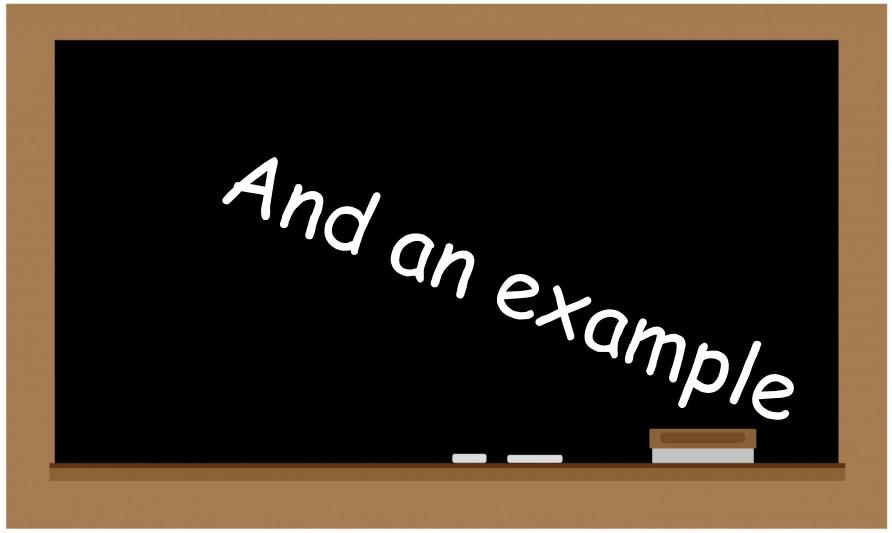
NEW CENELEC STANDARDS & CSM-RA

RAMBØLL

AGENDA

- New EN 501xx Standards
- What is new/changed/improved
- The use of CENELEC in CSM-RA process



CENELEC & CSM-RA TIMELINE

EN61508 (2000)

EN61508 (2010)

ENV50126 (1995)

EN50126 (1999)

EN50128 (2001)

EN50129 (2003)

EN50128 (2011)

EN50126 (2017)

EN50129 (2018)

TR50126-3 (2006)

TR50126-2 (2007)

TSI: 2010, 2012, 2015

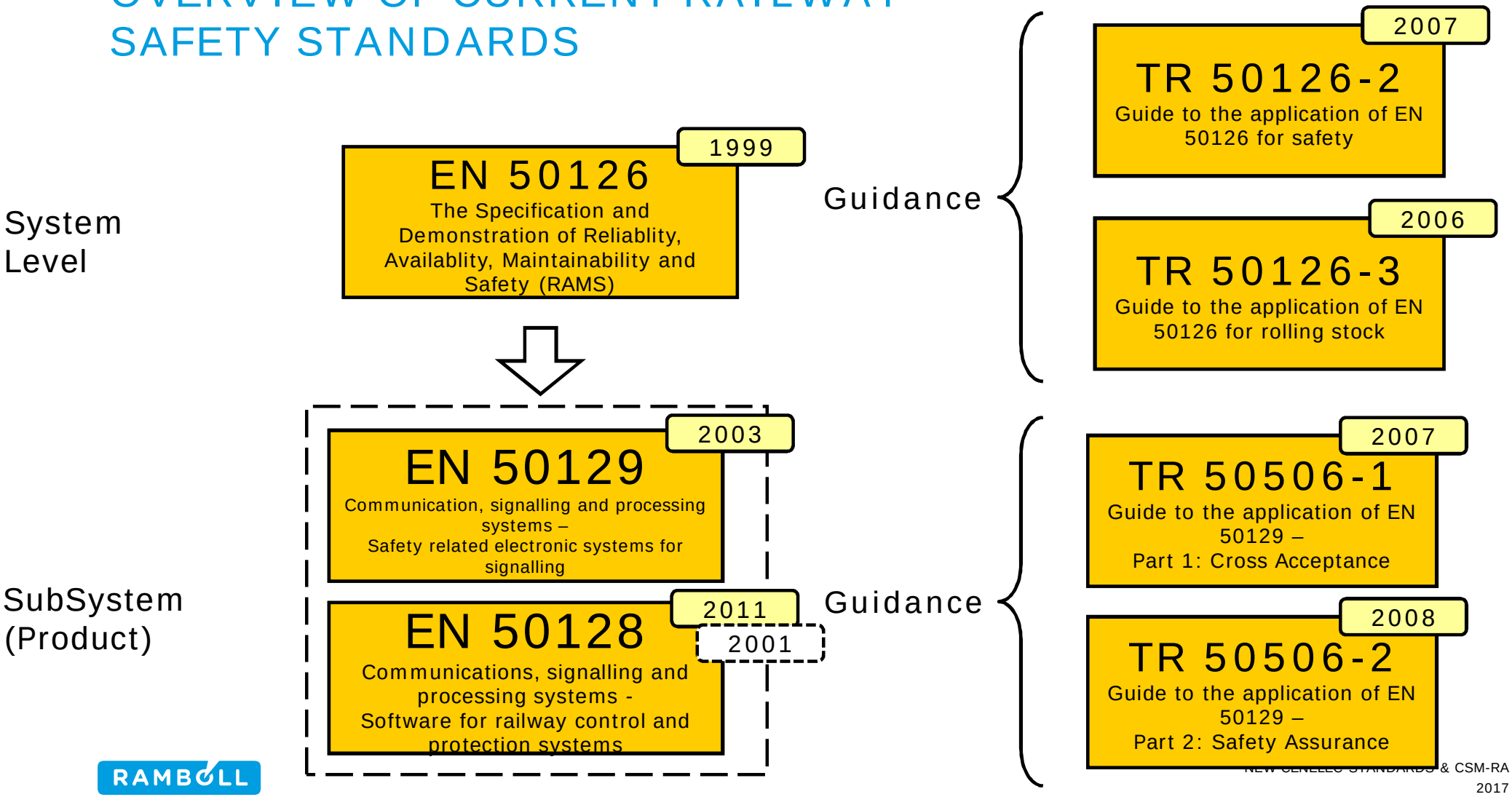
CSM-RA 352/2009 (2010)

CSM-RA 402/2013 (2015)

