European Rail Infrastructure Managers EIM

Position Paper

ETCS On-board Subsystem

Reliability Requirement for Operational Safety

06.10.2014

TABLE OF CONTENTS

Appendices

1. Introduction

1.1 Background

The European Commission (EC) Decision 2012/88/EU of 25 January 2012 [1] lays down the Technical Specification for Interoperability (TSI) relating to the Control-Command and Signalling (CCS) subsystems of the trans-European rail system. Availability and Reliability requirements for the On-board and Track-side subsystems are covered in Section 4.2.1.2 and Annex A 4.2.1.b of the document. However, Index 28 in Annex A, marked as "Reserved", does not contain any quantitative Reliability requirements for the ERTMS/ETCS subsystems.

As a result, Infrastructure Managers (IM) and/or Railway Undertakings had to derive quantitative Reliability requirements, either contract specific or at national level, using different considerations: commercial, Safety or both [2]. This approach could be seen as going against the principles of interoperability, particularly with regards to the CCS On-board subsystem, and could potentially lead to degraded situations the management of which could decrease the overall Safety of the system.

In an attempt to resolve this issue, in December 2012 UNISIG produced a paper [3] in which a Mean Time Between Immobilising Failures (MTBIF) for the On-board subsystem was derived based on Operational Safety considerations.

Note: *In the context of the UNISIG document, an 'immobilising failure' is defined as 'in general the CCS On-board subsystem is switched off and the train can only finish its mission without CCS On-board subsystem supervision'*.

After reviewing the UNISIG document, the members of the European Rail Infrastructure Managers (EIM) rejected the proposed MTBIF value as being too low and generally below the values that had already been derived or observed independently by EIM members. Disagreement with the Operational parameters assumed in the paper in order to derive the MTBIF value was also indicated on the basis that they were not covering the full range of values seen across the trans-European system.

However, EIM have indicated agreement with the following principles:

- Minimum Reliability requirements for the On-board subsystem should be defined in the TSI CCS, whilst Reliability requirements for the Track-side subsystems would be determined at a national level;
- The minimum Reliability requirements for the CCS On-board subsystem apply only to 'immobilising failures';
- The minimum Reliability requirements for the On-board subsystem are linked to Operational Safety.

Following consultation with the European Rail Agency (ERA) and in particular the workshop of 29 April 2014, the Railway Interoperability and Safety Committee (RISC) are proposing an amendment of the TSI CCS [4] to include, among others, the principles outlined above and corresponding quantitative Reliability requirements for the On-board subsystem. However, agreement on the numerical value to be included in the revised document is yet to be reached.

1.2 Purpose

The purpose of this document is to propose a quantitative Reliability requirement for the ETCS On-board subsystem for inclusion in the amendment of the TSI CCS and therefore applicable to the trans-European rail system. This requirement is derived based on Operational Safety principles and applies only to the On-board subsystem failures requiring isolation of the train protection functions.

1.3 Scope

The scope of this document covers the Reliability of the ETCS On-board subsystem with its functional constituents as defined in the TSI CCS [1].

1.4 References

[1] European Commission Decision on the Technical Specification for Interoperability relating to the Control-Command and Signalling subsystems of the trans-European rail system, Ref: 2012/88/EU, 25 Jan 2012.

[2] ERTMS Users Group, Reliability Study Oct 2009/Feb 2010, Issue A05, Ref: NR/EE/REP/00184, Sep 2010.

[3] UNISIG, ERTMS/ETCS – Reliability Requirement for CCS Onboard Subsystem from the viewpoint of operational safety, Issue 1.0.3, 14 Dec 2012.

[4] RISC, Draft Commission Decision amending Commission Decision 2012/88/EU on the technical specification for interoperability relating to the control-command and signalling subsystems of the trans-European rail system, Ref: 08/57-ST30, 16 May 2014.

1.5 Document structure

In addition to this section, Introduction, the document includes further sections as follows:

- Section 2: describes the approach to deriving the Reliability requirement;
- Section 3: includes the quantitative Reliability requirement for the ETCS On-board subsystem;
- Section 4: describes the proposed approach to demonstrating compliance with the requirement.

