系統保證歐規與美規之介紹

Andrea Colini

Introduction of System Assurance Based on European and U.S. Specifications

Abstract

For the application of railway, there are a variety of safety standards to be followed such as international standards, European specifications, U.S. specifications, etc. These standards coincide in many general aspects and concepts. However, there are several differences in detail (e.g. while the indexes adopted are very similar, the verification process for assuring the targets are met differs).

The most significant differences are:

- The concept of safety integrity level (SIL) is not very popular in the U.S. railway industry
- The application of standards (sometimes regarded as guidelines and sometimes as mandatory regulations)
- The terminology

Keywords: system assurance, safety regulation, French: Comité Européen de Normalisation Électrotechnique is the European Committee for Electrotechnical Standardization (CENELEC).

摘　要

在鐵道應用方面，有多種不同的安全標準可循(國際標準、歐規或美規標準等)。這些標準在許多整體層面及概念上大致相同。然而，細節部分卻有著數項差異(儘管採用指標非常類似，確認符合目標的驗證過程卻有出入)。

最重要的差異為：

- 安全完整度(SIL)概念在美國鐵道產業較不普及。
- 標準應用方式(有時視為指導準則，有時則視為強制性規定)。
- 用語。

關鍵詞：系統保證、安全規定、歐洲電子技術標準委員會

Andrea Colini, Ph.D. - RAMS Manager, Ansaldo STS S.p.A.　andrea.colini@ansaldo-sts.com

1、Preface

For railway applications the RAMS Standards aim to promote a common understanding and approach to the Management of Reliability, Availability, Maintainability, Safety. The systems-level approach defined by these Standards facilitates assessment of the RAMS interactions between elements of a complex distributed system such as a Metro line.

Combining contractual requirements and common practices, the main task for a good RAMS Management Organization is to know how to use at the best each approach in order to build a Safe and Reliable System.

Among the applicable standards there are several differences, mainly related on Safety activities with a critical look into Hazard tracking and Risk Management issues. In particular, it is widely recognized that the use of the CENELEC railway standards results in benefits concerning safety and cross-acceptance for rail systems.

A formal approach to safety assessment and management allows to ensure the existence of a fully documented, auditable safety management system, and identification and assessment of all potential risks related to functional safety. The implication is that if a good safety management system exists, and if risks are identified and controlled, an high level of safety will be assured. Systematic identification and elimination of risks for a railway systems is obviously an important aspect of design and development. To obtain this, high emphasis is laid by the applicable standards on a suitable safety management supported by an appropriate safety organization.

This paper highlights the most relevant differences among U.S. and European approach to RAMS and Safety. Starting from terminology, through the flow of technical safety activities and the methodological approach to mishap risk management, there could be several benefits in using European approach towards U.S. one. After a brief introduction to the MIL and CENELEC guidelines for RAMS, the Hazard tracking and Risk resolution activities are pointed out in section 3. The formal approach of CENELEC on quantitative safety requirements (SIL concept) and safety demonstration (Safety Cases) is described as strength of the European standard. Finally, in the conclusion chapter, the main differences among the standards are summarized.

2、U.S. Military Standards

MIL-STD-882, “System Safety Program Requirements”, outlines a standard practice for conducting system safety and provides a consistent means of evaluating identified risks.

According to this regulation, an SSPP (System Safety Program Plan), shall be prepared by the supplier and developed for a specific product or application. This document defines the system safety requirements to perform throughout the life cycle for any system, new development, upgrade, modification, resolution of deficiencies, or technology development. Within the system life cycle,

these requirements should ensure the identification and understanding of all known hazards and their associated risks, and mishap risk eliminated or reduced to acceptable levels. The objective of system safety is in fact to achieve acceptable mishap risk through a systematic approach of hazard analysis, risk assessment, and risk management.

Typical activities detailed in an SSPP include the following:

- safety management addressing organisational and other aspects for ensuring compliance with the safety program;
- hazard analyses and associated risk assessment to identify and assess hazards and their relative risks in all phases of life cycle;
- safety V&V to demonstrate the level of safety.

