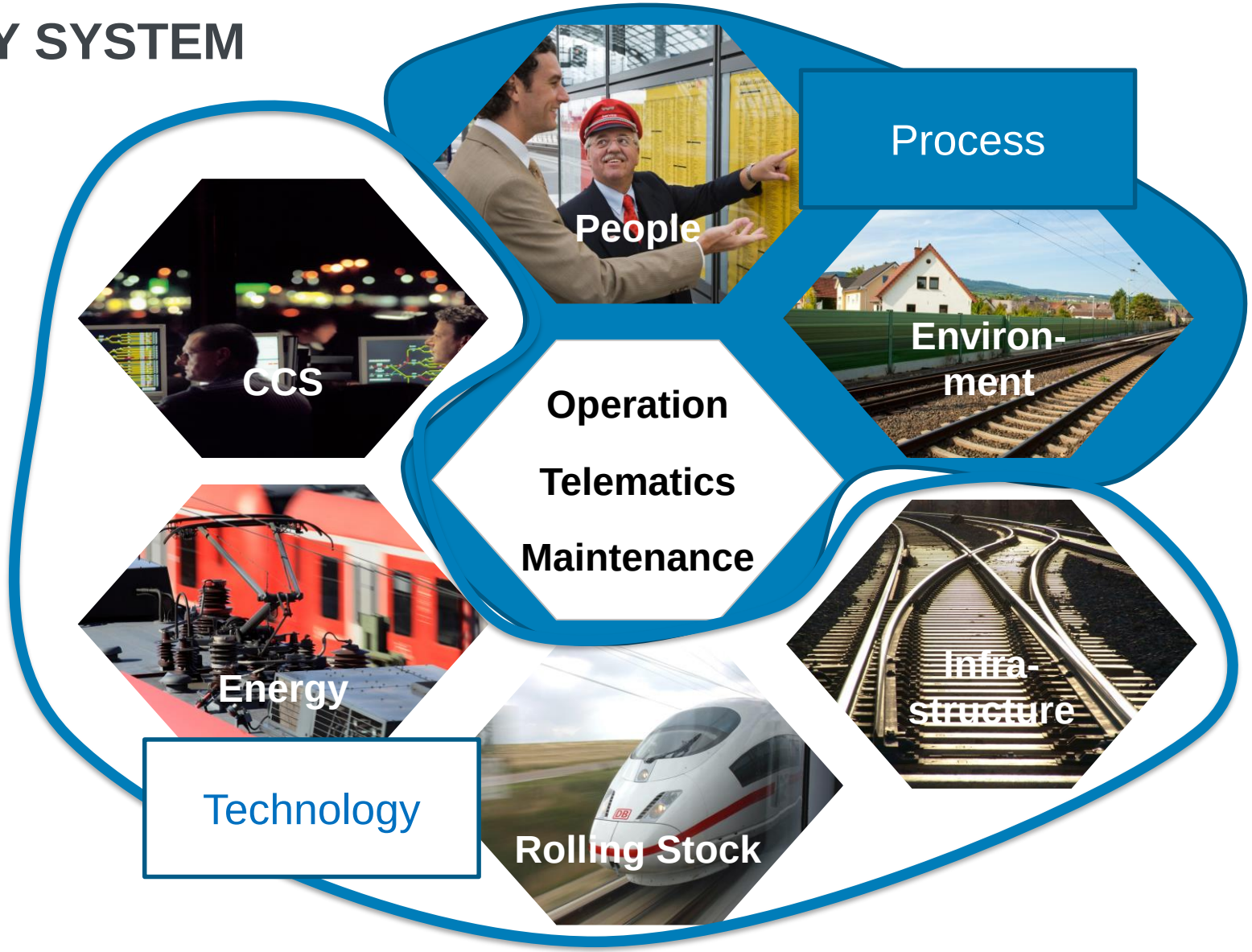
Also operational/human aspects need to be taken into account. This will highly influence the setting of requirements (steps 1 to 4) and should be checked and adequately tested in step 8 (integration)