CSM-RA 1136/2015

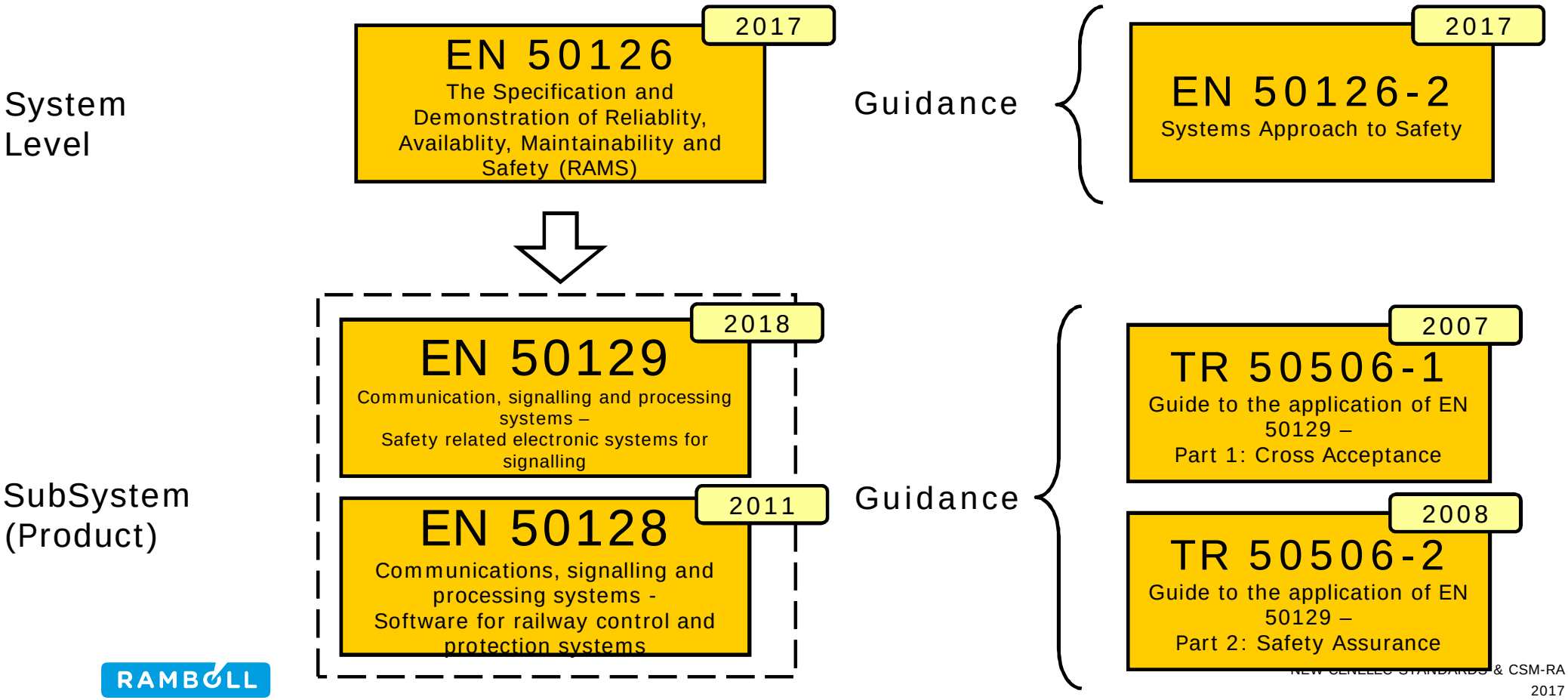
RAMBØLL

OVERVIEW OF CURRENT RAILWAY SAFETY STANDARDS



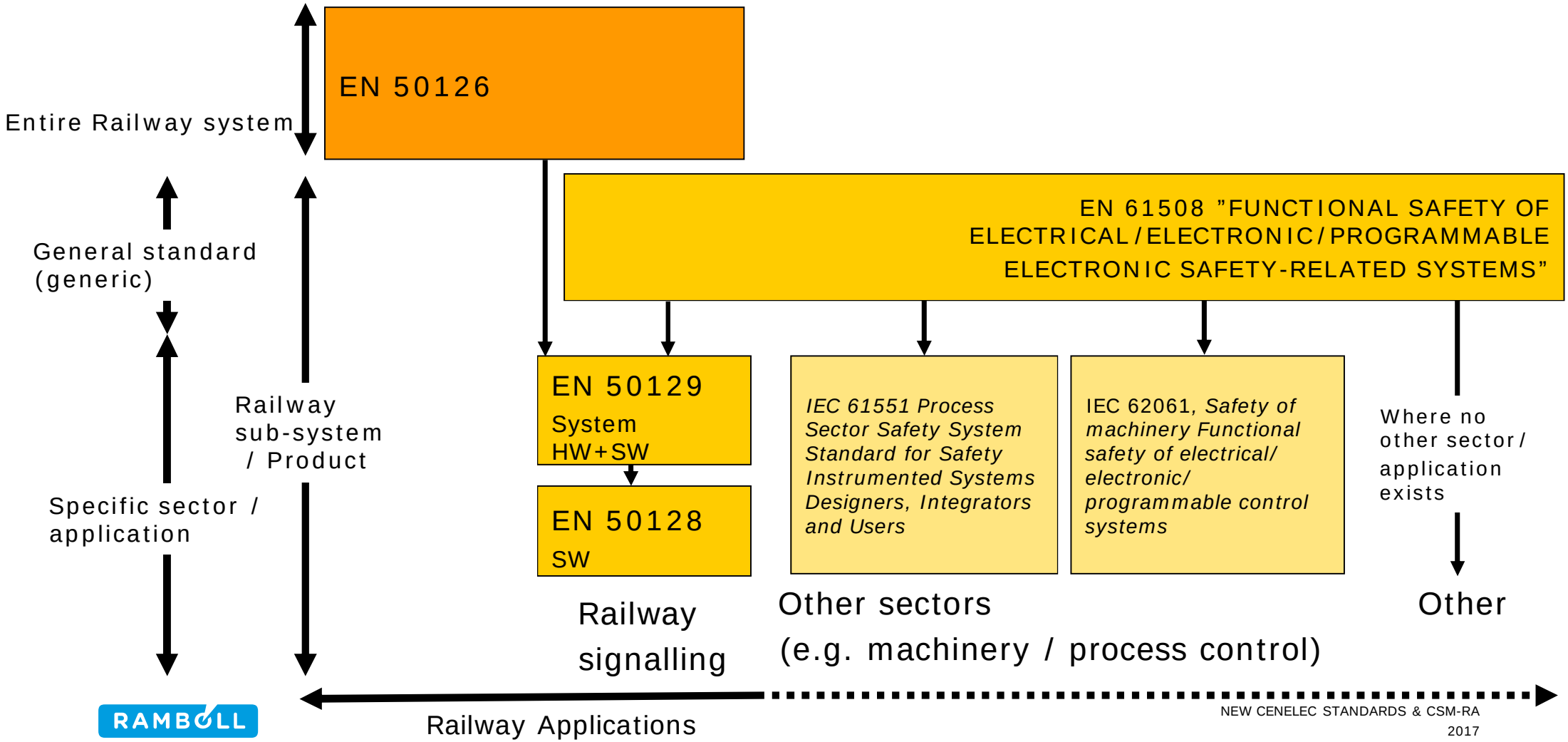
RAMBØLL

OVERVIEW OF NEW RAILWAY SAFETY STANDARDS



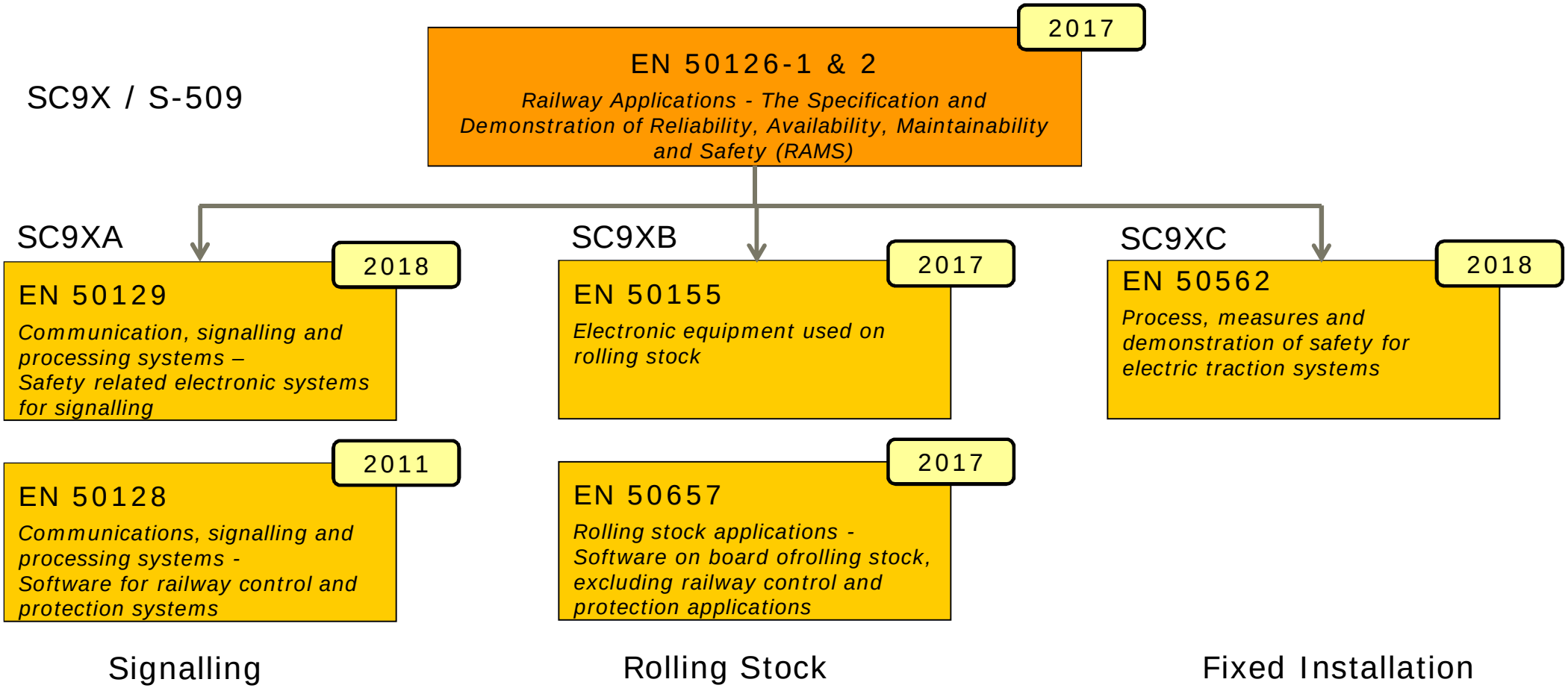
RAMBØLL

SAFETY STANDARDS RELATIONSHIPS



Adapted after EN 50129 / IEC WG group

RAILWAY SAFETY STANDARDS - SUBSYSTEM



RAMBØLL

EN 50126 OLD & NEW IN COMPARISON

Similarities

- System approach for RAMS
- Risk based approach
- RAMS lifecycle
- Safety demonstration principles