The hazard severity and hazard probability definitions in MIL-STD-882 are very similar to those in EN 50126, but there are some slight differences. For example, MIL-STD-882 describes five categories for hazard probability, while CENELEC has six. Some categories for both frequency and severity levels do not fully mach in definition.

Table 1　Accident Hazard Indices / Safety Assurance Levels according to MIL-STD-882D

	FREQUENCY LEVEL				
SEVERITY LEVEL	Frequent	Probable	Occasional	Remote	Improbable
Catastrophic	High	High	High	Serious	Medium
Critical	High	High	Serious	Medium	Medium
Marginal	Serious	Serious	Medium	Medium	Low
Negligible	Medium	Medium	Low	Low	Low

MIL-STD-882 is risk-based as are EN ones, but, unlike them, is not based on SILs.

On Hazard Tracking and Risk Resolution Process MIL-STD approach foresees the following steps:

a. Identification of Hazards;
b. Assessment of mishap risk;
c. Identification of mishap risk mitigation measures;
d. Reduction of mishap risk to an acceptable level.
e. Verification of mishap risk reduction.

In general MIL-STD-882 does not describe a definitive safety program, fixed set of activities, fixed safety case or set of associated documentation, but rather is tailored to the needs of a specific development program. However, the standard is very similar to EN 50126 with respect to the safety management aspects addressed.

3、Cenelec Standards

European Standards can be applied systematically by a railway authority and railway support industry, throughout all phases of the lifecycle of a railway application, to develop railway specific RAMS requirements and to achieve compliance with these requirements.

For railway applications, the European Committee for Electrotechnical Standardization, CENELEC, has produced a number of standards addressing the functional safety of railway applications.

Whilst EN 50126 (RAMS) applies to the total railway system, the remaining standards, EN 50129 (safety), EN 50128 (software) and EN 50159 (communication) are applicable to a "complete railway signalling system" including its individual sub-systems and items of equipment.

