Reference EEIG : 96S126
Chapter Ref : 02S1266-

Distribution date : 30/09/98
Document version : 6-

ERTMS/ETCS
RAMS Requirements Specification

Chapter 2 - RAM

COMMENT: This document (96s1266-) comprises of four **mandatory** chapters:

- Chapter 0 - Introduction Unit 96s1266-
- Chapter 1 - General Aspects 01s1266-
- Chapter 2 - RAM Requirements Specification 02s1266-
- Chapter 3 - Safety Requirements Specification 03s1266-

Informative guidance can be found in 98s7111-

THIS PROJECT IS BEING PART FINANCED BY THE EUROPEAN COMMISSION

VERSIONS & MODIFICATIONS

Version Nb	Date of distribution	Comments on the modification	Responsible for the modification
1-	15/05/1996	First issue	M. B.
2-	30/05/1996	Preliminary Overall RAMS Requirements	M. B.
3-	28/06/1996	+ Preliminary Apportionment	M. B.
4-	19/09/1996	Modified version: accepted comments, compliance with available ERTMS Specifications	M. B.
5-	20/12/1996	Final version: agreed by national railways, integrating the RAMS Workshop with Eurosig agreed results	M. B.
6-	30/09/98	Including the agreed modifications in the database	M. B.

APPROVAL

This document is approved by :

Title	Name	Signature
RAMS Manager	M. BERIEAU	
System Director	F. HEIJNEN	

This document is controlled by :

Title	Name	Signature
Quality Director	A. JANHSEN	

This document is authorised for distribution by :

Title	Name	Signature
Managing Director	J. PELLEGRIN	

TABLE OF CONTENTS
Chapter 2

2.0. REFERENCES

The complete list of References is presented in Chapter 0 - Introduction Unit. The following references apply to this chapter only.

[2.1]	UIC/ERRI	"ETCS - FRS Functional Requirements Specification", Version 4.01 **Mandatory**
[2.2]	EEIG ERTMS USERS GROUP	"ERTMS RAMS -Informative part", 98S711, Version 1 **Informative**
[2.3]	EEIG ERTMS USERS GROUP"	ERTMS Environmental Conditions, Version 5 **Mandatory**
[2.4]	EEIG ERTMS USERS GROUP	"ERTMS/ETCS - Specification of Service Requirements", included in [2.2] **Informative**
[2.5]	EN 50126	"Railway Applications - The Specification and Demonstration of Dependability, Reliability, Availability, Maintainability and Safety (RAMS)", CENELEC **Normative**
[2.6]	EN 50128	"Railway Applications - Software for Railway Control and Protection Systems", CENELEC **Normative**
[2.7]	EN50159-2	"Railway Applications - Requirements for Safety-Related Communication in Open Transmission systems", CENELEC **Normative**

[2.8] EN 29000-3	"Quality Management and Quality Assurance Standards - Guidelines for the Application of ISO9001 to the development, supply and maintenance of software", CEN, First Version, June 1993 **Normative**
[2.9] ISO/IEC DIS 9126	"Information Technology - Software Product and Evaluation - Quality Characteristics and Guidelines for their Use", ISO/IEC JTC-1, Draft, 1990 **Informative**
[2.10]MIL-STD-756B	"Reliability Modelling and Prediction", USA DoD, 18 November 1991 **Informative**
[2.11]MIL-STD-781D	"Reliability Testing for Engineering Development, Qualification and Production", USA DoD, 17 October 1986 **Informative**
[2.12]MIL-STD-785B	"Reliability Program for System and Equipment Development and Production", USA DoD, 15 September 1980 **Informative**
[2.13]MIL-STD-470B	"Maintainability Program for Systems and Equipment", USA DoD, 30 May 1989 **Informative**
[2.14]MIL-STD-471A	"Maintainability Verification/Demonstration/Evaluation", USA DoD, 27 March 1973 **Informative**

[2.15]MIL-HDBK-472	"Maintainability Prediction - Handbook", USA DoD, 24 May 1966 **Informative**
[2.16]MIL-STD-1629A	"Procedures for Performing a Failure Mode, Effects and Criticality Analysis", USA DoD, 24 November 1980 **Informative**
[2.17]EEIG ERTMS USERS GROUP	“Engineering documents and Eurosig documents” List in Contents.xls CDROM 31/07 98 **Mandatory**
[2.18] UIC/ERRI	"ETCS RAM Strategy", Final Draft, 28 July 1995 **Informative**
[2.19] Book	Michael R. Lyu, "Handbook of Software Reliability Engineering", IEEE Computer Society Press, McGraw-Hill, 1996 ISBN 0-07-039400-8 **Informative**

2.1. ERTMS PRELIMINARY RAM RELATED ANALYSES

The preliminary RAM related activities have the purpose of identifying the application environment of the *ERTMS/ETCS* system, in order to recognise the fundamental concepts which the overall RAM requirements have to be based on.

In this preliminary activities will be developed the following aspects:

- *similar systems review*: a list of the existing European Signalling Systems, applicable for providing suitable RAM-related information, is made;
- *preliminary system analysis*: the *ERTMS/ETCS* available documentation is reviewed in order to define, at a preliminary level, the overall system structure and its mission profile and to recognise the system failure conditions.

The outputs of these preliminary RAM related activities constitute the background necessary for defining the Overall RAM Requirements Specification in terms of:

- overall RAM requirements;
- overall demonstration and acceptance criteria;
- overall RAM programme requirements.

The preliminary RAM related activities consist in investigating all the EEIG ERTMS Users Group documentation, relevant to the ERTMS/ETCS specifications, in order to recognise all the functional requirements which may affect, both directly or indirectly, the RAM performances of the system.

The following outputs constitute the preliminary RAM related activities results:

1. **System identification.** The system has to be identified in terms of boundary limits, operation conditions, functions, interfaces and architecture.
2. **Failure conditions.** The failures of the system has to be identified and categorised in order to define appropriate requirements.

This paragraph intends to summarise the experiences carried out by European Railways on technologies similar to those utilised for the *ERTMS/ETCS* system. This references are useful for recognising RAM-related information in existing and operating signalling systems in order to improve the accuracy of the RAM parameters estimation

and to draw up credible and reachable RAM performances for the whole *ERTMS/ETCS* system.

In the following, some of the main experiences in Europe for the technologies employed in the *ERTMS/ETCS* are summarised.

– **Trackside equipment**:

Loop and Short Track circuit:	1. German railways continuous signalling system LZB. 2. French railways TVM-300 and TVM-430 systems.
Balise:	1. Italian railways experimental system ATC (RSDD) installed on the Cremona-Treviglio line. 2. Swedish, Norwegian and French railways KVB system.
Train detection and integrity:	national experiences matured on specific trackside Train Detection and Integrity systems. This is mandatory for the ERTMS Application Level 1 and 2 where Train Detection and Train Integrity are based on existing systems.

– **OnBoard equipment**:

individual experiences matured on specific onboard equipment of national signalling systems: speed control, odometry, ATO/ATP, train integrity (only for Level 3).

– **GSM Radio**:

no experiences are at present recognisable in European Railways at an acceptable experience level. The experience which may be taken under consideration is that one matured in GSM phone communications.

2.1.1 PRELIMINARY RAM ANALYSIS

This preliminary analysis aims at defining the inputs for the Overall *ERTMS/ETCS* RAM Requirements Specification.

Such inputs are composed by the following information:

- technical information for the definition of the *ERTMS/ETCS* mission profile including system boundary limits and operating, environmental and maintenance conditions;
- definition of the failure conditions of the system.

2.1.1.1 System Identification

The architecture of the *ERTMS/ETCS,* identifying its main subsystems and constituents in order to provide an input for the activity of defining the boundary limits of the system and then univocally defining the scope of the RAM Requirements Specification, is defined in the ERTMS Users Group document : 96e0148- [2.17]

2.1.1.2 Mission of the System

The mission of the *ERTMS/ETCS* is to supervise, at different levels of application, the movement of trains ensuring their safe running on different European railway networks [2.17]

2.1.1.3 Operating Conditions: Application Levels

The *ERTMS/ETCS* operating conditions depending of the Application Levels are described in the ERTMS Users Group document : 96e0136- [2.17]

2.1.1.4 Environmental and Maintenance Conditions

The ERTMS Environmental Conditions are described in [2.3].

Maintenance conditions have to constitute a not negligible subset of the *ERTMS/ETCS* mission profile.

In the context of *ERTMS/ETCS*, the reference maintenance conditions has to be identified in that common principle to be taken into account by the national maintenance systems for allowing the operational and/or technical interoperability according to the specific Level of Application.

In particular, an adequate availability of spare parts for *ERTMS* equipped foreign trains has to be ensured by each national maintenance system for *ERTMS* equipped lines.

Other principles, regarding diagnostics, trackside and onboard equipment standstill time constraints and software, are defined in [2.4].

2.1.1.5 Failure Conditions

The following general failure conditions may be defined for the *ERTMS/ETCS* according to the general failure conditions which may be experienced by a generic guided transport system.

- *Immobilising failure*
- *Service failure*
- *Minor Failure*

The above conditions, defined in the Glossary of Chapter 0 - Introductory Unit, constitute the input for establishing the criticality of the *ERTMS/ETCS* failures in reason of their impact on the general failure conditions. On the basis of the RAM strategy, this input will allow to differentiate RAM requirements for failures characterised by different criticality.

2.1.2 RAM V&V: OVERVIEW OF THE RAM PROGRAM

Aim of the RAM Programme is of ensuring, by means of verification, validation and demonstration activities, that the RAM Requirements are properly achieved.

The RAM Programme may be organised in the following subprograms:

- *Reliability Programme:*
  has the purpose of ensuring, during the design and evaluation phases, that the reliability targets are achieved.

- *Maintainability Programme:*
  has the purpose of ensuring, during the design and evaluation phases, that the maintainability targets are achieved.

- *Reliability Demonstration Programme:*
  has the purpose of demonstrating, by means of field testing, that the reliability targets are achieved.

- *Maintainability Demonstration Programme:*
  has the purpose of demonstrating, by means of field testing, that the maintainability targets are achieved.

The *ERTMS/ETCS* RAM Programme shall include, as a minimum, the following activities:

- RAM Programme Planning;
- System conditions and mission profile;
- Periodical RAM Programme reviews;
- Reliability modelling, prediction and apportionment;
- FMECA analysis;
- Software reliability analysis;
- Service dependability analysis and verification;
- Preventive maintenance analysis;
- Corrective maintenance analysis;
- Fault isolation and trouble-shooting plans;
- Reliability development/growth testing programme;
- Maintainability preliminary tests;
- Reliability demonstration tests;
- Maintainability demonstration tests;
- Failure data collection from the field (FRACAS).

The above list defines the minimum requirements for a RAM Programme for a system including hardware and software. A RAM Programme Specification will be tailored to the particular application and the relevant activities will be detailed in the *ERTMS/ETCS* RAM Requirements Specification.

2.2. ERTMS OVERALL RAM REQUIREMENTS

This chapter aims to define the contents of the *ERTMS RAMS Requirements Specification* which state the Overall RAM Requirements for the *ERTMS/ETCS* system.

The Overall RAM Requirements are defined in accordance with *CENELEC EN50126* on the basis of the principles established in [2.18] and of the currently available *ERTMS/ETCS* controlled, where applicable, documentation.

For better addressing system requirements along the text of the document, they are identified by placing the symbol ® at the left margin of the first line of the relevant paragraph. For more information about the use of the requirements marked with ®, refer to §2.3.3.

As stated in the *CENELEC EN50126*, the *ERTMS/ETCS Overall RAM Requirements Specification* is organised in the following four sections:

- Mission Profile identification
- Overall RAM Requirements definition
- Overall RAM Verification and Validation criteria
- Overall RAM Programme requirements

The specified Overall RAM Requirements, including Mission Profile, RAM Requirements, V&V criteria and RAM Programme requirements, will constitute the baseline for apportioning RAM Requirements to the *ERTMS/ETCS* subsystems and for defining the ERTMS Subsystem RAM Requirements Specification.

2.2.1 MISSION PROFILE OF THE ERTMS SYSTEM

The *ERTMS/ETCS* mission profile defines the conditions under which the system is required to accomplish its mission. Those conditions constitute the reference conditions for:

1. defining the *ERTMS/ETCS* system RAM requirements up to the System Requirements Apportionment phase of the system Lifecycle;
2. demonstrating, by analysis and tests, that each specific implementation fulfils the above requirements in all the Lifecycle phases starting from the Design and Implementation phase.

2.2.1.1 Mission of the ERTMS/ETCS

The *ERTMS/ETCS* mission has been identified in § 2.1.1.2..

2.2.1.1.1 ERTMS/ETCS Scope

The target system is defined, in the RAM Requirements Specification context, as follows:

- 1 *ERTMS/ETCS* equipped train plus all the *ERTMS/ETCS* trackside and lineside equipment encountered during 1 hour of trip in the worst case (at the maximum allowed speed in european railways of 500 km/h considering the most complex possible configuration);

It is important to identify in this context the boundary limits of the *ERTMS/ETCS* equipment, establishing in this way the scope of the RAM Requirements defined in this specification.

In § 2.1.1.1. the constituents which compose the *ERTMS/ETCS* categorised in Trainborne and Trackside equipment are identified.

The following functional boundary limits are defined *for ERTMS/ETCS* [2.17]:

1. Traffic regulation does not form part of the system. It forms part of an external system taking into consideration national peculiarities. It is not mandatory for it to be linked with the *ERTMS/ETCS* system. However, an interface between the regulation system and *ERTMS/ETCS* must be provided in order to:

    - communicate to *ERTMS/ETCS*, and ultimately to the train, driving advises drawn up by the regulation intended to optimise the traffic flow;
    - inform the regulation of the train location known to *ERTMS/ETCS* for the real time uptake of its regulation strategies according to environmental conditions.

2. Signal boxes do not form part of the *ERTMS/ETCS*, but they are interfaced with that in order to:

    - communicate to *ERTMS/ETCS*, the positions of points or routes set or, indeed in the cases of levels 1 and 2, block conditions drawn up by existing external systems;

- transmit to the signal box both information known to *ERTMS/ETCS* relating to train location for the purpose of train announcements or monitoring and any other information of concerning for the signal boxes.

3. Other systems interoperable with *ERTMS/ETCS*, like KVB, TVM, LZB, BACC, TBL and so on, do not form part of *ERTMS/ETCS* itself, but an interface between *ERTMS/ETCS* and those systems has to be provided (STM) in order to make as transparent as possible the running of ERTMS equipped trains on not-equipped lines.

4. Additional systems like fault detectors, announcement systems and so on, are to be considered outside *ERTMS/ETCS* and will be provided with appropriate standardised interfaces with this one.

