Accompanying Report N. ERA-REC-116-2015-ACR to the Recommendation

of the European Railway Agency

on

the amendment of the Commission implementing Regulation (EU) No 402/2013 on the common safety method for risk evaluation and assessment

Disclaimer:

The present document is a non-legally binding report 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.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

0. EXECUTIVE SUMMARY

0.1. The aim of the revision of Regulation 352/2009 for risk assessment, carried out in the period 2010-2012, was to enhance the mutual recognition of the application of the Regulation and of the results of the risk management process specified therein. The Agency developed additional requirements for the independent CSM assessment body and further harmonised risk acceptance criteria to be used to assess the acceptability of risks arising from failures of technical systems. For various reasons explained in this report, in 2012 it was not possible to achieve a sufficient consensus on harmonised risk acceptance criteria with the railway stakeholders. Regulation 402/2013 includes only the developments on the independent CSM assessment body. Howver, all stakeholders agreed that such criteria are necessary to support the mutual recognition between Member States of TSI compliant structural sub-systems and vehicles.

0.2. The impact assessment highlighted also the importance of including in Regulation 402/2013 other consequence severities of risks than currently only the catastrophic severity one contained in point 2.5.4 of Annex I of the regulation. Basically, the impact assessment shows a strong qualitative indication that harmonised CSM-DT are expected :

(a) to lower the amount of explicit risk estimations to be redone due to the use of different quantitative requirements for the design of technical systems. There should thus be less redesigns of technical systems, as well as less paper work for safety cases;

(b) to decrease the number of additional unnecessary administrative, risk assessment and safety demonstration work, as well as inappropriate cost, time and resources investments for the railway undertaking, infrastructure manager and national safety authority;

(c) to improve the mutual recognition of technical systems in compliance with Article 5 of Regulation 402/2013 and in particular to facilitate the authorisations for placing into service structural sub-systems and vehicles.

0.3. In agreement with the European Commission and the railway stakeholders, more time was taken for the validation of those concepts and for reaching a consensus. This was necessary to get the assurance and to check that the use of harmonised risk acceptance criteria for technical systems (*renamed into CSM design targets for technical systems*) will neither decrease the existing safety performance of EU railways nor increase the development costs of the associated technical systems. The work on the harmonisation of further CSM design targets was thus continued with the stakeholders till 2014 until a common and agreed view was reached and a recommendation can be made for amending Regulation 402/2013.

0.4. The validation of the CSM-DT was done with the strong support and involvement of NSAs and representative bodies (CER-EIM-UNIFE-UIP). The method for the validation was agreed with those stakeholders through a "CSM-DT way forward note" {Ref. 11.}. The criteria or rules on the sufficiency of the validation work were also discussed and agreed with the networks of NSAs and Representative Bodies (see paragraph § 4.2.3.). The progress with the validation of CSM-DT was reported to the network of NSAs, EC and RISC.

0.5. The "CSM-DT way forward note" proposed the following categories of harmonised CSM-DT:

(a) **10^{-9} h^{-1} for catastrophic accidents** affecting a group of people and resulting in fatalities and/or severe injuries and/or major damages to the environment;
(b) **10^{-7} h^{-1} for critical accidents** affecting an individual person and resulting in fatality and/or severe injury;
(c) **10^{-5} h^{-1} for marginal accidents** resulting in one or more light injuries.

Very early in the validation process, the stakeholders expressed at the unanimity that the last category concerning "light injuries" is not necessary for mutual recognition and could be excluded from the scope of work. In addition to that, all stakeholders requested to include in the CSM explicit requirements for the management of risks arising from systematic failures and systematic faults related to the design of technical systems.

0.6. The validation work was done in compliance with the agreed rules. During the validation the milestone were extended several times to understand the progress, solve the misunderstandings and adapt progressively the proposed text based on the experience and practice from real cases of use of quantitative requirements for the design of existing technical systems.

0.7. The validation of CSM-DT on the German NeGSt project has shown that many failures of technical functions do never lead to fatalities but only to injuries. Consequently, the initially proposed CSM-DT, that grouped "fatalities and injuries" in the same category, appeared to be too penalising and, compared to the current experience, leading to an unjustified increase of safety requirements, and so of the associated costs, for the development of the associated technical systems. It was thus commonly agreed in the workshop that considering that the most severe outcome of a technical system failure is a fatality, it would result in setting up the highest safety requirements for the design of technical systems. It was thus decided to exclude from the wording both the injuries and damages to the environment.

0.8. The scope of Directive 2004/49 does not include any explicit requirement for the protection of the environment. Other national and EU legislation deal with the environmental protection. Refer to "*Directive 2004/35/CE of the European parliament and of the Council of 21 April 2004 on environmental liability with regard to the prevention and remedying of environmental damage*" and to the following link :
http://ec.europa.eu/environment/legal/liability/
In order to avoid writing redundant legislation, the Agency excluded the environmental consequences from the wording of the CSM-DT categories

0.9. The representative bodies (CER, EIM, UNIFE) unanimously confirm that the two proposed CSM-DT categories are validated. They have verified the proposed figures for a set of functions of existing technical systems. For those functions, the stakeholders verified whether the CSM-DTs differ from the safety requirements contained either in national rules/legislation or in relevant standards. The validation indicates that, compared to the current practice, the CSM-DT would neither decrease the safety performance in the EU railways nor increase the development costs of technical systems. The proposed "CSM-DT categories and values" correspond thoroughly to the present reality, experience and practice in EU railways. From the representative body point of view, and the majority of the involved NSAs, the CSM-DTs are usable for their purpose.

This point of view could not be shared entirely by the German and Swiss NSAs who request :

(a) further validation work to be done on the proposed CSM-DT;
(b) solve the existing overlap between the two categories;
(c) limit the use of harmonised CSM-DT to a list of functions contained in a legal text (either in TSIs for functions necessary for the interoperability or in an annex of the application guideline on CSM-DT for other functions). This list of functions should be agreed on, and updated on a regular basis with additional functions, for which use of CSM-DT would be allowed, by a group of representative experts.