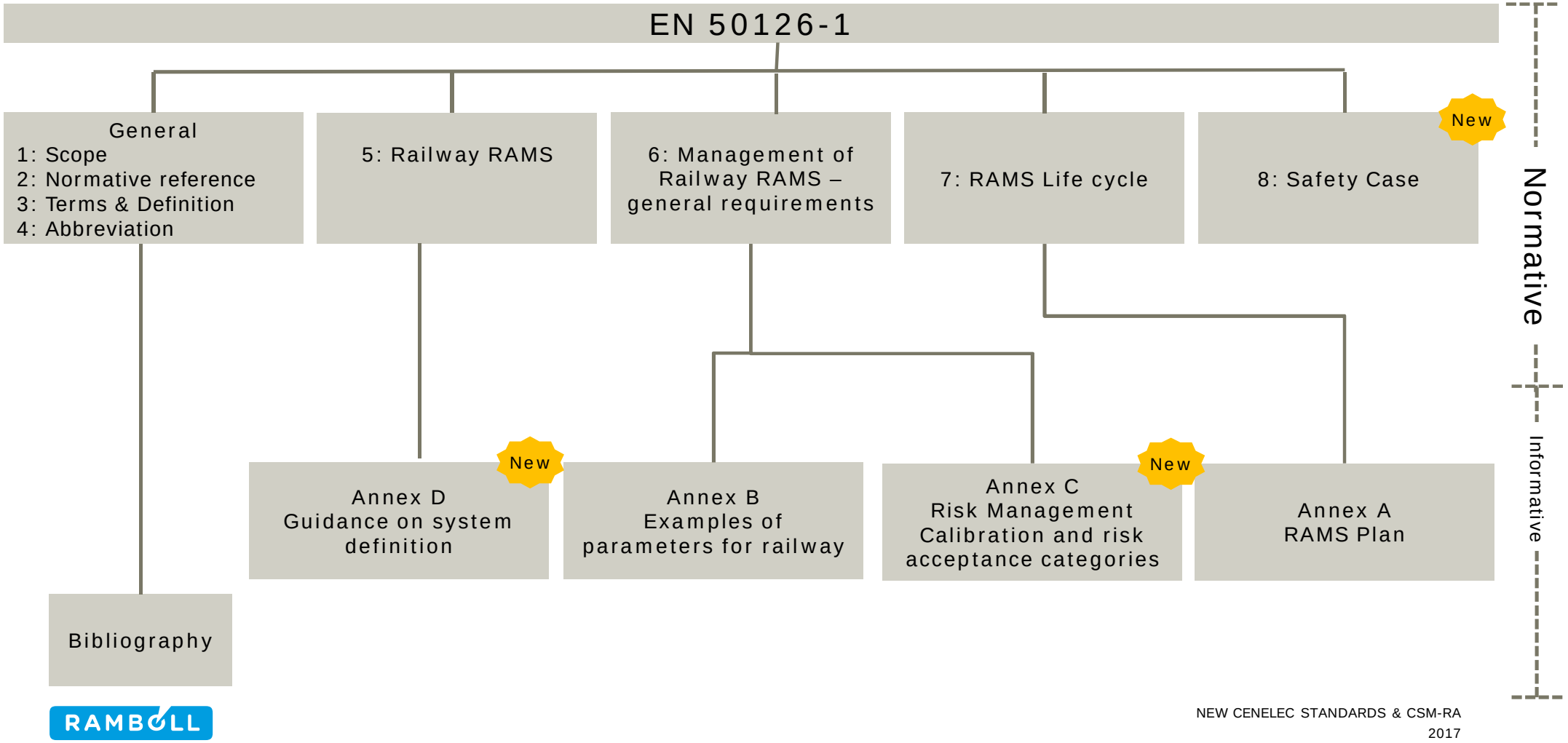
New/changed

- More mature and consistent
- CSM-RA approach
  - Multilevel system approach (hierarchies)
  - Aligned risk evaluation
- Safety demonstration
- Safety requirements Spec.
- Guidance integrated part
- Clear linkage to TSI

Improved/detailed

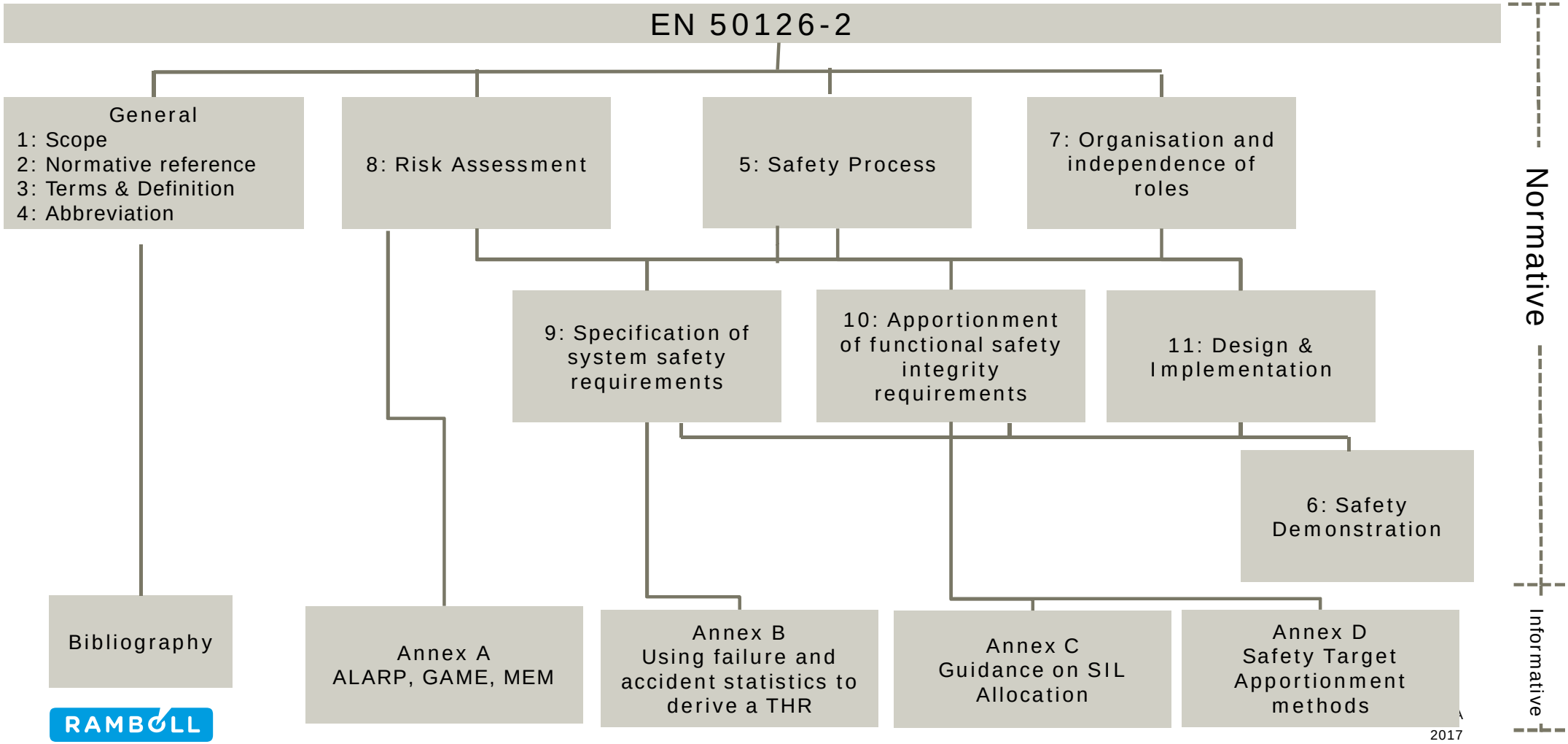
- Clear hazard identification and classification
- Classification of safety requirements
- Method to derive THR from statistics
- Safety Case structure
  - Modularity
  - Handling of product/Generic / specific Application
- Safety Apportionment methods
- Key system safety roles & responsibilities

RAMBØLL



RAMBØLL

NEW CENELEC STANDARDS & CSM-RA
2017


EN 50126-2
General
1: Scope
2: Normative reference
3: Terms & Definition
4: Abbreviation
8: Risk Assessment
5: Safety Process
7: Organisation and independence of roles
9: Specification of system safety requirements
10: Apportionment of functional safety integrity requirements
11: Design & Implementation
6: Safety Demonstration
Bibliography
Annex A
ALARP, GAME, MEM
Annex B
Using failure and accident statistics to derive a THR
Annex C
Guidance on SIL Allocation
Annex D
Safety Target Apportionment methods
Normative
Informative

RAMBØLL

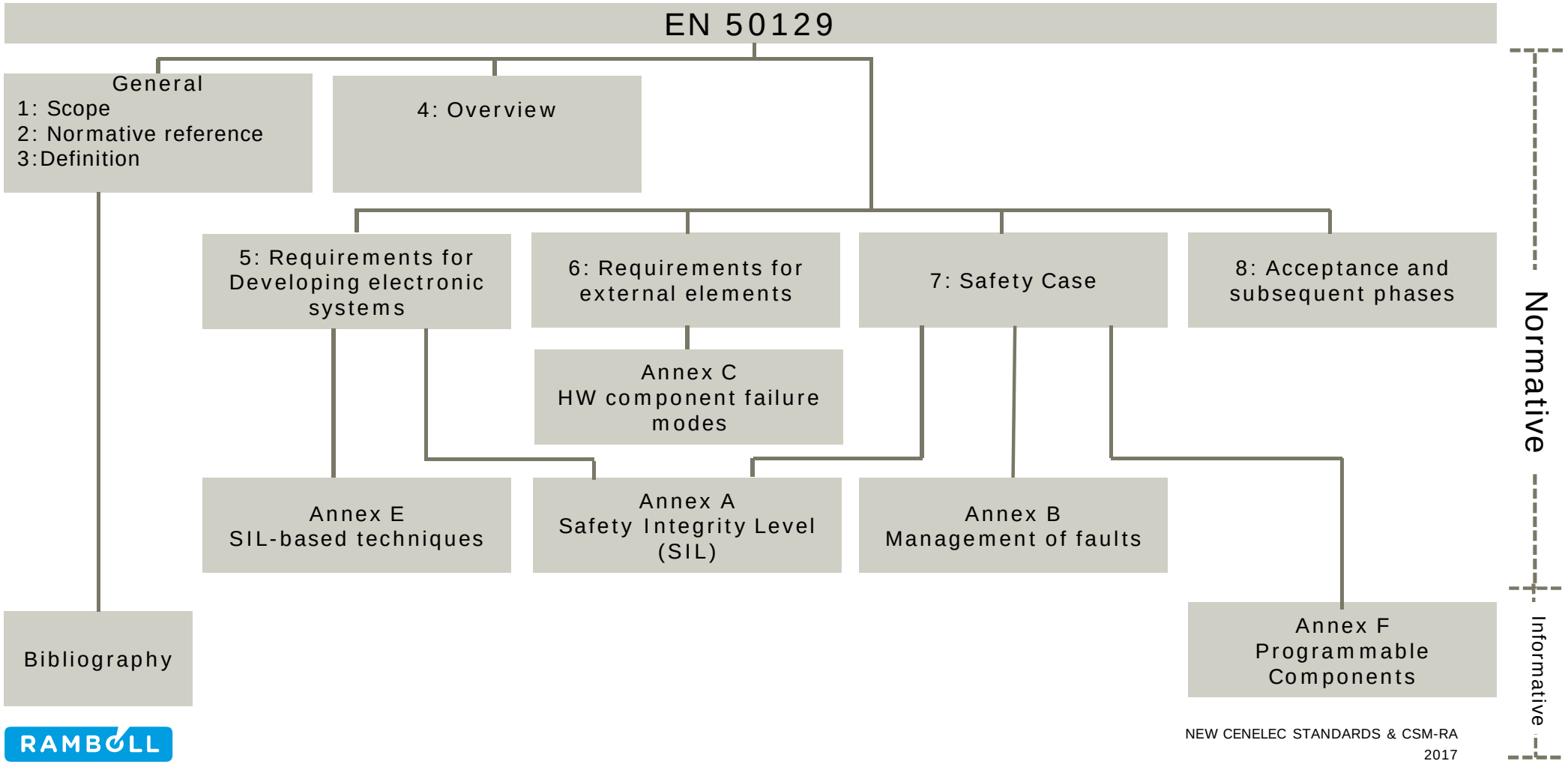
PRODUCTS IN CENELEC PROCESS

EN 50126

- Provide the overall process for development of products
- Lifecycle
- Hazard identification and management
- Safety requirements identification and apportionment
- Safety target (THR, TFFR, SIL)
- Implementation evidence
- Documentation