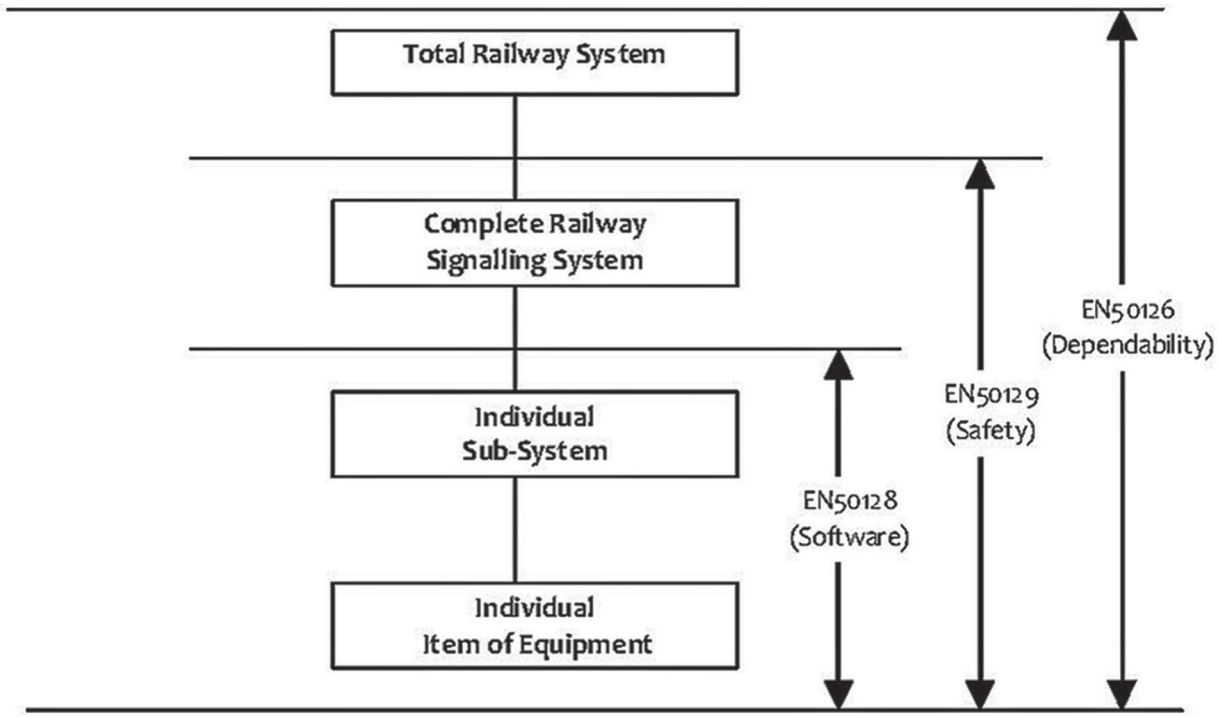

Figure 1 Coverage of CENELEC Standards

EN 50126 is the top-level document that covers the overall process for the total railway system. It defines a comprehensive set of tasks for the different phases of a generic life cycle for a total rail system and provides baseline information on the subject of RAMS and RAMS Engineering, linking RAMS to Quality of Service. It identifies the elements of railway RAMS and "defines a process to support the identification of factors which influence the RAMS of railway systems". It then describes "the means to achieve RAMS requirements" and the concepts of risk, safety integrity

and the fail-safe concept. It then goes on to define a management process based on a system life cycle that has a total of 14 phases, from Concept to De-commissioning and Disposal, with detailed descriptions of the objectives, inputs, requirements, deliverables and verification of each phase. The system life cycle as defined in EN 50126 is shown in the typical V-shape curve.

