European Railway Agency

Executive Director

OPINION

ERA/OPI/2014-8

OF THE EUROPEAN RAILWAY AGENCY

FOR

EUROPEAN COMMISSION

REGARDING

QUESTION OF UNIFE - APPLICATION GUIDE RELATED TO THE ERTMS MAINTENANCE RELEASE 1

Disclaimer:

The present document is a non-legally binding opinion of the European Railway Agency. It does not represent the view of other EU institutions and bodies, and is without prejudice to the decision-making processes foreseen by the applicable EU legislation. Furthermore, a binding interpretation of EU law is the sole competence of the Court of Justice of the European Union.

1 General Context

1. In its letter referenced as MOVE/B2/JS/fz and dated 9/12/2014 addressed to the European Railway Agency (ERA), the European Commission requested ERA to prepare a technical opinion regarding the issues described in a letter from UNIFE dated 21/11/2014 (see annex 3 to this Technical Opinion).
2. The question is related to the Commission Decision 2012/88/EU of 25 January 2012 on the technical specification for interoperability relating to the control-command and signalling subsystems[1] ("CCS TSI"), more in particular to some hazardous situations for the functions of the ETCS Driver Machine Interface (DMI), evaluated in the informative specification SUBSET-118, version 1.2.6 and included in the mandatory requirements of SUBSET-091 version 3.3.0 (listed in Annex A of the CCS TSI).
3. UNIFE notes that there are editorial inconsistencies between the results of the evaluation and the values of three of the Tolerable Hazard Rates (THR) indicated in SUBSET-091.
4. This Technical Opinion analyses the issues presented in the UNIFE letter and provides indication for correction of errors in both SUBSET-091 and SUBSET-118 that could have negative impact on the certification of ETCS on-board Interoperability Constituents.

2 Legal Background

1. Article 10 (2b) of Regulation (EC) No 881/2004 of the European Parliament and of the Council of 29 April 2004 establishing a European Railway Agency[2] (Agency Regulation), together with art 7 (1) of Directive 2008/57/EC of the European Parliament and of the Council of June 2008 on the interoperability of the rail system within the Community[3] (Interoperability Directive) provide the European Commission with the possibility to request an opinion from the Agency on urgent modifications to TSIs concerning "deficiencies in the TSIs".
2. The Interoperability Directive sets out the principles concerning the placing on the market of Interoperability Constituents and the EC verification of subsystems.
3. Art. 5/3/b of such Directive states that the TSIs "lay down essential requirements for each subsystem concerned..."
4. Art 5/3/c of such Directive states that the TSIs "establish the functional and technical specifications to be met by the subsystems..."
5. Art 5/3/d of such Directive states that the TSIs "determine the interoperability constituents and interfaces which must be covered by European specifications..."
6. The CCS TSI defines the ETCS on-board as interoperability constituents and makes reference to mandatory specifications (listed in its Annex A) that must be complied with to ensure the respect of essential requirements; in particular SUBSET-091 specifies mandatory requirements for the functions of the DMI (that is a part of the ETCS on-board interoperability constituent).
7. Requirements stated in SUBSET-091 must be respected, in order to obtain a certificate of conformity for the ETCS on-board.

[1] OJ L 51, 23.2.2012, p.1. CCS TSI has been subsequently amended by Commission Decision 2012/696/EU of 6 November 2012 (OJ L 311, 10.11.2012, p. 3) and by Commission Decision (EU) 2015/14 of 5 January 2015 (OJ L 3, 7.1.2015, p. 44).

[2] OJ L 164, 30.04.2004, p. 1, as last amended by Regulation (EC) No 1335/2008 (OJ L 354, 31.12.2008, p. 51)

[3] OJ L 191, 18.7.2008, p. 1.

8. The requirements of SUBSET-091 are supported by informative specifications (referenced in the CCS TSI Application Guide[4]), justifying the requirements and providing support for the manufacturer and the Notified Bodies. SUBSET-118 is the informative specification related to the safety requirements for the ETCS DMI.