50129/50128

- Provide the process for development of products
- Tailored system/hardware/software development process
- Detailed analysis of failure and hazard control
- SIL demonstration
- Product specific implementation evidence
- Product specific documentation


EN 50129
General
1: Scope
2: Normative reference
3:Definition
4: Overview
5: Requirements for Developing electronic systems
6: Requirements for external elements
7: Safety Case
8: Acceptance and subsequent phases
Annex C
HW component failure modes
Annex E
SIL-based techniques
Annex A
Safety Integrity Level (SIL)
Annex B
Management of faults
Annex F
Programmable Components
Bibliography
Normative
Informative

RAMBØLL

CSM-RA VERSUS EN50126

CSM-RA

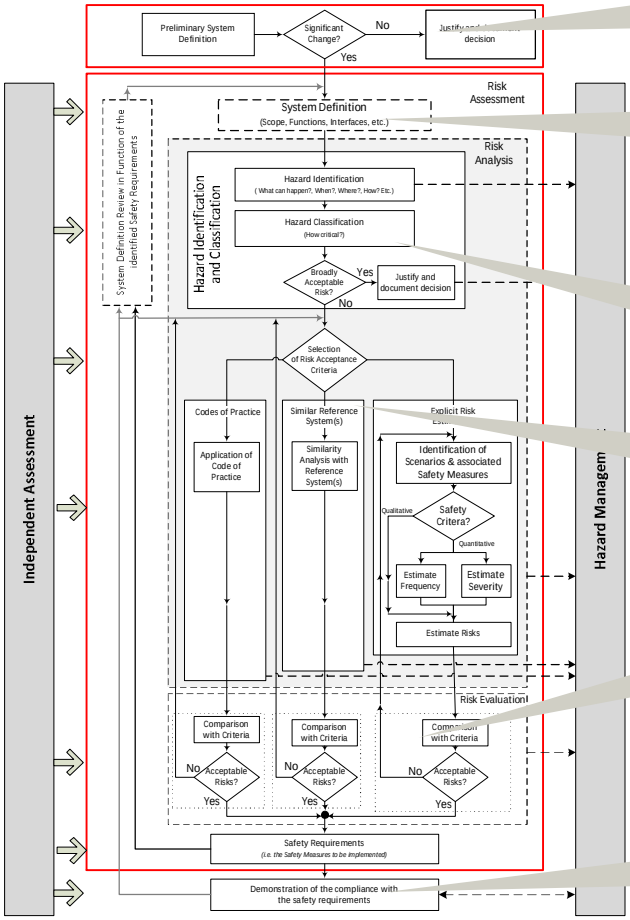
- Focus on a change
- Significance
- Emphasis on hazard identification & control
- Hazard normally controlled by well known measures
- Independent safety assessor as NSA proxy

EN 50126

- Can be applied for changes and products
- Always applicable
- Life cycle approach in hazard identification and control
- Generic control of hazards
- Verification and validation process
- Independent safety assessor to ensure process
- Functional Safety & Safety Integrity
- *RAM (dependability)*

CSM-RA IN SHORT

EN50126



RAMBØLL

Significance evaluation
CSM-RA relevant ?

System Definition
The Change in short

Hazard identification
What is the risk?

Risk evaluation
How to control risk

Risk Acceptance
Control risk

Safety documentation
Risk was in control

EN50126

EN50126

EN50126

EN50126

EN50129/EN50128

EN50126

EN50129/EN50128

Concept | Design | Imple-mentation

System definition

Hazard Record

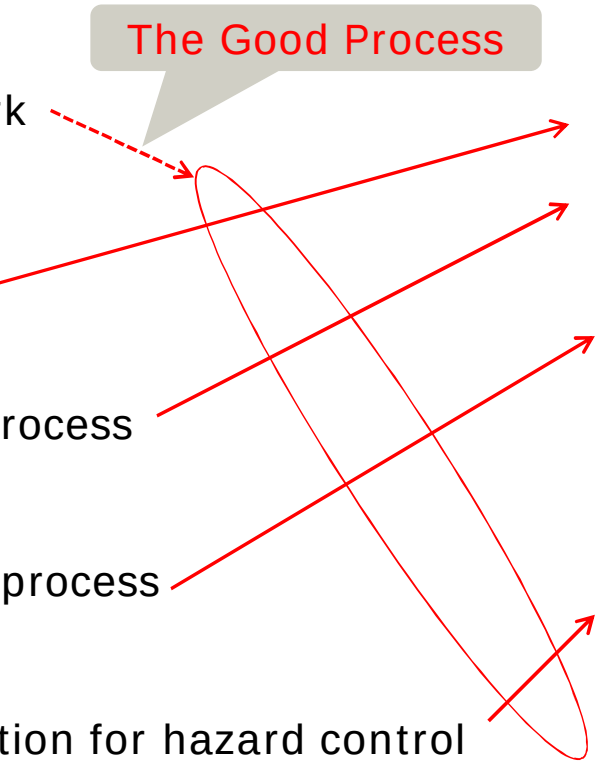
Safety Documentation

2017

CSM-RA SUPPORTED BY EN50126

CSM-RA

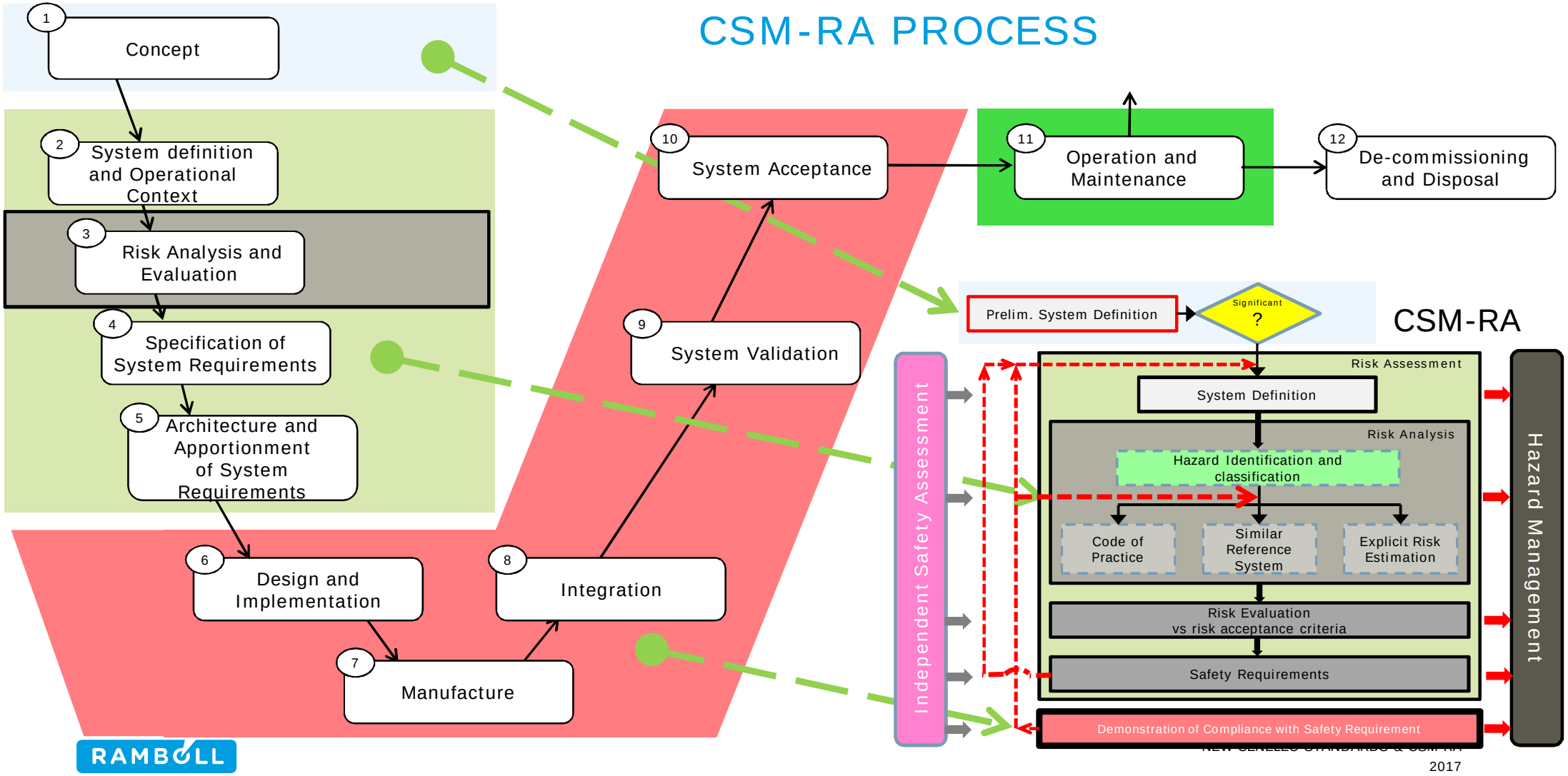
- The Legal framework
- System definition
- Risk Management process
- Require systematic process
- Require documentation for hazard control