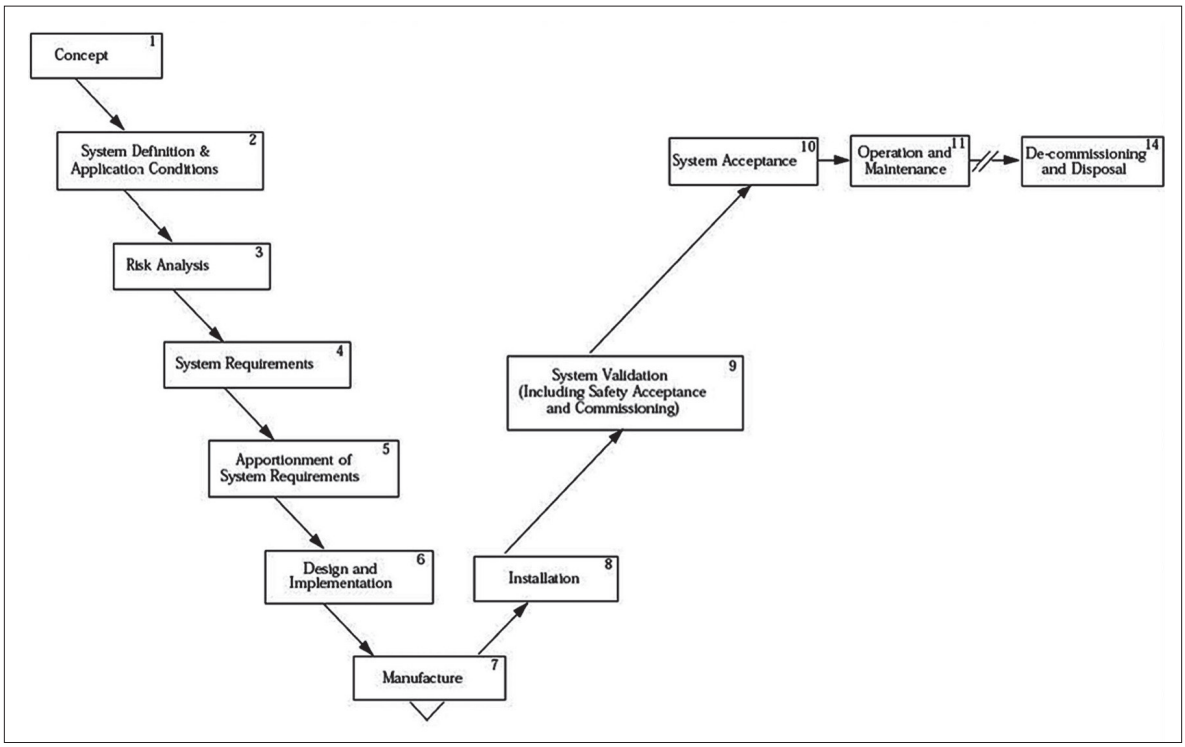

Figure 2　CENELEC Phases

In defining and apportion System Requirements (phases 4 and 5) it was required, that the concept of Safety Integrity Levels (SIL's) shall be used and that the overall SIL for the entire Metro shall be four. The relationship among SIL and Tolerable Hazard rate (THR) is described by the table below.

Table 2　SIL Levels

Tolerable Hazard Rate (THR) per hour and function	Safety Integrity Level (SIL)
$10^{-9} \leq THR < 10^{-8}$	4
$10^{-8} \leq THR < 10^{-7}$	3
$10^{-7} \leq THR < 10^{-6}$	2
$10^{-6} \leq THR < 10^{-5}$	1

Safety Integrity Levels give estimation of system's integrity against systematic failure while Failure Rates are related to Random failures and addressed in the RAM process. Both are linked as shown in the previous table and allow to give adequate set of methods and tools to the relative functions.

