SINTEF

SINTEF ICT

Address: P.O.Box 4760 Sluppen
NO-7465 Trondheim
Norway
Location: S.P. Andersens v 15B
Telephone: +47 - 73 59 30 00
Telefax: +47 - 73 59 43 02

Enterprise number: NO 948 007 029 MVA

SJS MEMO

MEMO CONCERNS

SJS practice and interpretation related to parts of European railway legislation and standardisation

FOR YOUR ATTENTION	COMMENTS ARE INVITED	FOR YOUR INFORMATION	AS AGREED

DISTRIBUTION

FILE CODE	CLASSIFICATION
NOT-2010-05	Open

ELECTRONIC FILE CODE

SJS practice and interpretation SJS MEMO_2010-05 v1.0

ISSUE/REVISION	PREVIOUS FILE CODE	PERSON RESPONSIBLE / AUTHOR	DATE
1.0		Narve Lyngby, Thor Myklebust, Ulrik Johansen	2012-09-06
PROJECT NO.	NUMBER OF PAGES	CHECKED BY	DATE
22330405	24	Odd Nordland Odd Nordland	2012-09-11
PROJECT NAME	NUMBER OF ANNEXES	APPROVED BY	DATE
		Thor Myklebust Thor Myklebust	2012-09-12

Contents

Version	Date	Description
0.1	2012-08-04	For internal QA
1.0	2012-09-12	First issue

1 Introduction

This memo presents SINTEF SJSs interpretation of a common practice related to those parts of European railway legislation applying to independent safety assessment and certification of railway signalling systems. The document is based on SINTEFs experience through ISA (Independent Safety Assessor) and NoBo (Notified Body) work (related to control, command and signalling).

This memo does not contain any legally binding advice. It may serve as a clarification tool without however dictating in any way procedures to be followed, and without establishing any legally binding practice. This is SINTEF's preferred/recommended approach, but other approaches that meet requirements of the relevant Directives/TSIs are acceptable.

1.1 EU law

Cited from (europa.eu); *The main goal of the EU is the progressive integration of Member States' economic and political systems and the establishment of a single market based on the free movement of goods, people, money and services.*

To this end, its Member States cede part of their sovereignty under the Treaty on the Functioning of the European Union (TFEU) which empowers the EU institutions to adopt laws.

These laws (regulations, directives and decisions) take precedence over national law and are binding on national authorities. The EU also issues non-binding instruments, such as recommendations and opinions, as well as rules governing how EU institutions and programmes work, etc.

1.2 SJS practice and interpretation

Figure 1 shows the relationship between this memo, EU guidelines and EU legislation.

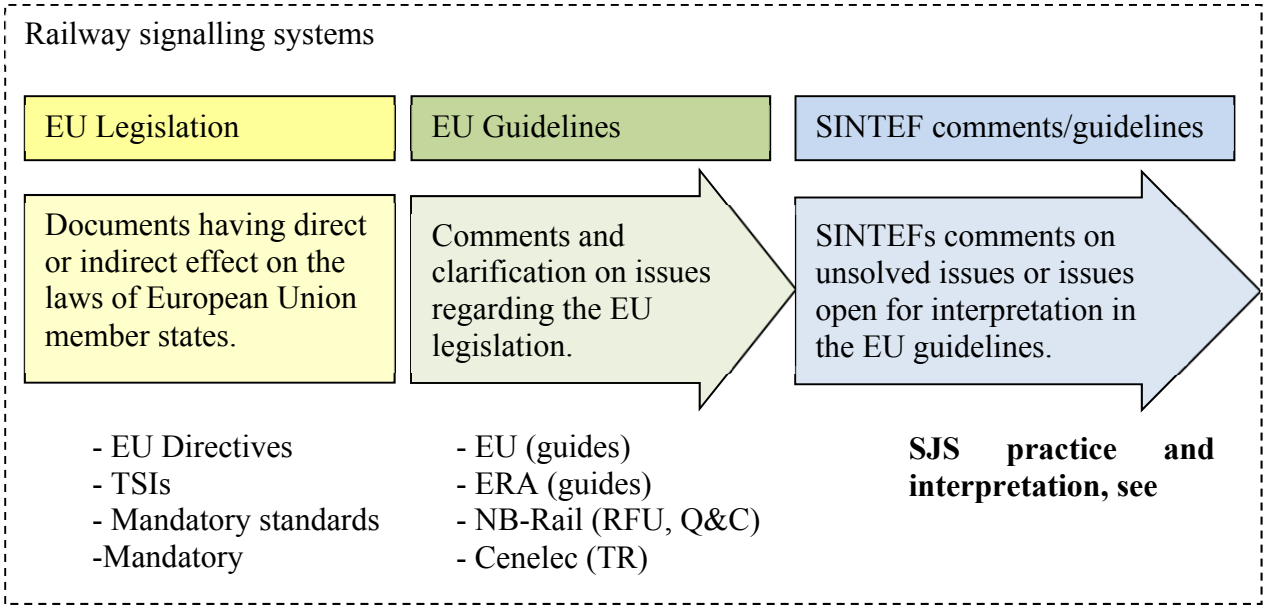

Figure 1 Relationship between the current memo, EU guidelines and EU legislation

Figure 2 shows the relationship between this memo and other memos/guides produced by SINTEF SJS.