Source: CENELEC TC 9X WG 21, EN 50126: 2017

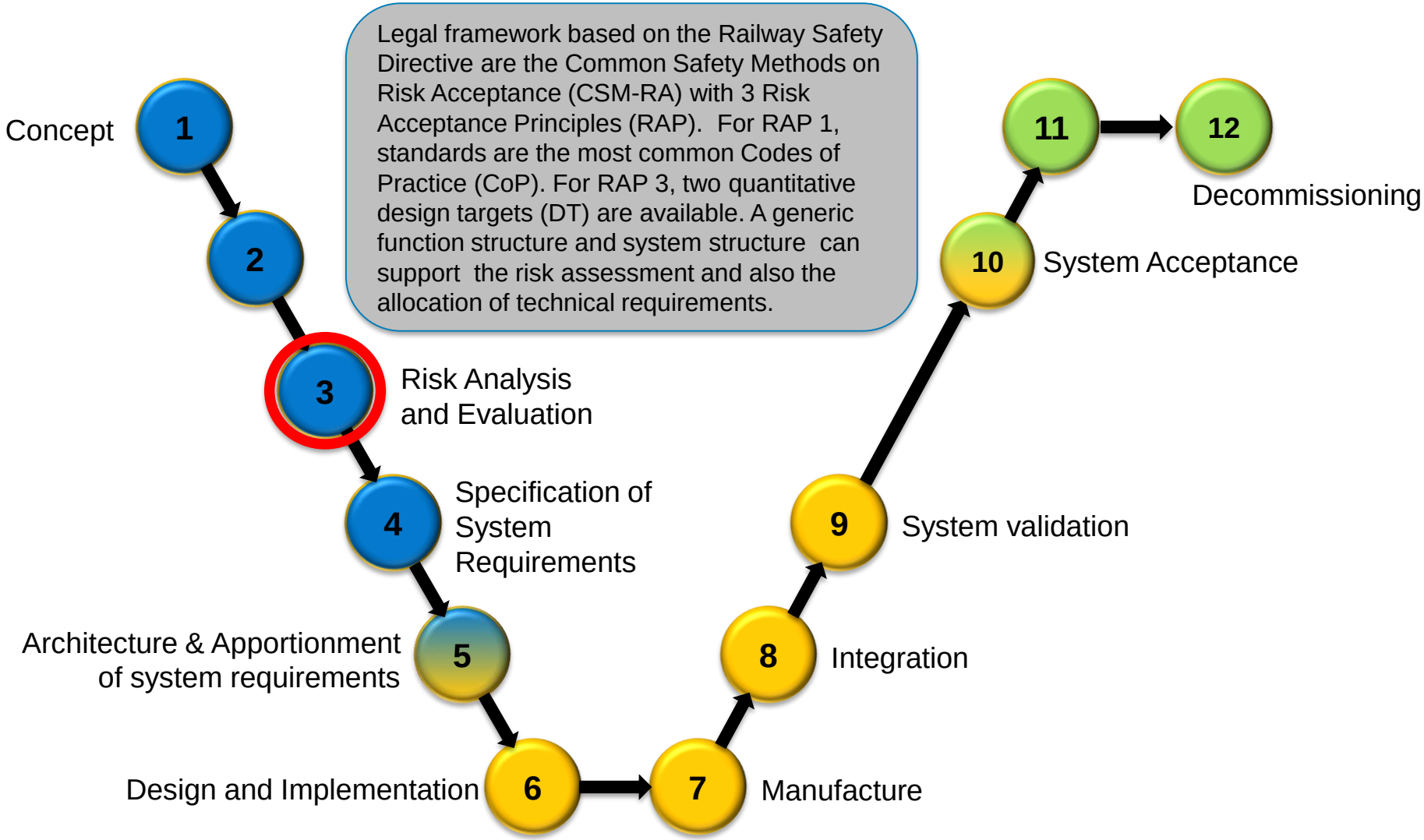
LIFE-CYCLE OF A TECHNICAL PRODUCT



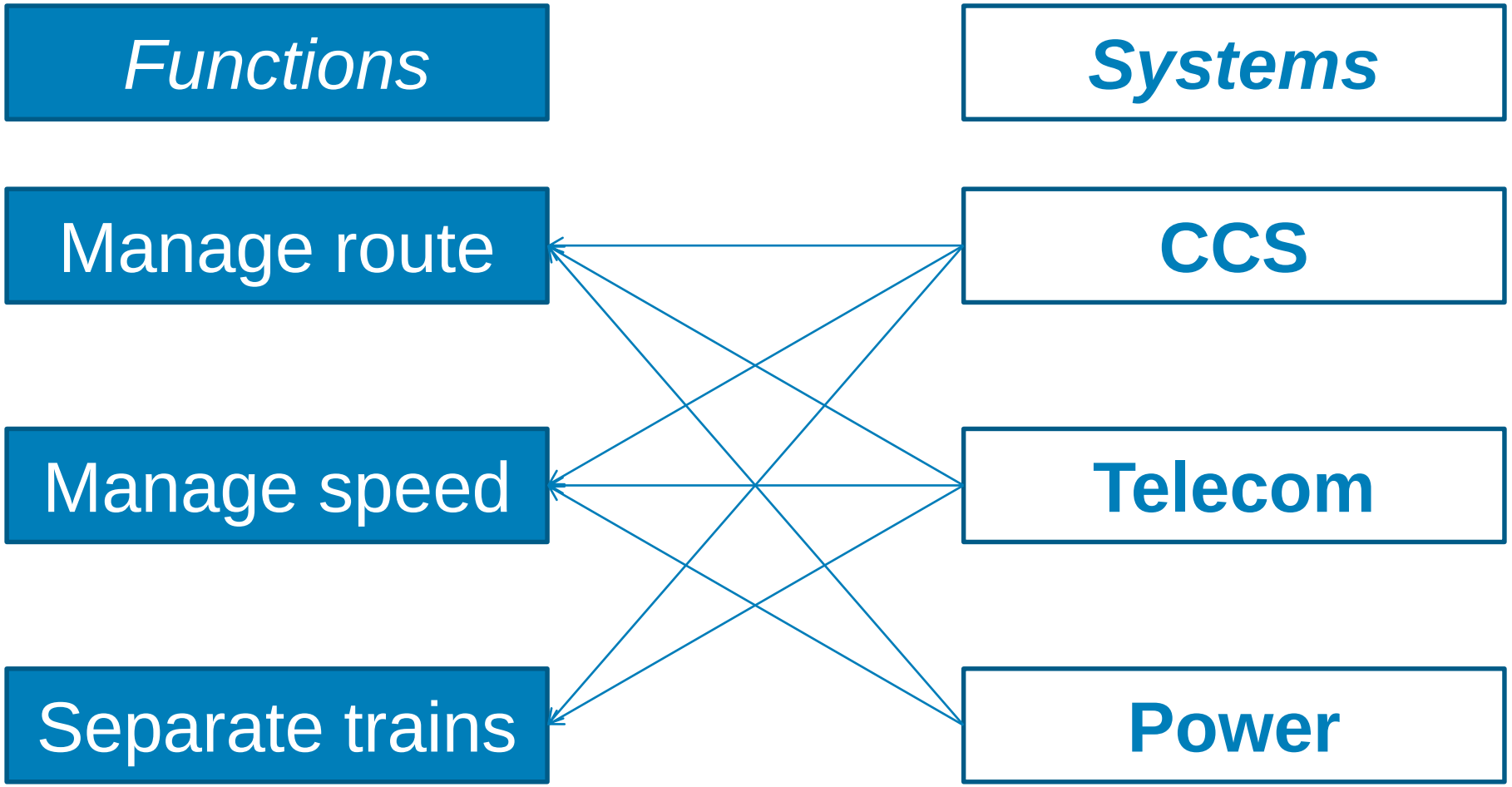
THE RAILWAY SYSTEM