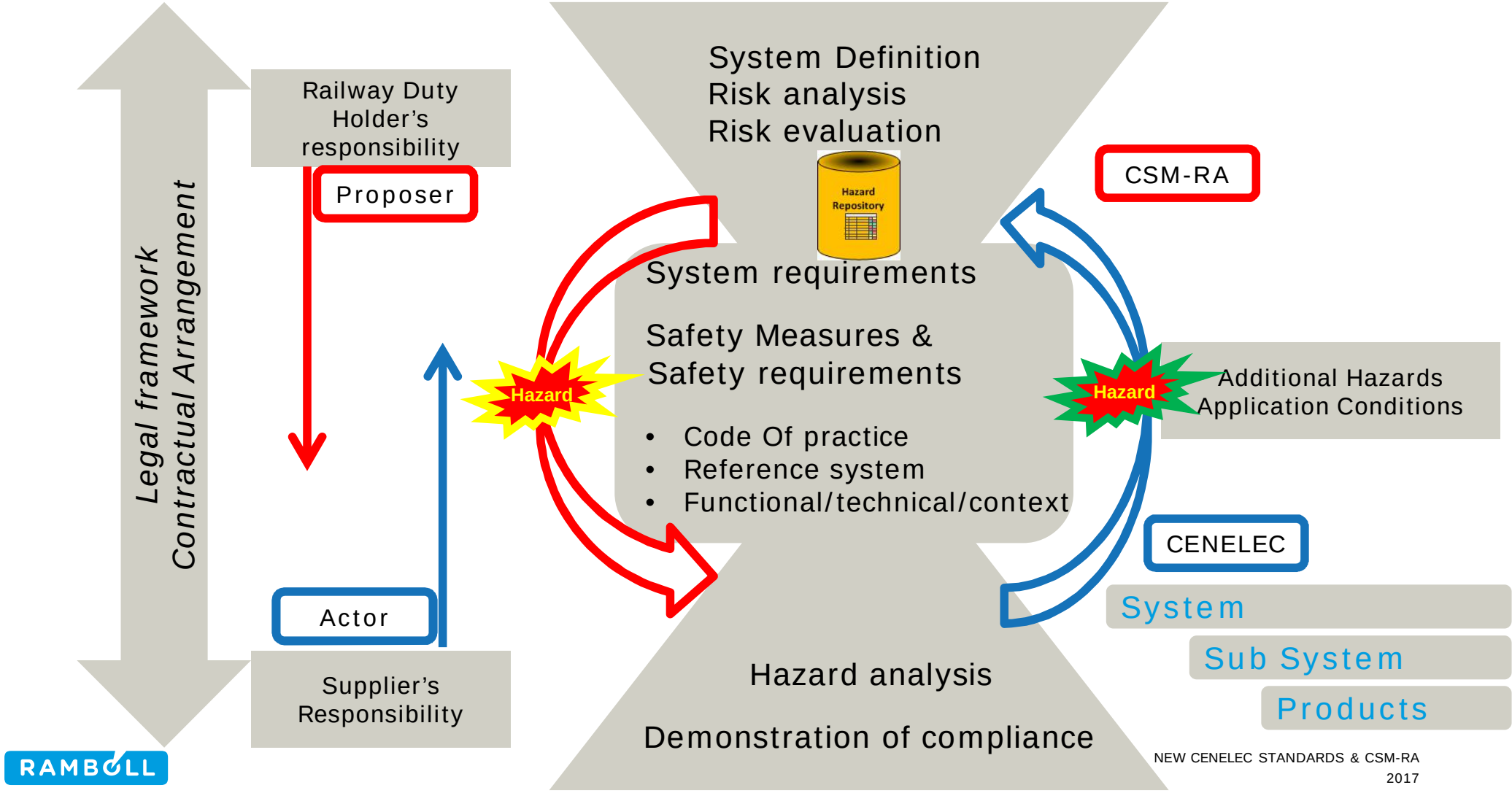
EN 50126

- Hierarchical system definition model
- Detailed risk management process & evaluation principles
- The systematic process
  - Standard lifecycle to be tailored to project
  - Detailed risk management process
  - Engineering process requirements
- Provide the principles for safety documentation
  - Safety Case structure
  - Verification & Validation process

EN 50126 LIFECYCLE COMPARED TO CSM-RA PROCESS



RAMBØLL

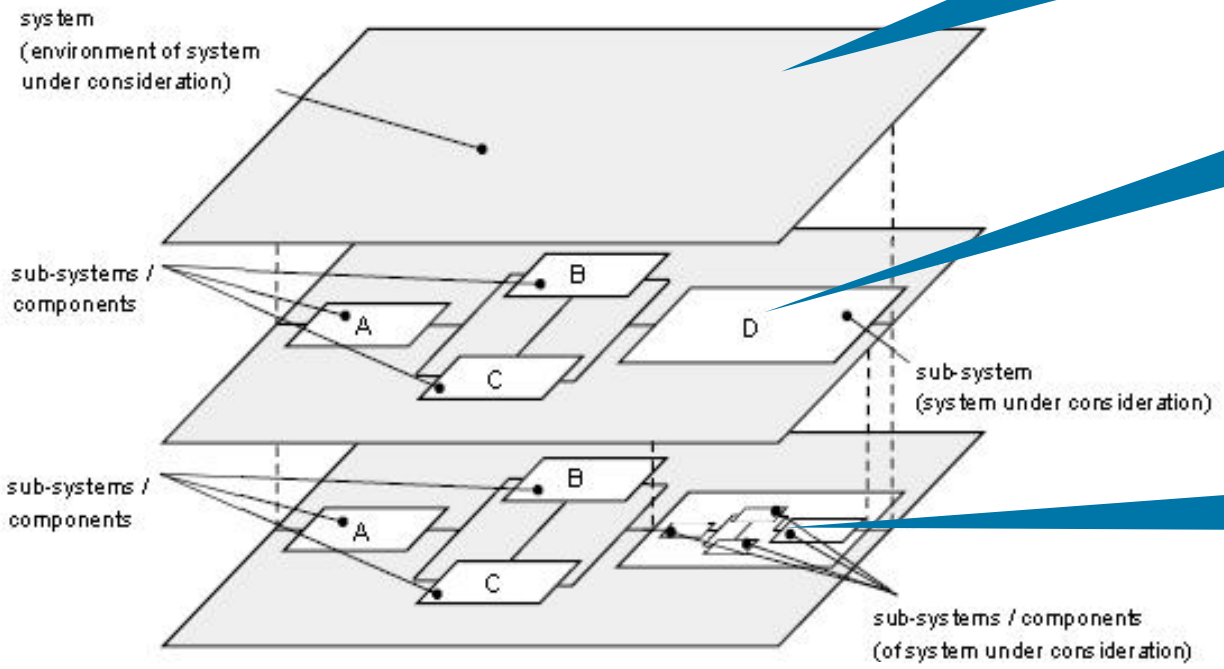

Legal framework
Contractual Arrangement
Railway Duty Holder's responsibility
Proposer
Actor
Supplier's Responsibility
System Definition
Risk analysis
Risk evaluation
Hazard Repository
System requirements
Safety Measures &
Safety requirements
• Code Of practice
• Reference system
• Functional/technical/context
Hazard analysis
Demonstration of compliance
Hazard
Hazard
CSM-RA
Additional Hazards
Application Conditions
CENELEC
System
Sub System
Products

SYSTEM DEFINITION

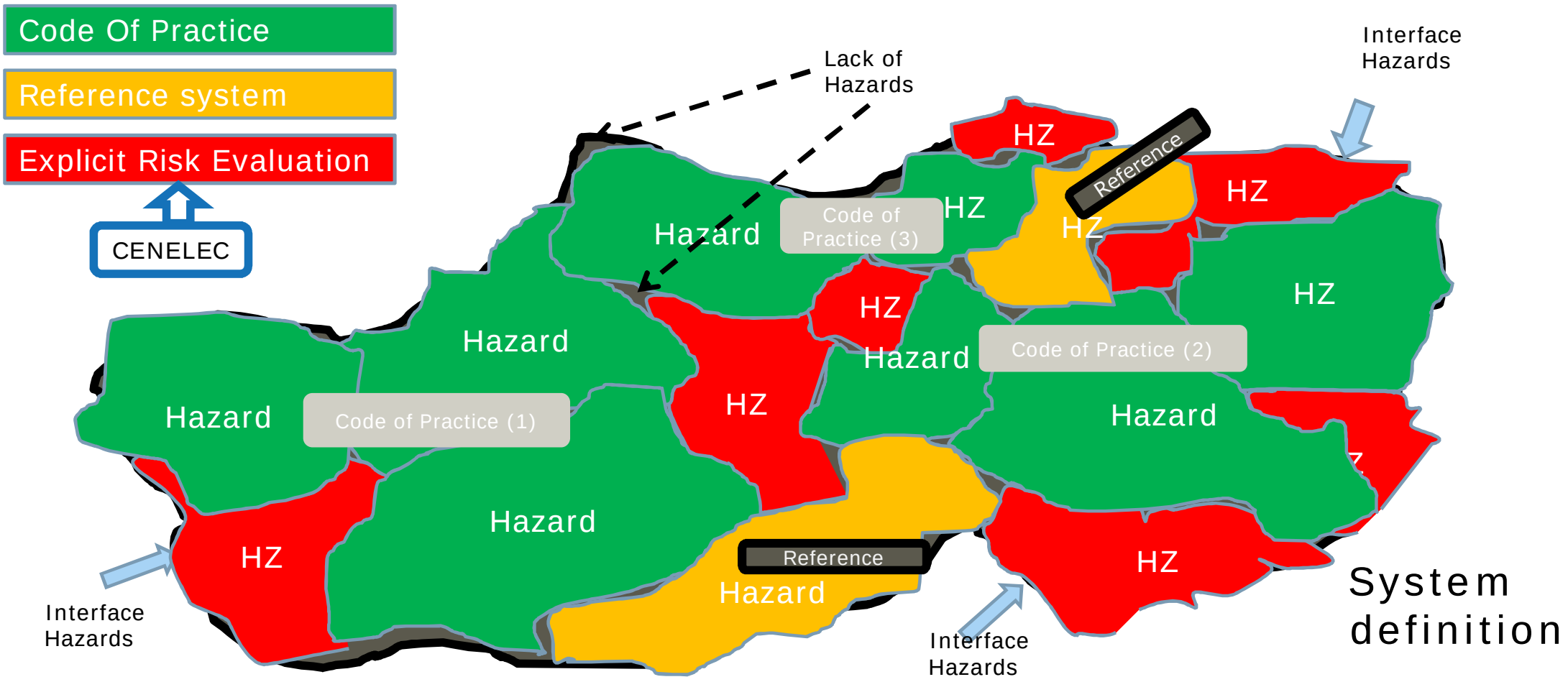
Contextual Requirements
The operational environment