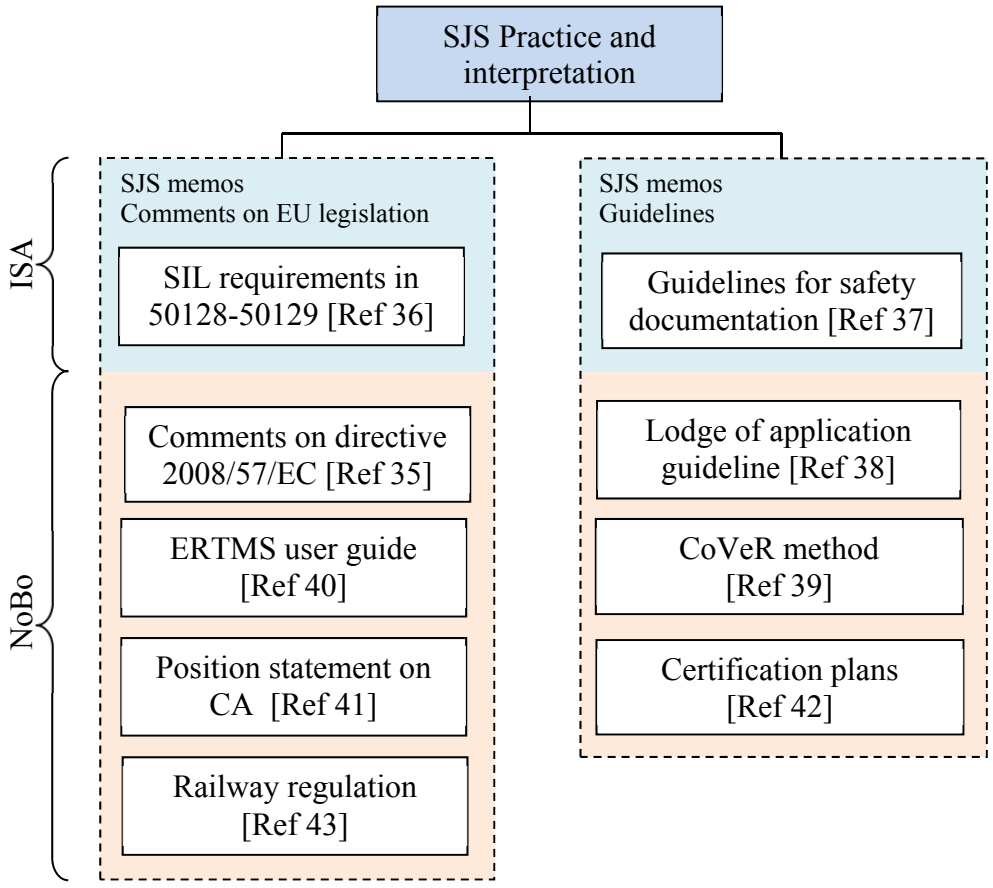

Figure 2 Relationship between current memo and other SJS memos

The target group of this memo is:

- Infrastructure managers
- Railway undertakings
- Manufacturers

In addition the document can be used for educational purposes.

1.3 Scope

This memo is intended as a guide to a common practice and presentation of SJS's interpretation of selected issues related to European railway legislation and guidelines. The scope of this memo, and its relationship to EU legislation, EU guides and other SINTEF SJS memos, are shown in Figure 2. This memo is intended to apply to safety assessment and certification of railway signalling systems.

1.4 Objectives

The overall objective of this memo is to create an understanding (for the target group, see section 1) on how SJS will interpret and practice European railway legislation and standardisation. In addition, this memo may form the basis for e.g. possible RFUs and papers.

In the following sections we address selected issues regarding the assessment/certification process. Chapter 2 presents Directives, standards etc. and their relationship. Chapter 3 presents independent assessment and certification. Chapter 4 gives comments on selected issues and chapter 5 lists references.

2 Directives, TSIs, specifications and standards

Trains in international operation have to comply with national laws of the countries through which they pass and have to be formally approved by each country. The first interoperability directive (96/48/EC [Ref 8], replaced by 2008/57/EC [Ref 1]) introduced a regime where approval by one country, against a set of TSIs and corresponding specifications, must result in EU-wide approval against those TSIs and specifications.

The interoperability directive is designed to achieve the goal of an interoperable railway by specifying the essential requirements for interoperability of the various subsystems[1]. The essential requirements (safety, reliability and availability, health, environmental protection and technical compatibility) specify at a very high level the interfaces between subsystems.

Since the essential requirements are set at too high a level for design and operational purposes, Technical Specifications for Interoperability (TSI) have been (or are in the process of being) created, see Figure 3.

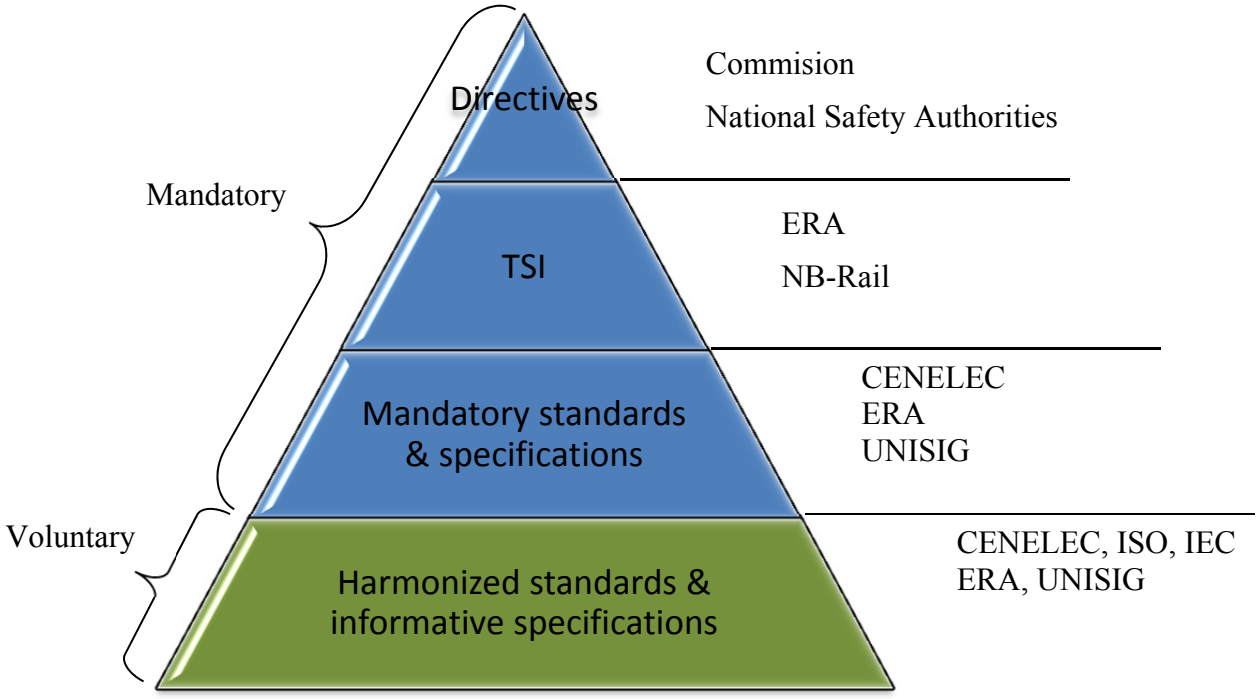

Figure 3 Relationship between Directives, TSI and standards

2.1 Directives

A directive is a legislative act of the European Union that lays down certain end results that must be achieved in every Member State. National authorities in the member states have to adapt their laws to meet these goals, but are free to decide how to do so.

For an updated list of Directives, see the ERTMS Guide [Ref 40], RFU PLG-013 (*Obligation to check conformity to other regulations arising from the treaty*) [Ref 29] and listing of Directives relating to RFU-PLG-013 (WKD-STR-004 [Ref 31]).

[1] Subsystems concerned: INS Infrastructure, RST Rolling Stock, ENE Energy, CCO Control Command and Signalling (on-board) and CCT Control Command and Signalling (trackside)

2.1.1 Directive 2008/57/EC Interoperability

Directive 2008/57/EC [Ref 1] came into force on the 19th of July 2010 and replaced the earlier Directives of interoperability for high-speed rail system (96/48/EC [Ref 8]) and conventional rail system (2001/16/EC [Ref 9]).

