Organisation intergouvernementale pour les transports internationaux ferroviaires
Zwischenstaatliche Organisation für den internationalen Eisenbahnverkehr
Intergovernmental Organisation for International Carriage by Rail

Commission d'experts techniques
Fachausschuss für technische Fragen
Committee of Technical Experts

TECH-16015-CTE9-5.2a

01.04.2016

Original: EN

AMENDMENT TO UTP GEN-G

Proposal to amend the implemented UTP GEN-G on the common safety method for risk evaluation and assessment

Tel. +41 (0) 31 359 10 10 Fax +41 (0) 31 359 10 11 info@otif.org Gryphenhübeliweg 30 CH - 3006 Bern

1. INTRODUCTION

On 1.5.2012 the first version of the UTP GEN-G on a common safety method (CSM) for risk evaluation and assessment entered into force, which was particularly useful and was necessary to assess the conformity of vehicles before being admitted to international traffic. This version of the UTP was equivalent to Commission Regulation (EC) No 532/2009.

The UTP GEN-G was subsequently amended with effect from 1.1.2014 in order to ensure continued equivalence after the adoption of Commission Implementing Regulation (EU) No 402/2013, which repealed Commission Regulation (EC) No 532/2009. This amendment to the UTP GEN-G introduced harmonised criteria for CSM assessment bodies.

In 2015 the Implementing Regulation (EU) No 2015/1136 of the European Commission amended the EU CSM provisions by including additional risk acceptance criteria. The aim of these changes was to facilitate the mutual recognition between States of assessment results related to structural subsystems and vehicles, in particular in cases where the proposer chose to use explicit risk estimation. In such cases, harmonised design targets could be used to demonstrate the acceptability of risks which were arising from failures of functions of a technical system. Furthermore, in order to distinguish the acceptance of risks associated with technical systems from the acceptance of operational risks and of the overall risk at the level of the railway system, the term "risk acceptance criteria" with respect to technical systems was changed to "harmonised design targets" for such technical systems.

The aim of the proposals in this document is to amend the UTP GEN-G so that it will be equivalent to Commission Implementing Regulation (EU) No 402/2013 as amended by Implementing Regulation (EU) No 2015/1136 of the European Commission. These amendments were reviewed and discussed at the 26th, 27th and 28th sessions of the WG TECH.

2. PROPOSALS FOR DECISION

The Committee of Technical Experts adopts the following decisions:

1. The UTP GEN-G (A 94-01G/1.2012 version 3, in force as of 1.1.2014) should be amended as set out in the Annex to this document.
2. The OTIF Secretariat will notify the CTE's decision and the amendments concerned in accordance with the process described in Article 35 §§ 3 and 4 of the Convention.
3. The OTIF Secretariat will publish the amendments to UTP GEN-G and a consolidated version of UTP GEN-G on the OTIF website.

ANNEX

The UTP GEN-G is amended as follows:

1. Section 3 is amended as follows:

a) point 9 is replaced by the following:

"9. "safety requirements" means the safety characteristics (qualitative or quantitative, or when needed both qualitative and quantitative) necessary for the design, operation (including operational rules) and maintenance of a system in order to meet legal or company safety targets;"

b) point 23 is replaced by the following:

"23. "catastrophic accident" means an accident typically affecting a large number of people and resulting in multiple fatalities;"

c) point 29 is replaced by the following:

" "accreditation" means accreditation as defined in

Article 2 ab) of ATMF;	Article 2 of Regulation (EU) No 765/2008;"

d) the following points (32) to (37) are added:

"32. "systematic failure" means a failure that occurs repeatedly under some particular combination of inputs or under some particular environmental or application conditions;

33. "systematic fault" means an inherent fault in the specification, design, manufacturing, installation, operation or maintenance of the system under assessment;

34. "barrier" means a technical, operational or organisational risk control measure outside the system under assessment that either reduces the frequency of occurrence of a hazard or mitigates the severity of the potential consequence of that hazard;

35. "critical accident" means an accident typically affecting a very small number of people and resulting in at least one fatality;

36. "highly improbable" means an occurrence of failure at a frequency less than or equal to 10– 9 per operating hour;

37. "improbable" means an occurrence of failure at a frequency less than or equal to 10– 7 per operating hour."

Annex I is amended by the following:

1. Section 2.5.1. is replaced by the following:

"2.5.1. If the hazards are not covered by one of the two risk acceptance principles laid down in points 2.3 and 2.4, the demonstration of risk acceptability shall be performed by explicit risk estimation and evaluation. Risks resulting from these hazards shall be estimated either quantitatively or qualitatively, or when necessary both quantitatively and qualitatively, taking existing safety measures into account."