Their fear is that because of insufficient validation and overlap between the two categories, as perceived only by the German NSA, different interpretations of the CSM-DT wording are possible and lead to an incorrect allocation of the CSM-DT categories. This might make the

mutual recognition of the results of quantitative risk assessments impossible if the use of CSM-DT is not limited to such a list. In addition to jeopardising the mutual recognition of results from risk assessments, this could lead to an incorrect use of the CSM Regulation and thus to a decrease of the safety level in EU.

0.10. The Agency justified why these suggestions cannot be taken into account :

(a) there is no overlap between the two categories as they refer to different types of accidents. The first one refers to "big accidents" whereas the second one to "small accidents". They affect respectively either a large number of persons or a small number of persons. They correspond exactly to same categories of accidents considered in the aviation domain;

(b) such a list cannot be exhaustive, as it is not the purpose of the CSM to carry out an exhaustive functional analysis, and subsequent allocation of quantitative requirements, for all functions of the railway system. Restricting the use of CSM-DT only to a limited list of functions of TSIs or of a guide would make illegal their use for functions not in the list. In addition to that, quantitative requirements cannot be allocated safely to a function outside its operational context and making abstraction of how the function is architectured in the railway system. That could either over specify or under specify the safety requirements;

(c) according to Regulation 402/2013 the proposer's risk assessment and appropriateness of the results (i.e. including the allocation of CSM-DT and the demonstration of their achievement) shall be checked by a competent CSM assessment body accredited or recognised according to the requirements and criteria contained in Annex II of Regulation 402/2013. This provides assurance that the errors of possible incorrect allocation of CSM-DT are detected by the safeguards put in place by the EU railway legislation.

0.11. The proposed amendment was subject to Public Consultation in compliance with the applicable procedures, presented to RISC and NSA Network. This did not reveal new comments or suggestions that were not already raised by the stakeholders involved in the validation activity. On the contrary, the urgency and benefits of having additional harmonised CSM-DT was confirmed.

0.12. In order to verify the similarity with other fields of industry, the Agency coordinated with the aviation domain. This cross-check demonstrated the equivalence or similarity of the use of quantitative requirements and quality and safety assurance processes via relevant standards :

(a) similarly to railways, for big aircraft and for the same types of accidents or consequence severities, the same categories of design targets are used in the aviation;
(b) in aviation the "single fatality" is included in "relatively small number of persons" category;
(c) standards with similar requirements are used for the design of technical systems. This presumes that the technical systems in both fields are expected to achieve equivalent levels of safety performance;
(d) equivalent processes are used for the safety assessments, hardware & software development, verification & validation & management of systematic failures and systematic faults;
(e) similar requirements and standards are applicable in both fields for the demonstration of the achievement of quantitative requirements, including the use and modelling of safety barriers external to the technical system under assessment. This includes among others :

(1) the use of qualitative and quantitative demonstrations;
(2) the use of top down [Fault Tree Analyses – FTA – analysing the combination of failures] and bottom-up [e.g. Failure Mode Effect (and Criticality) Analysis – FME(C)A – analysing the effect of individual failures] approaches

0.13. Based on the results of the validation of CSM-DT in the railway sector, and taking into account also the similarities with the aviation, there should be a great confidence that the proposed

quantitative design targets will not decrease the existing safety levels in EU railways. For each consequence severity of a failure of a railway technical system, the same quantitative design target is specified for the corresponding consequence severity also for big aircrafts.

0.14. Therefore, there is no justification for defining more severe and more demanding design targets for railways than those used in aviation. The validation by the representative bodies shows that neither the safety performance would be decreased nor the cost for implementing the CSM-DT would be increased compared to the current practice. On the contrary, imposing different values for the same categories would be too penalising for railways and, compared to the current experience, it would lead to an unjustified increase of safety requirements, and therefore of the associated costs, for the development of the technical systems in railways.

0.15. Based on the validation work of CSM-DT, comparison with the aviation and the bilateral coordination meetings with NSAs and representative bodies, the Agency proposes the following wording of the two CSM-DT categories (this is a part of the whole legal text) :

2.5.5. If hazards arise from failures of functions of a technical system, …the following requirements 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 failures of the associated function is 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 failures of the associated function is demonstrated to be **improbable**.*

Where :

*(23) '**catastrophic accident**' means an accident typically **affecting a large number of persons** and resulting in **multiple fatalities**;'*

*(35) '**critical accident**' means an accident typically **affecting a small number of persons** and resulting in **at least one fatality**;*

*(36) '**highly improbable**' means a failure occurring at a frequency less than or equal to 10^{-9} per operating hour;*

*(37) '**improbable**' means a failure occurring at a frequency less than or equal to 10^{-7} per operating hour;*

2.5.7. The risks arising from failures of functions of technical systems … shall be considered as acceptable if the following requirements are fulfilled:

(a) The compliance with the applicable harmonised design target is demonstrated;

(b) The associated systematic failures and systematic faults are controlled in compliance 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) …

0.16. In order to help the EU railway sector with the application of the CSM-DT, all involved experts unanimously agree on the necessity to produce an application guideline. The application guide should support the legal text with additional explanations. It should be available at the stage when the recommendation will be put to vote by the Member States. The guideline should provide assurance to the NSAs and representative bodies that the CSM-DT are not going to be misused and that mutual recognition of the risk assessment results is achieved.