3 Analysis

1. UNIFE notes that in SUBSET-118 version 1.2.6 the final values of the THR for three "hazardous situations" (MMI-1d, MMI-1g and DMI-04h) because of an editorial error are not the correct values evaluated in the safety analysis.
2. The Agency agrees with this finding, that has also been reported to the CCS Working Party (meeting on November 18th 2014), where the representative of sector organisations also agreed.
3. In addition, with a deeper check of the approach and the content of SUBSET-118, the Agency identifies the need of a further correction in SUBSET-118 and in SUBSET-091.
4. More in details:
   a) The safety study in SUBSET-118 started with the identification of a set of hazardous situations that, according to the judgment of experts, could generate safety related consequences.
   b) The safety related consequences have been classified in classes, according to severity, and a Risk Acceptance Criterion (RAC) in terms of acceptable rate of occurrence for each class of consequences has been specified.
   c) Analysisng the "barriers" for each hazardous situation, it has been judged that for some of them further investigation was not necessary, because the credibility of occurrence of safety relevant consequences was very low or because the consequences were strongly dominated by external circumstances.
   d) For the remaining hazardous situations a quantification by means of an Event Tree has been performed. Each hazardous situation has been assigned a THR, such that the rate of occurrence of each "sequence" originated by a hazardous situiation and terminating with a safety releant consequence does not exceed the corresponding RAC (see statement 5.5.1.5 and 5.5.1.6 in SUBSET-118). The results are in table 4 of SUBSET-118.
   e) Finally, a safety factor of 5 has been applied to each calculated THR.
5. The results of the process described above are summarized in table 8 of SUBSET-118, where THRs less restrictive than 10^{-5} h^{-1} are not listed.
6. The reason is that, according to statement 7.1.1.2 of SUBSET-118, SIL0 requirements should not be considered as safety requirements.
7. The Agency considers that this in contradiction with the approach followed:
   a) SUBSET-118 makes a clear distinction between the hazardous situations excluded from quantification and the ones for which quantification has been considered necessary.
   b) The evaluation shows that an exceedance of the calculated THR for a hazardous situation could cause a safety relevant consequence to exceed its RAC,and this may happen also for hazardous situations for which the calculated THR is less stringent than 10^{-5} h^{-1}.
8. Considering that the supplier of ETCS on-board shall respect the requirements stated in the CCS TSI and that the track-side may not require an on-board subsystem to implement any other additional function or performance (in order to respect the essential requirements), if a requirement explicitely identified and evaluated in SUBSET-118 as relevant for safety and interoperability is not

[4] "Guide for the Application of the TSI for the subsystems Control-Command and Signalling Track-Side and On-Board" (ERA/GUI/07-2011/INT – Version 2.0).

enforced in SUBSET-091, this could generate different interpretations on the use of the information in SUBSET-118 with consequent problems in the certification process and for interoperability

9. Finally, the fact that the resulting THR is not stringent, is not a reason to make this information disappear in the final results.

4 The opinion

1. On the basis of the analysis, the opinion of the Agency is:
   a) The errors identified in UNIFE letter need to be corrected.
   b) In addition, the final results in table 8 of SUBSET-118 version 1.2.6 and in table ETCS_OB10 of SUBSET-091 version 3.3.0 need to include the full set of quantitative requirements (THRs) that have been calculated.
2. The following modifications are therefore necessary in SUBSET-118 version 1.2.6:
   a) in table 4, the SIL for the hazardous situation MMI-1g must be changed to "SIL0" (editorial error).
   b) in table 4, the SIL for the hazardous situation DMI-04h must be changed to "SIL0" (editorial error).
   c) table 8 must be substituted with the table in Annex 1 of this Technical Opinion
   d) the sentence "Note: Only THRs < 1e-5 /h are presented here, since the THRs> 1e-5 /h (SIL0) shall not be considered as safety requirements" at the end of statement 7.1.1.2 must be deleted.
3. The following modifications are therefore necessary in SUBSET-091 version 3.3.0:
   a) table ETCS_OB10 in section 7.2.1.5 must be substituted with the table in Annex 2 of this Tecnhical Opinion.
4. Pending the revision of the CCS TSI, the Agency proposes that this Technical Opinion is published and used, according to art 7/2 of the Interoperability Directive.