1.6 Abbreviations

CCS	Control Command & Signalling
EC	European Commission
EIM	European Rail Infrastructure Managers
ERA	European Rail Agency
ERTMS	European Rail Traffic Management System
ETCS	European Train Control System
EU	European Union
IM	Infrastructure Managers
MTBIF	Mean Time Between Immobilising Failures
TSI	Technical Specification for Interoperability

2. APPROACH

2.1 Definitions

The following terminology is used throughout this document:

Failure	Means the termination of the ability of an item to perform a required function with the required performance
Failure Mode	Means the effect by which the Failure is observed
Immobilising Failure	A Failure of the CCS On-board subsystem requiring isolation of the train protection function
Mean Time Between Immobilising Failures	The arithmetic mean of the time between successive independent Immobilising Failures

2.2 Principles

The derivation of the Reliability requirement for the CCS On-board subsystem presented in this paper follows the following principles:

ID	Principle	Rationale
1	Minimum Reliability requirements for CCS On-board subsystem are included in the TSI CCS. Reliability requirements for the CCS Track-side subsystem are derived at national level.	The requirements for the CCS On-board subsystem are applicable to the trans-European system. The Reliability of the Track-side subsystem is managed at national level by the Infrastructure Managers.
2	The minimum Reliability requirement for the CCS On-board subsystem is derived based on Operational Safety considerations.	To enable Infrastructure Managers to manage degraded situations without decreasing the overall Safety of the system.
3	The minimum Reliability requirement for the CCS On-board subsystem applies to Immobilising Failures only.	An Immobilising Failure requires isolation of the train protection function and its removal from service, thus generating a degraded situation.
4	The system Safety level is decreased when a single Immobilising Failure occurs.	The train movement with CCS On-board protection function isolated could create hazardous situations for all the trains in the area.
5	The Infrastructure Managers do not have the authority to deny access to their network to vehicles having lower Reliability than the minimum requirement.	As per European Union Rules and Regulations.
6	The Infrastructure Managers cannot apply higher track access charges to vehicles having lower Reliability than the minimum requirement.	This is against the EC legislation.
7	The Reliability requirement for the CCS On-board subsystem is related to the most severe Operating conditions in the trans-European system.	The requirement needs to be applicable to each specific ERTMS/ETCS implementation in the EU.
8	An Immobilising Failure can occur as the result of a failure of a single constituent of the CCS On-board subsystem (single point failure) or as a result of a combination of failures of two or more constituents.	All causes of Immobilising Failures need to be considered.
9	An Immobilising Failure can be caused by functional failure of CCS On-board subsystem constituents or failure of the interface between subsystem constituents.	Subsystem integration issues at the interface between constituents can generate Immobilising Failures.

2.3 Assumptions

The general assumptions used in the derivation of the Reliability requirement for the CCS On-board subsystem are as follows:

ID	Assumption	Rationale
1	Immobilising Failures of the CCS On-board subsystem include both hardware and software failures.	In accordance with the Systems Engineering principles, the hardware and software elements cannot be separated as both contribute to the successful operation of a system/subsystem.
2	A train experiencing an Immobilising Failure cannot continue its mission.	As a result of the Immobilising Failure the train protection function needs to be isolated and hence the CCS On-board supervision is lost. The train mission is terminated.
3	The derivation of the minimum Reliability requirement assumes steady-state Reliability, i.e. constant failure rates.	The Safety considerations during a Reliability growth period would be different from the steady-state operation. Therefore the approach to managing degraded situations during that period would be different.
4	The minimum Reliability requirement for the CCS On-board subsystem is expressed as Mean Time Between Immobilising Failures (MTBIF).	As stated in the amendment to the TSI CCS [4]
5	Derivation of the minimum Reliability requirement is based on an operational scenario where the railway network in an area controlled by a signalman is at its busiest time of the day: peak hours. It is assumed that two such busy periods occur during a typical operational day: morning peak and afternoon peak.	In accordance with Principle 7 in previous section, most severe Operating conditions need to be used in deriving requirements.