1. INTRODUCTION

1.1. Following

(a) Directive 2004/49/EC on railway safety in the Community (Safety Directive - {Ref. 2.}),
(b) Regulation (EC) No 881/2004 establishing the European Railway Agency (Agency Regulation - {Ref. 3.}),
(c) The mandate to the European Railway Agency for the revision of the common safety method on risk evaluation and assessment- C(2010) 6931 final - of 12.10.2010

This mandate to the European Railway Agency, as referred to in Article 6(2) of Directive 2004/49/EC concerns the revision of the Commission Regulation (EC) N° 352/2009 on a common safety method on risk evaluation and assessment.

the Agency shall submit to the Commission a recommendation on the revision of the CSM on risk evaluation and assessment. The scope of that revision shall cover developments in:

(d) the roles and the responsibilities of the assessment body referred to in Article 6 of Regulation (EC) No 352/2009,

(e) the risk acceptance criteria that could be used to assess the acceptability of a risk during explicit risk estimation and evaluation.

1.2. In July 2012, the Agency submitted to the Commission its final recommendation on the revision of the CSM on risk evaluation and assessment with the developments on the work of CSM assessment body.

1.3. In spite of all indications from the sector (clearly identified within the impact assessment of the proposal) of how important the harmonisation of further risk acceptance criteria is, the second point could not be included in the recommendation of 2012. It was not possible for the sector to provide enough inputs and to achieve a common agreement within the working group on this topic quickly enough in order to include it in the same recommendation as the one regarding the work of the assessment bodies. The work on the harmonisation of further risk acceptance criteria was thus continued in the following years until the necessary common view and agreement were reached and a recommendation is possible to be made.

1.4. **The present report provides information regarding the development process applied for the achievement of a proposal for harmonised risk acceptance criteria to fulfil the second part of the mandate from 12.10.2010.**

1.5. The development of harmonised risk acceptance criteria, which took place in the years before July 2012 is described in detail in the "*Agency report on the experience with the existing regulation (EC) N° 352/2009 on a common safety method on risk evaluation and assessment and on the revision of that regulation*" {Ref. 10.}. Therefore, the present report describes only the development, which took place since July 2012.

1.6. Note: After detailed discussions and for various reasons, the railway sector has decided and agreed to change the terminology "Risk Acceptance Criteria for Technical Systems" (RAC-TS) 'which is the focus of the present report) into "Design Targets for technical systems" (CSM-DT). As this is the more correct terminology to apply, and in order to be consistent with the suggested recommendation, the present report will refer to CSM-DT instead of RAC-TS.

2. WORKGROUPS

2.1. On the side of the Agency, the team working on the revision of the CSM for risk assessment (CSM-RA) with regards to the CSM-DT was composed of one main responsible project officer, supported by another project officer within the Safety Unit, 2 project officers ensuring interfaces and coherence with other EU legislation and one project officer dealing with the impact assessment related to the proposal. Internal consultation, reviews and discussions involving all team members were carried out when relevant activities or outcomes had to be decided upon. Furthermore, the Legal Office of the Agency has given a considerable support to the project team whenever legal interface questions were faced.

2.2. Due to staff turnover within the Agency, in overall, the CSM-DT project has been led for 2 years by Marcus ANDERSSON, then for 5 years by Maria ANTOVA and since November 2014 by Dragan JOVICIC.

Table 1 : Members of the Agency staff working on the harmonised CSM-DT

Member of staff	Role	Activity
Maria ANTOVA	Project Officer – CSM-DT Project Administrator (took over the project from Marcus ANDERSSON in 2009)	CSMs
Dragan JOVICIC	Project Officer - CSM WG Administrator and later CSM-DT administrator (took over from Maria ANTOVA in 2014)	CSMs
Wouter MALFAIT	Project Officer from Economic Evaluation Unit responsible for the impact assessment on changes related to RAC-TS	Economic Evaluation
Hubert LAVOGIEZ	Head of Sector from the Interoperability Unit responsible for the closure of safety-related open points from the LOC&PAS TSI	LOC&PAS TSI
Angelo CHIAPPINI, Dominique LIGIER	Project Officers from the ERTMS Unit of ERA, taking care for coordination with the related points	ERTMS
Erika TARR, Guido STARKLE	Project Officers – ERA Legal Office	Legal

2.3. In 2005, in accordance with Article 3 of the Agency Regulation, the Agency created a specific working group (CSM WG) with the aim of taking into account the experiences and expectations of the different parties affected by the CSM for risk assessment. This CSM WG is composed of delegates from National Safety Authorities and railway associations (Representative Bodies) notified by the Article 21 Committee. This working group participated with the Agency to the development of risk acceptance criteria for technical systems between 2007 and 2012.

2.4. In July 2012, the working group was composed of 25 experts representing:

(a) 15 National Safety Authorities (AT, BE, DE, DK, ES, FI, FR, IT, LV, LT, NO, PL, RO, SE, UK), and;
(b) 4 sector organisations (CER 4; EIM 2; UIP 1; UNIFE 3)

2.5. Due to the difficulty in validating the CSM-DT, the Agency agreed with the networks of NSAs and of representative bodies to open the validation of the CSM-DT not only to the CSM WG members but also to all stakeholders who wanted to take part actively to this work. The following participants were invited: all members of the CSM WG, all NSAs of the NSA network and all representative bodies (CER, EIM, UIP, UNIFE, i.e. railway undertakings, infrastructure managers, private wagon keepers and manufacturers). In the period July 2012-September 2014, the Agency invited all those actors to a series of public workshops in order to present the progress with the validation of CSM-DT, to discuss the next steps and finally to agree on the sufficiency of the validation activity. The Swiss national safety authority took also part to the validation of CSM-DT and participated to all workshops.

2.6. Further to the workshops organised by the Agency, an intensive work on the subject has taken place also together with the Network of National Safety Authorities and the Network of Representative Bodies.

3. MEETINGS

3.1. In the period July 2012-February 2015, in the framework of the development and validation of the CSM-DT, the Agency organised or participated to a series of internal and external meetings.