It states:

Article 1 Purpose and scope

This Directive sets out to establish the conditions to be met to achieve interoperability within the Community rail system in a manner compatible with the provisions of Directive 2004/49/EC. These conditions concern the design, construction, placing in service, upgrading, renewal, operation and maintenance of the parts of this system as well as the professional qualifications and health and safety conditions of the staff who contribute to its operation and maintenance.

The purpose of Directive 2008/57/EC is to strengthen the competitive ability of the railway, by gathering all requirements in one single legislative act rather than several and thereby creating simplicity and clarity. This implies changes to replaced directives [Ref 8 and Ref 9]; SINTEF points out some important changes[2]:

- Gradually extend the scope of the Directive to the whole rail system and all railway vehicles.
- All regulations regarding approval of vehicles in use are integrated into the Directive.
- For vehicles that are already in accordance with all existing relevant technical specifications, the national safety authority of a member state shall give approval without further control. Still, the national safety authority may control the interoperability between vehicles and the infrastructure and if the vehicle fulfills the requirements in special national regulations [Ref 11]: *In the case of vehicles that have been authorized to be placed in service in one Member State in accordance with Article 21(12) or Article 24, other Member States may decide in accordance with this Article whether additional authorizations to place in service are necessary on their territory.*
- More detailed regulations and simpler procedures for cross acceptance of vehicles already approved in one state. (The National Safety Authorities shall also henceforth examine the interoperability with the infrastructure, including the environment.)
- Prepare procedures for approval of vehicle types. Simplified process of approval of (identical) vehicles instances of an already approved vehicle type.

Harmonised standards for the Directive 2008/57/EC can be found at:

http://ec.europa.eu/enterprise/policies/european-standards/documents/harmonised-standards-legislation/list-references/interoperability-rail-system/index_en.htm

2.2 Technical specification for interoperability, TSI

TSI (Technical Specification for Interoperability) means the specifications by which each subsystem or part of a subsystem (assembly) is covered in order to meet the essential requirements in the Directives (see chapter 2.1) and to ensure the interoperability of the trans-European high speed and conventional rail systems.

The first set of Technical Specifications for Interoperability, prepared by the European Association for Railway Interoperability (AEIF), was adopted in 2002 for the trans-European high

[2] Further details on SINTEFs comments to the Directive 2008/57/EC is given in the memo *Comments to Directive 2008/57/EC* [Ref 35].

speed rail system. These TSIs related to infrastructure, energy, rolling stock, control command and signalling, maintenance and operation have been in force since the 1st of December 2002[3]. The first priority Conventional Rail (CR) TSIs related to freight wagons, (signalling) applications for freight, control command and signalling, noise emitted by rolling stock, and traffic operation and management were adopted in late 2004 and mid 2005. The TSIs related to safety in railway tunnels and accessibility for people with reduced mobility were adopted by the Commission decisions in 2007 and entered into force on the 1st of July 2008. These two TSIs are applicable for both high speed and conventional rail systems.

A link to all the TSIs in force is provided at the ERA home page (www.era.europa.eu/Core-Activities/Interoperability/Pages/TechnicalSpecifications.aspx). A table of TSIs, their date/version and status/information with respect to any revisions in progress are also included in the ERTMS sub group User Guide [Ref 40]. The table accounts for the fact that the TSI itself and its Annex A (all TSIs have an Annex with lists of specifications and standards (mandatory and informative)) live their own lives. The table also contains links to the TSIs.

Each TSI specifies how the essential requirements are specified for a specific subsystem, how the compliance to the TSI is to be assessed (similarly for any interoperable constituents[4]), and what are the implementation arrangements to drive forward compliance across the essential requirements.

TSIs are mandated by law and take precedence over any other standard, including national standards. A TSI may call up a European standard, either in whole or part to specify particular elements of subsystems, or identify items/open points, which are to be specified by an individual Member State.

To assess compliance to a subsystem described in a TSI, a Contracting Entity is required to contract with a Notified Body (NoBo), which has been appointed by the Member State as being competent to assess compliance to that particular TSI. A Contracting Entity is typically, but not necessarily, the party paying for or owning the project. During the assessment the NoBo prepares a Technical File for the subsystem, which details how the assessment was carried out and other matters specified in the Directive. Once the Technical File is complete the NoBo issues a certificate for the subsystem (e.g. Certificate of Verification (CoV) [Ref 32]).

[3] The new control command and signalling TSI [Ref 6] replaces the old control command and signalling TSIs [Ref 4] and [Ref 5]. In this memo, TSI is used to refer the new control command and signalling TSI [Ref 6].

[4] Interoperability constituents means any 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 rail system depends [Ref 1].

2.3 Standards

2.3.1 Mandatory standards

A mandatory standard is according to ISO/IEC Guide 2:2004 General vocabulary [Ref 47] "*a standard the application of which is made compulsory by virtue of a general law or exclusive reference in a regulation*".

For control command and signalling the mandatory standards are explicitly identified in the TSI [Ref 6]. This TSI is adopted by EC decisions and is therefore mandatory. The listed standards are mandatory according to this requirement in the directive 2008/57/EC, Article 5 (8) : "*TSIs may make an explicit, clearly identified reference to European or international standards or specifications or technical documents published by the Agency where this is strictly necessary in order to achieve the objective of this Directive. In such case, these standards or specifications (or the relevant parts) or technical documents shall be regarded as annexes to the TSI concerned and shall become mandatory from the moment the TSI is applicable. In the absence of such standards or specifications or technical documents and pending their development, reference may be made to other clearly identified normative documents; in such case, this shall concern documents that are easily accessible and in the public domain*".

According to the ERA Guide [Ref 25] ch.3.2.5: "*Where a standard referred to in a TSI contains a reference to another standard, unless otherwise provided in the TSI, this second standard also becomes mandatory*". For the control command and signalling TSI, this is related to the references in the Mandatory standards. The references are listed in the chapter "*Normative references*" in these standards.

For safety assessments outside the scope of the TSIs, the term "*mandatory standards*" is not used. In Norway, the safety standard EN 50126 (for products outside the scope of ERTMS) is required by the *Safety Regulation* ("Sikkerhetsforskriften" [Ref 45]), whilst EN 50128 and EN 50129 are required by the *Comments on the Safety Regulation* ("Kommentarer til sikkerhetforskriften" [Ref 46]) issued by the Norwegian Railway Authority.

2.3.2 Harmonised standards

The term "*Harmonised standards*" is used in relation to the TSI, and not for safety assessments outside the scope of the TSIs.

The task of drawing up the harmonised standards are given to the standardisation bodies CEN, CENELEC and ETSI.