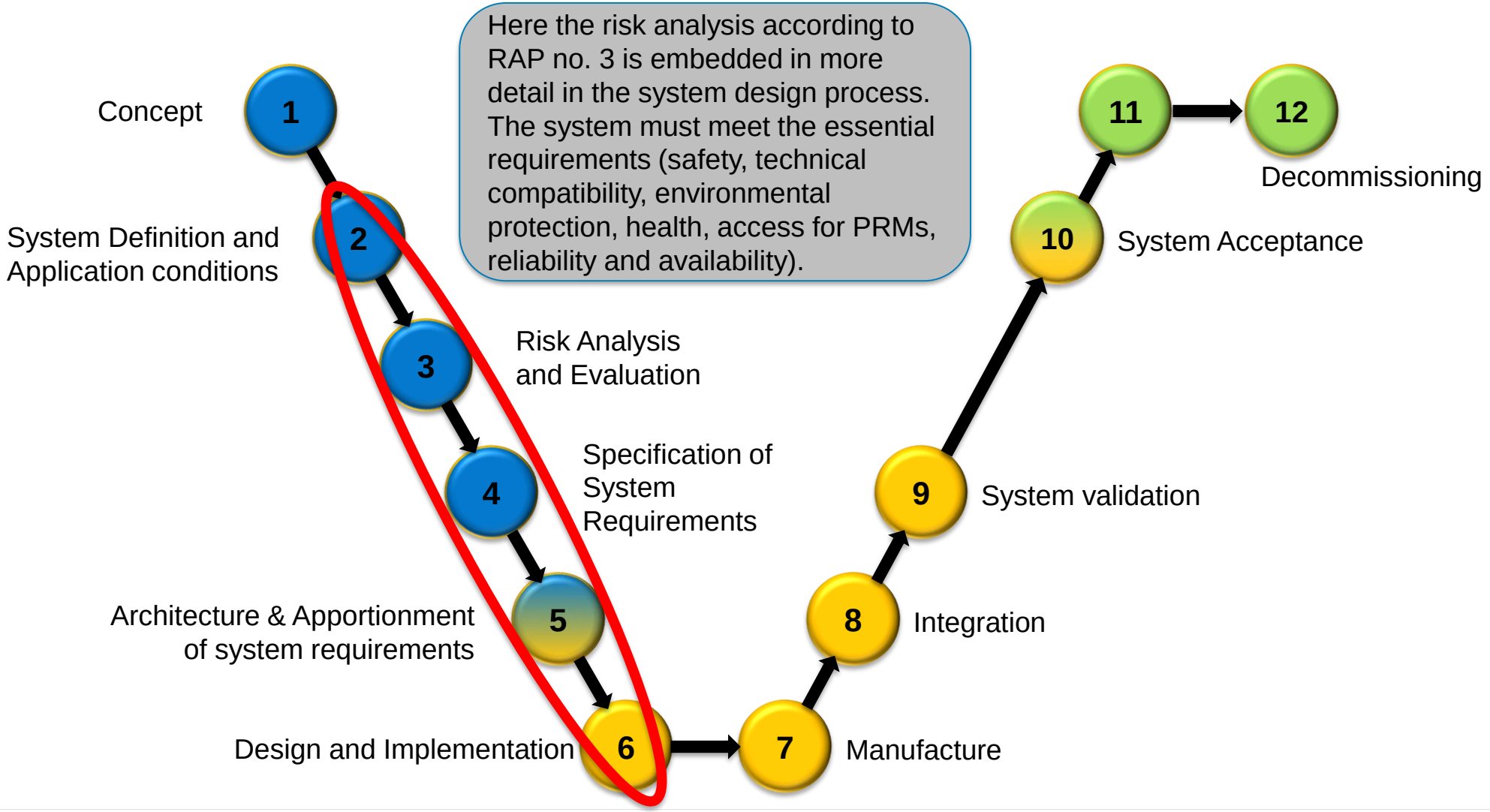
LIFE-CYCLE OF A TECHNICAL PRODUCT



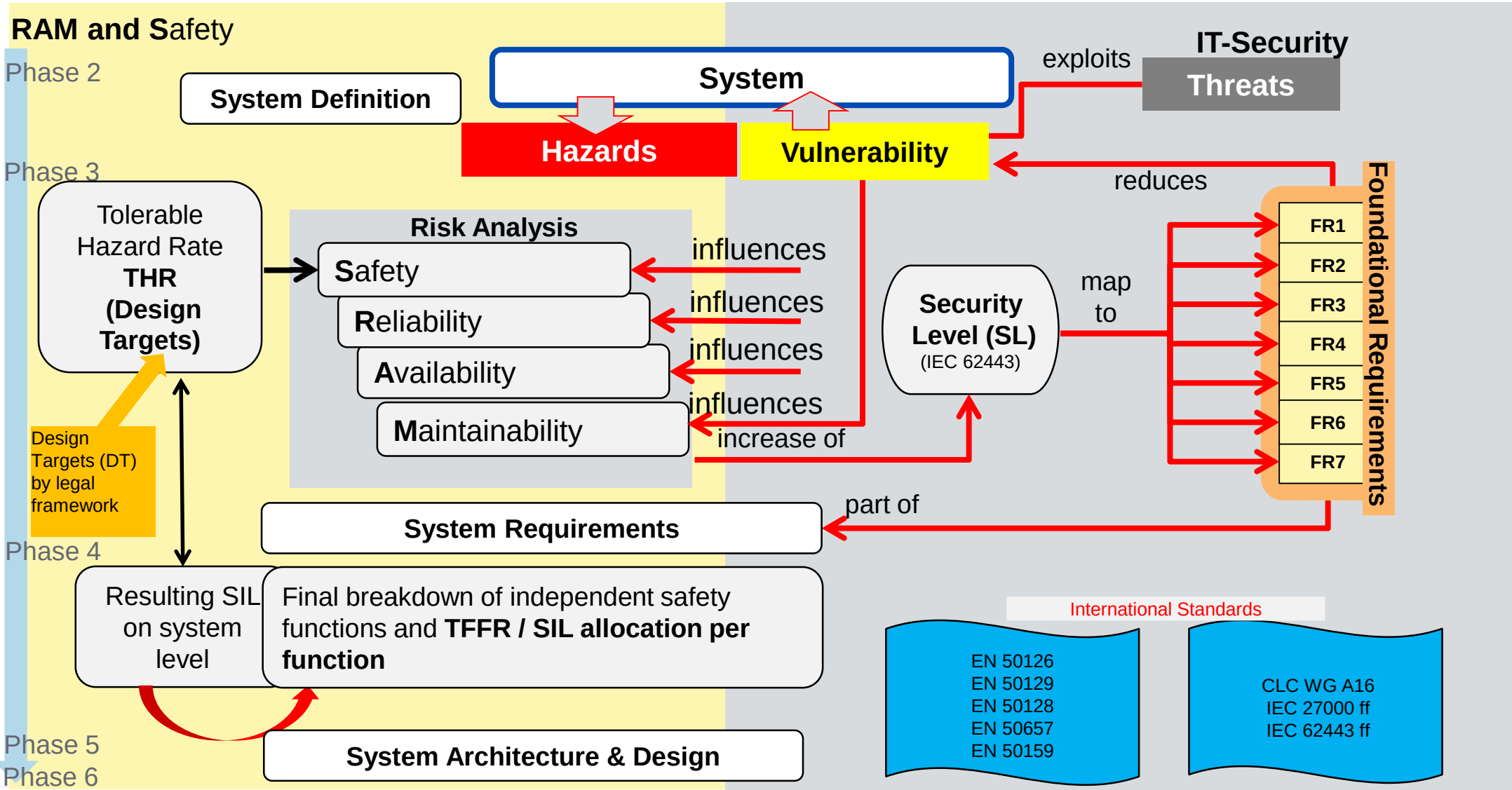
RISK ASSESSMENT: FUNCTION OR SYSTEM