3.2. **Internal meetings in the Agency:**

(a) Various Agency-internal meetings to draft and consult on the contents of the "*CSM-DT Way Forward Note*" {Ref. 13.};

(b) Various Agency-internal meetings to ensure the coordination and coherence of the suggested texts with other existing EU legislation (LOC&PAS TSI, ERTMS, etc.);

(c) Various coordination meetings to ensure coherence with the work stream, dealing with the harmonisation of RAC for the transport of dangerous goods (railway, water, road);

3.3. **Presentations and discussions in NRB Network and with the representative organisations:**

(a) 2013/05/14 – Network of Representative Bodies – Presentation and discussion of the work done since July 2012 – Discussion and agreement on the next steps; inviting them for validation. The sufficiency of the validation and its deadline were discussed;;

(b) 2013/09/05 – Meeting with CER and EIM in Brussels to discuss the Agency answers to their list of questions received after the workshop in June 2013;

(c) 2013/11/28 - Meeting with CER, EIM and UNIFE in Brussels to discuss the progress of work on the validation of the CSM-DT;

(d) 2013/12/18 – Meeting with UNIFE in Brussels to discuss UNIFE's inputs in the scope of the validation of the CSM-DT;

(e) 2014/02/19 - Meeting with UNIFE in Brussels to discuss UNIFE's inputs in the scope of the validation of the CSM-DT;

(f) 2014/05/15 – Meeting in Frankfurt with representatives of the project team of the German Project called NeGSt to discuss the relevance of the project results to the validation of the CSM-DT, which has been discussed at the 2nd CSM-DT validation workshop in Lille;

(g) 2014/05/16 – Meeting with RSSB (representing the UK ATOC organisation on the side of CER) to exchange views on the draft legal text;

(h) 2015/03/03 – Meeting with CER-EIM-UNIFE to present the results of the Public Consultation, the RISC and NSA Network opinion, as well as the agreements reached at bilateral meetings with interested NSAs;

(i) in addition to those meetings, the Agency replied on a regular basis to questions received by e-mail from different representative bodies or their members.

3.4. **Presentations and discussions in NSA Network meetings:**

(a) 2013/02/20 – NSA Network meeting – Presentation of the work done since July 2012 to discuss and agree on the next steps and invite the NSAs to take part to the validation work. The sufficiency of the validation and its deadline were discussed;

(b) 2013/05/22 – NSA Network meeting – Present and discuss on the progress of work, investigate and discuss the ways how NSAs handle CSM-DT within authorisation for placing in service;

(c) 2013/09/25 – NSA Network meeting – Present and discuss on the progress of work, investigate and discuss the ways how NSAs handle CSM-DT within authorisation for placing in service;

(d) 2014/04/29 – NSA Network meeting – Information note on the progress of work given to the NSA Network *(without a supplementary presentation during the dedicated network meeting)*;

(e) 2014/09/17 – NSA Network meeting – Presentation and discussion of the progress of work on the recommendation; information regarding the upcoming public consultation;

(f) 2015/02/24 – NSA Network meeting – Summary of the validation of CSM DT and presentation of the results of the Public Consultation and RISC opinion.

3.5. **Bilateral meetings with NSAs:**

(a) 2013/05/28 – Meeting with NSA IT in Italy to discuss and explain the difference between the CSM DT and other types of RAC (i.e. RAC at national level), learn that NSA IT has the behaviour defined within Model 1 (during APIS) and will not deliver validation;

(b) 2014/03/25 – Meeting with NSA DE and representatives of the German railway sector (both industry and operators) to discuss the validation of the CSM-DT;

(c) 2014/11/18 – Bilateral meeting with NSA DE to understand their concerns and try to find a common solution that does not conflict with the consensus reached in the Workshop;

(d) 2015/02/02 – Bilateral meeting with NSA IT to understand their concerns and try to find a common solution that does not conflict with the consensus reached in the Workshop;

(e) 2015/02/09 – Bilateral phone meeting with Swiss NSA to discuss the Agency replies to their comments on CSM DT and agree on an improvement of the draft proposal;

(f) 2015/02/11 – Bilateral phone meeting with NSA IT to discuss the Agency replies to their comments on CSM DT and agree on an improvement of the draft proposal without conflicting with the consensus reached in the Workshop;

(g) 2015/02/13 – Bilateral phone meeting with NSA DE to discuss the Agency replies to their comments on CSM DT and agree on an improvement of the draft proposal;

(h) 2015/03/06 – Bilateral phone meeting with NSA IT to discuss their post-Public Consultation comments on CSM DT and agree on further improvement of the draft proposal without conflicting with the consensus reached in the Workshop;

(i) in addition to those meetings, the Agency replied on a regular basis to questions received by e-mail from different NSAs.

3.6. **Workshops organised on the validation of CSM-DT:**

(a) 2013/06/25-2013/06/26 – 1st RAC-TS validation (public) workshop in Lille to present and discuss the intermediate results from the validation of the texts within the "*CSM-DT way forward note*";

(b) 2014/04/01 – 2nd CSM-DT validation workshop in Lille – Presentation and discussion of the results from the validation of the texts within the CSM-DT Way Forward Note – The Agency presented its review based on the received inputs. The actors who submitted validation inputs presented and discussed their inputs with the other involved parties;

(c) 2014/07/16 – 3rd CSM-DT validation workshop in Lille where CER, EIM and UNIFE presented a common view on a few points regarding the latest text of the CSM-DT;

(d) 2014/09/18 – 4th CSM-DT validation workshop in Lille – CER, EIM and UNIFE presented a common list of functions supporting the latest version of the text of the CSM-DT. Last discussion of the texts before launching the public consultation.

3.7. **Presentation to RISC and coordination with the European Commission:**

(a) 2014/11/06 – RISC meeting – Presentation of the progress of the validation work and information about the public consultation;

(b) 2015/02/10 – RISC meeting – Presentation of the results of the public consultation;

(c) Regular coordination meetings with the EC to ensure coherence of the work and planning.