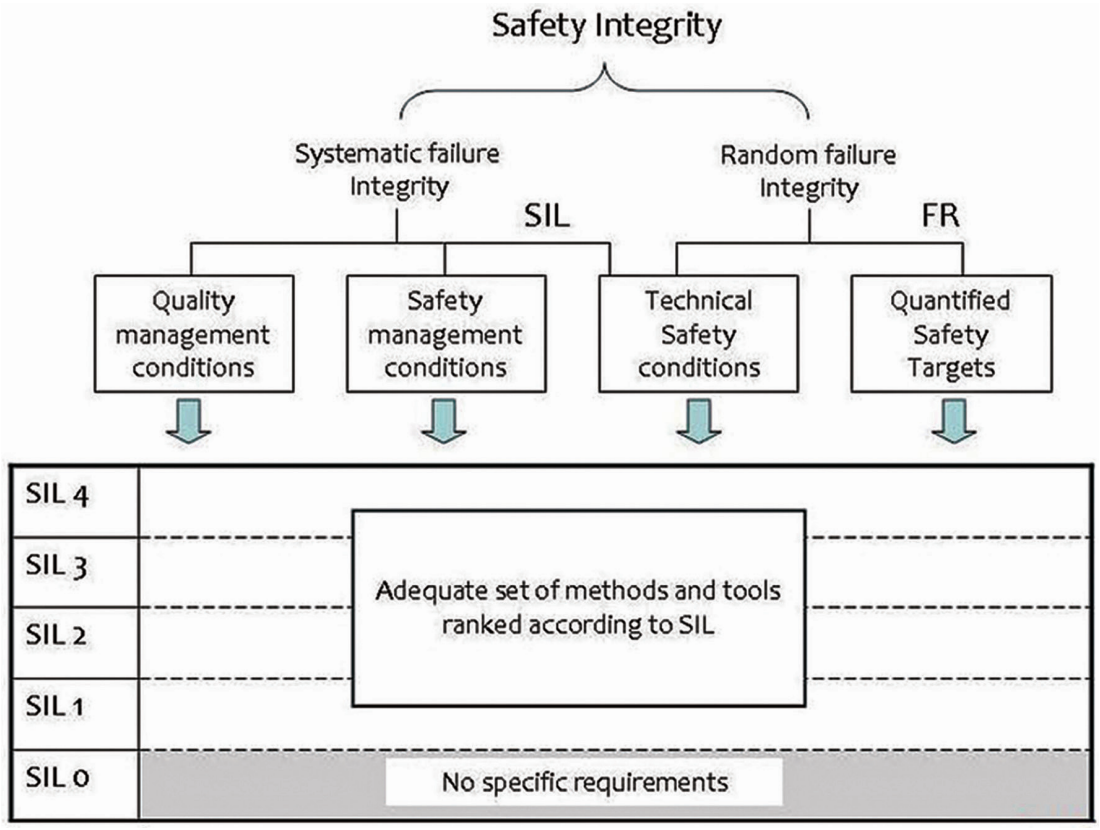

Figure 3 Safety Integrity Level (SIL) and failure Rates (FR)

Following SILs definition, an Hazard and risk analyses and classification is employed to identify adequate lower-level SIL's to subsystems and/or safety functions. The methodology used to apportion SIL's to safety functions/sub-systems is derived from the CENELEC standards and has been performed according to the following steps:

a. Functional Analysis of the overall Metro to identify all safety related functions.

b. Identification of the required level of safety/SIL assignment to safety related functions.

c. Assignment of each safety related function to safety systems.

d. Identification, where applicable, of external risk reduction facilities.

Figure 4 shows the flow of activities aiming to define Safety Integrity Level.

- The process starts with the identification of Hazard Risks and their respective Tolerable Hazard rates (THR).
- In a first phase of the causal analysis the tolerable hazard rate (THR) for each hazard is

apportioned to a functional level (system functions).

- Starting from system and subsystems architectures (as highlighted in the fault Tree Analyses) it is possible to identify which subsystem and then which equipment is responsible for a particular safety function.
- The THR for a function is then translated to a SIL for the subsystem involved using the SIL correspondence (Table 2). Safety Integrity Levels (SIL) are so defined at this functional level for the sub-systems implementing the functionality.