Functional Requirements
What the system shall do

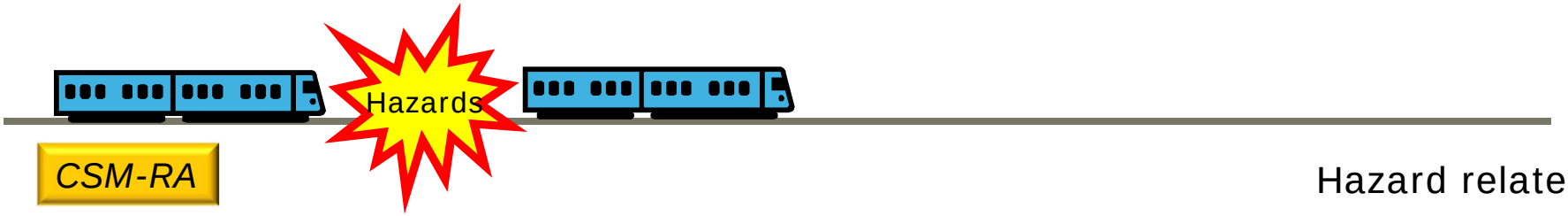
Technical Requirements
Ensure the system function



HAZARD IDENTIFICATION & ACCEPTANCE



EXAMPLE



CSM-RA

Trains too close - > separate

EN50126

Block sections
Indicate free/occupied

Hazard related to Specific Appl.

Specific Appl.

Axle counter

indicate free
while occupied

Specific

Generic
Application
SC

Generic
Product
SC

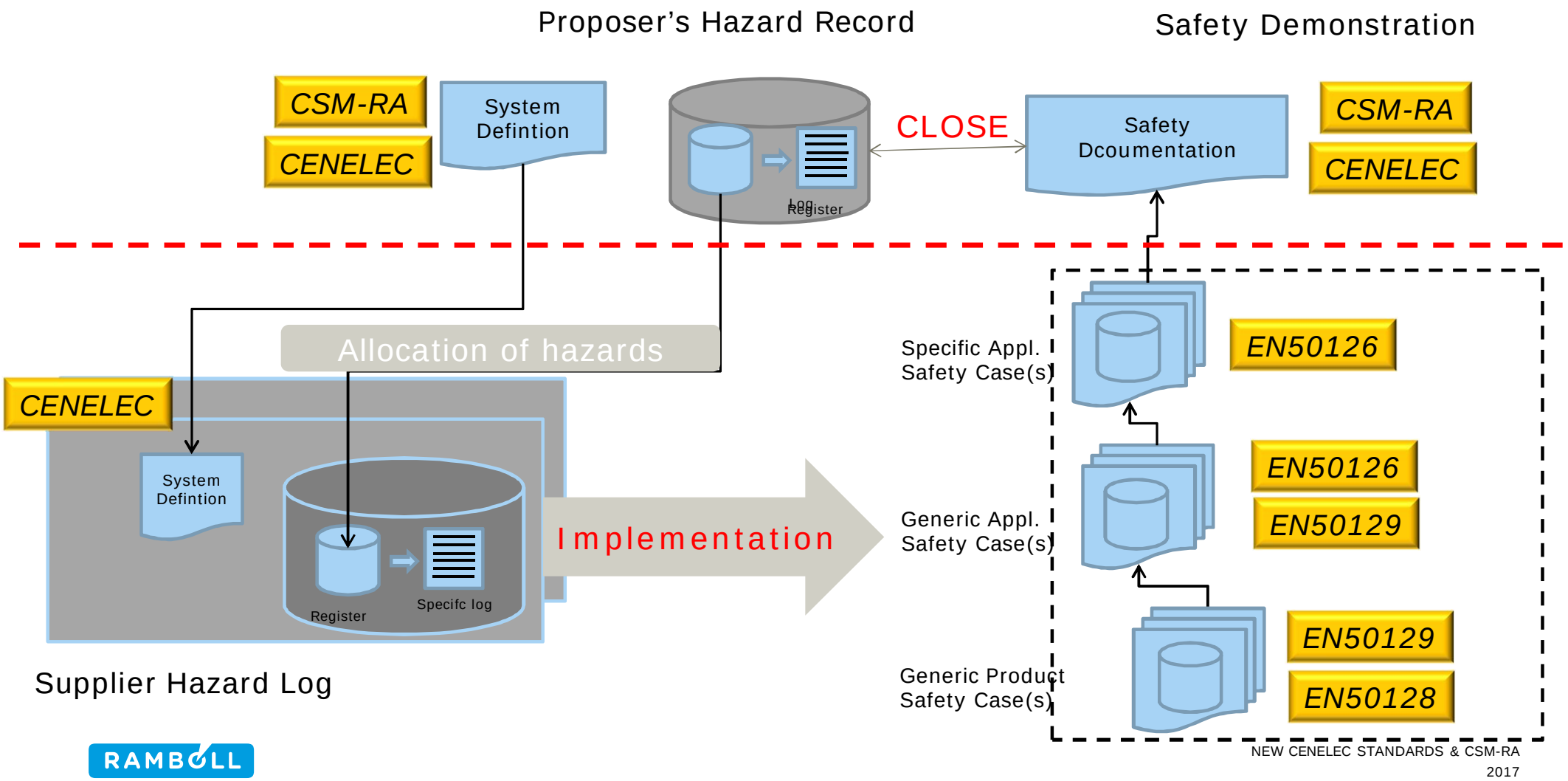
Hazard related to Generic Appl.