Valenciennes, 28.01.2015

Josef DOPPELBAUER
Executive Director

ANNEX 1

Table 8 of SUBSET-118

Top-Level DMI Hazard		Hazardous Situation		THR for Hazardous Situation (per hour)	SIL
H1	Information NOT displayed when it should have been	DMI-01a	Failure to provide Warning indication	$1.0*10^{-4}$	0
		DMI-01b	Valid ETCS Onboard output via DMI obscured by erroneous output (audio or visual)	$2.0*10^{-4}$	0
		DMI-01c	Failure to display request for acknowledgement	$2.0*10^{-5}$	0
		DMI-01d	Failure to display Geographical Position data	-	-
		MMI-2f	Failure to display Override status (failure mode deletion), including false enabling of override selection	$2.0*10^{-5}$	0
		DMI-01f	Failure to display ACK for RV request	$2.0*10^{-4}$	0
		DMI-01g	Failure to display Air Tightness Control	$2.0*10^{-5}$	0
		MMI-2i	Failure to present "LX not protected" information	-	-
H2	Information displayed when it SHOULD NOT have been	DMI-02a	False presentation of Warning	$2.0*10^{-5}$	0
		DMI-02b	False presentation of IS mode (shown as IS mode when not)	$2.0*10^{-2}$	0
		DMI-02c	False presentation of brake indication	$1.0*10^{-3}$	0
		MMI-2f	Failure to display Override status (failure mode insertion), including false enabling of override selection	$1.0*10^{-3}$	0

Top-Level DMI Hazard		Hazardous Situation		THR for Hazardous Situation (per hour)	SIL
		DMI-02e	Spurious notification of Train Data change (which normally is from source different from the driver)	-	-
		DMI-02g	False presentation of "LX not protected"	$2.0*10^{-5}$	0
		MMI-2c	False presentation of track adhesion factor (shown as applied when not)	$1.3*10^{-5}$	0
H3	Erroneous but valid information displayed	**DMI-03a**	Incorrect Geographical Position data displayed	-	-
		DMI-03c	Wrong acknowledgement request displayed	-	-
		DMI-03d	Wrong Trip Reason displayed	-	-
		DMI-03e	Wrong fixed text message displayed	$2*10^{-6}$	1
		DMI-03f	"Tunnel stopping area" displayed at the wrong geographical place	$2.0*10^{-4}$	0
		MMI-2a.1	False presentation of train speed	$7.4*10^{-7}$	2
		MMI-2b	False presentation of mode	$1.0*10^{-6}$	1
H4	Erroneous but valid input to the ETCS Onboard via the DMI	**DMI-04a**	False command to exit shunting	$4.0*10^{-3}$	0
		DMI-04c	False START command	$2.0*10^{-2}$	0
		DMI-04d	False UN acknowledgement	-	-
		MMI-1g	False request for SH Mode	$8.0*10^{-5}$	0
		DMI-04f	Spurious or wrong language requested distracting the train Driver	-	-
		DMI-04g	Spurious request to change to another ETCS Level	$4.0*10^{-5}$	0

Top-Level DMI Hazard	Hazardous Situation		THR for Hazardous Situation (per hour)	SIL
	DMI-04h	Spurious acknowledgement of intervention leading to release of emergency or service brake	$2.0*10^{-6}$	1
	DMI-04j	False Isolation command	$2.0*10^{-7}$	2
	MMI-1a	False acknowledgement of mode change to less restrictive mode	$4.0*10^{-6}$	1
	MMI-1b	False Command to enter NL mode	$2.0*10^{-2}$	0
	MMI-1d	False acknowledgement of Level Transition	$4.0*10^{-5}$	0
	MMI-6	Falsification of Virtual Balise Cover (failure mode corruption)	$4.0*10^{-7}$	2
	MMI-6	Falsification of Virtual Balise Cover (failure mode insertion)	$3.0*10^{-6}$	1
H5 Deleted input to the ETCS Onboard via DMI	**DMI-05a**	Deleted Level transition acknowledgement	$1.0*10^{-5}$	0
	DMI-05b	Deleted acknowledgement	$1.0*10^{-5}$	0
	DMI-05c	Deleted request for GPI	-	-
	DMI-05d	Deleted change of language request	-	-
	DMI-05e	Deleted driver request to apply Track Adhesion Factor	$2.0*10^{-5}$	0
	DMI-05f	Deleted Reversing mode acknowledgement	$2.0*10^{-4}$	0
	DMI-05g	Deleted "PT distance exceeded" acknowledgement	-	-
	DMI-05i	Deleted "reversing distance exceeded" acknowledgement	-	-
	DMI-05j	Deleted Isolation command	-	-
	DMI-05l	Deleted Train Trip acknowledgement	-	-