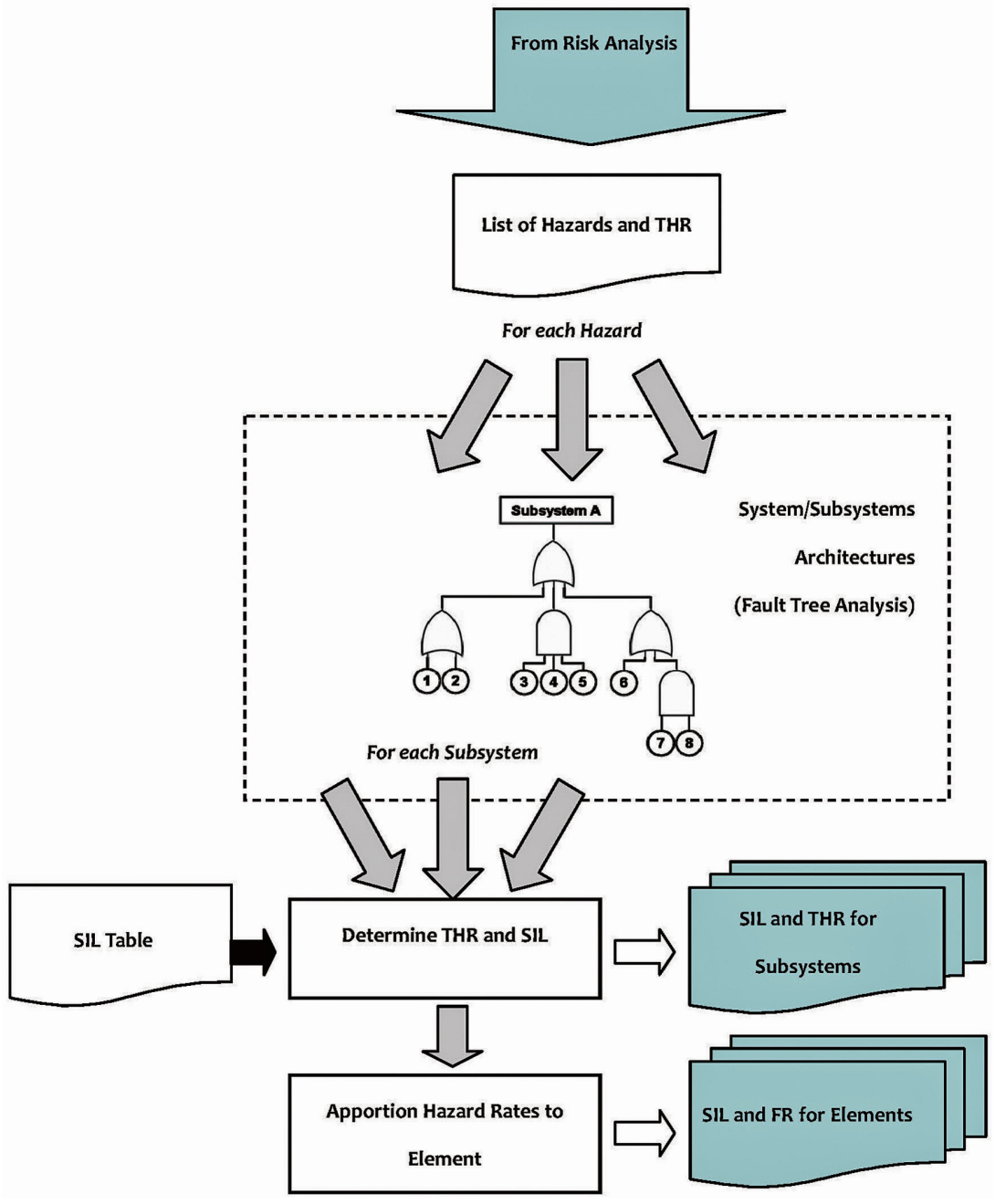

Figure 4　SIL Definition

At the end of design phase all safety related documentation required to assure the safety level will be organized in a comprehensive document which forms the “Safety Case”. Here CENELEC has all the advantages that allow to consider that European approach totally covers the U.S. one:

- a clear safety case structure;
- considerations for the cross-acceptance of safety cases by following a structured standardised life cycle and harmonised documentation set;
- support for reuse and modularisation by defining different types of approvals: generic product, generic application and specific application;
- concise independence requirements for designer, verifier, validator and assessor.

Main scope of this part of the process is to demonstrate that all the main risk of the Metro system are assessed, giving evidence of the fulfilments of the safety requirements and details on risk assessment and risk ranking. The document will be updated during the entire life cycle of the project.