5. The links between the regulation system and signal boxes do not form part of *ERTMS/ETCS*.

2.2.1.2 Environmental Conditions

The environmental conditions under which the *ERTMS/ETCS* is called to operate are specified in the ERTMS Environmental Conditions (97s066 V5-).

The RAM Requirements defined in this specification refer to the above environmental conditions.

Those environmental conditions shall constitute the reference conditions for performing the reliability analyses, for reliability verification and validation, and the reliability demonstration tests planned in the *ERTMS/ETCS RAM Programme Plan*.

2.2.1.3 Maintenance Conditions

The *ERTMS/ETCS* Maintenance Conditions relates to the Maintenance System defined in the *Specifications for "Service and Repair" of the ETCS-System* [2.4].

The document [2.4] adds to the qualitative requirements, partially covered by this specification in § 2.2.2.3.1. and relevant to the construction principles for the *ERTMS/ETCS* installations, general requirements for the *ERTMS/ETCS* Maintenance System as far as the maintenance documentation, the diagnostic and test equipment and the availability of spare parts are concerned.

Furthermore specific requirements for software development and for the *ERTMS/ETCS* documentation are defined in [2.4].

Being [2.4] the unique applicable documentation for identifying the *ERTMS/ETCS* Maintenance Conditions, all the RAM Requirements, both qualitative and quantitative, established in this specification are referred to the principles stated in that document.

As far as the interoperability principles are concerned, the *ERTMS/ETCS* Maintenance System is structured as summarised in following paragraphs.

Trackside Equipment

The *ERTMS/ETCS* Maintenance System, for trackside equipment, is determined by the National Railway Authorities responsible for the specific application. Anyway, the general requirements defined in [2.4] shall be fulfilled.

Onboard Equipment

The *ERTMS/ETCS* Maintenance System, for onboard equipment, has to take into account the interoperability principles. Each National Railway Authority responsible for *ERTMS/ETCS* equipped lines shall define a Maintenance System able to allow faulty *ERTMS/ETCS* equipped vehicles being repaired regardless to their nationality. This shall be accomplished as follows:

1. by providing spare parts for exchangeable *ERTMS/ETCS* onboard equipment items. The availability of spares on stock shall be determined, and declared in terms of stocks location and of parts availability, by the National Railway Authority responsible for the line operation, in order to fulfil the Logistic Support Requirements defined in this specification;
2. by providing specific spare parts for not exchangeable *ERTMS/ETCS* onboard equipment life critical items, whose faults result in an *immobilising failure*. The availability of spares on stock shall be determined, and declared in terms of stocks location and of parts availability, by the National Railway

Authority responsible for the line operation, in order to fulfil the Logistic Support Requirements defined in this specification;

3. by providing facilities for maintain both exchangeable and not exchangeable *ERTMS/ETCS* onboard equipment items in workshop (Depot Level Maintenance). The Subsystems Corrective Maintenance Requirements for Depot Level Maintenance, defined later in this specification, shall be fulfilled.

The RAM Requirements defined in this Specification relates to the general principles defined in [2.4] and in the current paragraph regardless to the specific national application and, consequently, to the specific maintenance system.

For RAM Requirements demonstration purposes, the specific maintenance conditions shall be clearly defined and declared, including the location of stocks and the relevant availability of spares if applicable, at the definition of the contracts stipulated with contractors, sub-contractors and suppliers, for the *ERTMS/ETCS* equipment provision, in the context of each specific national application.

2.2.1.4 Operating Conditions

Each specific implementation of *ERTMS/ETCS* shall fulfil the *Overall RAM Requirements* defined in this specification. For this reason, the *ERTMS/ETCS* subsystems RAM requirements shall relate to the worst possible case, in terms of severity of the operating conditions, which corresponds to the maximum level of implementation of the system.

The *ERTMS/ETCS* operating conditions shall be expressed in terms of the number of elements which may be met by one *ERTMS* equipped train during 1 hour of run, as done in [2.18].

2.2.1.4.1 Reference Conditions for RAM Requirements definition

For RAM Requirements definition purposes, the following conditions may be taken as a reference for the worst case application

- Trip duration = 1 hour
- Train speed = 500 km/h
- Balise Messages = 940
- Radio Messages = 1200
- Continuous Info Points met (RBC) = 10
- Discontinuous Info Points met
- (Switchable and Non-Switchable Locations) = 940
- Population for each Information Point (1 each 1.25 km)
  - *LAT* = 2
  - *LCU* = 1
- Population for each Entry/Exit Point (1 each 12.5 km)
  - *LAT* = 8
  - *LCU* = 1
- Population for each Reset Point (1 each 1 km)
  - *LPT* = 2

The RAM Requirements defined, for the *ERTMS/ETCS* subsystems, on the basis of the above worst case operating conditions guarantee that, at less severe application conditions, the *ERTMS/ETCS* Overall RAM Requirements are certainly fulfilled.

2.2.1.4.2 Reference Conditions for RAM Requirements demonstration

For RAM requirements demonstration purposes, the *ERTMS/ETCS* operating conditions shall be dependent on the specific application.

The system Operating Conditions, relevant to the specific application, shall be clearly defined in the *ERTMS/ETCS RAM Programme Plan* and shall constitute the reference conditions for all the RAM V&V activities performed during the system Lifecycle up to the System Acceptance phase.

Anyway, the application specific operating conditions shall not influence:

- the *ERTMS/ETCS Overall RAM Requirements*;
- the on-board part of the *ERTMS/ETCS Functions RAM Requirements*, defined for the worst case conditions.

On the other hand, the application specific operating conditions shall influence:

- the system conditions which the RAM analysis, relevant to the RAM verification, will be based on;
- the test conditions for the RAM demonstration activities.

2.2.2 SYSTEM RAM REQUIREMENTS

The *ERTMS/ETCS* RAM requirements are derived from [2.18] with some numeric and methodological adjustments.

These adjustments look at improving the *ERRI-A200* targets, defined in [2.18], in compliance with the manufacturing cost constraints, as far as the current technologies allow to do.

Numeric adjustments regard the quantities defined for determining the *ERTMS/ETCS* availability target starting from schedule adherence figures. Those quantities have been redefined as follows:

Train delay

A train is considered delayed when its delay exceed 1 min.

Probability parameters

Probability of having a trip delay for generic causes:		= 15%
Probability of having delay because of technical causes:	40%·15%	= 6%
Probability of having delay caused by Signalling Systems failures:	30% · 6%	= 1,8%
Probability of having delay due to ERTMS failures(P_{ds}):	15%·1,8%	= 0,27%

Time parameters

Average trip normal duration:	T_{dnd} / T_{dn}	=	= 90 min
Average value for the delay (at the end of the trip):	T_{dy}		= 10 min
Average duration of ERTMS failure time for each delayed trip:			= 0,9 T_{dy}

The above figures can be interpreted, where applicable, as schedule adherence requirements for the *ERTMS/ETCS*.

The methodological adjustment regards the contribution of software on the *ERTMS/ETCS* failures. As mentioned in [2.2, §R.1.1.], the operational availability target is subdivided in a not quantifiable contribution, due to software, and a quantifiable one due to hardware faults and transmission errors.

The quantifiable contribution is defined as the 60% of the total downtime of the *ERTMS/ETCS* system and corresponds to the quantitative system requirement to be demonstrated by analysis and testing.

The not quantifiable contribution is relevant to software reliability, which involves systematic aspects only, for which merely qualitative requirements are defined. In particular, the evidence of Quality Management, including the Testing Plan, shall be provided during the design phases and the results of testing, at the different testing levels foreseen for the application, shall demonstrate that the operational availability target is fulfilled, tacking into account the achieved quantifiable contribution.

2.2.2.1 ERTMS Availability Targets

2.2.2.1.1 Schedule Adherence

This quantitative requirement relates both to the probability of having delay on a train running due to *ERTMS/ETCS* unavailabilities and to the allowed mean value of the delay itself.

® The probability of having delay caused by *ERTMS/ETCS* failures shall be not greater than ***0.0027***.

® The allowed average delay per train due to *ERTMS/ETCS* failures, at the end of an average trip of duration of 90 min., shall be not greater than ***10 min***.

2.2.2.1.2 Operational Availability

The operational availability target is determined utilising of the formula defined in [2.2, § R.1.1.5]. on the basis of the figures stated in § 2.2.2.:

$$A_o = \frac{T_{op}}{T_{op} + T_{fault}} = \frac{T_{dn} + P_{ds} \cdot \left(T_{dy} - 0.9 \cdot T_{dy}\right)}{T_{dn} + P_{ds} \cdot T_{dy}} = \frac{90 + 0.0027 \cdot 0.1 \cdot 10}{90 + 0.0027 \cdot 10} = 0.99973$$

® The operational availability of the *ERTMS/ETCS*, due to all the causes of failure, shall be not less than ***0.99973***.

The quantifiable contribution, which represents the availability figure to be quantitatively demonstrated, corresponds to the 60% of the *ERTMS/ETCS* unavailabilities:

$$A_o = \frac{T_{op}}{T_{op} + T_{fault}} = \frac{T_{dn} + 0.6 \cdot P_{ds} \cdot \left(T_{dy} - 0.9 \cdot T_{dy}\right)}{T_{dn} + 0.6 \cdot P_{ds} \cdot T_{dy}} = \frac{90 + 0.6 \cdot 0.0027 \cdot 0.1 \cdot 10}{90 + 0.6 \cdot 0.0027 \cdot 10} = 0.99984$$

® The *ERTMS/ETCS* quantifiable contribution to operational availability, due to hardware failures and transmission errors, shall be not less than ***0.99984***.

2.2.2.1.3 Downtime Requirements

The downtime requirements are defined in terms of the allowed mean downtimes which correspond to the operational availability targets defined in § 2.2.2.1.2.

These downtimes, useful for demonstration purposes, can be calculated as follows, expressed in hours on a *per year* basis:

$$DT = \left(1 - A_O\right) \cdot 8760$$

2.2.2.2 ERTMS Mission Reliability Targets

The *ERTMS/ETCS* Mission Reliability Targets are composed of qualitative and quantitative requirements. Quantitative requirements are expressed in terms of Mean Time Between Failures (MTBF) and are differentiated in reason of the criticality (Immobilising, Service or Minor) of the failures under consideration. The following prerequisites are identified:

1. Immobilising Failures shall not exceed the 10% of the total amount of failures which affect the system operation (contributing to Operational Availability);
2. Service Failures shall not exceed the 90% of the total amount of failures which affect the system operation (contributing to Operational Availability);
3. Minor Failures shall contribute to an availability target not less than 0,995;
4. the Onboard Equipment contribution is stated in the 4,34% of the total system failures (see [2.2])
5. the Trackside Centralised Equipment contribution is stated in the 0,08% of the total system failures (see [2.2]);
6. the Trackside Distributed Equipment (LNS) contribution is stated in the 95,58% of the total system failures);
7. the Mean Time To ReStore (MTTRS) of the Onboard Equipment (ONB) is 1,737 hours, the appropriate value for ensuring that the Onboard Equipment standstill time is less than 4 hours in the 90% of the unscheduled repairs, assuming exponentially distributed repair time (see §2.2.2.3.3.);
8. the Mean Time To ReStore (MTTRS) of the Trackside Centralised Equipment (TRK) is 0,869 hours, the appropriate value for ensuring that the Trackside Equipment standstill time is less than 2 hours in the 90% of the unscheduled repairs, assuming exponentially distributed repair time (see §2.2.2.3.3.).
9. the Mean Time To ReStore (MTTRS) of the Trackside Distributed Equipment (LNS) is 1,737 hours, the appropriate value for ensuring that the Trackside Equipment standstill time is less than 4 hours in the 90% of the unscheduled repairs, assuming exponentially distributed repair time (see §2.2.2.3.3.).

2.2.2.2.1 Qualitative Requirements

Reliability qualitative requirements regard mainly the requirements for the implementation of a *ERTMS/ETCS* Reliability Programme as a subset of the system RAM Programme.

Reliability qualitative requirements are particularly critical for the *ERTMS/ETCS software* in that they represent the only reliability requirements which can be defined and demonstrated to be accomplished.

Specific qualitative requirement, related to the *ERTMS/ETCS* design criteria at system level, are also defined.

The following reliability qualitative requirements are defined at the overall RAM Requirements level:

® a System Reliability Programme, subset of the RAM Programme, shall be implemented and a System Reliability Programme Plan, subset of the RAM Programme Plan, shall be produced and maintained in accordance to the *RAM Programme Plan Requirements* specified in § 2.4 and to the System Quality Plan of the *ERTMS/ETCS*.

® Software Quality Assurance and V&V Programs shall be implemented in compliance with the international standards [2.6 and 2.8,] and, in particular, with [2.6] as far as software integrity is concerned. Software Quality Assurance and V&V Plans, shall be produced and maintained in accordance to the above standards.

® no one single fault shall cause *immobilising failures* as defined in § 2.2.2.2.2.

® when redundancies are utilised in order to prevent single failures to cause *immobilising failures*, appropriate measures which guarantee the independence of the redunded equipment shall be adopted and documented. For redunded safety-related functions, a Common Cause Failures Analysis shall be performed.

2.2.2.2.2 Immobilising Failures

Immobilising Failures are defined, for the *ERTMS/ETCS* context, in the Glossary contained in Chapter 0.

The purpose of this paragraph is to identify the *ERTMS/ETCS* system level failures which can result in one of the above conditions and to define, for these failures, appropriate reliability targets.

In the *ERTMS/ETCS* context, *Immobilising Failures* may be identified (see [2.2]), as all *the ERTMS/ETCS* failures which cause two or more trains to be switched in *on sight* mode.

The relevant *mission* is then defined as the *ERTMS/ETCS* operation in absence of *Immobilising Failures* and, for that mission, the following reliability requirements are defined:

® The Mean Time Between Immobilising hardware Failures *MTBF-I_{ONB}*, defined for Onboard equipment, shall be not less than ***$2.7 \cdot 10^6$ hours***.
® The Mean Time Between Immobilising hardware Failures *MTBF-I_{TRK}*, defined for Trackside Centralised equipment, shall be not less than ***$3.5 \cdot 10^8$ hours***.
® The Mean Time Between Immobilising hardware Failures *MTBF-I_{LNS}*, defined for Lineside Distributed equipment, shall be not less than ***$1.2 \cdot 10^5$ hours***.

2.2.2.2.3 Service Failures

Service Failures are defined, for the *ERTMS/ETCS* context, in the Glossary contained in Chapter 0.

The purpose of this paragraph is to identify the *ERTMS/ETCS* system level failures which can result in one of the above conditions and to define, for these failures, appropriate reliability targets.