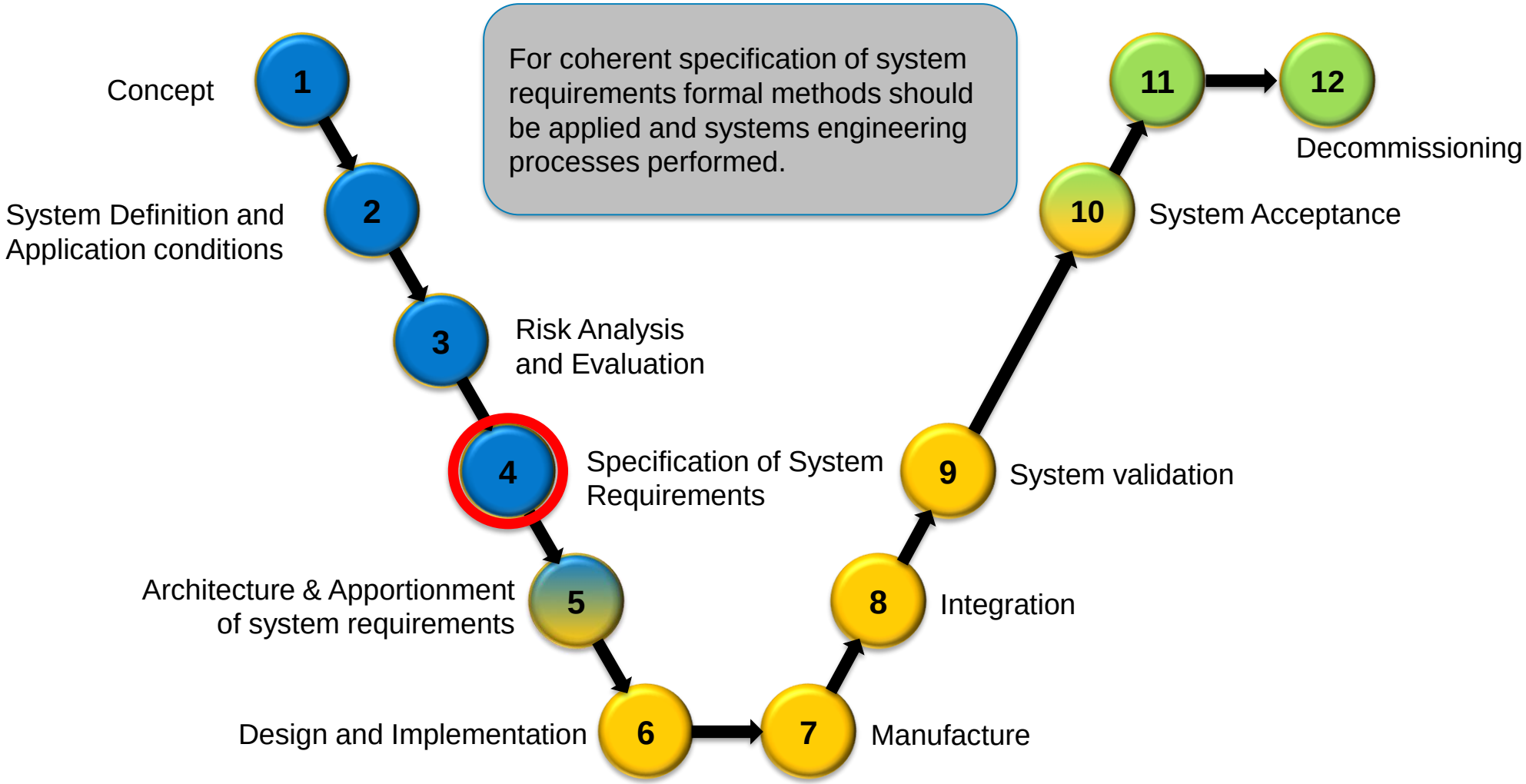
LIFE-CYCLE OF A TECHNICAL PRODUCT



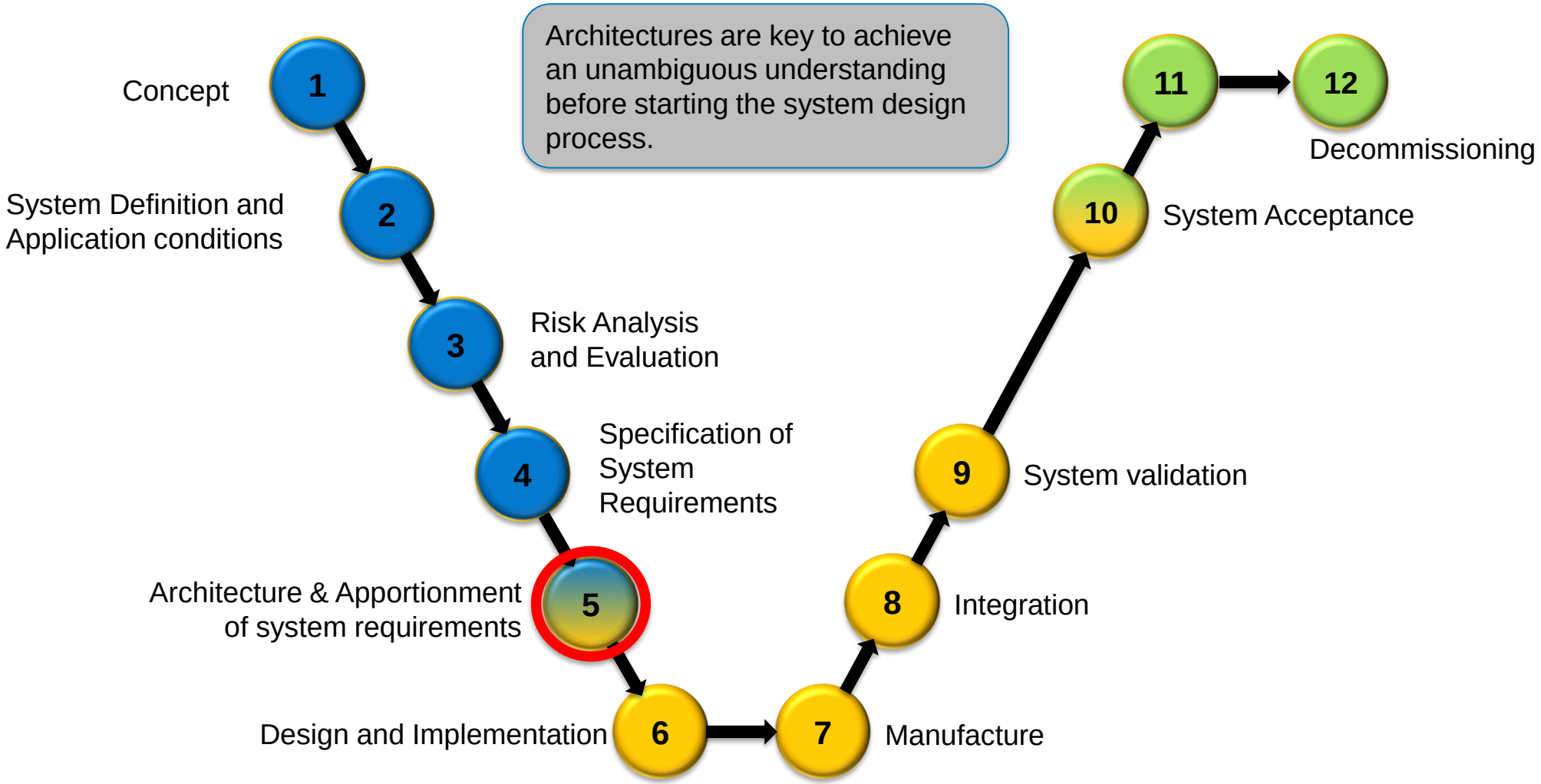
SAFETY AND IT-SECURITY



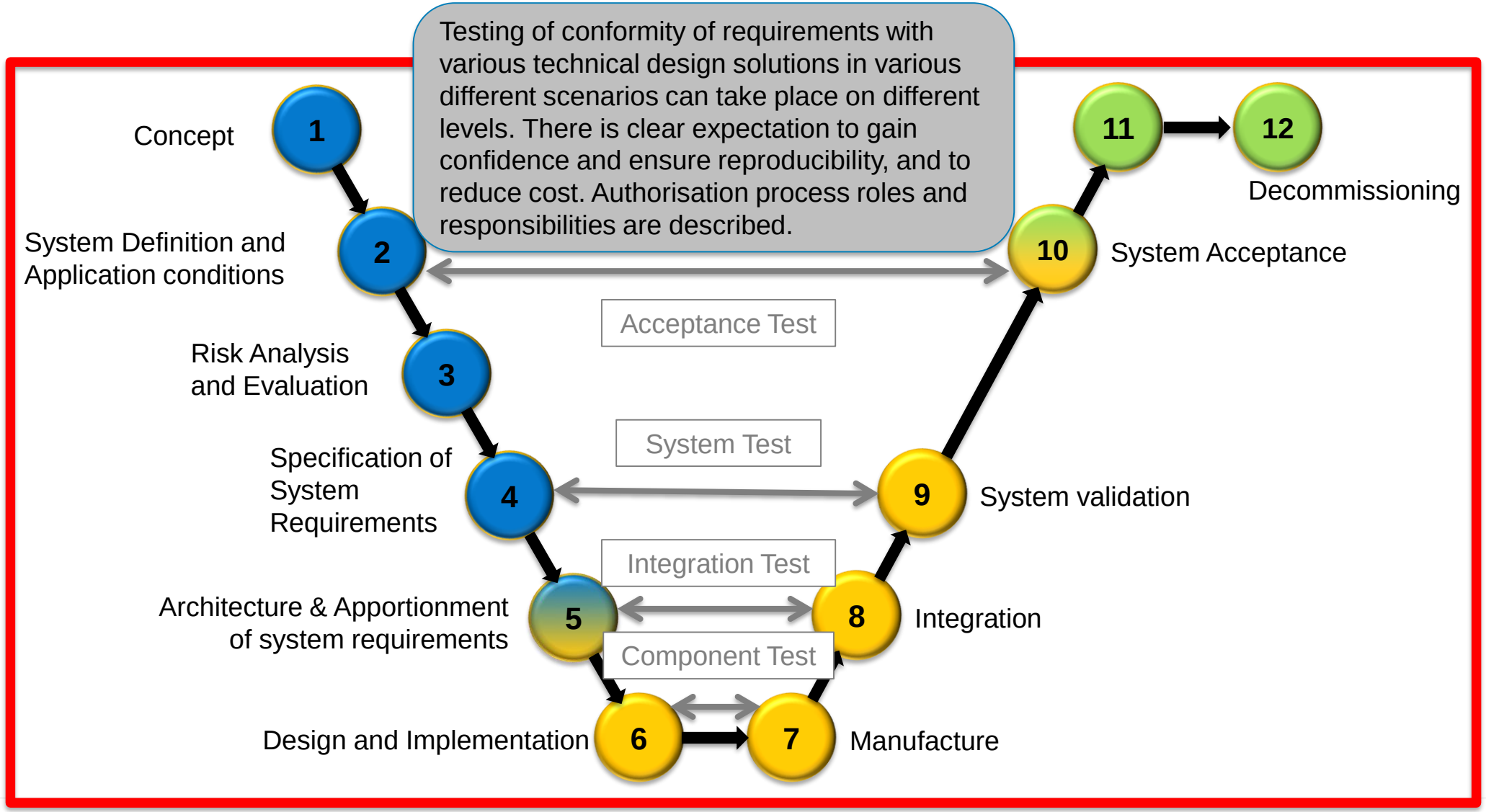