3.8. Further to the above meetings, in order to ensure that the CSM-DT proposal to be validated has reached as many stakeholders as possible, as well as to collect their feedback, discuss challenges and try to support the validation process, the Agency participated in the following events:

(a) 2013/02/27 – Meeting in Frankfurt with a German project consortium (Project called NeGSt) to present and discuss the work on CSM/DT. The work of the NeGSt project investigated a list of over 100 functions with regards to various types of risk acceptance;

(b) 2013/11/05 – Presentation of the CSM-DT development and validation process at the seminar “Safety in Transportation” in Braunschweig, Germany;

(c) 2013/11/18 – Meeting, explanation of the work and discussion with a French project group for a project of NSA FR, investigating the practices regarding risk acceptance, SIL and etc.

(d) 2014/03/13 – Seminar in Dresden, Germany on the authorisation for placing into service structural sub-systems in Germany and the links with the work on the CSM-DT.

4. WORKING METHODS

4.1. Revision of Regulation 352/2009 - Needs of harmonised CSM-DT for technical systems (former RAC-TS)

4.1.1. Following the adoption of Regulation 352/2009 on the CSM for risk evaluation and assessment, the European Railway Agency (the "Agency") continued with further developments and harmonisation of additional requirements for that Regulation. In 2010 the Commission issued a mandate to the Agency for revising it based on the results of those **further developments** concerning the **roles and the responsibilities of the assessment body**, referred to in Article 6 of that Regulation, and the **risk acceptance criteria** that could be used for assessing the acceptability of risks during explicit risk estimation and evaluation.

4.1.2. While the objectives of the revision were met for the assessment body part, an agreement could not be reached yet between the European railway stakeholders on harmonised risk acceptance criteria for technical systems. The stakeholders were only able to agree that **the harmonised risk acceptance criteria are not to relate to operational and organisational provisions** to be put in place by the operators and maintainers of the railway system.

4.1.3. In 2012, the Agency submitted to the Commission its recommendation on the revision and amendment of the parts of the CSM related to the assessment body. This resulted in the adoption of Regulation 402/2013. The **impact assessment report** done at that time highlighted nevertheless the **importance** of **including** also **in the CSM** consequence severities of **risks other than** currently only the **catastrophic severity** one. There was a unanimous agreement that such criteria would be **necessary to support the mutual recognition** between Member States of TSI compliant **structural sub-systems and vehicles**. More time was thus assigned for checking that the proposed harmonised risk acceptance criteria for technical systems will ensure that **railway safety** is **at least maintained in the European Union**. The work on the harmonisation of further risk acceptance criteria was thus continued with the stakeholders till 2014 until a common and agreed view was reached and a recommendation can be made for amending Regulation 402/2013.

4.2. Validation work of CSM-DT between 2012 and 2014

4.2.1. Scope of application of CSM-DT for technical systems vs. other types of risk acceptance criteria (RAC)

4.2.1.1. Before proceeding with the validation of the CSM-DT for technical systems, it was necessary to understand the reasons of why an agreement on the CSM-DT could neither be reached between the representative bodies (CER, EIM, UIP, UNIFE) nor with the national safety authorities during the revision of Regulation 352/2009. Despite relevant guidance is provided in the existing application guidelines on the CSM for risk assessment, a lack of common understanding concerning the level of the railway system at which the CSM-DT (former RAC-TS) are to be applied has been demonstrated once more during coordination meetings with the networks of national safety authorities and of representative bodies.

4.2.1.2. The **CSM-DTs are harmonised quantitative requirements to be used for the design of technical systems.** Some stakeholders were still confusing those requirements with the following types of general criteria that relate also in some way to "safety targets" or "safety requirements":

(a) other types of risk acceptance criteria (RAC) such as the acceptance of risks related to operational or organisational risk control measures put in place through the safety management systems of railway undertakings and infrastructure managers and through the system of maintenance of entities in charge of maintenance. Those criteria are related to the acceptance of risks related to the human interactions within the operation and maintenance of the railway system;

(b) the indicators of the safety performance levels currently achieved at the level of Member States, e.g. National Reference Values or NRVs, CSIs and CSTs referred to in the Commission Decision 2009/460;

(c) the CSTs to be achieved at the level of the European Union.

4.2.1.3. Consequently, in order to distinguish clearly the quantitative requirements necessary for the acceptance of risks related to failures of technical systems from the acceptance criteria of other types of risks, and in particular of operational and organisational risks, as well as of the overall risk at the level of the railway system, the **terminology** "risk acceptance criteria for technical systems" (RAC-TS) was **changed into "CSM design targets for technical systems" (CSM-DT)**.

4.2.1.4. In addition to these quantitative requirements for the CSM-DT, the stakeholders stressed the **importance of defining** in the amendment of Regulation 402/2013 **explicit requirements for the control of systematic failures and systematic faults** that might be introduced during the development process of a technical system to which the CSM-DT are to be applied.

4.2.2. CSM-DT way forward note

4.2.2.1. To solve all those problems and help arriving at a consensus with all the stakeholders, the Agency wrote a "**CSM-DT way forward note**" {Ref. 11.} which, based on previous developments, proposed the following three categories of CSM-DT:

(a) **10^{-9} h^{-1}** for **catastrophic accidents** affecting a group of people and resulting in fatalities and/or severe injuries and/or major damages to the environment;

(b) **10^{-7} h^{-1}** for **critical accidents** affecting an individual person and resulting in fatality and/or severe injury;

(c) **10^{-5} h^{-1}** for **marginal accidents** resulting in one or more light injuries.

4.2.2.2. The Agency organised also a series of "communication workshops" on the subject. That CSM-DT way forward note was presented and discussed repeatedly at the network meetings of national safety authorities and of representative bodies, as well as in working meetings with the stakeholders, for agreement:

(a) It analyses the work that took place till 2012, identifies challenging issues and suggests solutions for arriving at an agreement between all interested parties on CSM-DT;
(b) It makes a proposal for regulatory text on additional categories of CSM-DT;
(c) It gives a proposal for topics to be explained further in supporting guidelines;
(d) It requires the manufacturers, RUs, IMs and NSAs to validate the given proposal for the CSM-DT and to send their results to the Agency;
(e) It explains synergies with the LOC & PAS TSI and the work on the ERTMS DMI.