In the *ERTMS/ETCS* context, *Service Failures* may beidentified as all *the ERTMS/ETCS* failures which cause the nominal performance of one or more trains to be reduced and/or at most one train to be switched in *on sight* mode (see [2.2]).

The relevant *mission* is then defined as the *ERTMS/ETCS* operation in absence of *Service Failures* and, for that mission, the following reliability requirements are defined:

® The Mean Time Between Service hardware Failures *MTBF-S_{ONB}*, defined for Onboard equipment, shall be not less than ***$3.0 \cdot 10^5$ hours***.
® The Mean Time Between Service hardware Failures *MTBF-S_{TRK}*, defined for Trackside Centralised equipment, shall be not less than ***$4.0 \cdot 10^7$ hours***.
® The Mean Time Between Service hardware Failures *MTBF-S_{LNS}*, defined for Lineside Distributed equipment, shall be not less than ***$1.4 \cdot 10^4$ hours***.

2.2.2.2.4 Minor Failures

Minor Failures are defined, for the *ERTMS/ETCS* context, in the Glossary contained in Chapter 0.

The purpose of this paragraph is to identify the *ERTMS/ETCS* system level failures which can result in the above condition and to define, for these failures, appropriate reliability targets.

The relevant *mission* is then defined as the *ERTMS/ETCS* operation in absence of *Minor Failures* and, for that mission the following reliability requirements are defined:

® The Mean Time Between Minor hardware Failures $MTBF\text{-}M_{ONB}$, defined for Onboard equipment, shall be not less than ***8.0·10³ hours***.
® The Mean Time Between Minor hardware Failures $MTBF\text{-}M_{TRK}$, defined for Trackside Centralised equipment, shall be not less than ***1.0·10⁵ hours***.
® The Mean Time Between Minor hardware Failures $MTBF\text{-}M_{LNS}$, defined for Lineside Distributed equipment, shall be not less than ***3.6·10² hours***.

The above requirements are referred to the whole system, as defined in §2.2.1.1.3., and represent the mean time between any required corrective maintenance action not involving a degradation of the system performance.

2.2.2.3 ERTMS Maintainability Targets

2.2.2.3.1 Qualitative Requirements

The purpose of Maintainability Qualitative Requirements is to address the design toward solutions which allow to facilitate both corrective and preventive maintenance actions to be performed on the *ERTMS/ETCS* equipment and trouble-shooting and modification activities to be performed on the *ERTMS/ETCS* software modules.

2.2.2.3.1.1 Hardware

Accessibility: The *ERTMS/ETCS* equipment shall be designed in such a way that all its parts and related connections permit inspection, repair, revision and replacement, taking into account the dimensions of the required equipment.

Dismounting: During a maintenance action it shall be possible to disassemble and to take out any item without being

compelled to involve other items not directly related to the specific maintenance action.

Handiness: The *ERTMS/ETCS* equipment subjected to disassembling related to a maintenance action shall be designed in order to be easily transportable. They shall not exceed the weight established by the national regulatory authorities in reason of the number of operators assigned to its movement. They shall be fitted out with appropriate devices enabling actions carried out with hooks, anchor plates, loading forks, etc.

Cleaning-friendliness: Compartments, equipment and so on, being parts of *ERTMS/ETCS* shall be designed in order to facilitate at a maximum all external cleaning actions.

Standardisation : Early in the design phase of the *ERTMS/ETCS* system Lifecycle, solutions shall be applied leading to the lowest possible diversification of the *ERTMS/ETCS* system components. Parts interchangeability shall be maximised making use of standardised elements where possible.

Interchangeability: An item can be removed and another item installed in its place without affecting any equipment characteristics. The replacement shall be compatible in form, fit and function.

Testability: Each item belonging to the *ERTMS/ETCS* system shall be provided of appropriate testability features in compliance with [2.4].

2.2.2.3.1.2 Software

Analysability: The *ERTMS/ETCS* software shall be designed in order to minimise the effort requested for tracing defects or failure causes and for identifying the parts to be modified.

Changeability: The activities of modification and of defect removal shall be facilitated, and the effort needed for adapting software to environment changing (i.e., operating system, hardware architecture, etc.) shall be minimised.

Stability: The risk that undesirable effects may occur as a consequence of a modification shall be minimised.

Testability: Software testing and validation activities consequent to a modification shall be facilitated as much as possible.

2.2.2.3.2 Preventive Maintenance

For Preventive Maintenance, at system level, qualitative requirements only are defined.

® Each Contractor/Sub-contractor/Supplier responsible for the provision of *ERTMS/ETCS* equipment or parts, shall declare, providing appropriate documentation, the Preventive Maintenance Requirements necessary for ensuring the required RAM Performance, as defined in this specification, for the equipment under its competency.

® The Preventive Maintenance Requirements, defined by each Contractor/Sub-contractor/Supplier shall comply with the Logistic Support Requirements defined in this specification and shall require the agreement of the Customer Project Management for becoming effective requirements to be verified and demonstrated in the further phases of the System Lifecycle by means of appropriate activities of the RAM Programme.

2.2.2.3.3 Corrective Maintenance

The Corrective Maintenance Requirements are subdivided in two categories: *General Quantitative Requirements* and *Specific Quantitative Requirements*.

- *General Corrective Maintenance Quantitative Requirements* regard the maximum standstill times tolerable in the case of any unscheduled repairs; they represent operative requirements [2.4].
- *Specific Corrective Maintenance Quantitative Requirements* regard the allowed times for detecting/locating faults, replacing faulty modules and restarting the system interested by the failure occurred; they represent design requirements

to be fulfilled and demonstrated by the Contractor/Sub-Contractor(s)/Supplier(s) responsible for providing *ERTMS/ETCS* equipment.

The following *General Corrective Maintenance Quantitative Requirements* are defined for *ERTMS/ETCS* (see [2.4]):

Maximum standstill time tolerable for the ***90%*** of the unscheduled repairs of *onboard* equipment:	***4 hours***
Maximum standstill time tolerable for the ***90%*** of the unscheduled repairs of *trackside centralised* equipment:	***2 hours***
Maximum standstill time tolerable for the ***90%*** of the unscheduled repairs of *trackside distributed (lineside)* equipment:	***4 hours***

The following Specific Corrective Maintenance Quantitative Requirements are defined for ERTMS/ETCS:

® The maximum amount of time for detecting/isolating/replacing a faulty item shall not exceed, in the ***90%*** of the cases, the ***65%*** of the maximum tolerable standstill time defined for the relevant equipment

2.2.2.4 ERTMS Logistic Support Constraints

2.2.2.4.1 Maintenance Cost

The maintenance cost constraints shall be defined by the national regulatory authorities responsible for each specific application of *ERTMS/ETCS* in reason of the Level of Application chosen.

The *ERTMS/ETCS* maintenance cost constraints shall be expressed in terms of the maximum allowed percentage of the whole system Lifecycle Cost to be expended for:

- training of the maintenance personnel;
- preventive, scheduled and corrective maintenance actions including the cost of the personnel employed;
- travel costs sustained for reaching the maintenance sites;
- spare parts acquisition, provision and storage;
- assistance contracts with suppliers of commercial computer systems.

® The maintenance cost of *ERTMS/ETCS* shall not exceed the ***2%*** per year of the System acquisition Cost, for a duration of ***30 years*** of the *ERTMS/ETCS* Lifecycle.

2.2.2.4.2 Supply and Administrative Delay

The fulfilment of the constraints related to the maximum allowed delays on maintenance actions, due to administrative causes, is responsibility of the national regulatory authorities responsible for each specific application of *ERTMS/ETCS* in reason of the Level of Application chosen.

The following constraints need to be guaranteed at least in the ***90%*** of the occurrences, for ensuring the effective fulfilment of the technical RAM requirements:

1. The maximum amount of time necessary to inform a maintenance staff for performing on-site maintenance action, cannot exceed the ***5%*** of the maximum tolerable standstill time defined for the interested equipment. This requirement is valid both if the advice to the maintenance staff is automatically produced by the diagnostics and if it is given manually.
2. The maximum amount of time necessary to reach the maintenance site cannot exceed the ***30%*** of the maximum tolerable standstill time defined for the interested equipment.

2.2.2.4.3 Spare Parts Availability

The Contractor shall guarantee the supplying of spare parts for all *the ERTMS/ETCS* equipment for the entire system Lifecycle duration agreed by the parts of the contract.

The Contractor shall submit for approval a Parts Provisioning Plan to the Customer.

The Parts Provisioning Plan shall detail, for each of the items identified by means of the System Analysis (see § 2.4.1.7.), the way by which the Contractor shall guarantee the availability of Spare Parts in reason of the relevant MTBF.

The constraints related to the availability of Spare Parts *on stock* shall be defined by the national regulatory authorities responsible for each specific application of *ERTMS/ETCS* in reason of the Level of Application chosen.

When a national railway will accept *ERTMS/ETCS* equipped foreign vehicles on its *ERTMS/ETCS* equipped lines, it shall ensure, jointly with the train operator, that spare

parts are available for foreign vehicles so that depot level maintenance actions can be performed when failures to the *ERTMS/ETCS* equipment occur. The relevant details shall be agreed by the railways called to exchange vehicles.

2.2.3 RAM VERIFICATION AND VALIDATION

In this paragraph, the basic principles for the demonstration of compliance with the System RAM Requirements for the *ERTMS/ETCS* system are defined in accordance to [2.5], [2.6], and to the *ERTMS/ETCS* Validation Procedures.

Specifities for the RAM Verification and Validation, including the relevant management structure, shall be agreed between the parts in specific supply contracts for specific national applications on the basis of the relevant national regulations and of the national Railway Authorities needs.

The above specificities shall be clearly defined and declared in the specific supply contracts.

At system level, the RAM Validation is based on the evaluation of the RAM Demonstration Test results or, where testing is not applicable for practical or economical reasons, of the documental proof of the fulfilment of RAM targets, in order to establish the compliance with the System RAM Requirements, as defined in the present section of the *ERMTS Control/Command* RAM Requirements Specification.

Details about the RAM Validation will be provided in the context of the *ERTMS/ETCS* Test Specification including:

- Test duration
- Test environment
- Test conditions
- Equipment subject to test
- Confidence intervals for testing
- Other demonstration methods and details for not cost-effectively testable equipment (e.g. documental proof)
- Organisational structure of the Test Case (e.g. subjects responsible for maintenance, logistic support, and so on)
- Roles and responsibilities
- Other details

The output of this activity is the Validation of the system as far as the RAM aspects are concerned.

2.2.3.1 Acceptance Criteria

2.2.3.1.1 Reliability Acceptance Criteria

The reliability acceptance is conditioned to the adequacy of the RAM Validation Report, issued by the Validation Team, which purpose is to document the success, or the unsuccess, of the Reliability Demonstration Tests or of the documental proof, where applicable, as stated in the *ERTMS/ETCS* Test Specification.

The Reliability Demonstration Tests shall be considered as successful if the following conditions are respected:

® the *ERTMS/ETCS* Qualitative Mission Reliability Targets defined at § 2.2.2.2.1. and the Quantitative Mission Reliability Targets defined at § 2.2.2.2.2., § 2.2.2.2.3. and § 2.2.2.2.4. are fulfilled;
® all the *ERTMS/ETCS* equipment have been operated in the specified conditions (as defined in § 2.2.1.1., § 2.2.1.2., § 2.2.1.3. and § 2.2.1.4.2.) for the specified testing time.

The documental proof shall be considered as successful if also all the relevant conditions stated in the Test Specification are fulfilled.

If the Reliability Demonstration Test or the documental proof, where applicable, are unsuccessful, the Validation Team will identify the responsibility of the non-conformity and will require appropriate corrective actions.

In case the responsibility is recognised in the system operator activity, for instance due to wrong or missing preventive maintenance, any intervention of the Contractor is required and the relevant corrective actions shall be responsibility of the system operator.

Otherwise, the Contractor responsible for the system provisioning shall require to the appropriate Sub-Contractor(s)/Supplier(s) and, if necessary, shall perform, appropriate modifications able to improve the System Reliability for complying with the specified targets.

The measures to be adopted for performing the above modifications shall be proposed by the Contractor responsible and agreed by the Customer Project Management.

2.2.3.1.1.1 Chargeable failures

The following failures shall be considered as chargeable, for the Contractor, for the Reliability Demonstration:

- failures occurred during the system operation under the rated conditions;
- failures due to wrong operation, unappropriate maintenance actions or uncorrect test procedures clearly traceable to Sub-Contractor(s)/Supplier(s) deficiences;
- missed planning of scheduled maintenance of items for which a time limit is foreseen in the Preventive Maintenance Plan.

2.2.3.1.1.2 Unchargeable failures

The following failures shall be considered as not chargeable, for the Contractor, for the Reliability Demonstration:

- induced faults;
- faults due to human errors;
- failures to accidental events;
- faults occurred during the operation out of the rated system conditions;
- degrade of items subject to wear for which sheduled maintenance actions has been performed in a wrong way or have not been performed.

2.2.3.1.2 Maintainability Acceptance Criteria

The maintainability acceptance is conditioned adequacy of the RAM Validation Report, issued by the Validation Team, which purpose is to document the success, or the unsuccess, of the Maintainability Demonstration Tests.

The Maintainability Demonstration Tests shall be considered as successful if the following conditions are respected:

® the *ERTMS/ETCS* Qualitative Maintainability Requirements defined at § 2.2.2.3.1. are fulfilled

® the Quantitative Preventive Maintenance Targets agreed as described at § 2.2.2.3.2. by the Project Management as a result of the Preventive Maintenance Analysis and the Quantitative Corrective Maintenance Targets,

both defined at § 2.2.2.3.3. and resulting from the Corrective Maintenance Analysis, are fulfilled;

® all the *ERTMS/ETCS* equipment have been operated in the specified conditions (as defined in § 2.2.1.1., § 2.2.1.2., § 2.2.1.3. and § 2.2.1.4.2.) for the specified testing time.

If the Maintainability Demonstration Tests are unsuccessful, the Validation Team will identify the responsibility of the non-conformity and will require appropriate corrective actions.

In case the responsibility is recognised in the system operator activity, for instance due to not sufficient skills of the maintenance personnel, any intervention of the Contractor is required and the relevant corrective actions shall be responsibility of the system operator.

Otherwise, the Contractor responsible for the system provisioning shall require to the appropriate Sub-Contractor(s)/Supplier(s) and, if necessary, shall perform, appropriate modifications able to improve the System Maintainability for complying with the specified targets.

The measures to be adopted for performing the above modifications shall be proposed by the Contractor responsible and agreed by the Customer Project Management.