LIFE-CYCLE OF A TECHNICAL PRODUCT



LIFE-CYCLE OF A TECHNICAL PRODUCT

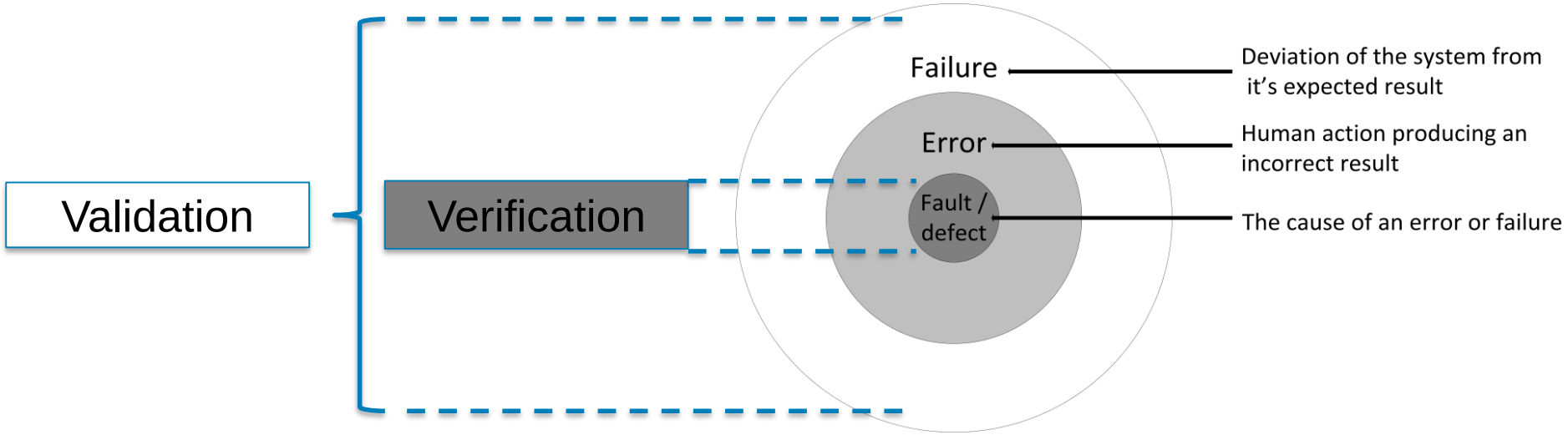


LIFE-CYCLE OF A TECHNICAL PRODUCT



TESTING – WHY AND WHERE