According to Directive 2008/57/EC : "*'harmonised standard' means any European standard adopted by one of the European standardisation bodies listed in Annex I to Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services (1) in connection with a mandate by the Commission drawn up in accordance with the procedure referred to in Article 6(3) of that Directive, which, by itself or together with other standards, provides a solution as regards compliance with a legal provision*"

In accordance with the principle of the 'new approach' and the 'global approach' to technical harmonisation, products manufactured in compliance with any harmonised European standards benefit from a presumption of conformity with the corresponding essential requirements of the relevant interoperability directives. For further information, see www.newapproach.org.

Products (including constituents and subsystems) manufactured in conformity with harmonised standards are presumed to be conformant to the essential requirements in the relevant directives.

Harmonised standards are not mandatory, the use of them is voluntary. Alternative paths are possible but the manufacturer has then an obligation to prove that his products are conformant to the essential requirements of the relevant directives. However the standards' transposition into national standards and the withdrawal of diverging national standards is mandatory according to the internal rules of the European Standards Organisations.

Harmonized standards and publication

To give presumption of conformity, the harmonised standards must satisfy the general conditions according to the New Approach: the standard is based on a mandate, it is presented by the relevant European standards organisation to the Commission, its reference is published by the Commission in the *Official Journal*, and it is transposed as a national standard.

An overview of harmonised standards can be found at www.newapproach.org for several directives, but still not for the interoperability directive 2008/57/EC (see chapter 2.1.1). In the future, ERA plans to issue a list of relevant harmonised standards regularly.

Harmonized standards and Annex ZZ in CENELEC standards

Copy from www.cenelec.org: *2004 initiated a change for easier standards. Upon a Commission request, CENELEC committed itself to offer all the new harmonized standards accompanied by an "Annex ZZ". The purpose of this change is to identify the link between the harmonized standards and the Directive requirements. As from now, the Annex ZZ will indicate which essential requirements are covered by the harmonized standards.*

3 Assessment and certification

3.1 ISA (Independent Safety Assessor).

An independent person or agent appointed to carry out the safety assessment. The basis for safety assessment and verification activities has normally been EN 50126 [Ref 14], EN 50128 [Ref 15] and EN 50129 [Ref 17].

The assessor's task according to EN 50129 is to "*... determine whether the design authority and the validator have achieved a product that meets the specified requirements and to form a judgement as to whether the product is fit for its intended purpose*".Confined to the aspect of safety, (independent) safety assessment is to give an evaluation of a system with respect to safety and its operation and use. The safety assessment may as an example be performed on the basis of a Safety Case, guided by the requirements to the contents of a Safety Case as specified by EN 50129 chapter 5. In general, the supplier/railway organisation issuing the Safety Case may have included (additional) evidence in the Safety Case that is not related to safety, such evidence will normally not be subject to the safety assessment.

An independent safety assessment will normally consist of following up safety and quality assurance activities, and pointing out matters on the way that need to be improved. The work will result in reports with conclusion, recommendations concerning the approval processes and conditions for use. The systems and objects to be examined will be restricted to those portions that involve safety functions.

3.2 NoBo (Notified Body)

Notified Bodies are authorised to verify compliance with TSIs as part of the system to effectively and safely facilitate interoperable railway services within the European Union. A Notified Body (NoBo) is a body that has been deemed competent by a Member State to verify whether a developed subsystem or interoperability constituent (IC) meets the specified requirements in the directive [Ref 1] and relevant TSI [Ref 6]. The Notified Body will use the Safety Assessment Report (if existing) worked out by the independent safety assessor (ISA) as part of the evidence for determining compliance with the essential requirement safety.

To qualify for notification, a NoBo must also demonstrate that it fulfils the criteria set down in Annex VIII to Directive 2008/57 [Ref 1], which deals with independence, integrity, confidentiality and competence. Individual NoBo notifications will specify the subsystems for which they are deemed to be competent. Lists of Notified Bodies can be searched on the NANDO web site.

When placing an order for a new subsystem (e.g. rolling stock), the Applicant must choose a Notified Body to verify compliance with relevant requirements in the TSIs (i.e. the Contracting Entity must select a NoBo whose appointment is appropriate to his project). When the requirements in the TSI are met, the Notified Body will issue a Certificate of Conformity (cf. RFU-STR-001 [Ref 32]) that the operator can use as a Declaration of Verification towards the relevant railway authority.

SINTEF has issued a memo presenting an approach for the certification of subsystems (the CoVeR method, [Ref 39]).

4 Issues

Comments and clarification on issues regarding the EU legislation are given in Guides (issued by EU or ERA), Recommendations For Use (RFU, issued by NB rail) etc. see Figure 1. However, there are unsolved issues or issues open for interpretation in the EU guidelines.

There are other issues currently not included in this version of the document (e.g. terminology). These issues are not yet concluded. This document will be continuously updated and future versions will include some of these issues. Already included issues may be updated or removed in future versions if new legislation or EU guides are issued.

4.1 Issues related to Directives

4.1.1 The EMC directive and safety

It is common to believe, even for safety engineers, that products declared by their manufacturer to be in conformity with the EMC directive [Ref 13] must be free from all EMC problems. But the directive is concerned mainly with removing technical barriers to trade. Safety compliance in the EU involves consideration of reasonably foreseeable low-probability events. The scope of the EMC directive specifically excludes safety considerations. In addition, some of the EMC standards harmonised under the EMC Directive either explicitly or implicitly exclude safety considerations. As a consequence it may not be sufficient for a safety product (constituent or subsystem) to only satisfy the EMC directive.

Copy from the EMC directive:

Article 1 ***Subject matter and scope***

This Directive regulates the electromagnetic compatibility of equipment. It aims to ensure the functioning of the internal market by requiring equipment to comply with an adequate level of electromagnetic compatibility. This Directive applies to equipment as defined in Article 2.

Harmonised standards for the EMC directive can be found at:
http://ec.europa.eu/enterprise/sectors/electrical/documents/emc/standardisation/index_en.htm

Quotes from the EMC Directive,

- "Whereas" on page 1: "*(10) This Directive should not deal with the safety of equipment, since that is dealt with by separate Community or national legislation."*
- Article 1, number 5: *"This Directive shall not affect the application of Community or national legislation regulating the safety of equipment."*
- Article 2: "*This Directive shall not affect the application of Community or national legislation regulating the safety of equipment*."

For the Railway domain, safety is dealt with trough the Safety directive 2004/49/EC [Ref 12] and the Interoperability directive 2008/57/EC [Ref 1]. Relevant EMC standards within the railway sector are listed in the Annex of the TSI and in the list of Harmonised standards for Directive 2008/57/EC: http://ec.europa.eu/enterprise/policies/european-standards/harmonised-standards/interoperability-rail-system/index_en.htm.