2.2.3.1.3 Software Acceptance Criteria

The quantitative contribution of Software Reliability to the *ERTMS/ETCS* RAM, and Safety, performance is taken into account during one or more of the following activities of the RAM, and Safety, Programme:

- reliability and maintainability demonstration tests;
- operational availability assessment;
- system safety demonstration.

In none of the above cases the quantitative measure of the Software Reliability shall constitute a direct constraint for the software acceptance.

The quantitative estimation, or measure, of the Software Reliability shall only affect the whole system acceptance, as it impacts the system operational availability and safety.

Several qualitative RAM targets shall instead be reached during the software development according to the IL assigned to the *ERTMS/ETCS* functions.

Therefore, the Contractor responsible for the system provisioning shall collect the appropriate Sub-Contractor(s)/Supplier(s) documentation, to be agreed by the Customer Project Management, for demonstrating that:

1. Throughout the Software Lifecycle, the parties involved in V&V activities are independent of those involved in development activities, to the extent required by the Software Integrity Level.
2. Definition of the responsibilities satisfies RAM Programme Plan and Software Quality Assurance (SQA) Plan.
3. The lifecycle model for the development of software is in accordance with the model detailed in the Software Quality Assurance Plan, where for each phase the following items have to be defined:
   - activities and elementary tasks;
   - entry and exit criteria;
   - inputs and outputs
   - major quality activities
   - organisational unit responsible for each activity and elementary task.
4. All documents are structured to comply with the RAMS Programme Plan and the Software Quality Assurance Plan. Traceability of them is provided for by each document having a unique reference number and a defined and documented relationship with other documents.
5. Software requirements are complete, clear, precise, unequivocal, verifiable, testable, maintainable, feasible and traceable back to all documents throughout the system lifecycle.
6. The software architecture achieves the software requirements to the extent required by software integrity level;
7. Safety-related aspects are limited in well defined functional areas. The development of these functional areas is submitted to the most rigorous control, defined by the Contractor, and agreed by the Customer Project Management.
8. The complexity and size of the software is kept to a minimum, and satisfies the required Software Integrity Level. Their value is monitored using some static software metrics.

9. Each software module is readable, understandable and testable, and it has been developed in accordance with the required integrity level allocated to the specific function.
10. The programming language and the translator/compiler have integrity features to the extent required by the software integrity level.
11. Operational profile and test environment are defined on the basis of estimated real life conditions, and the final effects of modification on the input space have been examined and evaluated.
12. The degree of test coverage satisfies the required software integrity level and it complies with everything defined by the Contractor and agreed by the Customer Project Management.
13. Software failures data have been rigorously collected and they have been classified according to their effects on system safety and quality of service. The corrective actions have been effective to reach overall RAMS requirements.
14. Problem reporting , corrective action management and changes control comply with the Configuration Management Plan, established by the Contractor, and agreed by Customer Project Management.
15. Maintainability levels facilitate the corrective maintenance actions to reach, during the operational life of the system, the required availability target.
16. During the operational life of the system, the adaptive and perfective maintenance actions have been planned to be carried out off-line. The effects of the modification or change will be analysed in order to maintain the actual performances of the system.

If these qualitative requirements are not met, the Contractor responsible for the system provisioning shall require to the appropriate Sub-Contractor(s)/Supplier(s) and, if necessary, shall perform, appropriate modifications and/or shall produce additional documentation able to improve software quality for complying with the specified targets.

The measures to be adopted for performing the above modifications shall be proposed by the Contractor responsible and agreed by the Customer Project Management.

2.2.3.1.4 Availability Acceptance Criteria

The availability acceptance is conditioned to the adequacy of the RAM Validation Report, issued by the Validation Team, which purpose is to document the success, or the unsuccess, of the Operational Availability Assessment aimed to

evaluate the *ERTMS/ETCS* Operational Availability on the basis of the actual system Reliability and Maintainability performance resulting from the Reliability Demonstration Tests, the Maintainability Demonstration Test and the Software Acceptance Tests.

The Operational Availability Assessment takes into account the contribution of the *ERTMS/ETCS* software by means of appropriate metrics allowing to charge software failures in the Operational Availability Computation.

The *ERTMS/ETCS* Operational Availability can be Validated if the following conditions are respected:

- the *ERTMS/ETCS* Availability Targets defined at § 2.2.2.1.1., § 2.2.2.1.2. and § 2.2.2.1.3. are fulfilled;
- all the *ERTMS/ETCS* equipment have been operated in the specified conditions (as defined in § 2.2.1.1., § 2.2.1.2., § 2.2.1.3. and § 2.2.1.4.2.) for the specified testing time during the Reliability and Maintainability Demonstration Tests and during the Software Acceptance Tests.

If the Operational Availability Assessment does not result in the system Operational Availability Validation, the Validation Team will identify the responsibility of the non-conformity and will require appropriate corrective actions.

In case the responsibility is recognised in the system operator activity, for instance due to a bad organisation of the Logistic Support, any intervention of the Contractor is required and the relevant corrective actions shall be responsibility of the system operator.

Otherwise, the Contractor responsible for the system provisioning shall require to the appropriate Sub-Contractor(s)/Supplier(s) and, if necessary, shall perform,appropriate modifications able to improve the System Availability for complying with the specified targets.

The measures to be adopted for performing the above modifications shall be proposed by the Contractor responsible and agreed by the Customer Project Management.

2.2.3.2 V&V Program

The RAM Verification and Validation is carried out, at system level, by means of appropriate activities, and relevant documentation, defined in the RAM Demonstration Programs constituting subsets of the System RAM Programme, as specified in the § 2.4.

2.2.3.2.1 Reliability Verification and Validation

The activities relevant to the Reliability Verification and Validation deal with Reliability Demonstration Tests and shall be carried out according to the Reliability Demonstration Plan.

The Reliability Demonstration Plan shall comply with the applicable sections of the *ERTMS/ETCS* Validation Procedures.

The Reliability Demonstration Plan shall be established by each contractor and agreed by the Project Management in the context of the activities relevant to the *ERTMS/ETCS* RAM Programme (see § 2.4.).

2.2.3.2.2 Maintainability Verification and Validation

The activities relevant to the Maintainability Verification and Validation deal with Maintainability Demonstration Tests and shall be carried out according to the Maintainability Demonstration Plan.

The Maintainability Demonstration Plan shall comply with the applicable sections of the *ERTMS/ETCS* Validation Procedures.

The Maintainability Demonstration Plan shall be established by each contractor and agreed by the Project Management in the context of the activities relevant to the *ERTMS/ETCS* RAM Programme (see § 2.4.).

2.2.3.2.3 Software Verification and Validation

The activities relevant to the Software Verification and Validation, as far as RAM aspects are concerned, deal with Software Validation Tests and shall be carried out according to the Software Validation Plan.

The Software Validation Plan shall comply with the applicable sections of the *ERTMS/ETCS* Validation Procedures.

The Software Validation Testing Plan shall be established by each contractor and agreed by the Project Management in the context of the activities relevant to the *ERTMS/ETCS* Software Quality Assurance Plan.

2.2.3.2.4 Availability Assessment

As far as Operational Availability is concerned, the Verification and Validation activities consist in performing an Operational Availability Analysis on the basis of the results of the Reliability and Maintainability Tests and of the Software Acceptance Tests.

The Operational Availability Analysis shall comply with the applicable sections of the *ERTMS/ETCS* Validation Procedures.

The Operational Availability Analysis shall be carried out in compliance with the requirements defined in § 2.4.4..

2.3. APPORTIONMENT OF RAM TARGETS

In this section, an apportionment of the ERTMS/ETCS Operational Availability target, defined in § 2.2.2.1.2. of this specification, is performed.

2.3.1 ERTMS FUNCTIONAL ANALYSIS

<Intentionally deleted>

2.3.2 CONTRIBUTIONS TO THE ERTMS/ETCS OPERATIONAL AVAILABILITY

Aim of this section is to define the contributions to the quantifiable *ERTMS/ETCS* Overall Operational Availability Target due to the different causes of failure, dealing with hardware and transmissions, in reason of their severity.

These contributions define constraints, related to the maximum tolerable impact of each type of failure, for the RAM functional apportionment.

2.3.2.1 Hardware Contribution

The contribution due to hardware to the system unavailabilities is stated as the 90%.

As a consequence the hardware contribution A_{HW} to the quantifiable portion of the operational availability A_{OP} is established on the basis of the following formula:

$$A_{HW} = \frac{T_{op}}{T_{op} + T_{fault}} = \frac{\left[\left(1 - P_{ds}\right)T_{dn} + P_{ds}T_{dnd}\right]}{\left[\left(1 - P_{ds}\right)T_{dn} + P_{ds}T_{dnd}\right] + 0.9 \cdot 0.6 \cdot P_{ds} \cdot 0.9 \cdot T_{dy}} =$$

$$= \frac{90}{90 + 0.9 \cdot 0.6 \cdot 0.0027 \cdot 0.9 \cdot 10} = 0.999854$$

® The *ERTMS/ETCS* quantifiable contribution to operational availability, due to hardware failures, shall be not less than ***0.999854***.

2.3.2.1.1 Immobilising Failures

® The maximum contribution of IMMOBILISING hardware failures to the *ERTMS/ETCS* unavailabilities shall not exceed the ***10%***.

As a consequence, the maximum downtime due to hardware IMMOBILISING failures shall not exceed the 10% of the hardware related *ERTMS/ETCS* downtime.

Being

$$DT_{HW} = 1.279\text{h} = 1 \text{ hour } 17 \text{ minutes}$$

the mean downtime per year due to hardware, then

$$DT_{HW,I} = 0.1 \cdot 1.279 \text{ h} = 8 \text{ minutes}$$

the mean downtime per year tolerable as consequence of IMMOBILISING failures.

The corresponding availability target is calculated as follows

$$A_{HW,I} = 1 - DT_{HW,I} / 8760 = 0.9999854$$

® The minimum tolerable availability, related to hardware IMMOBILISING failures, shall be ***0.9999854***

2.3.2.1.2 Service Failures

® The maximum contribution of Service hardware failures to the *ERTMS/ETCS* unavailabilities shall not exceed the ***90%***.

As a consequence, the maximum downtime due to hardware SERVICE failures shall not exceed the 90% of the hardware related *ERTMS/ETCS* downtime.

Being

$$DT_{HW} = 1.279 \text{ h} = 1 \text{ hour } 17 \text{ minutes}$$

the mean downtime per year due to hardware, then

$$DT_{HW,S} = 0.9 \cdot 1.279 \text{ h} = 1.151 \text{ h} = 1 \text{ hour } 9 \text{ minutes}$$

the mean downtime per year tolerable as consequence of SERVICE failures.
The corresponding availability target is calculated as follows

$$A_{HW,S} = 1 - DT_{HW,S} / 8760 = 0.99987$$

® The minimum tolerable availability, related to hardware SERVICE failures, shall be ***0.99987***

2.3.2.1.3 Minor Failures

This requirement is not related to the *ERTMS/ETCS* Operational Availability in that it does not influence service by definition.

Anyway an appropriate availability requirement has to be defined also for this category of failures in order to avoid an excessive request of logistic support for not service critical subsystems.

The following requirement is therefore defined:

® The minimum tolerable availability, related to hardware MINOR failures, shall be ***0.995***

® the corresponding mean downtime per year due to MINOR failures shall be

$$DT_{HW,M} = (1 - A_{HW,M}) \cdot 8760 \text{ h} = 43 \text{ hour } 48 \text{ minutes}$$

2.3.2.2 Transmission Errors Contribution

As transmission error is intended the event that, in absence of any kind of fault occurred to the transmission equipment, a message is not received, is received in wrong way or is not received within the allowed time delay causing a system failure.

The contribution to the system unavailabilities due to transmission errors is stated as the 10%.

As a consequence the transmission errors contribution A_{TX} to the quantifiable portion of the operational availability A_{OP} is established on the basis of the following formula:

$$A_{TX} = \frac{T_{op}}{T_{op} + T_{fault}} = \frac{\left[\left(1 - P_{ds}\right)T_{dn} + P_{ds}T_{dnd}\right]}{\left[\left(1 - P_{ds}\right)T_{dn} + P_{ds}T_{dnd}\right] + 0.1 \cdot 0.6 \cdot P_{ds} \cdot 0.9 \cdot T_{dy}} =$$

$$= \frac{90}{90 + 0.1 \cdot 0.6 \cdot 0.0027 \cdot 0.9 \cdot 10} = 0.999984$$

® The *ERTMS/ETCS* quantifiable contribution to operational availability, due to transmission errors, shall be not less than ***0.999984***.

2.3.2.2.1 Continuous TX Contribution

The contribution to the transmission errors unavailabilities due to continuous transmission errors is stated as the 50%.

This contribution is calculated by means of the following formula:

$$A_{TX,C} = \frac{T_{op}}{T_{op} + T_{fault}} = \frac{\left[\left(1 - P_{ds}\right)T_{dn} + P_{ds}T_{dnd}\right]}{\left[\left(1 - P_{ds}\right)T_{dn} + P_{ds}T_{dnd}\right] + 0.5 \cdot 0.1 \cdot 0.6 \cdot P_{ds} \cdot 0.9 \cdot T_{dy}} =$$

$$= \frac{90}{90 + 0.5 \cdot 0.1 \cdot 0.6 \cdot 0.0027 \cdot 0.9 \cdot 10} = 0.999992$$

The following requirement is then defined:

® the quantifiable contribution to operational availability, due to continuous transmission errors, shall be not less than ***0.999992***.

® the corresponding mean downtime per year due to continuous transmission errors shall be

$$DT_{TX,C} = (1 - A_{TX,C}) \cdot 8760 \text{ h} = 4.2 \text{ minutes}$$

Assuming that in 1 hour trip 1200 messages are exchanged between onboard and trackside equipment (cfr. § 2.2.1.4.1.) via continuous transmissions, then the Availability figure for each message, meaning the probability that a message is not corrupted, is the following:

® the probability that a message transmitted by continuous transmission systems is not corrupted shall be not less than ***0.9999999932***.

2.3.2.2.2 Discontinuous TX Contribution

The contribution to the transmission unavailabilities due to discontinuous transmissions is stated as the 50%.

This contribution is calculated by means of the following formula:

$$A_{TX,D} = \frac{T_{op}}{T_{op} + T_{fault}} = \frac{\left[(1 - P_{ds})T_{dn} + P_{ds}T_{dnd}\right]}{\left[(1 - P_{ds})T_{dn} + P_{ds}T_{dnd}\right] + 0.5 \cdot 0.1 \cdot 0.6 \cdot P_{ds} \cdot 0.9 \cdot T_{dy}} =$$

$$= \frac{90}{90 + 0.5 \cdot 0.1 \cdot 0.6 \cdot 0.0027 \cdot 0.9 \cdot 10} = 0.999992$$

The following requirement is then defined:

® the discontinuous transmissions availability shall be not less than ***0.999992***.