2.4 Analysis scenario

The scenario analysed for the purpose of deriving the Reliability requirement is based on the UNISIG paper [3] and the principles outlined above and can be described as follows:

- Operating environment: the railway network in an area controlled by a signalman during peak hours.
- Operating status: the railway network is in Normal Operation state.

- A train moving through the area experiences an Immobilising Failure. This can be caused by the CCS On-board subsystem or any other On-board subsystem. Thus a degraded situation has occurred.
- The signalman needs to confirm the failure and manage the safe removal of the train from the area.
- During the time it takes to remove the affected train and return the controlled area to its Normal Operation, the likelihood of a second train experiencing an Immobilising Failure, caused by the CCS On-board subsystem or any other On-board subsystem, must be as low as reasonable practicable.

2.5 Operational parameters

The Operational parameters involved in the scenario described above are as follows:

Parameter (units)	Description	Comments
PE (events/yr per controlled area)	The frequency of peak hour periods within the controlled area.	This would depend on national railway and location of the controlled area. Typically two such periods per day are observed: morning peak and afternoon peak.
Tpe (hrs)	The duration of the peak hour period when the railway network is at its busiest.	It would depend on national railway and location of controlled area.
IFccs (failures/hr)	Failure rate for Immobilising Failures of the CCS On-board subsystem	Under steady-state Reliability conditions, IF_{CCS} = 1/MTBIF; An MTBIF value needs to be derived as the Reliability requirement for the CCS On-board subsystem.
r	The ratio between failure rate for Immobilising Failures caused by *any* On-board subsystems *other* than CCS to the failure rate IFccs for CCS.	This would depend on type of rolling stock, its age, maintenance regime, etc. Higher values of this parameter are expected for old rolling stock where CCS On-board subsystem is retro-fitted; lower values are expected for new, modern rolling stock.
N	Number of trains present within controlled area at the time Immobilising Failure occurs	Varies at national level from IM to IM. The number would vary according to the size of the railway network, train frequency, number of control centres, etc.

Parameter (units)	Description	Comments
Tr (hrs)	Time taken to remove affected train from the area and return to Normal Operation	Would vary according to the number of trains N and also rolling stock class, size of the network, time of the day (peak, off-peak), etc.
HE (events/yr per controlled area)	The frequency of a second Immobilising Failure occurring within the controlled area during time Tr.	This would depend on the failure rate IF_{CCS}, the time Tr and the number of trains in the area N. Acceptable values would vary at national level from IM to IM.

3. RELIABILITY REQUIREMENT

The minimum Reliability requirement for the CCS On-board subsystem is:

MTBIF = 100,000hrs

The equation used to estimate this value is given below (for detailed calculations see Appendix 1):

$$MTBIF(hrs) = \sqrt{\frac{(1+r)^2 xNx(N-1)xT_{pe}xTr}{HE(event/yr)/PE(event/yr)}}$$

The Operational parameters used in the equation above to estimate the MTBIF value are given in the table below:

Parameter	Value	Justification
PE	730 events/yr	Two peak periods per day have been assumed throughout the year.
Tpe	3hrs	Typical duration of a peak period.
r	10	A typical value can be estimated from data collected from rolling stock with fitted CCS On-board subsystem. From UK operational experience with class 158 on Cambrian Line ETCS application, an approximate value of 7 has been estimated. Since most stringent Operation conditions need to be considered, a value of 10 for this parameter is considered suitable.

Parameter	Value	Justification
N	50	A value of 30 trains has been quoted for the Netherlands, whilst in the UK values just over 50 trains have been observed around busiest areas at peak time. The maximum value of 50 trains is considered to cover most stringent Operation conditions.
Tr	2hrs	This is considered to be maximum time required under stringent Operation conditions (peak time, busy area, etc) to remove faulty train and return to normal operations.
HE	0.1 events/yr per area	The value of this parameter depends on the risk acceptability criteria used by each IM. To check acceptability of the proposed value, consideration should be given to the following: o 0.1 events/yr at local level (controlled area/signalman) translates into 1 hazardous event occurrence every 10yrs; o At national level, for 10 controlled areas/signalmen, this value translates into 1 hazardous event every year.