Top-Level DMI Hazard	Hazardous Situation	THR for Hazardous Situation (per hour)	SIL
	MMI-06 Falsification of Virtual Balise Cover (failure mode deletion)	-	-

ANNEX 2

Table in SUBSET-091, section 7.2.1.5, ETCS_OB10

Hazardous Situation		THR for hazard rate (failures per hour)
DMI-01a	Failure to provide Warning indication	$1.0*10^{-4}$
DMI-01b	Valid ETCS Onboard output via DMI obscured by erroneous output (audio or visual)	$2.0*10^{-4}$
DMI-01c	Failure to display request for acknowledgement	$2.0*10^{-5}$
MMI-2f	Failure to display Override status (failure mode deletion), including false enabling of override selection	$2.0*10^{-5}$
DMI-01f	Failure to display ACK for RV request	$2.0*10^{-4}$
DMI-01g	Failure to display Air Tightness Control	$2.0*10^{-5}$
DMI-02a	False presentation of Warning	$2.0*10^{-5}$
DMI-02b	False presentation of IS mode (shown as IS mode when not)	$2.0*10^{-2}$
DMI-02c	False presentation of brake indication	$1.0*10^{-3}$
MMI-2f	Failure to display Override status (failure mode insertion), including false enabling of override selection	$1.0*10^{-3}$
DMI-02g	False presentation of "LX not protected"	$2.0*10^{-5}$
MMI-2c	False presentation of track adhesion factor (shown as applied when not)	$1.3*10^{-5}$
DMI-03e	Wrong fixed text message displayed	$2*10^{-6}$
DMI-03f	"Tunnel stopping area" displayed at the wrong geographical place	$2.0*10^{-4}$
MMI-2a.1	False presentation of train speed	$7.4*10^{-7}$
MMI-2b	False presentation of mode	$1.0*10^{-6}$
DMI-04a	False command to exit shunting	$4.0*10^{-3}$
DMI-04c	False START command	$2.0*10^{-2}$
MMI-1g	False request for SH Mode	$8.0*10^{-5}$
DMI-04g	Spurious request to change to another ETCS Level	$4.0*10^{-5}$

Hazardous Situation		THR for hazard rate (failures per hour)
DMI-04h	Spurious acknowledgement of intervention leading to release of emergency or service brake	$2.0*10^{-6}$
DMI-04j	False Isolation command	$2.0*10^{-7}$
MMI-1a	False acknowledgement of mode change to less restrictive mode	$4.0*10^{-6}$
MMI-1b	False Command to enter NL mode	$2.0*10^{-2}$
MMI-1d	False acknowledgement of Level Transition	$4.0*10^{-5}$
MMI-6	Falsification of Virtual Balise Cover (failure mode corruption)	$4.0*10^{-7}$
MMI-6	Falsification of Virtual Balise Cover (failure mode insertion)	$3.0*10^{-6}$
DMI-05a	Deleted Level transition acknowledgement	$1.0*10^{-5}$
DMI-05b	Deleted acknowledgement	$1.0*10^{-5}$
DMI-05e	Deleted driver request to apply Track Adhesion Factor	$2.0*10^{-5}$
DMI-05f	Deleted Reversing mode acknowledgement	$2.0*10^{-4}$

ANNEX 3

Original request: UNIFE letter of 11 November 2014