® the corresponding mean downtime per year due to discontinuous transmissions failures shall be

$$DT_{TX,D} = (1 - A_{TX,D}) \cdot 8760 \text{ h} = 4.2 \text{ minutes}$$

Assuming that in 1 hour trip 940 messages are exchanged between onboard and trackside equipment (cfr. § 2.2.1.4.1.) via discontinuous transmissions, then the Availability figure for each message, meaning the probability that a message is not corrupted, is the following:

® the probability that a message transmitted by discontinuous transmission systems is not corrupted shall be not less than ***0.9999999914***.

2.3.3 ERTMS (UN)AVAILABILITY REQUIREMENTS FOR CONSTITUENTS

The availability (or unavailability) and reliability (or unreliability) requirements marked with the ® symbol stated in the Paragraphs 2.2 and 2.3.2, will not need to be demonstrated if the specific requirements for the ERTMS Constituents, as listed in the following Table, are fulfilled and demonstrated.

This means that the National Railways are free to choose between the availability (or unavailability) requirements stated in the Paragraphs 2.2 and 2.3.2 and those given in the following table when preparing their specific supply contracts for ERTMS/ETCS Applications.

This option does not apply to Maintainability and Logistic Support Requirements, that remain as specified in paragraph 2.2.

		Unavailability
On board		
	Kernel (Vital functions)	< 1E-6
	Kernel (non-Vital functions)	< 1E-6
	BTM	< 1E-8
	RTM	< 1E-6
	MMI	< 1E-7
	TIU	< 1E-7
	Odometer	< 1E-7
Line		
	Non-switchable Balise	< 1E-7
	Switchable Balise	< 1E-7
	LEU (Interoperable part)	< 1E-7
Trackside		
	RBC	< 1E-6

2.3.4 ERTMS FUNCTIONS RAM-BASED ALLOCATION OF SOFTWARE INTEGRITY LEVELS

The qualitative characterisation of software Integrity Level presumes that only qualitative RAM targets shall be defined at the requirement stage and reached during the software development.

The impact of the failure of an *ERTMS/ETCS* function on the system operational availabiliy can require that the software IL assigned to that function on the basis of the SIL, is increased.

For doing this, it is necessary to re-analyse the *ERTMS/ETCS* functions for recognising their impact on the operational availability establishing a criteria (which will be defined below) for increasing the relevant ILs.

This process is named RAM-based allocation of software ILs.

For this reason,

® the RAM-based allocation of software Integrity Levels shall be performed only once the assignment of the SIL-related Integrity Levels has been carried out (see Chapter 3).

The RAM-based allocation process shall be the following:

1. identify the functions IL target based on the functions SIL targets;
2. determine the functions RAM-based IL, on the basis of criticality deriving from their failures on of the relevent weakness, as defined in [2.2];
3. if the functions RAM-based IL is more severe than the SIL-based one, increase the SIL-based IL to the RAM-based one;
4. if the functions RAM-based IL is less severe than the SIL-based one, maintain the SIL-based IL.

2.3.4.1 RAM-based IL determination

The function criticality is expressed in terms of the severity of the function failure in reason of the failure categorisation, presented in § 2.1.1.5 The criticality is assigned to each *ERTMS/ETCS* function as in § 2.3.1.2. Weakness takes into account the function liability to fail, due to the software structure and to the environmental conditions.

® Weakness shall be evaluated by means of a Weakness Estimation, to be performed by the Contractor or by the personnel responsible for the relevant development phase and agreed by the Project Management, on the basis of the considerations made in [2.2].

The RAM-based choice of the appropriate IL for the *ERTMS/ETCS* functions shall be done on the basis of the following table:

Weakness Class → Criticality ↓	**W C0**	**W C1**	**W C2**	**W C3**	**W C4**
0 - NOT RELEVANT	IL0	IL0	IL0	IL0	IL0
1 - MINOR	IL0	IL0	IL1	IL1	IL1
2 - SERVICE	IL0	IL1	IL1	IL2	IL2
3 - IMMOBILISING	IL1	IL1	IL2	IL2	IL3

Once the above process is performed, the resultant ILs, assigned to the *ERTMS/ETCS* functions, shall be considered as definitive.

The Contractor shall be responsible, against the Project Management, for this allocation.

2.3.4.2 ERTMS Functions Weakness Estimation Requirements

The basis for *ERTMS/ETCS* software functions RAM-based Integrity Level allocation is the Weakness Estimation, as presented in [2.2]. Function weakness gives a qualitative measure of how much implemented function will be liable to fail.

The following requirements are defined, for the *ERTMS/ETCS* functions Weakness Estimation:

® Structural and Environmental parameters shall be qualitatively evaluated by the Sub-contractor(s)/Supplier(s) responsible for the relevant development phase using the metrics presented in [2.2].

® The Contractor shall guarantee for the uniformity of the qualitative judgement adopted by the Sub-contractor(s)/Supplier(s) in the software functions Weakness Estimation, and for the relevant documentation adequacy against the procedures and criteria formalised in Software Quality Assurance Plan, and agreed by the Project Manager. The results of *ERTMS/ETCS* function Weakness Estimation, as well as the relevant documentation produced by the Sub-contractor(s)/Supplier(s), shall be collected and harmonised by the Contractor and shall be submitted to the Project Management for the final approval.

2.3.5 REQUIREMENTS FOR THE ERTMS SOFTWARE INTEGRITY LEVELS APPORTIONMENT

The above mentioned four different ILs, from 1 to 4, in addition to the level 0, which indicates absence of specific integrity requirements, are considered in compliance with [2.6]: IL4 indicates the maximum integrity, while IL1 indicates the minimum integrity for a software implemented function according to the following table:

Software Integrity Level (IL)	**Description**
4	Very High Integrity
3	High Integrity
2	Medium Integrity
1	Low Integrity
0	No Integrity Requirements (comply with EN29000-3 only)

For the software implementing functions is always required the compliance with [2.8].

For IL1 to IL4 it is also required the compliance with [2.6].

The Verification and Validation Plan has to be applied for each defined IL..

Note that the reference document [2.6] is currently in progress, so changes to the number of ILs can occur in further document issues.

The following requirements shall be fulfilled in apportioning the *ERTMS/ETCS* function ILs to the relevant software components:

® On the basis of the ILs functional allocation and of the system architecture, the Subcontractor(s)/Supplier(s) shall assign the appropriate IL to the software components involved by the functions of their competency, and shall submit the results of this sub-allocation to the Contractor for approval.

® The Contractor shall guarantee the adequacy of the IL assigned to each software component against the IL of the relevant function, and shall submit the documentation to the Project Management for approval.

® The appropriate techniques and measures, to be applied to the extent required by the software Integrity Level, shall comply with [2.6] and shall be detailed, at the beginning of the software lifecycle, in the *ERTMS/ETCS* Software Quality Assurance Plan and Software Verification and Validation Plan.

2.4. SYSTEM RAM PROGRAMME PLAN REQUIREMENTS

This paragraph aims to define the basic requirements for the *ERTMS/ETCS* RAM Programme.

The *ERTMS/ETCS* RAM Programme is a set of activities to be performed along the *ERTMS/ETCS* Lifecycle for ensuring that the RAM Requirements stated for the system are fulfilled at each development phase.

An efficient RAM Programme shall be established and maintained by each subject responsible for performing activities related to the *ERTMS/ETCS* Lifecycle, including contractors for specific national supply contracts, starting from the early design phases subsequent to the *ERMTS Control/Command* Specification Phase up to the System Decommissioning Phase of each national application.

In the context of each specific *ERTMS/ETCS* supply contract for specific national applications, the activities relevant to the RAM Programme shall be performed by each Sub-Contractor/Supplied for the system(s)/subsystem(s) of its competency, and integrated by the Contractor at system level. The surveillance on the RAM Programme activities shall be responsibility of the Project Management of the Customer structure.

The activities of the *ERTMS/ETCS* RAM Programme, also for each national specific application, shall comply with this specification according to the specific System Quality Plan constraints set up in the context of the supplying contract.

2.4.1 GENERAL

2.4.1.1 Purpose

The RAM Programme aims to identify the system RAM Requirements and the activities of analysis, verification and demonstration, to be developed by the subjects responsible for performing activities related to one or more *ERTMS/ETCS* Lifecycle phases, for ensuring the compliance with the above requirements.

The RAM Programme Plan establishes all the programme management tasks, in terms of timing and implementation details of the programme activities, to accomplish the RAM Programme Requirements.

2.4.1.2 Scope

The RAM Programme applies to the following *ERTMS/ETCS* Lifecycle Phases:

- Design and Implementation
- Manufacture
- Installation
- System Validation
- System Acceptance
- Operation and Maintenance
- Performance Monitoring
- Modification and Retrofit
- Decommissioning and Disposal

® All the functions and equipment constituting parts of the *ERTMS/ETCS* system shall be subject of RAM activities and then shall be subject to the present RAM Programme.

2.4.1.3 RAM Structure and Responsibilities

Each subject responsible for performing RAM activities, intended as a Contractor/Sub-Contractor/Supplier, in one or more of the *ERTMS/ETCS* Lifecycle phases, shall document to the Project Management, by means of the RAM Programme Plan, its general structure and, in particular, the structure responsible for the above activities.

In each specific supply contract for specific *ERTMS/ETCS* applications, the Customer shall examine the above structure, proposed by each Contractor/Sub-Contractor/Supplier, and, if necessary, shall request modifications where applicable.

The Contractor/Sub-Contractor/Supplier shall indicate to the Customer its interfaces which will constitute the reference, for all the duration of the supply contract, for the RAM Programme activities.

2.4.1.4 RAM Requirements

The RAM Requirements to be verified and demonstrated by means of the RAM Programme are represented, at system level by the *ERTMS/ETCS* Overall RAM Requirements defined in § 2.2.2..

Each Contractor/Sub-Contractor/Supplier shall declare, in its RAM Programme Plan, the RAM Requirements defined/apportioned for the system(s)/subsystem(s) of its competency. This, at first, for demonstrating that the correct RAM requirements are receipt for the system/subsystem and, secondarily, for clearly indicating the requirements to be verified and demonstrated by the RAM Programme.

2.4.1.5 RAM Programme Plan

The *ERTMS/ETCS* System RAM Programme Plan shall integrate all the RAM Programme Plans defined by each Sub-Contractor/Supplier for the *ERTMS/ETCS* subsystems of its competency.

The responsibility for the integration of the System RAM Programme Plan shall be assumed by the subject responsible for the system integration, represented by the Contractor (see Glossary).

In the RAM Programme Plan, the Contractor shall declare the procedures, the tools and the timing foreseen for implementing the RAM Programme aimed to ensure the compliance with the *ERTMS/ETCS* Overall RAM Requirements defined in §2.2.

The RAM Programme Plan includes the following sub-plans:

- Reliability Programme Plan;
- Maintainability Programme Plan.

The above sub-plans should comply with [2.12] and [2.13], which tailoring should be agreed by the parts of the supply contract in the context of each specific application.

Anyway, the RAM Programme Plan shall comply, as a minimum, with [2.5].

The RAM Programme Plan shall be issued by the Contractor, and submitted for acceptance to the Project Management, within a time agreed by the parts of the supply contract in accordance with the System Quality Plan.

2.4.1.6 System Conditions and Mission Profile

Aim of this activity is to identify the specific conditions under which an equipment is called to operate, in compliance with the specified system conditions as summarised in §2.2.1. and inner, to be referred for the demonstration of the relevant RAM Requirements.

To this purpose, each Sub-Contractor/Supplier shall submit to the Contractor an analysis of the technical conditions, for the system(s)/subsystem(s) of its competency, which constitute the reference for the RAM analyses.

This documentation shall be integrated by the Contractor and submitted to the Customer Project Management for approval.

The following shall be specified, as a minimum:

- System Conditions, including Environmental Conditions, Mission Profile, Useful Life and so on;
- Operating Conditions;
- Maintenance Conditions.

The *ERTMS/ETCS* Overall technical conditions, which shall constitute the basic reference for the system(s)/subsystem(s) technical conditions, are defined in § 2.2.1.1, § 2.2.1.2. and § 2.2.1.3. and shall be ensured by the system integration.

2.4.1.7 System Analysis

Within a time agreed by the parts of the supply contract, in accordance with the System Quality Plan, each Sub-Contractor/Supplier shall submit to the Contractor a report containing the following:

- the definition of the layout of the system(s)/subsystem(s) of its competency indicating the typology and the configuration of all the hardware and software items constituting part of the system(s)/subsystem(s);
- the definition of a configuration management system.

This documentation shall be integrated by the Contractor and submitted to the Customer Project Management for approval.

As the above report is accepted by the Project Management, and within a time agreed by the parts of the supply contract, a meeting among the Customer and the Contractor shall be held in order to define the system hierarchical structure and the list of the items belonging to it.

The hierarchical structure and the items list here defined shall constitute a reference for all the duration of the supply contract.

2.4.2 RELIABILITY PROGRAMME SPECIFICITIES

2.4.2.1 Reliability Programme Reviews

In the context of each specific supply contract for *ERTMS/ETCS* specific applications, the Customer Project Management and the Contractor need to monitor

and control the Sub-Contractor(s)/Supplier(s) activity for ensuring that the Reliability Programme milestones are respected.

The Contractor, responsible for the system integration, shall conduct, at specified points in time, agreed by the parts of the supply contract, Reliability Programme Reviews producing periodical reports specifying, as a minimum, the following:

- reliability related documentation delivered, indicating the relevant revisions;
- status of the current activities;
- notification of problems affecting reliability;
- updating of the documentation delivering plan.

Problems shall be notified by means of forms to be agreed by the parts of the supply contract and each problem notification shall include the corresponding corrective action.

2.4.2.2 Reliability Modelling, Prediction and Apportionment

Each Sub-Contractor/Supplier shall produce, for each item identified in the system hierarchical structure and for the critical functions of the system(s)/subsystem(s) of its competency, a Reliability Block Diagram and the relevant list of elemental hardware and software items, in compliance with the procedures defined in [2.10].

This documentation shall be integrated by the Contractor and submitted to the Customer Project Management for approval.

An appropriate failure rate shall be apportioned to each part belonging to the system(s)/subsystem(s) and the allocated failure rate together with the predicted failure rate, determined by reliability analysis, shall be specified.

The methodologies, the tools and the reliability data sources utilised for the reliability predictions shall be clearly declared and submitted to the Project Management for approval.