4.1.2 Declaration of conformity, DoC

Problem description:

Conformity is presented in different manners by the manufacturers. A common and internationally accepted method to present conformity of products to specifications is by issuing a "Declaration of conformity" (DoC). ISO and IEC have issued two standards ISO/IEC 17050-1

[Ref 20] and ISO/IEC 17050-2 [Ref 21] for how this may be performed in a transparent and harmonised way. The relevant topics to be included in the DoC are: unique identification of the DoC, responsibility for the DoC, unequivocal description of the product, relevant requirement documents, limitations and full name and function of the signing person (further information regarding these topics is to be found in Directives and TSIs). These two standards present the international approach for Supplier's (including manufacturer's) Declaration of Conformity. According to directives such as e.g. LVD (Low Voltage Directive), EMC and Railway, a DoC has to be issued by the supplier (manufacturer).

Railway specific information (the information below is based on the Annex 2 of the ERA Guide [Ref 26]):

There are four types of declarations:

For constituents:

- 'EC' declaration of conformity (see Article 13 in the directive 2008/57/EC)
- 'EC' declaration of suitability for use (see Article 13 in the directive 2008/57/EC)

For subsystems:

- 'EC' declaration of verification of subsystem (see Article 18 in the directive 2008/57/EC)
- 'EC' ISV declaration.The term 'EC ISV declaration' is used in Annex VI of the Interoperability Directive. In the 'new' modules in 2010/713/EC [Ref 7], this document is referred to as an 'EC declaration of intermediate subsystem conformity'.

Information to be provided on the declarations is indicated in Annexes IV and V of the Directive 2008/57/EC.

As stated in Article 13(3) of the Interoperability Directive, *"...where interoperability constituents are the subject of other Community directives covering other aspects, the „EC" declaration of conformity or suitability for use shall, in such cases, state that the interoperability constituents also meet the requirements of those other directives".*

ERA has issued a 0.1 version of a document presenting templates for declarations on its website [Ref 48].

ERA keeps EC declarations of verification of subsystems and EC declarations of conformity of constituents in the public database: http://pdb.era.europa.eu/. For further information, see the ERADIS Application Guide on: www.era.europa.eu/Document-Register/Pages/ERADIS-application-guide.aspx [Ref 34].

SINTEF recommends that ISO/IEC 17050 [Ref 20] is used if adequate recommendations are not found in relevant TSIs or EU guidelines.

4.2 Issues related to standards

4.2.1 Normative standards

Normative standards are listed in the chapter 2 "*Normative references*" in the relevant EN standards.

Normative reference is (www.bsigroup.com/) defined by BSI as a *"document to which reference is made in the standard in such a way as to make it indispensable for the application of the standard."* Normative references listed in mandatory standards (see chapter 2.3.1) are considered as mandatory. Copy from 08/57-DV44 [Ref 51]: "*Where in a TSI there is a reference to a standard or document (or a part of it) and within this latter text further normative references exist, these additional aspects also become mandatory. These further normative references can occur where the text includes reference to other clauses within the same standard or document, and/or to other standards or documents (or a part of them)*[5]*"*

For the normative references in the mandatory standards EN 5012X, there are a few exemptions for them being mandatory in practice. Some of the normative references are Guides and shall therefore be treated as Guides. An example is ISO 9000-3 (current issue is ISO/IEC 90003:2004). Vocabulary references as e.g. IEC 60050(191) are normally treated as Guides and not as mandatory. In addition the normative reference IEC 61508 series in EN 50126:1999 and the normative reference ISO/IEC 9126 series in EN 50129:2003 are normally not treated as mandatory (SINTEFs interpretation).

4.2.2 Use of different editions of standards

Standards are normally revised and issued as new editions every 5-12 years due to the development in technology and legislation.

Use of standards regulated through the directive 2008/57/EC

Following its internal regulations, the relevant European standard organisation gives the date of publication at national level of the revised harmonised standard, and the date of withdrawal of the old standard. The transitional period is normally the time period between these two dates. During this transitional period both harmonised standards give presumption of conformity, provided that the conditions for this are met. After this transitional period, only the revised harmonised standard gives a presumption of conformity.

References to standards in the TSIs may be strict which means that the version number is stated or it can be slipping which means that the version number is not mentioned and the version to be used is the one that was in force at the time of adoption of the latest version of the TSI in question. According to the ERA Guide [Ref 25]: "*In both cases, the version of the standard (or document) referred to in a TSI is the binding one. If, after the adoption of a TSI, a new version of this standard (or document) is adopted, it does imply any change in the TSI, the „old" version referred to in the TSI is still the binding one. That is, in both cases nothing actually „slips"*".

Normative references listed in the relevant standards may include the version number; then that version shall be used. If the version number is not mentioned, then the latest issue shall be used. SINTEF comment: if the latest version is not used, an impact analysis has to be performed to

---

[5] *In order to avoid the unwanted "propagation" of the mandatory character of a standard to other standards or documents, it is highly recommended that references are made to one or more specific clauses of a standard and not to the entire standard.*

check whether not using the latest version has any impact on safety. If it does not have any impact on safety, the former edition may be used.

4.3 Issues related to ISA and NoBo assessment

4.3.1 Impact Analysis

Impact Analysis (IA) is in general used to demonstrate consequences of changes or deviations. In relation to safety applications for railways an Impact Analysis is also used to demonstrate consequences of **not**- or insufficiently implemented system requirements or insufficient mitigation of hazards.

Standards where impact analysis is specified as a tool to be used are often not very specific about in which situations Impact Analysis shall be used, and also which methods should be applied. The objective with this document (based on railway specific, generically applicable and prereleases of up-coming standards) is to give an overview of how Impact Analysis can be applied to safety critical railway applications.

The following documentation is of relevance:

- Railway standards: EN50126-1:1999, EN50128:2001, EN50128:2011, EN50129:2003, prEN50126-4, being version 1.0 with date 30.09.2011.
- Railway guidelines: CLC/TR 50506-2:2009 [Ref 19].
- Generic standards: IEC61508-1, IEC61508-2, IEC61508-3, IEC61508-4, IEC61508-7 (describing parts of IEC61508-1 to 3), issued 2010.

EN50126:1999: Impact analysis is mentioned specifically in relation to phase 13 "*Modification and retrofit*", in EN50128:2001/2011 specifically with Clause 16 "Software maintenance", Table A10 "*Software Maintenance*" where Impact Analysis is mandatory for SIL3 & 4, and in CLC/TR50506-2 in section 6.3.1 "*Approval for modification and internal adaptation*". A rudimentary method (B.35) to be used is specified in EN50128:2011. Impact Analysis is not specifically covered in EN50129:2003.

In prEN50126:2011 the use of IA is far more specific than in EN50126:1999, now specifically covering system and hardware (prEN50126-4 [Ref 23]) in addition to software, and where also an analysis method is specified (H.2.15). Chapter 6.2 of prEN50126-2 [Ref 22] prescribes the use of Impact Analysis for modifications and changes done during integration and testing. prEN50126-4 prescribes use of Impact Analysis in a numerous different cases, ref sections 7.1.1.2, 7.8, 8.4, 10, 11.4, and Table A10 where use of Impact Analysis is highly recommended for SIL1-4.