4.2.3. Rules for sufficient validation of the CSM-DT

4.2.3.1. The **rules for sufficient validation of the CSM-DT** were also discussed at the network meetings of NSAs and of the representative bodies, as well as in working meetings with the stakeholders. The gathered inputs indicated that the **CSM-DT validation** will be **sufficient, if**:

(a) it is logical, consistent, does not have obvious controversies and makes sense;
(b) it is based on practical and real examples of what is currently acceptable through national legislation or relevant standards in terms of design targets for technical systems;
(c) it is not going to reduce the present level of safety of technical systems and is therefore the state of art;
(d) it is validated by the manufacturers, RUs and IMs and not only by the NSAs.

4.2.3.2. These commitments were important in order to base the validation on facts and real practice examples from the railway sector rather than on general fears, feelings, thoughts and statements.

4.2.4. Consultation of the national safety authorities (NSAs)

4.2.4.1. In order to understand better the NSA disagreement with the proposed CSM-DT categories and values, the **Agency investigated the current practice of the NSAs** regarding the way they consider the CSM-DT in the scope of the authorisation for placing into service structural sub-systems and vehicles (APIS). Three general models of acceptance of CSM-DT by the NSA were identified:

(a) **model 1:** when granting the APIS, the NSA does neither see nor questions neither the CSM-DT nor any other type of RAC. It decides based on the NoBo, DeBo, CSM assessment body (*CSM-AB when CSM for risk assessment is used*) or independent safety assessor (*ISA - when CENELEC 50129 is used*) reports. The NSA does not redo/recheck the work of the ISA/CSM-AB;

(b) **model 2:** when granting the APIS, the NSA accepts the reports of the CSM-AB, the ISA, the NoBo and the DeBo. But depending on the project, the NSA also checks additionally the content of the risk assessment and the way CSM-DT and other types of RAC are set. It might happen that the NSA disagrees with the CSM-DT or any other type of RAC and sets new targets;

(c) **model 3:** when granting the APIS, either at the beginning or at end of the project the NSA derives the RAC-TS or CSM-DT from National Reference Values (or similar statistics). This RAC-TS or CSM-DT represents "*how much safety the Member State can afford 'loosing with' or 'granting to' the respective project*". Based on that, the NSA requires the applicant to demonstrate compliance with these RAC-TS or CSM-DT.

Table 2 : Summary table of the main models of acceptance of CSM-DT by the NSA in the scope of APIS.

	Model 1	Model 2	Model 3
How many NSAs apply the model?	± 18	± 7	± 3
How many NSAs will probably deliver validation?	1 to 3	1 to 4	1 to 2
Candidates for validation inputs?	ES, UK, BE	FI, NO, FR, EE	SE, DE

4.2.4.2. Although small divergences were reported (*e.g. as a good practice, the NSA might follow the project* work*, including the risk assessment and the independent safety assessment by the CSM-AB, from an early stage*), the following table summarises the main three acceptance models of the CSM-DT by the NSAs within the APIS. The table is based on NSA replies and reports on whether NSAs would validate the proposed CSM-DT.

4.2.5. Coordination and work with the representative bodies (CER, EIM, UIP, UNIFE)

4.2.5.1. In parallel with the consultation of the NSAs, the Agency participated also to a series of coordination meetings with the representative bodies (CER, EIM, UIP, UNIFE) in order to agree on the actual scope of the CSM-DT for technical systems and to discuss with them on their validation work of the proposed CSM-DT. In addition to those meetings, the Agency was requested many times to support their work and discussions via e-mails, phone conferences/calls, dedicated bilateral meetings, provision of dedicated answers to questionnaires on the subject, etc.

4.2.5.2. The progress with the validation of the CSM-DT by the representative bodies was **reported to a group of experts, including the NSAs** who expressed their intention to take part to the validation of the CSM-DT, **during four workshops** on the CSM-DT for technical systems. The **results of the discussions** that took part during these four workshops were **logged into successive versions of a working document of the legal text**. The different versions of that document trace the successive requests for changing the proposed categories and values of the CSM-DT for technical systems based on the results of validation of the CSM-DT. Parallel to this, **the Agency traced also the requests for further explanations** to be contained **in the application guideline** on the CSM-DT for technical systems.

4.2.6. Workshops organised for the validation of the CSM-DT

4.2.6.1. Participants

4.2.6.1.1. Having agreed with the networks of NSAs and of representative bodies on the way forward, the Agency opened the validation of the CSM-DT to all stakeholders who wanted to take part actively to this work. The following participants were invited: all members of the dedicated working group on the CSM for risk assessment, all NSAs of the NSA network and all representative bodies (CER, EIM, UIP, UNIFE, i.e. railway undertakings, infrastructure managers, private wagon keepers, manufacturers).

4.2.6.2. 1st workshop on CSM-DT: 25th & 26th April 2013

4.2.6.2.1. With respect to the initial deadline (15/11/2013) for the validation of the CSM-DT, the Agency organised a mid-term validation workshop. The following experts attended the event: NSAs (BE, BG, CZ, DE, FI, FR, HR, IT, NO, RO, SE, UK), CSM assessment bodies, independent safety assessors (ISAs), notified bodies, CER, EIM, UNIFE and independent railway companies. The objectives of the workshop were:

(a) on one hand, to get an overview of the railway sector experience with the use of Regulation 352/2009 on the CSM for risk assessment and in particular their experience with quantitative risk assessments, and;

(b) on the other hand, to enable everyone to track the progress with the validation of the CSM-DT and to allow proactive discussions among the actors.

4.2.6.2.2. The work performed till then showed that the validation of the CSM-DT is possible but the sector needed clarifications on some topics. The Agency agreed to answer a list of pending questions of the representative bodies on the scope and content of the validation of the CSM-DT. Both the NSAs and representative bodies explained that the **"light injury" CSM-DT category does not need to be harmonised**.