The results of the activity shall be presented in the Reliability Modelling, Prediction and Apportionment Report which shall be submitted within a time agreed by the parts of the supply contract and reviewed in the appropriate milestones of the Reliability Programme.

The forms to be utilised for presenting the reliability apportionment and predictions results shall also be agreed by the parts of the supply contract.

2.4.2.3 FMECA analysis

Each Sub-Contractor/Supplier shall perform a FMECA, at an adequate indenture level agreed by the parts of the supply contract and defined by the items list introduced in § 2.4.1.7., for the system(s)/subsystem(s) of its competency. For highly critical items the relevant indenture level shall be as lower as appropriate.

A detailed functional analysis shall be performed preliminarily for identifying the items functions and for emphasising the mutual interfaces.

The results of the FMECA and of the functional analysis shall be the items FMECA cards and the system(s)/subsystem(s) Functional Block Diagram which shall comply with [2.16].

In particular, the Criticality Analysis (CA) shall identify the items, and the relevant failure modes, which result in each criticality level in reason of the different effects on the system performance as defined in § 2.1.1.5.

The above analysis shall be performed mandatorily before the Final Design Review, foreseen in the System Quality Plan, for allowing corrective actions to be effectively implemented.

The first FMECA shall be submitted to the Contractor and, after integration, to the Customer Project Management within a time agreed by the parts of the supply contract.

FMECA cards shall be updated at each modification of the system configuration and shall be verified at each design review.

2.4.2.4 Critical Items List

On the basis of the results of the system FMECA, obtained by integrating the Sub-contractor(s)/Supplier(s) FMECAs, and at a time agreed by the parts of the supply contract, the Contractor shall submit to the Customer Project Management a list of the items which failure modes result in system failures categorised as *Immobilising Failures*.

This list shall integrate the Maintainability Analysis documentation ad shall require, where appropriate, special reliability tests as agreed by the parts of the supply contract.

2.4.2.5 Software Reliability Estimation

Each Sub-Contractor/Supplier responsible for design and develop software items, shall perform and maintain a Software Reliability Estimation utilising metrics and forms to be agreed by the parts of the supply contract (see, for instance, [2.19]).

The purpose of the Software Reliability Estimation is to provide the Contractor with the data necessary for the *ERTMS/ETCS* Operational Availability Assessments.

It is responsibility of the Contractor to require, according to the Software Quality Assurance Plan milestones, Software Reliability Estimation updating when necessary and to examine and to accept the documentation and the reliability data obtained by the Sub-Contractor(s)/Supplier(s).

The Contractor shall produce copy of all the relevant accepted documentation to the Customer Project Management for information.

The first Software Reliability Estimation shall be presented to the Contractor at a time agreed by the parts.

2.4.2.6 Reliability Preliminary Tests

The Reliability Preliminary Tests aim at discovering weak points in the *ERTMS/ETCS* design or in the production process of *ERTMS/ETCS* specific parts so that adequate corrective measures can be adopted.

The Reliability Preliminary Tests shall be projected in order to emphasise or to induce the possible failures and shall be conducted in the Development and Qualification phases of the system(s)/subsystem(s) lifecycle.

2.4.2.6.1 Reliability Development/Growth Tests

Each Sub-Contractor/Supplier required to design and product ad hoc parts for *ERTMS/ETCS* or to provide parts never employed in railway control/command systems, shall conduct, for each applicable item identified in the system hierarchical structure, pre-qualification testing to provide a basis for resolving the majority of reliability problems early in the development phase, and incorporating corrective action to preclude recurrence, prior to the beginning of production.

A Reliability Development/Growth Test Plan shall be prepared by each Contractor/Sub-Contractor/Supplier, and submitted for acceptance to the Project Management, within a time agreed by the parts of the supply contract in accordance with the System Quality Plan. The Reliability Development/Growth Test Plan should comply with [2.11].

2.4.2.6.2 Reliability Qualification Tests

Each Sub-Contractor/Supplier required to design and product ad hoc parts for *ERTMS/ETCS* or to provide parts never employed in railway control/command systems, shall conduct Reliability Qualification Tests on equipment which shall be identified by the Project Management and which shall be representative of the approved production configuration.

The purpose of this task is to determine that specified reliability requirements have been achieved also in the respect of the interoperability of equipment. The Project Management shall retain the right to disapprove the test failure relevancy and chargeability determinations for the reliability quantification.

A Reliability Qualification Test Plan shall be prepared by each Sub-Contractor/Supplier, submitted for integration to the Customer and, consequently, submitted for acceptance to the Project Management, within a time agreed by the parts of the supply contract in accordance with the System Quality Plan. The Reliability Qualification Test Plan should comply with [2.11].

2.4.2.7 Reliability Demonstration Testing Plan

At the completion of the Reliability Program, the Contractor shall produce a Reliability Demonstration Plan which can be obtained by integration of the Sub-contractor(s)/Supplier(s) Reliability Demonstration Sub-Plans relevant to the system(s)/subsystem(s) of their competency.

The Reliability Demonstration Plan shall define as a minimum:

- reliability demonstration tests conditions and criteria;
- reliability demonstration tests duration during the warranty period agreed by the parts of the supply contract;
- data collection, classification and analysis during the above warranty period.

The management of the Reliability Demonstration activities planned in the Reliability Demonstration Plan shall be responsibility of the Validation Team.

In particular, the Validation Team shall, as a minimum:

- identify and manage all the reliability data arising from the Reliability Demonstration Programme activities;
- examine the collected reliability data on the basis of the results of the Reliability Programme activities;
- examine and accept the corrective measure requests;
- accept recommendations for failure classification and for decision concerning the failure chargeability;
- perform an audit on the verification documentation for validating the system and the interoperability and for providing recommendations for the system acceptance.

2.4.2.8 Reliability Demonstration Tests

Reliability Demonstration Tests aim at demonstrating the *ERTMS/ETCS* RAM Requirements are fulfilled during the system operation in the rated operating conditions.

The following specific conditions shall be respected:

- all the parts of the system subject to testing are complete and fulfil the configuration requirements foreseen in the supply contract;
- the data are collected from the field during the period stated by the Reliability Demonstration Plan;
- the interoperability is taken into account, then, for the equipment liable to be employed also under system conditions different from those stated for the specific national application, the test conditions shall fulfil the overall system conditions defined for *ERTMS/ETCS* in § 2.2.1.

The Reliability Acceptance Criteria are defined in § 2.2.3.1.1..

2.4.2.9 Failure data collection from the field (FRACAS)

Each Contractor/Sub-Contractor/Supplier shall have a closed loop system, during the System Warranty Period agreed with the Customer in the context of each supplying contract, that collects, analyses, and records failures that occur for specified levels of assembly prior to the acceptance of the hardware by the Customer Project Management (Failure Reporting, Analysis, and Corrective Action System).

Procedures for initiating failure reports, the analysis of failures, feedback of corrective action into the design, manufacturing and test processes shall be identified. Flow diagrams depicting failed hardware and data flow shall also be documented. The analysis of failures shall establish and categorises the cause of failure.

The closed loop system shall include provisions to assure that effective corrective actions are taken on a timely basis by a follow-up audit that reviews all open failure reports, failure analysis, and corrective action suspense dates, and the reporting to delinquencies to management. The failure cause for each failure shall be clearly stated.

The forms to be utilised for presenting the FRACAS results shall also be agreed by the parts of the supply contract.

2.4.3 MAINTAINABILITY PROGRAMME SPECIFICITIES

2.4.3.1 Maintainability Programme Reviews

In the context of each specific supply contract for *ERTMS/ETCS* specific applications, the Customer Project Management and the Contractor need to monitor and control the Sub-Contractor(s)/Supplier(s) activity for ensuring that the Maintainability Programme milestones are respected.

The Contractor, responsible for the system integration, shall conduct, at specified points in time agreed by the parts of the supply contract, Maintainability Programme Reviews producing periodical reports specifying, as a minimum, the following:

- maintainability related documentation delivered, indicating the relevant revisions;
- status of the current activities;
- notification of problems affecting maintainability;
- updating of the documentation delivering plan.

Problems shall be notified by means of forms to be agreed by the parts of the supply contract and each problem notification shall include the corresponding corrective action.

2.4.3.2 Preventive Maintenance Analysis

A Preventive Maintenance Analysis (PMA) shall be performed and maintained by each Sub-Contractor/Supplier by means of appropriate forms during the design development phases, in order to allow the evaluation of the personnel, infrastructures and spares employment for the *ERTMS/ETCS* Preventive Maintenance.
This documentation shall be integrated by the Contractor and submitted to the Customer Project Management for approval.

The PMA can be carried out according to [2.15], Procedure II, Method B. The structure of the PMA forms to be used and the timing of the PMA updating shall be agreed by the parts of the supply contract.

The identification of the items subject to PMA shall comply with what is defined by the configuration management system.

2.4.3.3 Corrective Maintenance Analysis

A Corrective Maintenance Analysis (CMA) shall be performed and maintained by each Sub-Contractor/Supplier by means of appropriate forms during the design development phases, in order to allow the evaluation of the personnel, infrastructures and spares employment for the *ERTMS/ETCS* Corrective Maintenance.

This documentation shall be integrated by the Contractor and submitted to the Customer Project Management for approval.

The CMA can be carried out according to [2.15], Procedure II, Method B. The structure of the CMA forms to be used and the timing of the CMA updating shall be agreed by the parts of the supply contract.

The identification of the items subject to CMA shall comply with what is defined by the configuration management system.

2.4.3.4 Fault Isolation and Trouble-Shooting Plan

A Procedure of Fault Isolation and Trouble-Shooting shall be defined by each Sub-Contractor/Supplier, and integrated by the Contractor, in order to detect the preferred trouble-shooting sequence for each failure mode and the sequence of steps necessary for clearly identify the faulty parts or equipment. This Procedure can comply with [2.4].

The Fault Isolation and Trouble Shooting Procedure shall follow the definition of the subsystem(s) maintenance levels (formalised in a Functional Levels Diagram) which can be carried out according to [2.15], Procedure II, Method A.

The conditions liable to cause each fault indication shall be identified in order to allow each trouble to be isolated to a level indicated in the Functional Levels Diagram ([2.15], Procedure II, Method A, § 3.1.1.2).

The time of delivery of the Fault Isolation and Trouble Shooting Procedure, the relevant forms and the methodologies shall be agreed between the parts of the supply contract.

2.4.3.5 Maintainability Qualification Tests

Specific Maintainability Tests shall be performed in the Qualification process of specific subsystems/equipment/parts as agreed by the parts of the supply contract.

Those tests aim at verifying the actual assembly/disassembly time and the fulfilment of the Qualitative Maintainability Requirements defined in § 2.2.2.3.1.

Each Sub-Contractor/Supplier shall submit to the Contractor a procedure defining the conditions for performing the Maintainability Qualification Tests and establishing, as a minimum:

- test location;
- test organisation;
- responsibilities;
- items to be tested and references to the relevant maintenance documentation;
- test facilities and personnel necessary;
- interoperability constraints
- forms for data recording.

This documentation shall be integrated by the Contractor and submitted to the Customer Project Management for approval.

2.4.3.6 Maintainability Demonstration Testing Plan

At the completion of the Maintainability Programme, the Contractor shall produce a Maintainability Demonstration Plan which can be obtained by integration of the Sub-contractor(s)/Supplier(s) Maintainability Demonstration Sub-Plans relevant to the system(s)/subsystem(s) of their competency.

The management of the Maintainability Demonstration activities planned in the Maintainability Demonstration Plan shall be responsibility of the Validation Team (see § 2.4.2.7.).

In particular, the Validation Team shall, as a minimum:

- identify and manage all the maintainability data arising from the Maintainability Demonstration Programme activities;
- examine the collected maintainability data on the basis of the results of the Maintainability Programme activities;
- examine and accept the corrective measure requests;
- accept recommendations for failure classification and for decision concerning the failure chargeability;
- perform an audit on the verification documentation for validating the system and the interoperability and for providing recommendations for the system acceptance.

2.4.3.7 Maintainability Demonstration Tests

Maintainability Demonstration Tests aim at demonstrating the *ERTMS/ETCS* RAM Requirements are fulfilled during the system operation in the rated operating conditions.

The maintenance actions performed on *ERTMS/ETCS* during the demonstration period stated in the Maintainability Demonstration Plan, shall be recorded by means of forms similar to those used for PMA and CMA, with indication of the source of the data ("*from the field data*"), in addition to the standard FRACAS cards.

The following specific conditions shall be respected:

- all the parts of the system subject to testing are complete and fulfil the configuration requirements foreseen in the supply contract;
- the data are collected from the field during the period stated by the Maintainability Demonstration Plan;
- the interoperability is taken into account, then, for the equipment liable to be employed also under system conditions different from those stated for the specific national application, the test conditions shall fulfil the overall system conditions defined for *ERTMS/ETCS* in § 2.2.1.

The Maintainability Acceptance Criteria are defined in § 2.2.3.1.2..

2.4.4 OPERATIONAL AVAILABILITY ASSESSMENT

The Contractor shall perform and maintain an Operational Availability Assessment on the basis of the results of the RAM analysis, verification and demonstration activities carried out in the context of the system RAM Programme. To this aim, the Contractor shall integrate, at system level, the results obtained by each Sub-Contractor/Supplier from the RAM activities performed on the system(s)/subsystem(s) of its competency.

The Operational Availability Assessment shall comprise, as a minimum:

1. assessment of the contribution of hardware and transmission failures to the quantifiable contribution to the operational availability target for each *ERTMS/ETCS* function (see § 2.3);
2. assessment of the contribution of hardware and transmission failures to the quantifiable contribution to the overall operational availability target of *ERTMS/ETCS* (see § 2.2.2.1.2.);
3. assessment of the contribution of software-caused failures to the operational availability target for each *ERTMS/ETCS* function (see § 2.3);
4. assessment of the contribution of software-caused failures to the overall operational availability target of *ERTMS/ETCS* (see § 2.2.2.1.2.).

The activities 1. and 2. aim to verify that the quantifiable contribution to the operational unavailability does not exceed the ***60%*** of the operational unavailability itself.

The activities 3. and 4. aim to verify that the contribution to the operational unavailability due to software defects, for which any quantitative requirements are defined, does not compromise the achievement of the global operational availability targets stated for *ERTMS/ETCS* and/or for its functions.

To this purpose, each Sub-Contractor/Supplier shall provide the Contractor with:

1. all the results of the RAM analysis necessary for performing the above assessments;
2. all the indications necessary for building the availability models of the functions and of the whole system;
3. periodical assessments of the software reliability.

The forms for the presentation of the Operational Availability Assessment and the relevant timing shall be agreed between the parts of the supply contract according to the system Quality Plan.