The generic standard IEC61508 frequently refers to Impact Analysis and also includes a definition in IEC61508-4: "*3.7.5 impact analysis: activity of determining the effect that a change to a function or component in a system will have to other functions or components in that system as well as to other systems*".

Impact analysis is specifically mentioned in relation to "*Overall modification and retrofit*" (section 7.16 in IEC61508-1), "*Decommissioning or disposal*" (section 7.17 in IEC61508-1), "*Requirements for proven in use elements*" (section 7.4.10 in IEC61508-2), "*E/E/PE system integration*" (section 7.5in IEC61508-2), and "*Software safety lifecycle requirements*" (chapter 7 in IEC61508-3). IEC61508-7 specifies a rudimentary methodology (C.5.23) for doing an impact analysis, being identical to the B.35/H.2.15 method as described in EN50128:2001/prEN50126-4:2011.

SINTEF's experience with use of Impact Analysis in relation to safety critical railway applications is mainly as a basis for modifications and upgrade of software and/or hardware for a previously assessed system. The results from such an Impact Analysis are useful with respect to delimiting

which parts of the system that need to be addressed in the safety assessment following a modification/upgrade, and also contributing to the justification why modifications have no impact on other parts of the system. It is recommended that conclusions from an Impact Analysis should have decisions according to the methods as specified (i.e. B.35 in EN50128:2001/2011 and H.2.15 in prEN50126-4, being specific on which parts of the system of concern that need to be re-verified.

Even if prEN50126-4 at the time of writing still is not put into force it is recommended to apply Impact Analysis according to the intention of this prEN50126-4 update (see Appendix H.2.15 of [Ref 23]).

4.3.2 COTS

COTS products are used more and more and the regulation and standards are not precise on how this shall be handled.

The Certification and safety approval process for Railway signalling systems using COTS according to European directives, standards and national regulation is presented. The Interoperability directive [Ref 1] for Railway requires a NoBo for the certification process while the Norwegian regulation normally requires an ISA for non-ERTMS signalling products like interlocking [Ref 45].

This issue only deals with the use of COTS components (HW and SW) that are already certified according to relevant EU directives (as e.g. the EMC directive). For further information regarding different directives, see [Ref 31]) and COTS SW that does not require certification in order to be put on the market.

The relevant directives and standards as referenced in the current memo use different definitions and terms for equipment, item, product, apparatus and component. In this COTS explanation, the word "*component*" is used for: equipment, products, apparatus and products that are commercially available as single functional units. Consequently these components are COTS. Two or more components are named: constituents, subsystems or assemblies. The relevant standards are issued by CENELEC, IEC and ISO.

EN 50128:2001 [Ref 15] and EN 50128: 2011 [Ref 16] has included a definition for COTS SW.

In the 2011 edition of EN 50128, COTS SW is included in the definition for pre-existing software together with a definition of "open source" SW. The standard defines pre-existing SW as: "*All software developed prior to the application currently in question is classed as pre-existing software including*

- COTS and open-source software (source code available to the general public with relaxed or non-existent copyright restrictions),

- software previously developed"

COTS Requirements

Below the COTS Requirements are presented based on requirements in directives and safety standards:

COTS SW: In the new editions of the railway standard EN 50128 COTS SW is included as part of pre-existing software.

Summary of the EN 50128:2011 (ch.7.3.4.7) requirements is presented below:

"*The use of pre-existing software shall be subject to restrictions related to information regarding requirements, assumptions and interfaces that shall be clearly documented.*

Pre-existing software shall be included in the validation process of the whole software.

For software SIL 3 or SIL 4, an analysis of possible failures and their consequences on the whole software shall be carried out, a strategy shall be defined to detect failures to protect the system from these failures. The V&V process shall ensure that the pre-existing software fulfils the allocated requirements, that failures of the pre-existing software are detected and the system where the pre-existing software is integrated into is protected from these failures and that the assumptions about the environment of the pre-existing software are fulfilled. The pre-existing software shall be accompanied by a sufficiently precise and complete description. The description shall include hardware and/or software constraints"

These requirements for COTS SW are not as comprehensive as the total number of requirements for SW in the safety standard.

COTS HW in general: A product must comply with the applicable New Approach and/or Global Approach directives when it is placed on the Community market for the first time and put into service [Ref 24]. A relevant directive is e.g. the EMC directive [Ref 13]. For further information, see www.newapproach.org.

From the Blue Guide [Ref 24]: " *The placing on the market and putting into service can only take place when the product complies with the provisions of all applicable directives, and when the conformity assessment has been carried out in accordance with all applicable directives*"

COTS HW within the Rail domain: Also when COTS HW is included in e.g. a constituent, assembly or subsystem, the constituent, assembly or subsystem has to comply with the current legislation when the certificate for the constituent, assembly or subsystem is issued. Further, it is stated in the Directive 2008/57/EC, Article 5, that subsystems shall comply with the TSIs (Technical Specification for Interoperability, e.g. [Ref 6]) in force at the time of their placing in service, upgrading or renewal, in accordance with this Directive; this compliance shall be permanently maintained while each subsystem is in use.

From Directive 2008/57/EC [Ref 1]: *"EC verification" is the procedure whereby a notified body checks and certifies that the subsystem; complies with the Directive and complies with the other regulations deriving from the Treaty, and may be put into operation.*

A COTS product that does not itself fulfil the requirements, may be found to fulfil the requirements in the system architecture in combination with other products, as long as the system architecture as a whole ensures the fulfilment of the safety requirements.

4.3.3 Cross Acceptance

The cross acceptance life cycle can, according to Engineering Safety Management [Ref 44], be seen as a branch of the life cycle model defined in EN 50126 [Ref 14], starting after the original approval of the generic product or generic application.

The term Cross Acceptance is mentioned in 2008/57/CE [Ref 1], standards and other documents (see below for examples). These documents give different approaches to the process of Cross Acceptance. The intention of this memo is to give a short summary of SINTEF's interpretation of parts of the process of cross acceptance. Further details may be found in SINTEF's position statement on cross acceptance [Ref 41].

The Interoperability Directive (2008/57/CE) addresses cross acceptance in its articles 24 & 25, and the roles of the ISA, supplier and authorities are presented in the following documents:

- TR 50506-1 [Ref 18],
- RFU 2-000-16 [Ref 27]

- Yellow Book Appendix D [Ref 44]
- IRSE ITC Rep. 6 [Ref 49]

SINTEF's practice/recommendations regarding the process of Cross Acceptance, covering the basic principles of the above mentioned references, is given below.

A number of stages for cross acceptance process are defined (see below). These stages are mainly based on the referenced documents above, and they are used to define ISA tasks presented.