EN50129

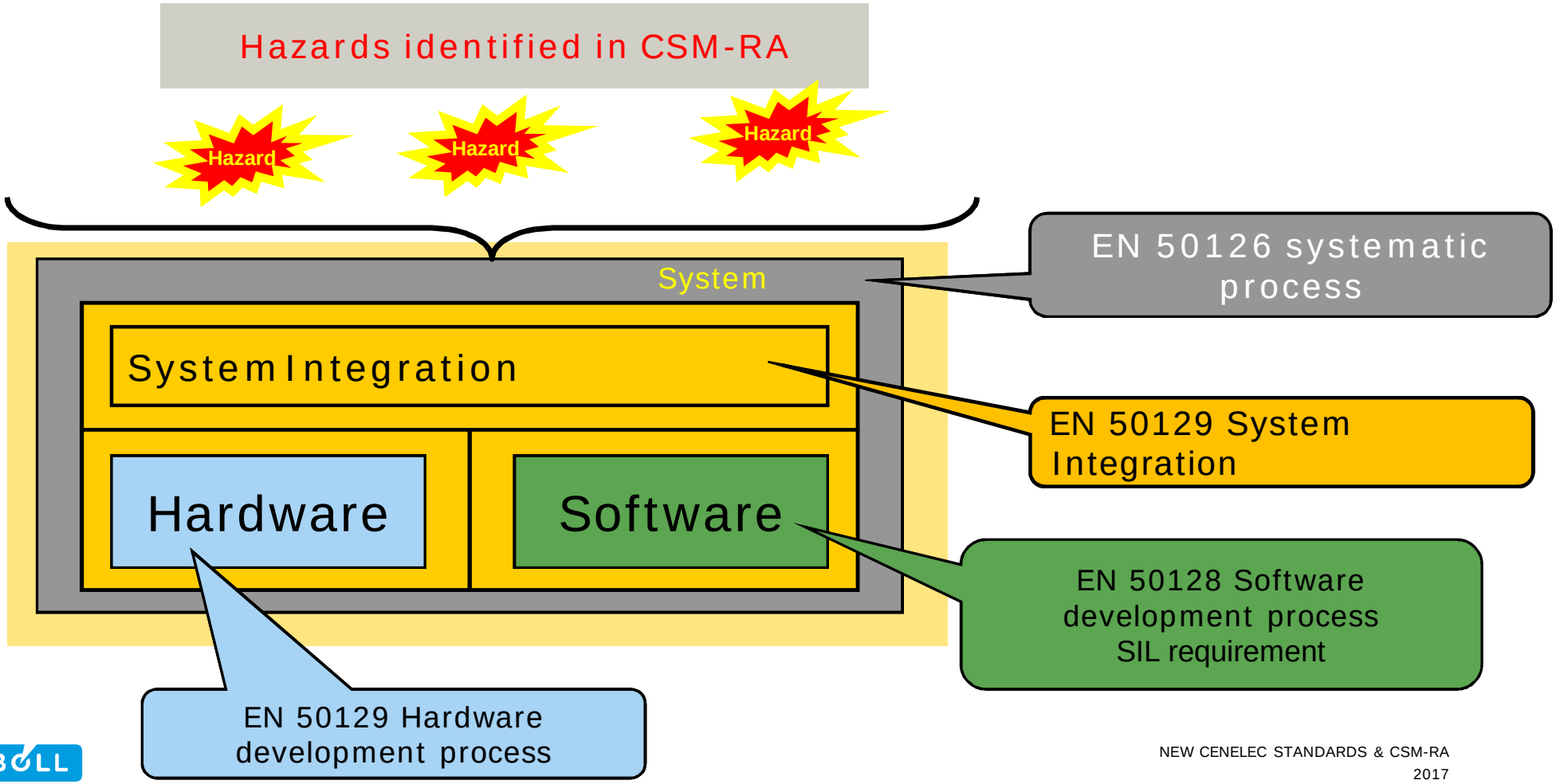
EN50128

Failures/Hazards in Product

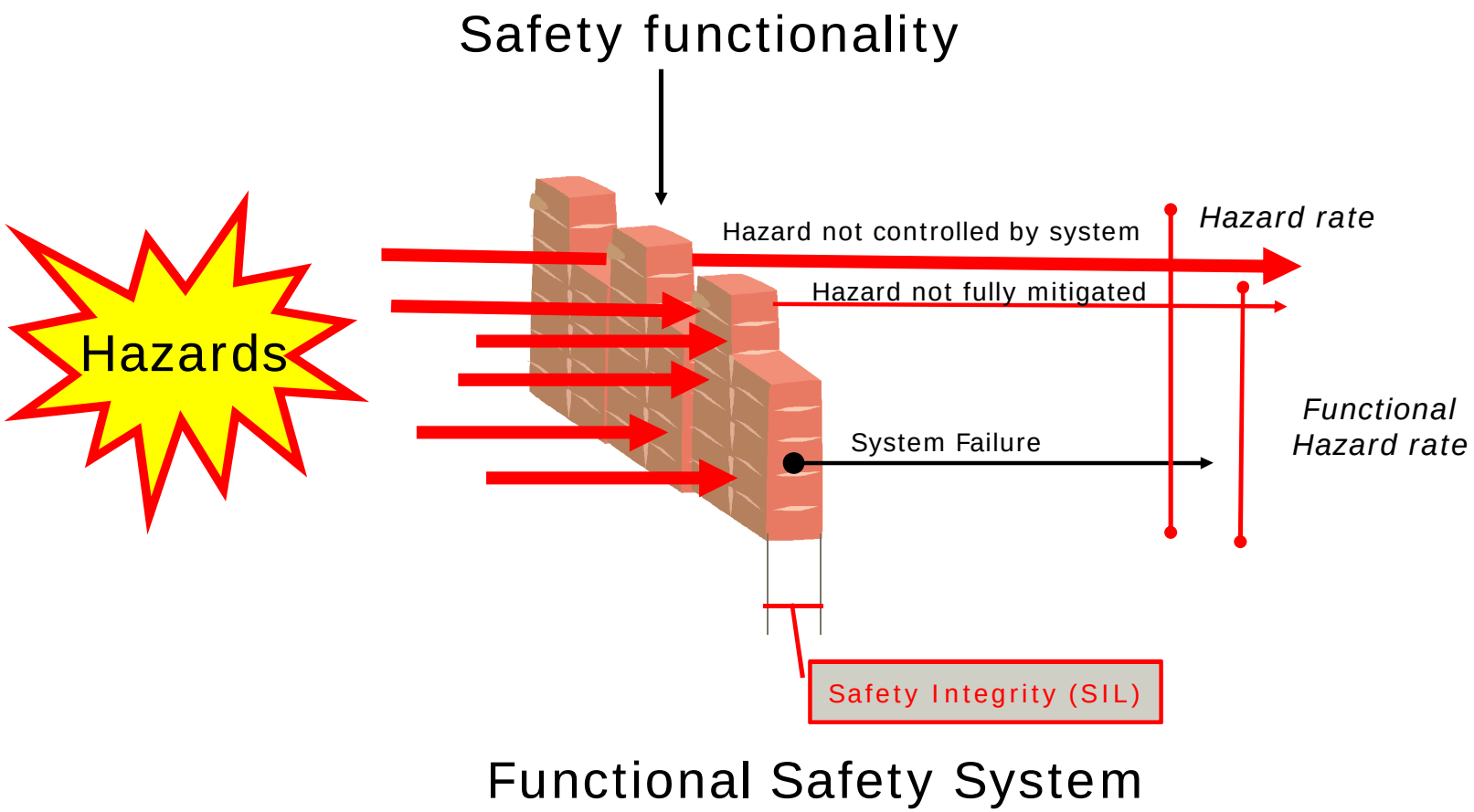
RAMBØLL


Proposer's Hazard Record
Safety Demonstration
CSM-RA
CENELEC
System Defintion
Log Register
CLOSE
Safety Dcoumentation
CSM-RA
CENELEC
Allocation of hazards
CENELEC
System Defintion
Register
Specifc log
Implementation
Specific Appl. Safety Case(s)
EN50126
Generic Appl. Safety Case(s)
EN50126
EN50129
Generic Product Safety Case(s)
EN50129
EN50128
Supplier Hazard Log
RAMBØLL
NEW CENELEC STANDARDS & CSM-RA
2017

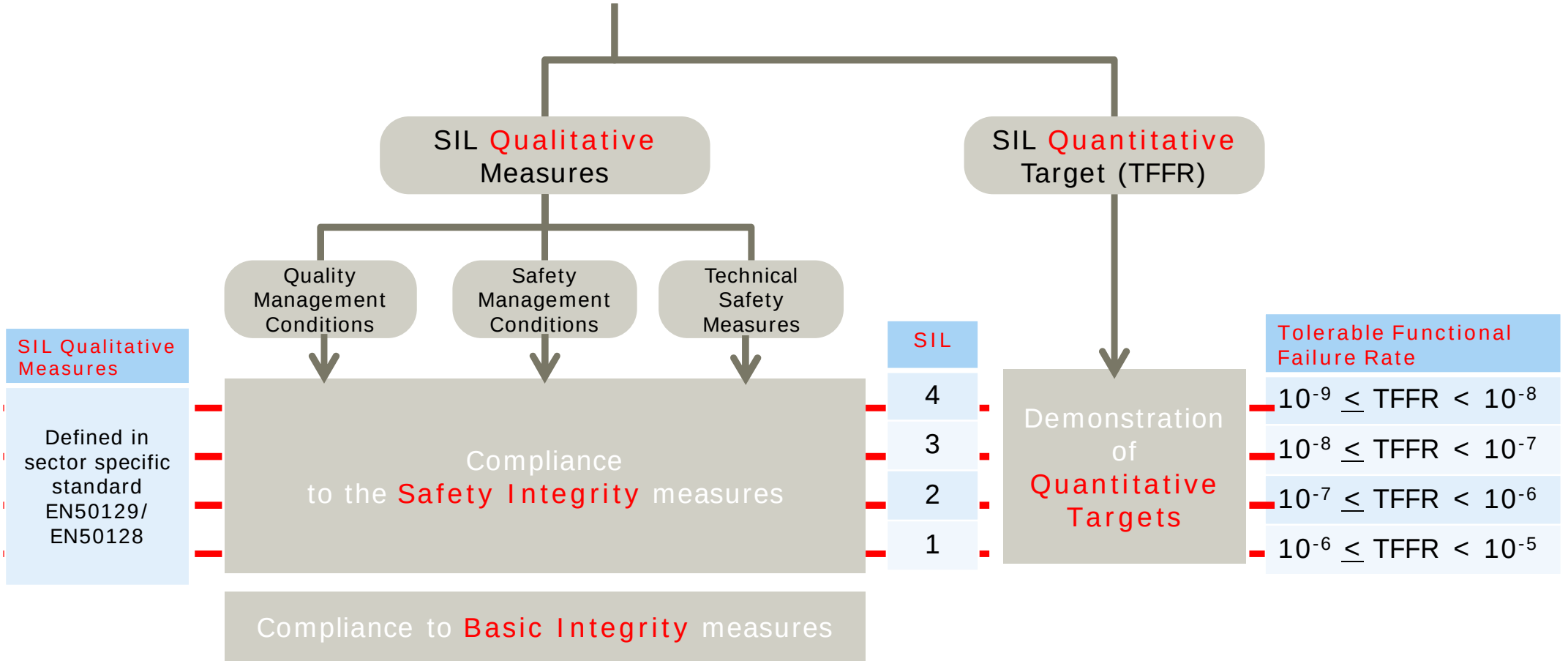
APPLICATION OF CENELEC STANDARDS ON SYSTEM / SUBSYSTEM LEVEL