2.4.5 INTERRELATIONSHIPS WITH THE SYSTEM QUALITY PLAN

The interrelationships between the System Quality Plan and the RAM Programme Plan regard the definition of points in time, coincident with the contractual milestones stated by the System Quality Plan, where the RAM Programme is reviewed in addition to the scheduled Reliability and Maintainability Programme Reviews specified in § 2.4.2.1. and § 2.4.3.1..

The System Quality Plan shall be defined according to each specific supplying contract and shall be agreed between the Customer, the Contractor and the Sub-Contractor(s)/Supplier(s). For this reason, the contractual milestones here cited are based on an assumption of the usual milestones in a standard System Quality Plan.

The RAM Programme Reviews to be performed in coincidence with the assumed contractual milestones shall identify and discuss all pertinent aspects of the RAM Programme such as explained in the following paragraphs from 2.4.5.1. to 2.4.5.4..

2.4.5.1 Preliminary Design Review

2.4.5.1.1 Reliability Programme Review

1. Updated Reliability Status including:
   a. Reliability Modelling;
   b. Reliability Apportionment;
   c. Reliability Predictions;
   d. FMECA;
   e. Reliability content of specification;
   f. Design Guideline Criteria;
   g. Other tasks agreed by the parts.
2. Other problems affecting Reliability
3. Reliability Critical items programme specificities.

2.4.5.1.2 Maintainability Programme Review

1. Updated Maintainability Status including:
   a. Maintainability Modelling;
   b. Maintainability Apportionment;

c. Maintainability Predictions;
d. FMEA (only Maintainability information);
e. Maintainability content of specification;
f. Design Guideline Criteria;
g. Establishment of data collection, analysis and corrective action system;
h. Results of the planned Maintainability Analysis which impact maintenance plan/concept, testability needs, Logistic Support or repair levels;
i. Subcontractor(s)/Supplier(s) Maintainability;
j. Other tasks agreed by the parts.

2. Projected maintenance, manpower and personnel, as far as skills are concerned, impacts based on assessed maintainability characteristics, and projected ability to meet maintainability requirements within manpower and personnel constraints.
3. Other problems affecting Maintainability.
4. Maintainability design approach including the extent of modularity and the fault detection and isolation approach to each level of maintenance.

2.4.5.2 Critical Design Review

2.4.5.2.1 Reliability Programme Review

1. Reliability content of specifications.
2. Reliability Predictions and Analysis.
3. Reliability Critical items programme specificities.
4. Other problems affecting Reliability
5. FMECA
6. Identification of circuit reference designators whose stress level exceed the recommended parts application criteria.
7. Other tasks agreed by the parts.

2.4.5.2.2 Maintainability Programme Review

1. Maintainability content of specifications.
2. Maintainability Predictions and Analysis.
3. Fault detection and isolation design approach and general testability assessment (for each appropriate maintenance level).
4. Quantity and types of maintenance tasks for each level of the system hierarchical structure, as stated in § 2.4.1.7., and of each maintenance level.

5. Final content and descriptions of all pertinent inputs to the maintenance plan.
6. FMEA as related to the fault detection and isolation system's design and characteristics.
7. Projected manpower skill requirements based on assessed maintainability characteristics.
8. Other problems affecting Maintainability.
9. Other tasks agreed by the parts.

2.4.5.3 Test Readiness Review

2.4.5.3.1 Reliability Programme Review

1. Reliability Analysis status, primarily prediction.
2. Test schedule.
3. Test profile.
4. Test plan including failure definition.
5. Test report format.
6. FRACAS implementation.

2.4.5.3.2 Maintainability Programme Review

1. Maintainability prediction.
2. Test schedule.
3. Review of adherence to appropriate portions of [2.14].
4. Test report format.
5. Review of the tasks defined in § 2.4.3.6. and § 2.4.3.7..
6. Availability of personnel (in number, skills and training as determined by the contract), technical manuals and support equipment.

2.4.5.4 Production Readiness Review

2.4.5.4.1 Reliability Programme Review

1. Results of applicable Reliability Qualification Tests.
2. Results of applicable Reliability Growth Testing.

2.4.5.4.2 Maintainability Programme Review

Results of the evaluation of entire diagnostic capabilities.

Annex A, Chapter 0 – Glossary Acronyms References

Normative References

EN 29000-3	"Quality Management and Quality Assurance Standards - Guidelines for the Application of ISO9001 to the development, supply and maintenance of software", CEN, First Version, June 1993
EN ISO 9000-1	"Quality Management and Quality Assurance Standards - Guidelines for Selection and Use", CEN, supersedes EN 29000, July 1994
EN 50126	"Railway Applications - The Specification and Demonstration of Dependability, Reliability, Availability, Maintainability and Safety (RAMS)", CENELEC
EN 50128	"Railway Applications - Software for Railway Control and Protection Systems", CENELEC
ENV 50129	"Railway Applications - Safety Related Electronic Systems", CENELEC
EN 50159-1	" Railway Applications - Requirements for Safety-Related Communication in Closed Transmission Systems", CENELEC
EN 50159-2	"Railway Applications - Requirements for Safety-Related Communication in Open Transmission Systems", CENELEC

Mandatory References

EEIG ERTMS USERS GROUP	"Engineering Documents and Eurosig Documents”, See the list in Contents.xls CDROM 31/07/98
EEIG ERTMS USERS GROUP	"ERTMS - Quality Requirements for Suppliers", Version 1-, 20/09/96
EEIG ERTMS USERS GROUP	"ERTMS - Validation Procedures", Version 3-
EEIG ERTMS USERS GROUP	"ERTMS/ETCS - Environmental conditions”, Version 5-
EEIG ERTMS USERS GROUP	"ERTMS Control/Command Test tool characteristics requirements for Software Safety Test”, Version 2-
EEIG ERTMS USERS GROUP	" The Attribution of the ERTMS SRS Functions to Constituents”, Version 1-
UIC/ERRI	"ERTMS - Requirement Specifications: Functional Requirements Specification FRS, Synopsis", Final Version, January 1996
UIC/ERRI	"ETCS - FRS Functional Requirements Specification", Version 4.01

Informative References

EEIG ERTMS USERS GROUP	RAMS Requirements - Informative Part 98s7111-
EEIG ERTMS USERS GROUP	"ERTMS/ETCS - Specification of Service Requirements", included in 98s7111- above
UIC/ERRI	"ETCS RAM Strategy", Final Draft, 28 July 1995
UIC/ERRI	“ETCS Safety Strategy” Final Draft, 31 December 1995
IEC 1508	"Functional Safety: Safety-Related Systems", IEC SC65A, Draft, June 1995
ISO/IEC DIS 9126	"Information Technology - Software Product and Evaluation - Quality Characteristics and Guidelines for their Use", ISO/IEC JTC-1, Draft, 1990
MIL-HDBK-338-1A	"Electronic Reliability Engineering Handbook", Vol. 1, USA DoD, 12 October 1988
MIL-HDBK-472	"Maintainability Prediction - Handbook", USA DoD, 24 May 1966
MIL-STD-1388-1A	"Logistic Support Analysis", USA DoD, 11 April 1983
MIL-STD-1629A	"Procedures for Performing a Failure Mode, Effects and Criticality Analysis", USA DoD, 24 November 1980
MIL-STD-470B	"Maintainability Program for Systems and Equipment", USA DoD, 30 May 1989
MIL-STD-471A	"Maintainability Verification/Demonstration/Evaluation", USA DoD, 27 March 1973
MIL-STD-721C	"Definitions of Terms for Reliability and Maintainability", USA DoD, 12 June 1981
MIL-STD-756B	"Reliability Modelling and Prediction", USA DoD, 18 November 1991
MIL-STD-781D	"Reliability Testing for Engineering Development, Qualification and Production", USA DoD, 17 October 1986
MIL-STD-785B	"Reliability Program for System and Equipment Development and Production", USA DoD, 15 September 1980

CENELEC SC9XA Ad Hoc	HAZARDOUS FAILURE RATES AND SAFETY LEVELS „Definition, methodology and figures to achieve cross-acceptance in Europe“, meeting in Marseille in June 1996
JAR 25	Joint Airworthiness Requirements, JAR 25, Large Aeroplanes, Section 1309, equipment, systems and installation.
Book	Michael R. Lyu, "Handbook of Software Reliability Engineering", IEEE Computer Society Press, McGraw-Hill, 1996 ISBN 0-07-039400-8
Memo	Dr. H. Krebs “Problems of a practicing Surveyor in applying the current draft CENELEC and IEC standards for the testing of safety-critical systems”, Proceedings of Forum European Railway Safety Standards (FERS) 1995

Glossary

The following definition arise in part from European and international standards and in part from EEIG ERTMS Users Group terminology. The source relevant to each definition is shown in parenthesis. The acronym EUG is for EEIG ERTMS Users Group.

Definitions

Application Level	Application Levels of the *ERTMS Control/Command* system are levels to which a given part of line, or an entire line, or a vehicle can be equipped with *ERTMS Control/Command* and other equipment. The Application Level and the information available from the signalling system, together with a railway's operating principles, determine the performance level of the ERTMS Control/Command system (EUG)
Assembly	A number of parts or subassemblies or any combination thereof joined together to perform a specific function and capable of disassembly (MIL STD 1388-2B)
Availability	The ability of a product to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval assuming that the required external resources are provided (EN50126)
Availability, Achieved	The ratio between the Up-time and the Total-time of a system or equipment including all repair time (corrective and preventive time), administrative and logistic time (MIL-HDBK-388-1A)
Availability, Intrinsic	Probability that a system or equipment is operating satisfactorily at any point in time when used under stated conditions, where the time considered is operating time and active repair time. Preventive maintenance, administrative and logistic times are excluded (MIL-HDBK-388-1A)
Availability, Operational	see Availability, Achieved
Conditions, Environmental	The characteristics of the application environment (EUG)
Conditions, Failure	The identification of failures of *ERTMS Control/Command* functions and the characterisation of their effects in term of criticality. *ERTMS Control/Command* failures are divided in three classes: • immobilising • service • minor (EUG)
Conditions, Maintenance	The maintenance criteria adopted for maintaining the system referred to its Operating Conditions (EUG)

Conditions, Operating	The rated performance required to the system (EUG)
Conditions, System	The conditions under which the system is called to operate, including: • environmental conditions; • operating conditions; • maintenance conditions (EUG)
Contractor	A private sector enterprise or the organisational element of a national railway responsible, against the Project Management, for the system integration in the context of each specific *ERTMS* application, and for all the Sub-contractors and Suppliers activities within agreed limits specified by the Customer (EUG)
Criticality	A relative measure of the consequence of a failure mode and its frequency of occurences (MIL-STD-721C)
Customer	The European national railways which intend to apply *ERTMS* (EUG)
Dependability	The ability of a product to perform one or several required functions under given conditions (EN 50126)
Downtime	The time interval during which a product is in a down state (EN 50126 / IEC50(191))
Context Weakness Parameters	Software function parameters utilised for providing an estimation of the probability that software defects become effective during the function execution and then cause a system failure (EUG)
Environment	The aggregate of all external and internal conditions (such as temperature, humidity, radiation, magnetic and electric fields, shock vibration, etc.) either natural or man made, or self-induced, that influences the form, performance, reliability or survival of an item (MIL-STD-721C)
Equipment/Set	A unit or units and necessary assemblies, or subassemblies and parts connected together or used in association to perform an operational function (MIL-STD-280A)
Error	An error is that part of the system state which is liable to lead to failure. A failure occurs because the system is erroneous (IEC Draft 1508)
ERTMS Control/Command	The European Railway Train Management System, defined from a train onboard point of view, composed by the onboard equipment and all the lineside and trackside equipment necessary for supervising, in real-time, the train operation according to the traffic conditions in reason of the appropriate Level of Application.

	The *ERTMS Control/Command* equipment boundary limits, both physical and functional, are defined in accordance to what is stated in the system FRS and SRS (EUG)
Failure	A system failure occurs when the delivered service deviates from the intended service. A failure is the effect of an error on the intended service (IEC Draft 1508)
Failure, Immobilising	An *ERTMS Control/Command* failure which causes the system to be unable to safely control two or more trains (EUG)
Failure, Minor	A failure which results in excessive unscheduled maintenance and cannot be classified in the above defined failure conditions (EUG)
Failure Rate	The limit, if exists, of the ratio of the conditional probability that the instant of time, T, of a failure of a product falls within a given time interval (t + δt) and the length of this interval, δt, when δt tends toward zero, given that the item is in an up state at the start of the time interval (EN50126)
Failure Risk Matrix	Matrix that correlates the failure effects, defined by the function criticality, and the probability of failure appearance, defined by the function weakness class (EUG)
Failure, Service	An *ERTMS Control/Command* failure which causes the nominal performance of one or more trains to be reduced and/or the system to be unable to safely control at most one train (EUG)
Fault	The cause of an error is a fault (e.g. hardware defect, software defect) which resides, temporarily or permanently, in the system (IEC Draft 1508)
Functional Profile	Profile of functions, where profile is a set of disjoint alternatives, each with the probability that it will occur (EUG)
Immobilising Failure	see Failure, Immobilising (EUG)
Interoperability, Operational	The ability of enabling the international safe running of trains on different European networks without: *a.* having to stop the train at borders; *b.* changing the engine at borders; *c.* changing the driver at borders; *d.* requiring the train driver to perform any other activity different from the standardised ERTMS operation
(EUG)	Interoperability, Technical A subset of operational interoperability, when condition *d.* is not fulfilled (EUG)

Lifecycle, System	The activities occurring during a period of time that starts when a system is conceived and ends when the system is no longer available for use (IEC draft 1508)
Lifecycle Cost, System	The total cost of acquiring and utilizing a system over its entire life span (MIL-HDBK-388-1A)
Lineside Equipment	see Trackside Equipment (distributed) (EUG)
Logistic Support Resources	The overall resources which are arranged and organised in order to operate and maintain the system at the specified availability level at the required lifecycle cost (EN 50126)
Maintainability	The probability that a given active maintenance action, for an item under given conditions of use can be carried out within a stated time interval when the maintenance is performed under stated conditions and using stated procedures and resources (EN 50126 / IEC50(191))
Maintenance System	A composite of all maintenance resources that must be acquired for maintaining the system throughout its life cycle, including: • spare parts data/documentation/storage; • maintenance procedures; • maintenance manuals; • maintenance facilities (power supplies, offices, building of testing centres); • external testing equipment; • special tools; • training of maintenance personnel (EUG)
Maintenance	The combination of all technical and administrative actions, including supervision actions, intended to retain a product in, or restore it to, a state in which it can perform a required function (EN 50126/IEC50(191))
Maintenance, Corrective	The maintenance carried out after fault recognition and intended to put a product into a state in which it can perform a required function (EN 50126 / IEC50(191))
Maintenance Levels	The basic levels of maintenance into which all maintenance activity is divided. (EN 50126)
Maintenance, Preventive	The maintenance carried out at pre-determined intervals or according to prescribed criteria and intended to reduce the probability of failure or the degradation of the functioning of an item (EN 50126/ IEC50(191))
Malfunction	see Failure