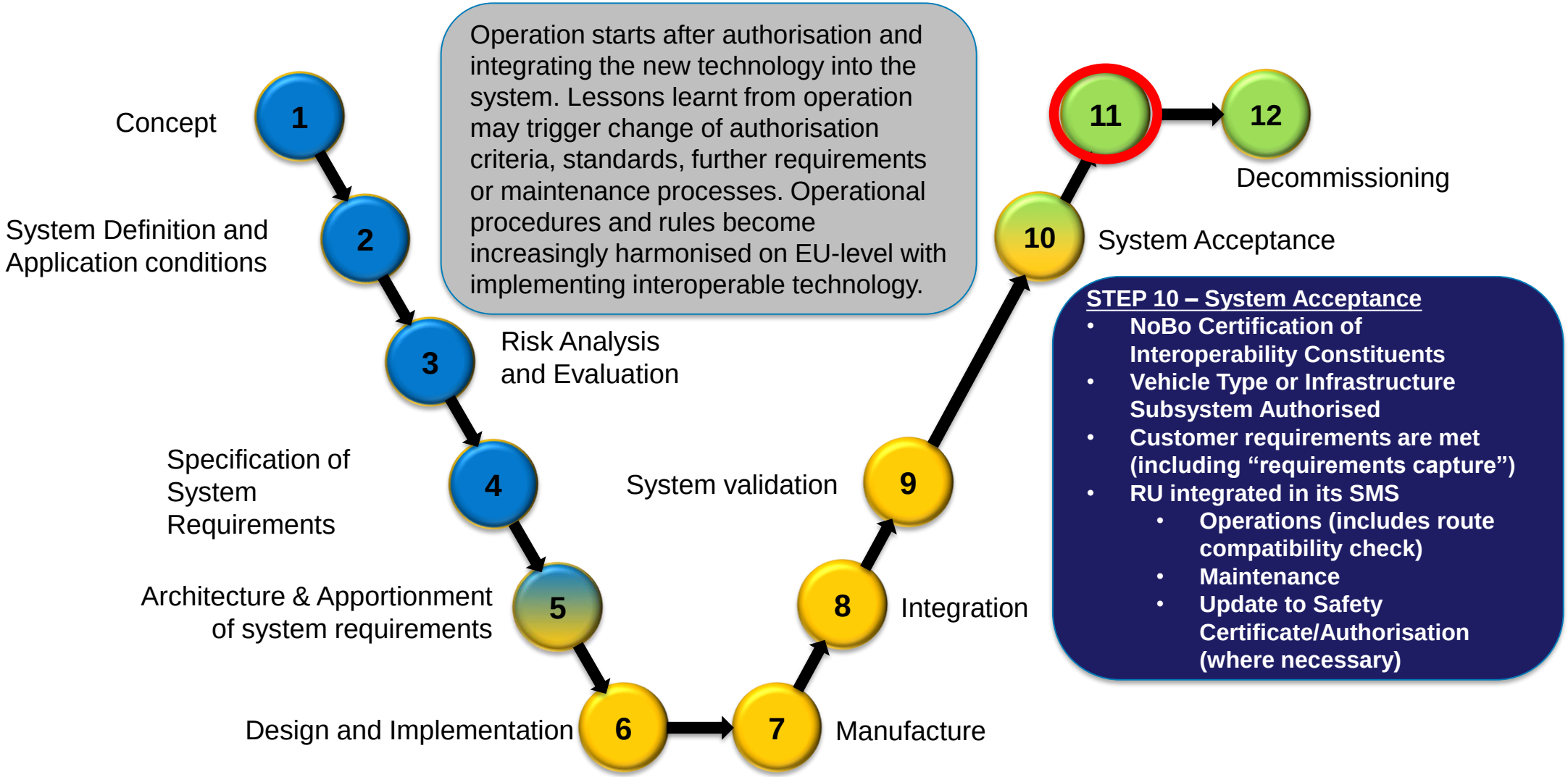
Aim: Failure detection and error reduction to enable a safe and reliable system (the railway system as a whole)



Lab or on-site tests?