4.2.6.3. 2nd workshop on CSM-DT: 1st & 2nd April 2014

4.2.6.3.1. The second workshop was planned to take place by the end of 2013. However, although the NSAs and representative bodies agreed to complete the validation of the CSM-DT by 15th November 2013, the validation efforts appeared to be more challenging and more time and resource-demanding. The **deadline for completing the validation work**, in line with the agreed "sufficiency conditions", had then to be **postponed three times to reach consensus among most of the involved experts**.

4.2.6.3.2. The second workshop took place in April 2014. It was open to all stakeholders who actively took part to the validation exercise. The following experts attended the event: European Commission, NSAs (BE, DE, ES, IT, NO, SE, CH), CER, EIM, and UNIFE.

4.2.6.3.3. The planned objective was to get the final results of the validation of the CSM-DT by the NSAs and representative bodies, as well as their suggestions for additional explanations to be provided in the associated application guidelines. **Although the validation progressed, there was neither full consensus among all representative bodies nor with some of national safety authorities**. Based on the results of the validation in the scope of the German NeGSt project, the UNIFE representatives reported that due to the current wording of the proposed CSM-DT categories their use would increase the safety requirements, and consequently the development costs, for at least 50 % of functions of technical systems that the NeGSt project examined in their validation.

4.2.6.3.4. The wording proposed in the "CSM-DT way forward note" {Ref. 11.} does not differentiate “several fatalities from several severe injuries” as well as "one fatality from one severe injury". This initial CSM-DT proposal assumes that the predictive studies done during the development of a technical system cannot distinguish whether an accident caused by failures of functions of a technical system results only in severe injuries or in fatalities. For derailments and collisions such an assumption is certainly true. **The NeGSt project proved** nevertheless that **there are many failures of technical functions which do not lead to fatalities** at all. Consequently, the formerly proposed CSM-DT, which group "fatalities and injuries" in the same category, are **too much penalising** and, **compared to the current experience, lead** in practice **to an unjustified increase of safety requirements, and** therefore **of the associated costs**, for the development of the associated technical systems.

4.2.6.3.5. To try solving the problem identified by the NeGSt project, the experts of the workshop agreed to change the wording of the first category for **including the type of accident ("*a train collision, a derailment, or another type of accident*")** that results "in fatalities and/or severe injuries and/or major damages to the environment". This new wording was expected to avoid over-specifying the design targets for most of technical systems. The second CSM-DT category, i.e. "*an accident affecting an individual person and resulting in a fatality and/or severe injury*" was not yet changed as there was not common agreement on the types of accidents that would result in such a consequence.

4.2.6.3.6. For the second workshop, there was **not yet any evidence which validated** that **it is possible to demonstrate compliance with quantitative requirements for purely mechanical and purely pneumatic technical systems**.

4.2.6.3.7. Due to all these reported inputs, the discussions gave basis to update the proposed legal text and to provide detailed explanations in the application guideline. Consequently, **the public consultation had to be postponed once more after another workshop**. The NSAs and representative bodies agreed to continue their validation of the CSM-DT with these new inputs and to come at the next workshop with a common position, as well as with an answer to the following list of questions:

(a) What technical systems do the CSM-DT apply to?
(b) What functional level do UNIFE, EIM and CER apply the CSM-DT to and what are possible rules to break down technical systems into such functions?
(c) What should be the consequence/severity categories to be included in the final recommendation (number of categories, their values and the legal text of the category)?
(d) Propose a validation of the different categories according to the above point (c) through examples of functions of technical systems to support the acceptance of the categories.
(e) What requirements related to barriers need to be included in the regulatory text and what can be put later on in an application guideline?

4.2.6.4. 3rd workshop on CSM-DT: 16th July 2014

4.2.6.4.1. Once more, the workshop was expected to be the last one before the public consultation on a harmonised set of CSM-DT for technical systems. It was open to all stakeholders who actively took part to the validation exercise. The following experts attended the event: NSAs (SE, DE, FR, CH), CER, EIM, and UNIFE.

4.2.6.4.2. The representative bodies presented their common answers to the list of questions defined at the 2nd workshop. However, due to the difficulties in finding the correct wording, which would enable to cover the failures of not only train-side technical systems, but also those of infrastructure side technical systems, **even by this moment the representative bodies did not agree on a common wording of the two CSM-DT categories**. Although some changes of wording of the first CSM-DT category were proposed at the second workshop (i.e. link through the wording of the category to the type of accident), UNIFE insisted that **the problems reported by the German NeGSt project were still not wholly solved**: "*the alternative wording of the CSM-DT still increases the safety requirements, and consequently the development costs, for at least 50 % of functions of technical systems the NeGSt project validated*".

4.2.6.4.3. To solve this problem, the experts of the workshop agreed to change the wording of the two categories into something more generic. Rather than referring to the type of accidents, a similar approach could be used as in the aviation. The two CSM-DT categories should refer to failures that have the potential to affect either ***"the whole train and which typically results in fatalities either inside or outside the train"*** or "**does not affect the whole train (i.e. failures that cannot be classified in the first category) and which leads to at least one fatality**". All experts agreed that it is acceptable since fatalities are the worst failure consequences. This new wording is expected now to avoid the over specification of design targets for technical systems for the two CSM-DT categories. For example "an unwanted opening of a train door could lead to several fatalities". With the CSM-DT wording proposed in the way forward note, as well as the alternative one proposed at the second workshop, the $10^{-9}\,h^{-1}$ category could have been imposed. In practice, statistics report that usually such events do not result in fatalities; so, the

10^{-9} h^{-1} category would be a too much demanding requirement. The wording proposed at the third workshop would neither decrease the safety performance currently achieved by the functions considered in the scope of the NeGSt project nor increase the costs of development and of the safety demonstration of the associated technical systems.

4.2.6.4.4. At the 3rd workshop:

(a) both the NSAs and representative bodies explained again that the **"light injury" CSM-DT category does not need to be harmonised**.