Minor Failure	see Failure, Minor (EUG)
Mission Profile	A description of the expected performance of the system in the operational phases of the lifecycle (EN50126)
OnBoard Equipment	see Trainborne Equipment (EUG)
Overlay, Overlaid	A *ERTMS Control/Command* application where *ERTMS Control/Command* cooperate with existing systems for accomplishing its mission (EUG)
Part	One piece, or two or more pieces joined together which are not normally subject to disassembly without destruction of designed use (MIL-STD1388-2B)
Project Management	All those activities related to manage the project at the Customer level, including: • system requirements definition; • ensuring the planning, implementation and accomplishment of project related tasks and activities; • definition of roles and responsibilities; • definition of resources (EUG)
Quality of Service	The collective effect of service performance which determines the degree of satisfaction of a user of a service (EN 50126)
RAM(S) Programme Plan	A document which declares organisation, methodologies, tools and timing for performing the RAM Programme activities (EUG)
RAM(S) Programme	A documented set of time scheduled activities, resources and events serving to implement the organisational structure, responsibilities, procedure, activities, capabilities and resources that together ensure that an item will satisfy given RAM requirements relevant to a given contract or project. (EN 50126 /IEC50(191))
RAM(S) Requirements	The qualitative and quantitative RAM(S) characteristics which the system has to comply with (EUG)
Reliability Growth	A condition characterised by a progressive improvement of a reliability performance measure of an item with time (EN 50126 / IEC50(191))
Reliability	The probability that an item can perform a required function under given conditions for a given time interval (t_1, t_2) (EN 50126 / IEC50(191))
Reliability, Basic	The duration or probability of failure-free performance under stated conditions. Basic reliability terms shall include all item life units (not just mission time) and all failures within the items (not

	just mission-critical failures at the item level of assembly). Basic reliability requirements is capable of describing item demand for maintenance manpower. The other system reliability parameters employ clearly defined subset of all item life units and all failures (MIL-STD-785B)
Reliability, Mission	The ability of an item to perform its required functions for the duration of a specified mission profile (MIL-STD-721C)
Safety Integrity Level	One of 4 possible discrete levels for specifying the safety integrity requirements of the safety functions to be allocated to the safety related systems. Safety Integrity Level 4 has the highest level of safety integrity and Safety Integrity Level 1, the lowest (EN 50126)
Safety Integrity	The probability of a system satisfactorily performing the required safety functions under all stated conditions within a stated period of time (EN 50126)
Schedule Adherence	The ability of a railway system of complying with the schedule of train running (EN 50126)
Service Failure	see Failure, Service (EUG)
Software	Intellectual creation comprising the programs, procedures, rules and any associated documentation pertaining to the operation of a data processing system (ISO9000/3)
Software Component	Software unit ‘considered logically indivisible’ (for example in the Modula II, Pascal, or C programming languages this term represents one Procedure or one Function) (EUG)
Software Integrity Level	A classification number which determines the techniques and measures that have to be applied in order to minimise residual software faults (prEN50128:1995)
Software Integrity	A measure that signifies the likelihood of software achieving its functions under all stated conditions within a stated period of time (prEN50128:1995)
Software Lifecycle	The activities occurring during a period of time that starts when the software is conceived and ends when software is no longer available for use (prEN50128:1995)
Software Quality	The totality of features and characteristics of a software product that bear on its ability to satisfy stated or implied needs (ISO9000-3)
Spare Parts on Stock	The spare parts which are available on stock (EUG)
Spares	Articles identical to or interchangeable with the end articles on contract which are procured over and above the quantity needed for initial installation for support of a system (MIL-STD-1388-2B)

SQA Plan	The document(s) which formalise(s) all those activities, both technical and managerial, which are necessary to ensure that the software achieves the quality required (prEN50128:1995)
SQA Programme	A documented set of time scheduled activities, both technical and managerial, which are necessary to ensure and to demonstrate, by providing the appropriate evidence, that the software achieves the required level of quality (prEN50128:1995)
Structural Weakness Parameters	Software function parameters utilised for providing an estimation of the probability of injecting defects n the software modules during the software development process (EUG)
Subassembly	Two or more parts which form a portion of an assembly or a unit as a whole, but having a part or parts which are individually replaceable (MIL-STD1388-2B)
Sub-Contractor	A subject responsible, against the Contractor, for providing services or products in the context of *ERTMS*; the sub-contractor is also responsible, if applicable, for its Suppliers within agreed limits specified by the Contractor (EUG)
Subsystem	A combination of equipment, units, assemblies, etc., which performs an operational function and is a major subdivision of the system (MIL-STD-721C)
Supplier	Each subject called to directly design and/or produce parts of the *ERTMS* system (EUG)
System	A composite of equipment, skills, and techniques capable of performing or supporting an operational role, or both. A complete system includes all equipment, related facilities, material, software, services and personnel required for its operation and support to the degree that it can be considered a self-sufficient unit in its intended operational environment (MIL-STD-721C)
System Lifecycle	The activities occurring during a period of time that starts when the system is conceived and ends when system is no longer available for use (EN 50126)
System Quality Plan	The document(s) which formalise(s) all those activities, both technical and managerial, which are necessary to ensure that the system achieves the quality required (EUG)
Trackside Equipment	The equipment with the aim of exchanging information with the vehicle for safely supervising train circulation. The information exchanged between track and trains can be either continuous or discontinuous according to the ERTMS Level of Application

	and to the nature of the information itself. Trackside Equipment is subdivided in two classes: • centralised; • distribuited, also called Lineside Equipment
(EUG)	
Trainborne Equipment	The equipment with the aim of supervising vehicle operation according to the information received from infrastructure installations, from other nonERTMS onboard equipment, from the driver and from the trackside signalling system (EUG)
Unit	An assembly or any combination of parts, subassemblies and assemblies mounted together, normally capable of independent operation in a variety of situations (MIL-STD-280A)
Unsafe state	ERTMS System state due to technical Hazards (excluding the human factor and the external systems), which could lead to an accident.
Validation	Confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use have been fulfilled (IEC draft 1508)
Validation Team	A workgroup jointly chaired by the Customer, responsible for all the specific aspects of the supplying contract, and by EEIG ERTMS Users Group, responsible for the aspects concerning interoperabilty, and composed by technical and RAMS personnel of EEIG ERTMS Users Group, of the Customer, of the Contractor, of the Sub-contractor(s) and of the Supplier(s) whose aim is to analyse the data resultant from the verification, to require corrective measures where necessary and to provide the RAMS Validation (EUG)
Verification	Confirmation by examination and provision of objective evidence that the specified requirements have been fulfilled (IEC draft 1508)
Weakness	Property of the software function utilised for providing an estimation the function liability to fail, due to the software structure and to the environmental conditions (EUG)
Weakness Graph	Qualitative graphical method utilised for giving the ERTMS Control/Command functions the appropriate weakness class, according to the factor, derived by the parameters estimation (EUG)
shall	Means that the relevant verb refers to a requirement
should	Means that the relevant verb refers to a recommendation

can	Means that the relevant verb is permitted
may	Means that the relevant verb is possible

Acronyms and symbols

®	Symbol utilised for addressing system requirements along the text of the document
ATO/ATP	Automatic Train Operation/Automatic Train Protection
A_{HW}	Availability of Hardware
$A_{HW,I}$	Mean availability target for Hardware from Immobilising failures per year
$A_{HW,S}$	Mean availability target for hardware service failures per year
$A_{HW,M}$	Mean availability target for hardware minor failures per year
A_{OP}	Operational Availability
A_{TX}	Contribution to availability from Transmission errors
$A_{TX,C}$	Contribution to availability from continuous Transmission errors
$A_{TX,D}$	Contribution to availability from discontinuous Transmission errors
$a_{X,i}$	Allocation factor for the function $f_{X,I}$
BTM	The **B**alise **T**ransmission **M**odule shall interrogate the balises encountered in the track as the trainborne antenna passes them.
CENELEC	Comité Européen de Normalisation Electrotechnique
CMA	Corrective Maintenance Analysis
CTODL	**C**urrent **T**ime and **O**dometer **D**istribution **L**ine is designed to provide all modules with frequent up-to-date time, train position, train speed and other train data.
DC	Data Complexity
DR	Defects Reduction
DS	Data Structure Complexity
DT_{HW}	Downtime allowed for hardware failures
$DT_{HW,I}$	Mean downtime allowed for hardware immobilising failures per year
$DT_{HW,S}$	Mean downtime allowed for hardware service failures per year
$DT_{HW,M}$	Mean downtime allowed for hardware minor failures per year
$DT_{TX,C}$	Mean downtime per year due to continuous Transmission errors
$DT_{TX,D}$	Mean downtime per year due to discontinuous Transmission errors
DT_X	Downtime allowed for X criticality failures due to HW
$DT_{X,i}$	Downtime requirement allocated to the function $f_{X,i}$
$DT_{TX,i}$	Downtime due to transmissions which may assume two values: DT_{CON} for continuous TX DT_{DIS} for discontinuous TX

	or the sum of the two values according to the type of communications required by the function $f_{X,i}$
EB	Emergency Braking
EBC	Emergency Braking Curve
ERTMS	European Rail Traffic Management System
ERTMS-T	It is the trackside of the ERTMS
ETCS	European Train Control System
EUG	EEIG ERTMS Users Group.
EVC	The functions which are located in the **E**uropean **V**ital **C**omputer have very high safety relevance.
FC	Control Flow Complexity
Fd	Defect-caused Failures Frequency
FMEA	Failure Mode and Effect Analysis
FMECA	Failure Mode, Effect and Criticality Analysis
FRACAS	Failure Reporting and Corrective Actions System
FRS	Functional Requirements Specification
FSB	Full Service Braking
FSBC	Full Service Braking Curve
FT	Fault Tolerance Features
FTA	The **F**ault **T**ree **A**nalyses is a graphical method of expressing the logical relationship between a particular failure condition and the failures or other causes leading to the particular failure condition.
$f_{X,i}$	*X* criticality function *i*;
GSM	Global System for Mobile Communications
HF	Human Factor Features
HW	Hardware
$k_{X,i}$	on/off factor: *0* if $f_{X,i}$ does not require communications *1* if $f_{X,i}$ requires communications
I	Immobilising
IL	Integrity Level
ISO	International Standardisation Organisation
LAT	Lineside Active Transducer
LCU	Lineside Control Unit
LNS	Lineside or Trackside Distributed
LPT	Lineside Passive Transducer
LTM	The **L**oop **T**ransmission **M**odule for track mounted semicontinuouse transmission shall be able to receive telegrams from the track mounted semicontinuous transmission device.

M	Minor
MA	Movement Authority
MC	The aim of the **M**anagement **C**omputer is to handle the non-vital trainborne ERTMS functions. To achieve this, the MC must receive the necessary train or track data and process them separately from the safety computations carried out in the EVC.
MMI	All functions which have to be shown to the driver and all choices of the driver are indicated on the **M**an **M**achine **I**nterface .
MTBF	Mean Time Between Failures
$MTBF\text{-}I_{ONB/TRK/LNS}$	Mean Time Between Immobilising Failures Onboard/Trackside/Lineside
$MTBF\text{-}M_{ONB/TRK/LNS}$	Mean Time Between Minor Failures Onboard/Trackside/Lineside
$MTBF\text{-}S_{ONB/TRK/LNS}$	Mean Time Between Service Failures Onboard/Trackside/Lineside
MTTR	Mean Time To Repair
MTTRS	Mean Time To ReStore
Nd	Expected Number of Defects
NVF	The vital functions of the radio block center are located in the **N**one **V**ital computer. These functions have not a very high safety relevance.
OC	Occurrences Level
OCSI	Onboard Complex System Interface
OGA	Onboard GSM Apparatus
OIRT	Onboard Intermittent RX/TX apparatus
ONB	On board
OSI	Onboard System Interface
OSM	Onboard Safe Module
OUI	Onboard User Interface
OUSM	Onboard Unsafe Module
P_{ds}	Probability of having delay due to ERTMS failures
PMA	Preventive Maintenance Analysis
RAM(S)	Reliability Availability Maintainability (Safety)
RBC	Radio Block Centre
Rd	Defects and Failures Reduction
RF	The **R**ecording **F**unction is optional. Its purpose is to record all events reported over the ERTMS Bus and to record these together with the time and odometer values at the time of reporting.

RIM	The **R**adio **I**nformation **M**odule shall be transparent to the messages passing it. It shall be able to distinguish between messages for the ERTMS functions and other messages.
RPP	Reliability Programme Plan
S	Service
SIL	Safety integrity level
SQA	Software Quality Assurance
SRS	System Requirements Specification
SSP	Static Speed Profile
SSRS	Sub-system Requirements Specification
STM	The trainborne equipment of the ERTMS must be able to be interfaced with the trainborne equipment of existing train supervision systems. The **S**pecific **T**ransmission **M**odule shall perform a translation function between these systems and the ERTMS.
SW	Software
SZ	Size
SZ1	Estimated Code Length
SZ2	Estimated Code Volume
TCCS	Train Control Command System
TCO	Traction Cut Off
TCOC	Traction Cut Off Curve
TCSI	Trackside Complex System Interface
T_{dn}	Average duration of not delayed trips
T_{dnd}	Average duration of delayed trips
T_{dy}	Acceptable average delay
TF	Time Features
T_{fault}	Time of ERTMS fault condition
TGA	Trackside GSM Apparatus
TIF	The **T**rain **I**nterface **F**unctions are designed to interface a large number of ERTMS functions or individual railway functions that will be technically very dependent on the vehicle type and accordingly cannot be directly connected to the ERTMS trainborne equipment or which are not part of the ERTMS, but which may be useful connected to the ERTMS.
TOF	The **T**ime and **O**dometer **F**unctions have to provide all other modules via a distribution network with frequent messages giving the odometer reading, train velocity, acceleration and a clock reading.

T_{op}	Time of ERTMS correct operation
TRK	Trackside Centralised
TSI	Trackside System Interface
TSM	Trackside Safe Module
T_u	Time of ERTMS unavailability per year
TUSM	Trackside Unsafe Module
V&V	Verification and Validation
VF	The **V**ital **F**unctions of the radio block center are located in the Vital computer. These functions have a very high safety relevance.
WC	Weakness Class
X criticality function	I=IMMOBILISING,S=SERVICE,M=MINOR