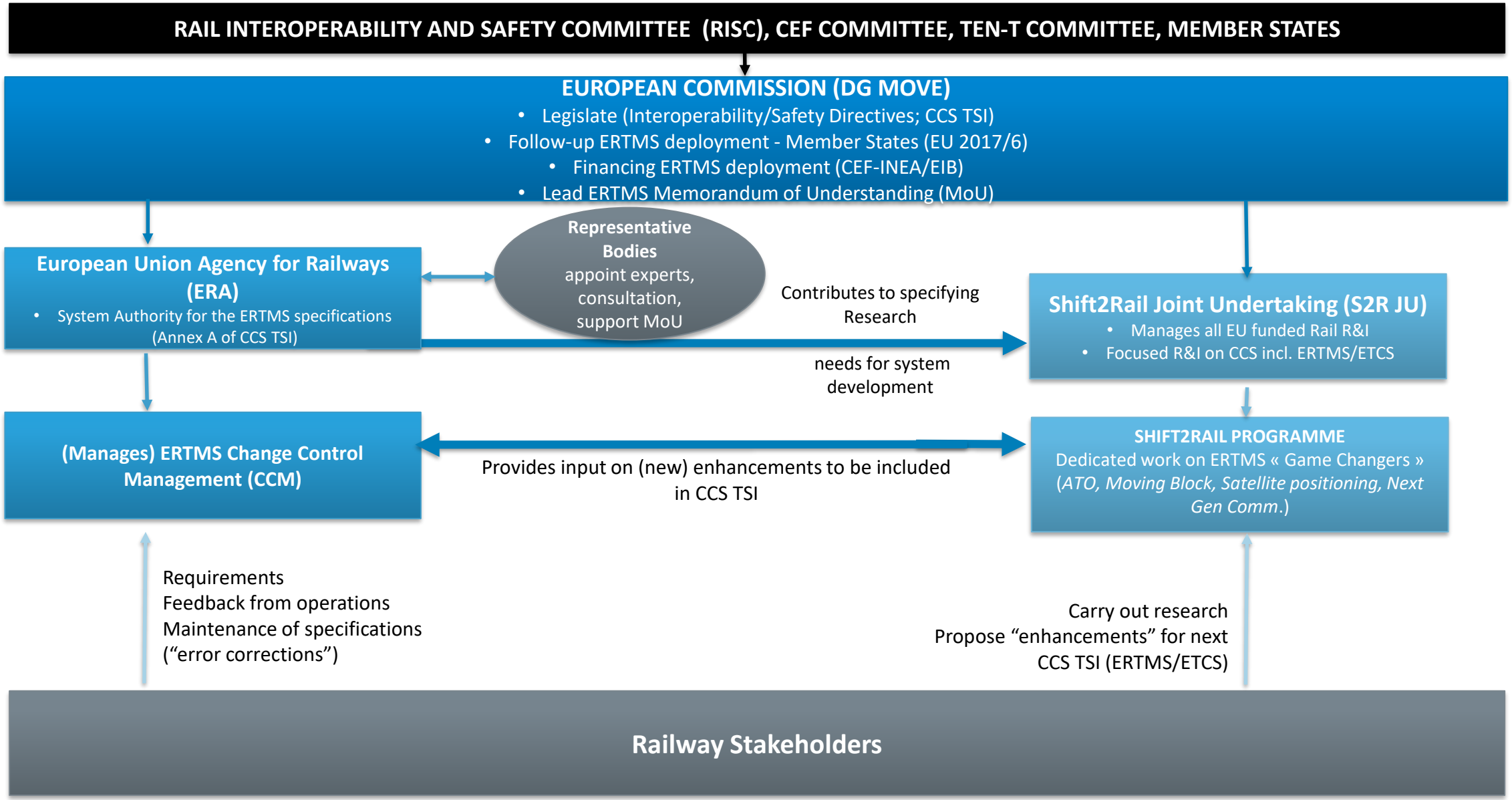
- Time and effort
- Reproducibility
- Worst-case scenarios
- number of units
- environmental conditions
- Individual system boundaries
- pass/fail criteria