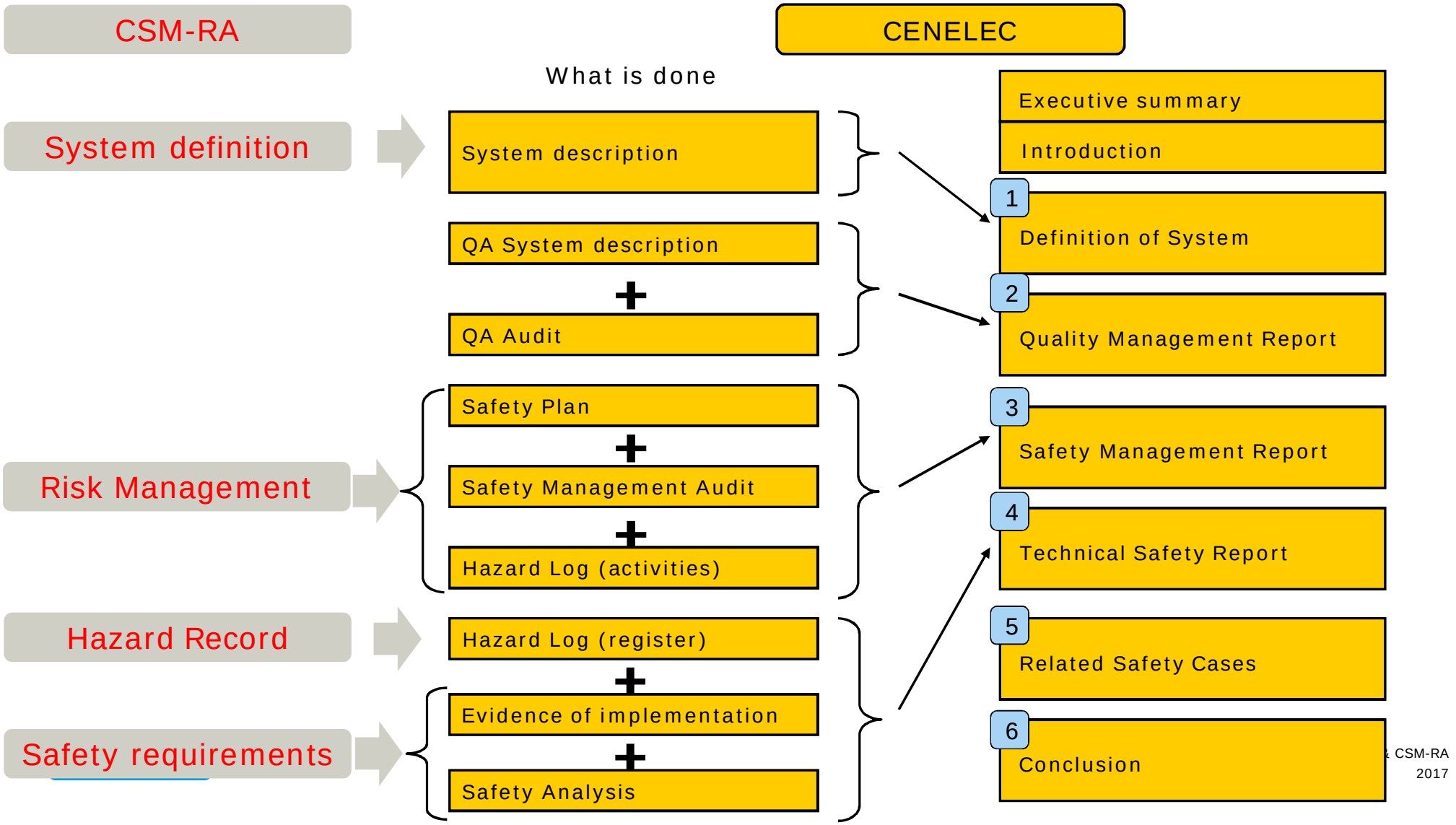
HAZARD RATES & SIL - PRINCIPLE

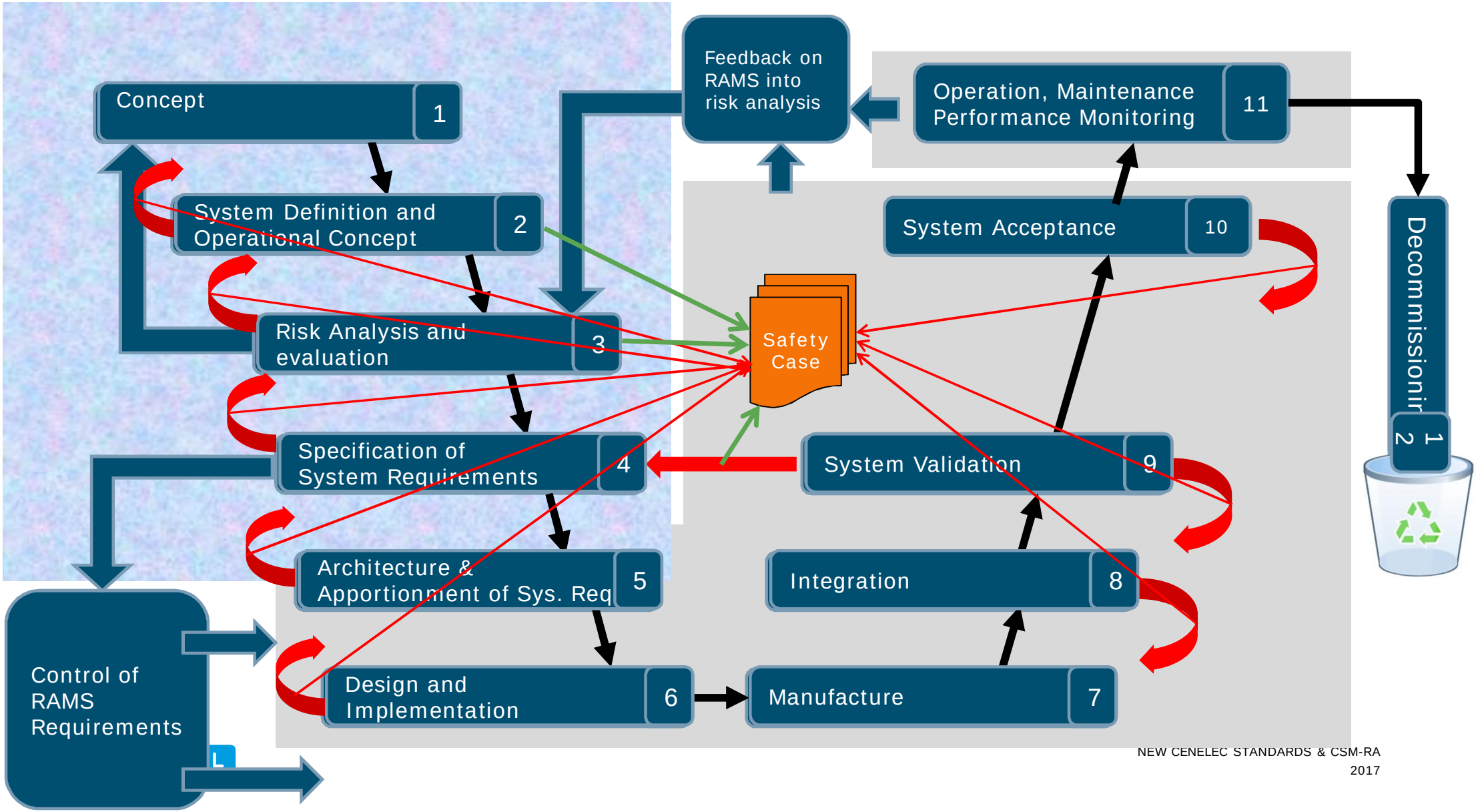


SAFETY INTEGRITY



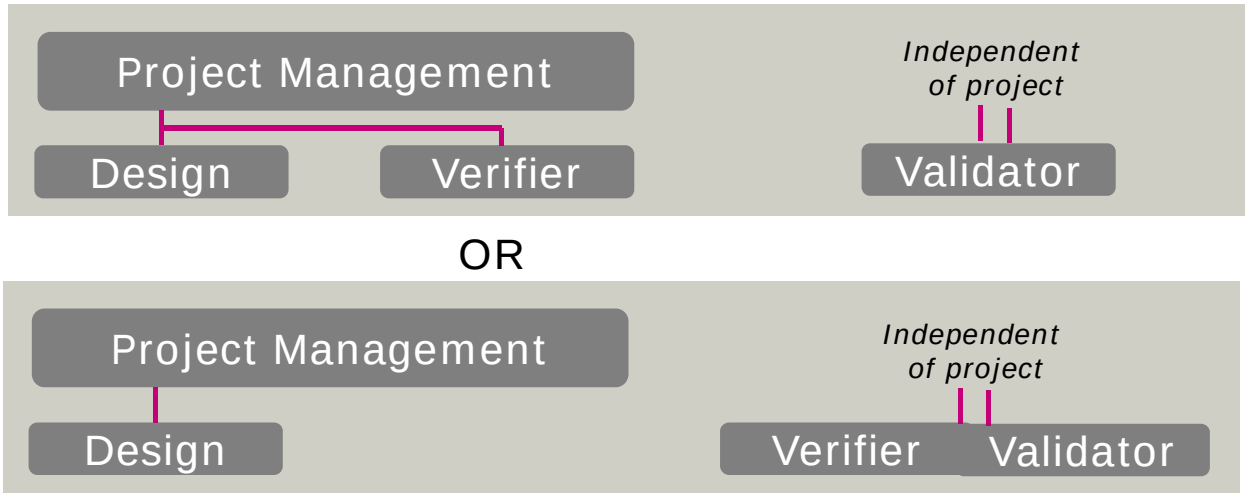
CSM-RA & SAFETY CASE




Concept
1
System Definition and Operational Concept
2
Risk Analysis and evaluation
3
Specification of System Requirements
4
Architecture & Apportionment of Sys. Req
5
Design and Implementation
6
Manufacture
7
Integration
8
System Validation
9
System Acceptance
10
Operation, Maintenance Performance Monitoring
11
Feedback on RAMS into risk analysis
Safety Case
Control of RAMS Requirements
Decommissionir
12

V & V INDEPENDENCE ARRANGEMENTS

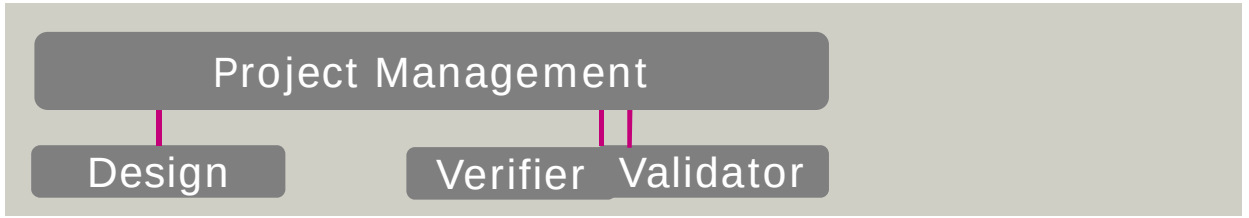
SIL 4 / SIL 3
(Vital)



Independent Safety Assessor

Independent Safety Assessor

SIL 2 / SIL 1
Basic Integrity



Independent Safety Assessor

CENELEC & CSM-RA

New EN 50126 & EN 50129

- No Contradiction with CSM-RA – but a good Code of Practice for the process
- CENELEC -> provide the good practice
- Fill-in on products

THANK YOU

QUESTIONS ?

STIG MUNCK

SGM@RAMBOLL.DK
+45 5161 6375

RAMBØLL