2. Sections 2.5.4. to 2.5.7. are replaced by the following:

"2.5.4. The proposer shall not be obliged to perform additional explicit risk estimation for risks that are already considered acceptable by the use of codes of practice or reference systems.

2.5.5. Where hazards arise as a result of failures of functions of a technical system, without prejudice to points 2.5.1 and 2.5.4, the following harmonised design targets shall apply to those failures:

a) where a failure has a credible potential to lead directly to a catastrophic accident, the associated risk does not have to be reduced further if the frequency of the failure of the function has been demonstrated to be highly improbable.

b) where a failure has a credible potential to lead directly to a critical accident, the associated risk does not have to be reduced further if the frequency of the failure of the function has been demonstrated to be improbable.

The choice between definition (23) and definition (35) shall result from the most credible unsafe consequence of the failure.

2.5.6. Without prejudice to points 2.5.1 and 2.5.4, the harmonised design targets set out in point 2.5.5 shall be used for the design of electrical, electronic and programmable electronic technical systems. They shall be the most demanding design targets that can be required for mutual recognition.

They shall neither be used as overall quantitative targets for the whole railway system of a

Contracting State	Member State

nor for the design of purely mechanical technical systems.

For mixed technical systems composed of both a purely mechanical part and an electrical, electronic and programmable electronic part, hazard identification shall be carried out in accordance with point 2.2.5. The hazards arising from the purely mechanical part shall not be controlled using the harmonised design targets set out in point 2.5.5.

2.5.7. The risk associated with the failures of functions of technical systems referred to in point 2.5.5 shall be considered as acceptable if the following requirements are also fulfilled:

a) Compliance with the applicable harmonised design targets has been demonstrated;

b) The associated systematic failures and systematic faults are controlled in accordance with safety and quality processes commensurate with the harmonised design target applicable to the technical system under assessment and defined in commonly acknowledged relevant standards;

c) The application conditions for the safe integration of the technical system under assessment into the railway system shall be identified and registered in the hazard record in accordance with point 4. In accordance with point 1.2.2, these application conditions shall be transferred to the actor responsible for the demonstration of the safe integration."

3. The following sections 2.5.8 to 2.5.12 are added:

"2.5.8. The following specific definitions shall apply in reference to the harmonised quantitative design targets of technical systems:

a) The term "directly" means that the failure of the function has the potential to lead to the type of accident referred to in point 2.5.5 without the need for additional failures to occur;

b) The term "potential" means that the failure of the function may lead to the type of accident referred to in point 2.5.5;

2.5.9. Where the failure of a function of the technical system under assessment does not lead directly to the risk under consideration, the application of less demanding design targets shall be permitted if the proposer can demonstrate that the use of barriers as defined in Article 3(34) allows the same level of safety to be achieved.

2.5.10 Without prejudice to Article 12 of APTU, | Member State either the procedure specified in Article 8 of Directive 2004/49/EC, or Article 17(3) of Directive 2008/57/EC of the European Parliament and of the Council,[1]

a more demanding design target than the harmonised design targets laid down in point 2.5.5. may be requested for the technical system under assessment, through a notified national rule, in order to maintain the existing level of safety in the Contracting State. | Member State.

In the case of additional technical admissions of vehicles, Article 6 of ATMF shall apply. | authorisations for placing in service of vehicles, the procedures of Articles 23 and 25 of Directive 2008/57/EC shall apply.

[1] Directive 2008/57/EC of the European Parliament and of the Council of 17 June 2008 on the interoperability of the rail system within the Community (OJ L 191, 18.7.2008, p. 1).

2.5.11 Where a technical system is developed on the basis of the requirements set out in point 2.5.5, the principle of mutual recognition is applicable in accordance with

section 15.5 of this UTP. | Article 15(5).

Nevertheless, if for a specific hazard the proposer can demonstrate that the existing level of safety in the Member State where the system is being used can be maintained with a design target that is less demanding than the harmonised design target, then this less demanding design target may be used instead of the harmonised one.

2.5.12 The explicit risk estimation and evaluation shall satisfy at least the following requirements:

a) the methods used for explicit risk estimation shall reflect correctly the system under assessment and its parameters (including all operational modes);

b) the results shall be sufficiently accurate to provide a robust basis for decision-making. Minor changes in input assumptions or prerequisites shall not result in significantly different requirements.”

****