LIFE-CYCLE OF A TECHNICAL PRODUCT

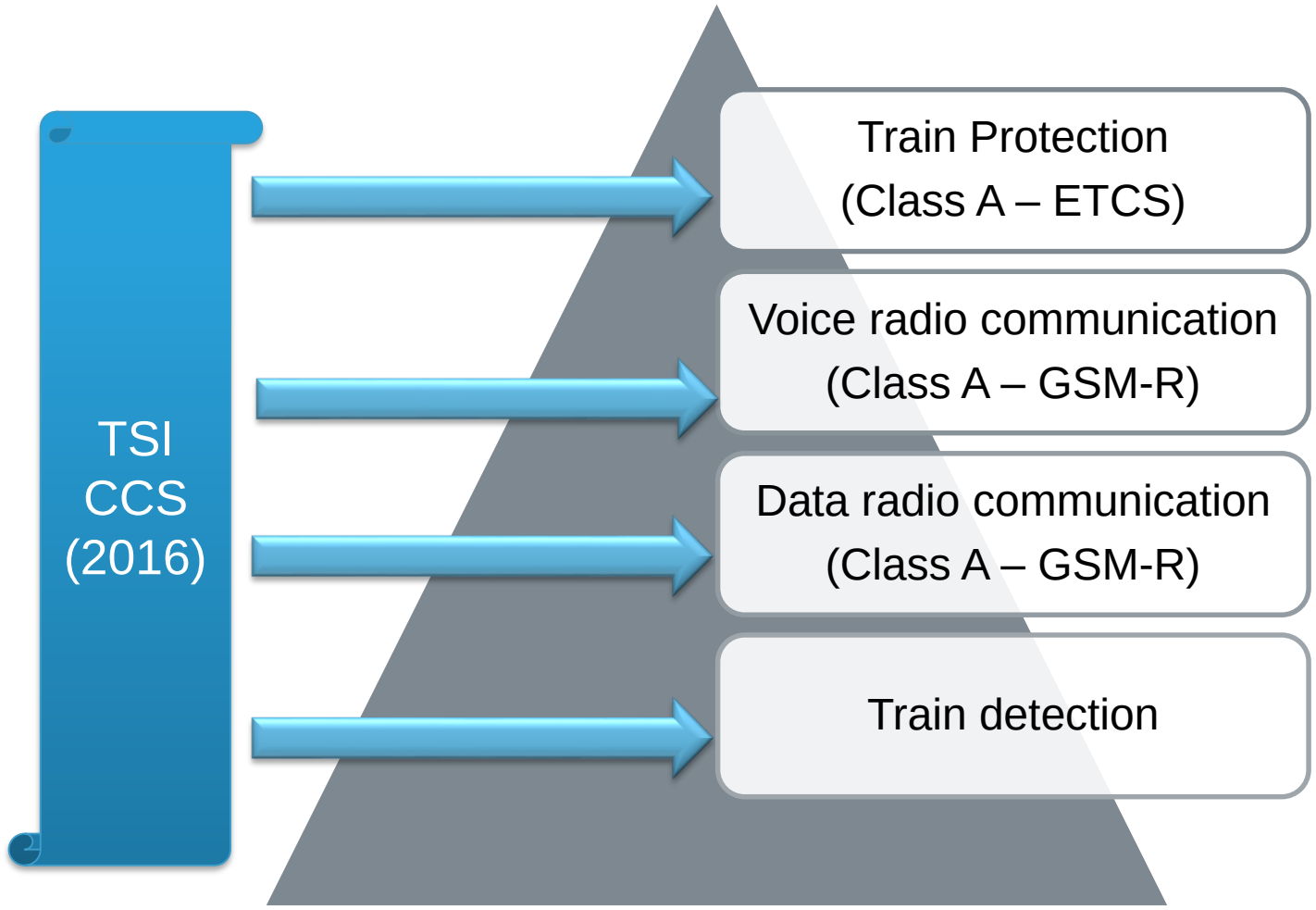


Chapter

CCS specificities

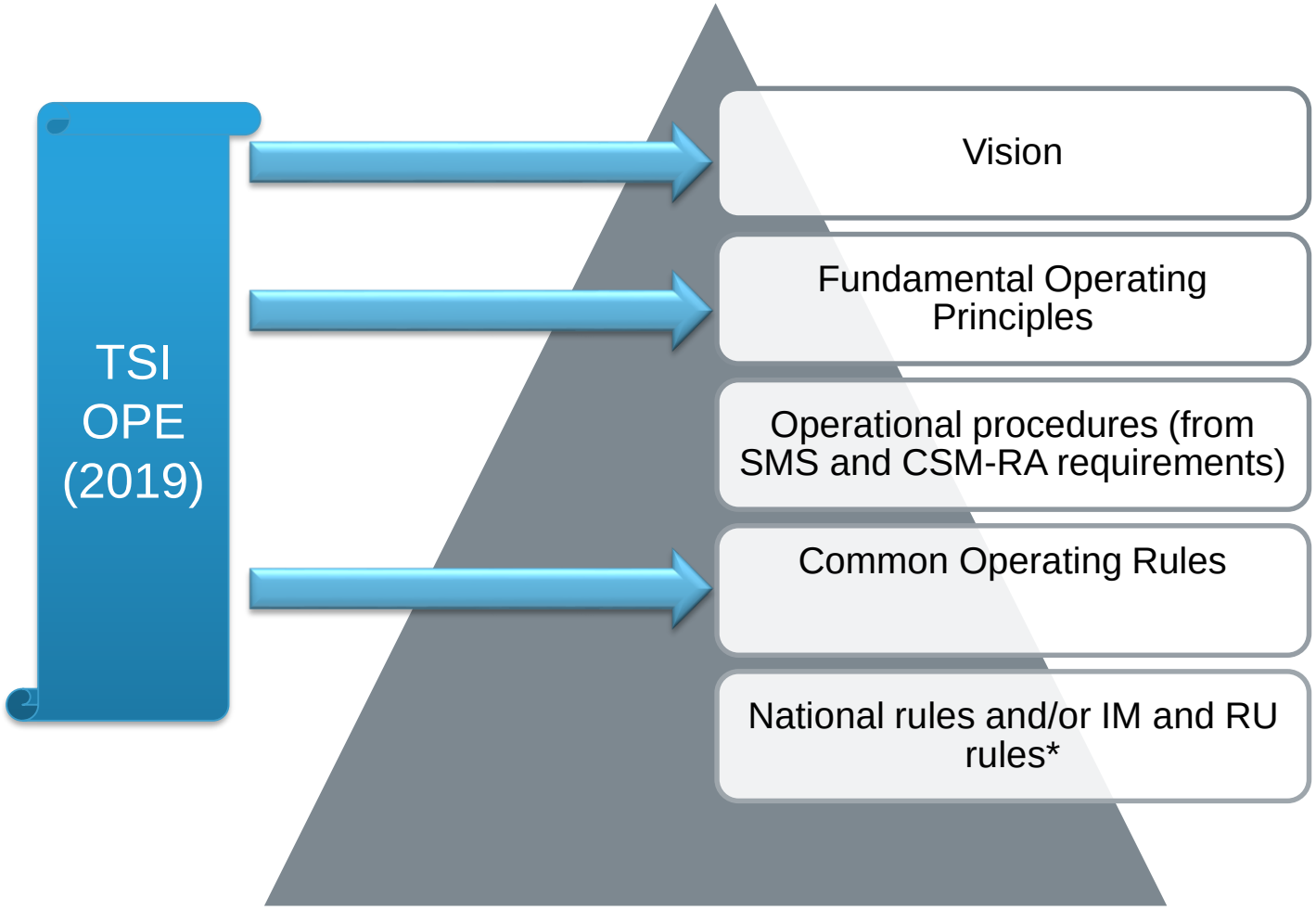

RAIL INTEROPERABILITY AND SAFETY COMMITTEE (RISC), CEF COMMITTEE, TEN-T COMMITTEE, MEMBER STATES
EUROPEAN COMMISSION (DG MOVE)
• Legislate (Interoperability/Safety Directives; CCS TSI)
• Follow-up ERTMS deployment - Member States (EU 2017/6)
• Financing ERTMS deployment (CEF-INEA/EIB)
• Lead ERTMS Memorandum of Understanding (MoU)
European Union Agency for Railways (ERA)
• System Authority for the ERTMS specifications (Annex A of CCS TSI)
Representative Bodies
appoint experts, consultation, support MoU
Contributes to specifying Research needs for system development
Shift2Rail Joint Undertaking (S2R JU)
• Manages all EU funded Rail R&I
• Focused R&I on CCS incl. ERTMS/ETCS
(Manages) ERTMS Change Control Management (CCM)
Provides input on (new) enhancements to be included in CCS TSI
SHIFT2RAIL PROGRAMME
Dedicated work on ERTMS « Game Changers » (ATO, Moving Block, Satellite positioning, Next Gen Comm.)
Requirements
Feedback from operations
Maintenance of specifications
("error corrections")
Carry out research
Propose "enhancements" for next CCS TSI (ERTMS/ETCS)
Railway Stakeholders

SCOPE OF TSI CCS*



* CCS on board/trackside subsystems = "*All the on-board/trackside equipment required to ensure safety and to command and control movements of trains authorised to travel on the network*"

SCOPE OF TSI OPE



*will be derived from operational procedures and individual requirements for RU/IM safe operation

ABBREVIATIONS

ATO: Automatic Train Operation
CEF: Connecting Europe Facility
CEN: European Committee for Standardization
CENELEC: European Committee for Electrotechnical Standardization
CER: Community of European Railway
CCS: Control Command and Signalling
CSM: Common Safety Method
DeBo: Designated Body
EC: European Commission
ECM: Entity in Charge of Maintenance
EIM: European Rail Infrastructure Managers
EN: European Norm
ERA: European Union Agency for Railways
ERATV: European Register of Authorised Types of Vehicles
ERTMS: European Rail Traffic Management Systems
ETCS: European Train Control System
ETSI: European Telecommunications Standards Institute
EUG: ERTMS Users Group
IM: Infrastructure Manager
INEA: Innovation and Network Executive Agency
ISO: International standard organisation
IP2: (Shift2Rail) Innovation Programme 2
LOC&PAS (TSI): Locomotive and Passenger
MAAP: Shift2Rail Multi Annual Action Plan
MoU: Memorandum of Understanding
NSA: National Safety Authority
NTR: National Technical Rules
NRV: National Reference Values
NoBo: Notified Body
RAC: Risk Acceptance Criteria
RAM: Reliability, Availability, Maintainability
RINF: Register of Infrastructure
RU: Railway Undertaking
S2R JU: Shift2Rail Joint Undertaking
SMS: Safety Management System
TR: Technical Report
TSI: Technical Specifications for Interoperability
TS: Technical Specification
UIC: Union Internationale des Chemins de Fer
UNIFE: Union des Industries Ferroviaires Européennes