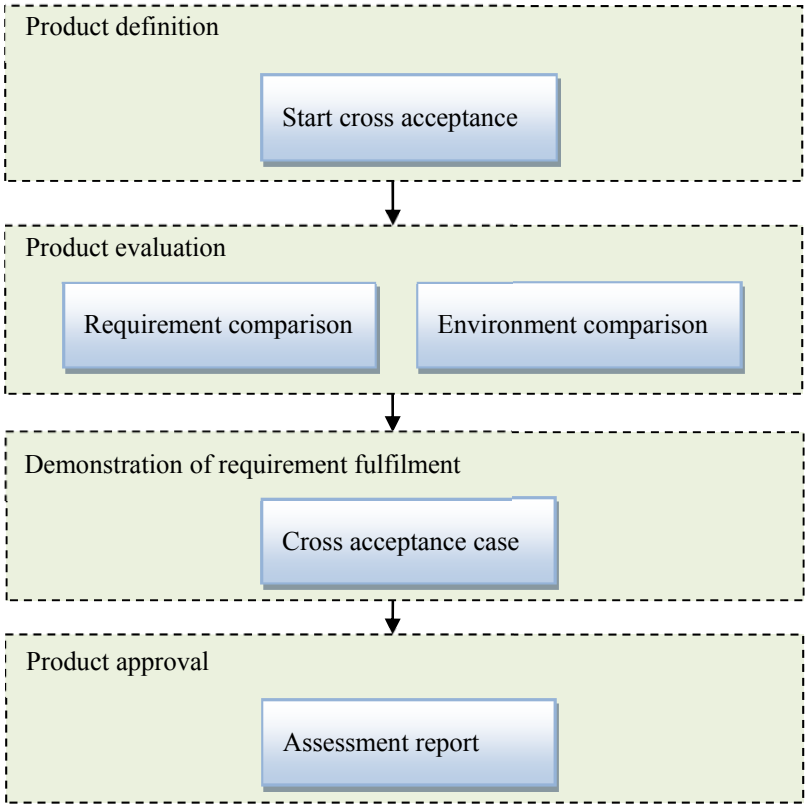

Figure 4 Stages for a cross acceptance process

Start cross acceptance

A reference application should be identified by the supplier that uses substantially the same product in a similar application which has either gone through a formal acceptance process that would be expected of European railways or which has an established record of service which is statistically meaningful.

If product/system names are changed, this should be specified in the early phases of the project.

The scope of what is to be cross accepted should also be clearly defined. In particular it should be clear whether the cross acceptance will be for

- Generic Products (GP) or Generic Application (GA).
- All relevant versions of the product/system to be included in the cross-acceptance

Note: Be aware of regulations and standards that have been changed since the product/system was approved.

Requirements comparison

A differences specification identifying all relevant differences between the requirement specification for the native and target applications should be performed.

Environment comparison

A differences specification, incorporating a hazard identification process identifying all relevant differences between the native and the target applications should be performed.

A difference assessment covering changes in environment and new or modified processes and procedures is required to cater for the differences in application.

Note: See also RFU 2-000-16 [Ref 27], RFU-STR-046 [Ref 30] and RFU-CCS-058 [Ref 28]

Cross acceptance case

A cross acceptance case is required (for GA and SA level) that demonstrates that the Requirement Specification, particularly the RAMS requirements, will be met by the cross accepted product after taking account of changes in environment or new or modified processes and procedures. Any exceptions or special constraints or restrictions shall be highlighted.

Assessment report

An assessment Report shall assess the cross acceptance activities to confirm that the above issues have been satisfactorily undertaken and reported in the cross acceptance case.

5 References

5.1 EU legislation

Ref.	Doc no	Ed	Date
Ref 1.	Directive 2008/57/EC, on the interoperability of the rail system within the community	-	2008-06-17
Ref 2.	Commission Directive 2009/131 of 16 October 2009 amending Annex VII to Directive 2008/57/EC of the European Parliament and of the Council on the interoperability of the rail system within the Community.	-	2009-10-17
Ref 3.	Commission Directive 2011/18 of 1 March 2011 amending Annexes II, V and VI to Directive 2008/57/EC of the European Parliament and of the Council on the interoperability of the rail system within the Community	-	2011-03-02
Ref 4.	2006/860/EC Commission Decision of 7. Of November 2006 on Control-command and signalling (CCS) for high speed rail.	-	2006-11-07
Ref 5.	2006/679/EC Commission Decision of 28 March 2006 on Control-command and signalling (CCS) for conventional rail.	-	2006-10-16
Ref 6.	2012/88/EU Commission Decision of 25 January 2012 on the technical specification for interoperability relating to the control-command and signalling subsystems of the trans-European rail system.	-	2012-02-23
Ref 7.	2010/713/EC Commission Decision of 9 November 2010 on modules for the procedures for assessment of conformity, suitability for use and EC verification to be used in the technical specifications for interoperability adopted under Directive 2008/57/EC of the European Parliament and of the Council	-	2010-11-09
Ref 8.	Directive 96/48/EC, interoperability of the trans-European high-speed rail system	-	1996-07-23
Ref 9.	Directive 2001/16/EC, interoperability of the trans-European conventional rail system	-	2001-03-19
Ref 10.	Directive 2004/50/EC, amending Council Directive 96/48/EC on the interoperability of the trans-European high-speed rail system and Directive 2001/16/EC of the European Parliament and of the Council on the interoperability of the trans-European conventional rail system	-	2004-04-29
Ref 11.	Directive 2004/17/EC of the European Parlament and of the Council, coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors.	-	2004-03-31

Ref. Doc no	Ed	Date
Ref 12. Directive 2004/49/EC of the European Parlament and of the Council of 29 April 2004 on safety on the Community's railways and amending Council Directive 95/18/EC on the licensing of railway undertakings and Directive 2001/14/EC on the allocation of railway infrastructure capacity and the levying of charges for the use of railway infrastructure and safety certification	-	2004-04-30
Ref 13. Directive 2004/108/EC of the European parlament and of the Council of 15 December 2004 on the approximation of the laws of the Member States relating to electromagnetic compatibility and repealing Directive 89/336/EEC	-	2004-12-15