4. DEMONSTRATION

To ensure that the relevant IM are given all the information they need to define appropriate procedures for managing degraded situations, the applicant for the authorisation of a CCS On-board subsystem shall provide to the IM calculated Reliability values for failure modes requiring the isolation of the train protection functions.

Appendix 1 Reliability requirement calculation

1. Reliability at time t, R(t), can be defined as the probability of an item to survive to time t; for steady-state Reliability, the item failure rate is constant and the reliability can be estimated as:

$$R(t) = e^{-\lambda t}$$

where λ is the item failure rate.

2. The probability of item failing between 0 and time t is then:

$$F(t) = 1 - R(t) = 1 - e^{-\lambda t}$$

3. Using the above definitions, the probability of a train experiencing an Immobilising Failure, caused by any On-board subsystem, during the peak period Tpe within the controlled area can then be written as:

$$1 - e^{-IF_{CCS} x (1+r) x Tpe}$$

4. For N trains present in the controlled area during the time Tpe, the probability that at least one of them fails is then:

$$1 - e^{-IF_{CCS} x (1+r) x N x Tpe}$$

5. Similarly, the probability of at least one other train experiencing an Immobilising Failure caused by any On-board subsystem within the time interval Tr taken to remove the first failed train and return to Normal Operation can be written as:

$$1 - e^{-IF_{CCS} x (1+r) x (N-1) x Tr}$$

6. Both events described above (items 4 and 5) need to happen in order to give rise to a hazardous event HE and therefore the two probabilities need to be multiplied to obtain the probability of a hazardous event:

$$(1 - e^{-IF_{CCS} x (1+r) x N x Tpe}) x (1 - e^{-IF_{CCS} x (1+r) x (N-1) x Tr})$$

7. The exponential function e^{-x} can be expanded into a series as follows:

$$e^{-x} = 1 - x + \frac{x^2}{2!} - \frac{x^3}{3!} \pm \ldots = \sum_{n=0}^{\infty} \frac{(-x)^n}{n!}$$

and for values of x << 1, the above series can be approximated with:

$$e^{-x} \approx 1 - x$$

8. Using this approximation, the probability of a hazardous event at 6) above can be written as:

$$\left[IF_{CCS}\, x(1+r)\, xNxTpe\right] x \left[IF_{CCS}\, x(1+r)\, x(N-1)\, xTr\right]$$

Note: a comparison between the probability values calculated using Eqs 6) and 8) with Operation parameter values given in Section 3 is shown at the end of this Appendix.

9. If PE is the frequency of peak hour periods in the controlled area during which N trains are present, then the frequency of hazardous events can be estimated as:

$$HE(event/\,yr) = PE(event/\,yr)\, x(1+r)^2\, xNx(N-1)\, xIF_{CCS}^2(\,failure/\,hr)\, xT_{pe}\, xTr$$

10. The above equation can be solved for IF_{CCS}(failure/hr):

$$IF_{CCS}\,(\,failure\ \ /\,hr\,) = \sqrt{\frac{HE\ (event\ \ /\,yr\,) / PE\ (event\ \ /\,yr\,)}{(1+r)^2\, xNx\ (N\ -1)\, xT_{\,pe}\, xTr}}$$

or

$$MTBIF(hrs) = \frac{1}{IF_{CCS}(\,failure/\,hr)} = \sqrt{\frac{(1+r)^2\, xNx(N-1)\, xT_{pe}\, xTr}{HE(event/\,yr) / PE(event/\,yr)}}$$

11. Using the Operation parameter values given in Section 3,

$$MTBIF\,(hrs) = \sqrt{\frac{(1+10)^2 x 50 x (50-1) x 3(hrs) x 2(hrs)}{0.1(event\,/\,yr)\,/\,730(event\,/\,yr)}} = 113{,}950 hrs$$