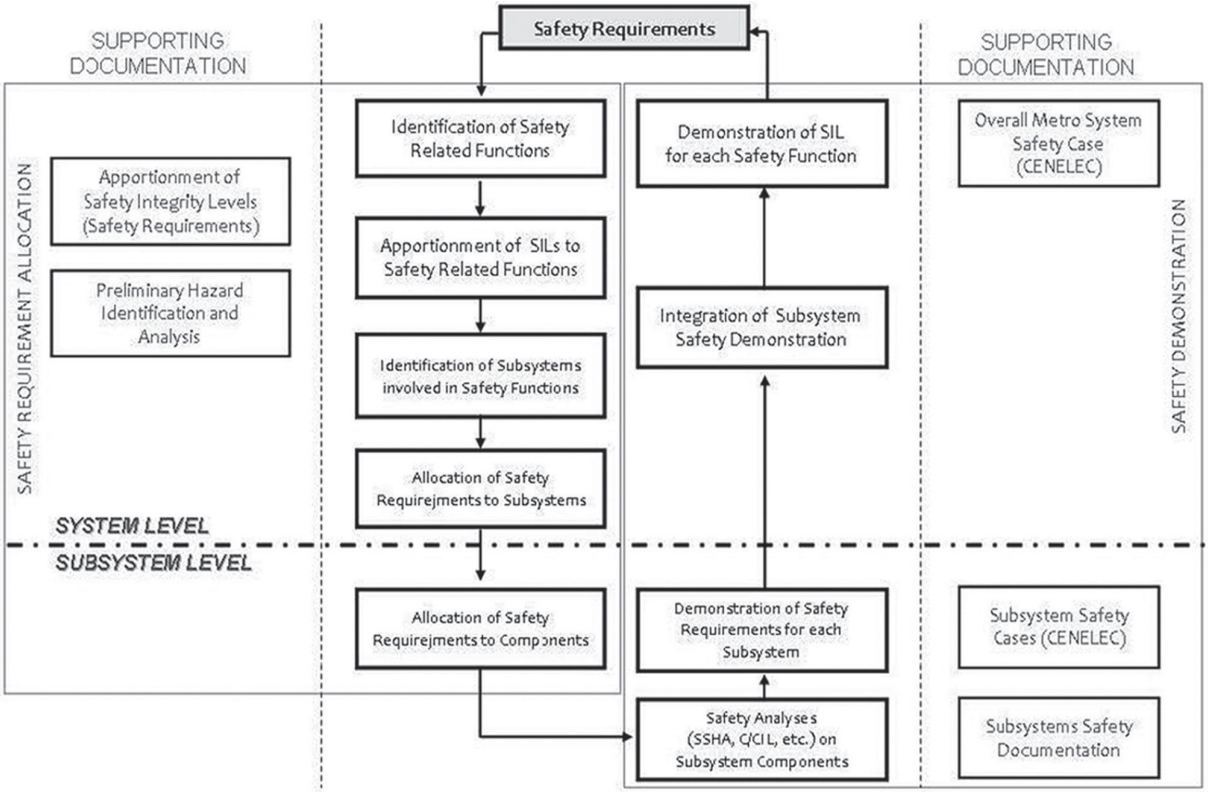

Figure 5 Safety Demonstration

4、Conclusion

A particular advantage of the CENELEC standards is that, due to EN 50126, RAM and safety activities are handled jointly, also from the point of view of RAMS management. EN 50128 and 50129 give quantitative and qualitative rules to gain a Safety Related Software and to manage the product developing phase for Signalling Systems. They also providing rules for demonstration phase (50129) allowing to guarantee a wide range of Safety. Safety integrity requirements are finally defined at a functional level. Moreover the CENELEC standards provide a structured approach and flexible methodology for the achievement and demonstration of the system safety of complex rail systems. Both, the integration of proven techniques and methods, as well as the analysis and evaluation of new technologies, is easily possible and meaningful.

More benefits are listed below:

- Systematic process to define, implement and follow up on a safety process.
- Traceability of activities performed.
- Stepwise process allows minimization of risks.
- Guidelines for demonstration phase allow to guarantee a wide range of Safety.
- Safety integrity requirements defined at a functional level giving a clear view of each safety function and which subsystems are involved in.
- Modularity and Portability of the approach.

Finally also in the US and in Asia the interest in the European norms has greatly increased since they are likely to become worldwide IEC standards in the near future by a fast-track procedure, making them the first worldwide standards in this field.

Reference

1. U.S. Department of Defense (Feb 2000), “MIL-STD-882D, Standard Practice for System Safety” (Superseding 882C), U.S. Military Standards.
2. CENELEC EN 50126, The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS), CENELEC (1999-09).
3. CENELEC EN 50128, Communications, signalling and processing systems - Software for railway control and protection systems, CENELEC (2002-04).

4. CENELEC EN 50129, Railway applications - Communication, signalling and processing systems – Safety related electronic systems for signalling, CENELEC (2004-01).
5. Braband et al. (2003), “The Relationship between the CENELEC Railway Signalling Standards and Other Safety Standards”, SIGNAL + DRAHT (95).
6. Wigger & vom Hovel (2002), “Safety Assessment - Application of CENELEC Standards - Experience and Outlook”, Copenhagen Metro Inauguration Seminar, 21.