5.2 Standards and CENELEC Technical reports

Ref. Doc no	Ed	Date
Ref 14. EN 50126 Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS).	1	September 1999
Ref 15. EN 50128 Railway applications. Communications, signalling and processing systems. Software for railway control and protection systems.	-	2001-05-15
Ref 16. EN 50128 Railway applications. Communication, signalling and processing systems. Software for railway control and protection systems.	-	2011-07-31
Ref 17. EN 50129 Railway applications – communication, signalling and processing systems – safety related electronic systems for signalling.	-	February 2003
Ref 18. CLC/TR 50506-1 Cross-acceptance.	1.0	November 2007
Ref 19. CLC/TR 50506-2:2009 Railway applications. Communication, signalling and processing systems. Application guide for EN 50129. Safety assurance	-	2010-01-31
Ref 20. ISO/IEC 17050-1 Conformity assessment – Supplier's declaration of conformity – Part 1: General requirements	1.0	2004-09
Ref 21. ISO/IEC 17050-2 Conformity assessment – Supplier's declaration of conformity – Part 2: Supporting documentation	1.0	2004-09
Ref 22. prEN50126-2 Railway applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems approach to safety	-	2012-06-22
Ref 23. prEN 50126-4 Railway Applications - Part 4: Functional Safety- Electrical/ Electronic I Programmable Electronic Systems	-	2011-09-30

5.3 EU guidelines

Ref. Doc no	Ed	Date
Ref 24. Guide to the implementation of directives based on the New Approach and the Global Approach, ISBN 92-828-7500-8 (Blue Guide).	-	September 1999
Ref 25. ERA/GUI/07-2011/INT Guide for the applications of Technical Specifications for Interoperability (TSIs)	1.00	2007-07-13
Ref 26. ERA/GUI/07-2011/INT Guide for the application of Technical Specifications for Interoperability (TSIs) Annex 2 – Conformity assessment and EC verification.	1.00	2011-04-18
Ref 27. RFU 2-000-16, cross acceptance of Safety Case Assessment.	02	April 2006
Ref 28. RFU-CCS-058, Modifications to already certified interoperability constituents.	01	2010-10-28
Ref 29. RFU-PLG-013 Obligation to "Check Conformity" to "Other Regulations Arising from the Treaty"	05	2010-07-20
Ref 30. RFU-STR-046 HW/SW modifications of already certified interoperability constituents	01	2010-02-10
Ref 31. WKD-STR-004 Listing of Directives relating to RFU-PLG-013 (can be found at: http://circa.europa.eu/irc/nbg/nbrail/info/data/en/information/nbrail/RFU.htm)	08	2010-11-01
Ref 32. RFU-STR-001, Content of issued certificates	04	2011-10-05
Ref 33. RFU-STR-045, Relevant and Applicable European Specifications	01	2009-10-14
Ref 34. ERADIS Application Guide; [online] www.era.europa.eu/Document-Register/Pages/ERADIS-application-guide.aspx	-	-

5.4 SINTEF comments/guidelines

Ref. Doc no	Ed	Date
Ref 35. SINTEF Memo, comments to directive 2008/57/EC, 90513021-NOT-2010-03.	1.0	2011-03-16
Ref 36. SINTEF Memo, SIL requirements in 50128-50129, NO90-OL0005.	1.0	2007-10-10
Ref 37. SINTEF Memo, Guidelines for safety documentation, 90513021-NOT-2009-01.	1.0	2011-02-03
Ref 38. SINTEF Memo, Lodge of application guideline	1.0	2010-09-19
Ref 39. SINTEF Memo, CoVeR method guideline, 90513021-NOT-2009-02	4.0	2011-12-16
Ref 40. SINTEF Memo, ERTMS user guide, 90513021-NOT-2011-12	1.0	2011-12-05

Ref. Doc no	Ed	Date
Ref 41. SINTEF memo, Position Statement on Cross Acceptance, 90513021-NOT-2010-14	1.0	2011-08-26
Ref 42. SINTEF memo, Guideline for Applicant and manufacturers certification plans, 90513021-NOT-2011-09	1.0	2011-06-16
Ref 43. Norwegian railway regulations and guidelines issued by ERA, 9051321-NOT-2011-10	2.0	2012-02-27

5.5 Other documents

Ref. Doc no	Ed	Date
Ref 44. Engineering Safety Management, Application Note 4 Independent Safety Assessment, Appendix D (Yellow Book)	2.0	May 2003
Ref 45. Forskrift om krav til jernbanevirksomhet på det nasjonale jernbanenettet (sikkerhetsforskriften). FOR-2005-12-19-1621	-	2005-12-19
Ref 46. SJT, Kommentarer til sikkerhetforskriften, [online] www.sjt.no/no/Lover-og-forskrifter/Kommentarer/Kommentarer-til-sikkerhetsforskriften/#del2	-	-
Ref 47. ISO/IEC Guide 2:2004 Standardization and related activities - General vocabulary	8	2004-11-03
Ref 48. ERA document about practical arrangements for transmitting interoperability documents; www.era.europa.eu/Document-Register/Documents/IU-ERADIS-20090827-Practical%20arrangements for transmitting interoperability documents to ERA - published in CIRCA.pdf	0.1	2009-08-27
Ref 49. Institution of railway signal engineers, international technical committee, 6th report, proposed cross acceptance processes for railway signalling systems and equipment.	-	April 2009
Ref 50. TSIs on ERA homepage; www.era.europa.eu/Core-Activities/Interoperability/Pages/TechnicalSpecifications.aspx	-	-
Ref 51. In the TSIs (Technical Specifications for Interoperability) 08/57-DV44 Reference to standards and other directives under Directive 2008/57/EC	EN02	21.05.2012

6 Abbreviations and definitions

Term	Description
AEIF	European Association for Railway Interpretation
BSI	British Standards Institute, the National Standards Body of the UK
CA	Cross Acceptance
CCO	Control Command and Signalling (on-board)
CCT	Control Command and Signalling (trackside)
CLC	CENELEC
COTS	Commercial Off The Shelf
CoV	Certificate of Verification
Commision decisions	A "Commission decision" only deals with a particular issue and is binding for those to whom it is addressed (e.g. an EU country or an individual company) and is directly applicable (europa.eu).
CR	Conventional Rail
Directives	A "directive" is a legislative act that sets out a goal that all EU countries must achieve. However, it is up to the individual countries to decide how (europa.eu).
DoC	Declaration of Conformity
ERTMS	European Rail Traffic Management System
IA	Impact Analysis
IC	Interoperability Constituent
IEC	International Electrotechnical Commission
ISA	Independent Safety Assessor, according to CENELEC 50126.
ISO	International Organization for Standardization
ISV	Intermediate Statement of Verification
Legislation	There are three basic types of EU legislation: regulations, directives and decisions (europa.eu).
LVD	Low Voltage Directive
NB-Rail	Group of Notified Bodies for the interoperability directives
NoBo	Notified Body
NSA	National Safety Authority
RAMS	Reliability, Availability, Maintainability, Safety
Regulations	A "regulation" is a binding legislative act. A regulation is similar to a national law with the difference that it is applicable in all EU countries. (europa.eu).
RFU	Recommendation For Use
SJS	”Senter for Jernbanesertifisering” (Centre for Railway Certification), a construct within SINTEF ICT to handle Notified Body assignments. See www.sintef.no/sjs
TSI	Technical Specification of Interoperability
WKD	Working document (NB-Rail)