(b) there was **not yet any evidence which validated** that **it is possible to demonstrate compliance with quantitative requirements for purely mechanical and purely pneumatic technical systems**.

4.2.6.4.5. The proposal for the legal text was also not mature enough to be sent for public consultation. In order to arrive at a wide consensus on the CSM-DT and large support within the railway actors, the NSAs and representative bodies agreed to perform a final check of whether the application of the latest proposal for the CSM-DT to failures of functions of existing technical system makes the associated risk acceptable, or on the contrary whether a more (or less) stringent CSM-DT is required. The objective was to validate whether the "CSM-DT categories and values" fit to the current reality and practice in the railways.

4.2.6.5. 4th workshop on CSM-DT: 18th September 2014

4.2.6.5.1. This was the final workshop. The objective was to get the final validation results from the NSAs and representative bodies on whether the proposed CSM-DT fit thoroughly to the current practice in the railways and whether the latest wording is appropriate or needs improvement.

4.2.6.5.2. As usual, the workshop was open to all stakeholders who actively took part to the validation exercise. The following experts attended it: NSAs (BE, SE, DE, HR, CH), CER, EIM, and UNIFE.

4.2.6.5.3. Based on the changes agreed at the 3rd workshop, the representative bodies (CER, EIM, UNIFE) unanimously confirm the validation of the two categories proposed by the legal text for the CSM-DT. The representative bodies have applied the CSM-DT to a set of functions of existing technical systems. They have compared for those functions the difference of the safety requirements that are specified either by national rules or by relevant standards to the new safety requirements that are defined by the CSM-DT. **The validation by the representative bodies shows that**, in the associated Member States, **neither the safety performance would be decreased nor the cost for implementing the CSM-DT would be increased compared to the current practice**. The risks of over-specification of the design targets for the technical systems reported by UNIFE during the 2nd and 3rd workshop on the German NeGSt project are now eliminated. Consequently, **the proposed "CSM-DT categories and values" correspond thoroughly to the present reality, experience and practice in the railways**. From the representative body point of view, the CSM-DTs are thus usable for their purpose. This **point of view** was **shared** also **by** the **UIP** representative **and the majority of the participants, even though not by all of the NSAs (DE and CH) who request further validation work on the proposed CSM-DT**.

4.2.6.5.4. All the workshop participants expressed the need to have an explanatory text of the CSM-DT in the application guideline in order to ensure that the legal text is applied correctly. In the absence of such a supporting guidance, the NSAs and the representative bodies fear the CSM-DT

can be misused and mutual recognition of the risk assessment results would not be achieved. The **application guideline should be ready with the entry into force of the amendment of Regulation 402/2013** with the agreed CSM-DT.

4.2.6.5.5. At the 4th workshop, it was decided to keep only two categories for the harmonised CSM-DT:

(a) the **"light injury" CSM-DT category does not need to be harmonised**.

(b) there was **not any evidence which validates** that **it is possible to demonstrate compliance with quantitative requirements for purely mechanical and purely pneumatic technical systems**.

4.2.6.5.6. Consequently, with the exception of the two points here after, **the legal text for the CSM-DT is now widely agreed among all the participants of the workshop. Everybody agreed that "the CSM-DT shall be used for the design of electrical, electronic and programmable electronic technical systems"**.

4.2.6.5.7. Due to time constraints and partially due to too extreme points of view on the side of some actors, it was not possible to achieve a full consensus on the two questions:

(a) Where should the list of functions of technical system, used by the representative bodies in the scope of their validation of the CSM-DT, be included (in the application guideline or another kind of document)?

(b) What should be the exact formulation of the legal text for the CSM-DT in order to be sure that purely mechanical or purely pneumatic systems are excluded from the scope of application of the CSM DT, *knowing that for mixed technical systems the CSM-DT are applicable for the "electrical, electronic and programmable electronic part or sub-systems*?

4.2.7. Consensus reached among the experts of the Workshop

4.2.7.1. At the fourth workshop, with the exception of the German and Swiss NSAs, all other experts involved in the validation of CSM-DT agreed on the wording below for the two categories of CSM-DT and on their applicability for the design of electrical, electronic and programmable electronic technical systems.

4.2.7.2. The following wording of the two CSM-DTs can be submitted to public consultation:

(a) **category 1:** for a failure that has a credible potential to lead directly to an accident, in which a **whole train is affected** and which **typically results in fatalities** either inside or outside the train, the frequency of the failure of the associated function does not have to be reduced further if it is demonstrated to be less than or equal to **10^{-9} failures per operating hour**.

(b) **category 2:** for a failure that has a credible potential to lead directly to an **accident typically resulting in at least one fatality** and **not classified in category 1**, the frequency of the failure of the associated function does not have to be reduced further if it is demonstrated to be less than or equal to **10^{-7} failures per operating hour**.

4.2.7.3. In order to avoid a misuse of the CSM-DT that would make difficult the mutual recognition of the risk assessment results, an application guideline should be ready with the entry into force of the amendment of Regulation 402/2013 with the agreed CSM-DT.

4.2.7.4. Concerning the two questions that remained open at the 4th workshop (see points (a) and (b) in section § 4.2.6.5.7.) above), the Agency decided to wait for the results from the public consultation. In general such kind of subjects can be explained fully in application guidelines. However, knowing that there is not any evidence which validates that it is possible to demonstrate compliance with quantitative requirements for purely mechanical and purely pneumatic technical systems, the Agency would suggest that the amendment of Regulation 402/2013 is clear enough that the CSM-DT are not to be applied to such technical systems.

4.2.7.5. The Agency shall coordinate with the representative bodies to agree on the next steps for the development of an application guideline associated to the CSM-DT subject.

5. IMPACT ASSESSMENT OF CSM-DT

5.1. The impact assessment of the work on CSM-DT was already performed in the period June 2011 – February 2012 in the scope of the revision of Regulation 352/2009. It was based on the version of the legal text (and respectively the CSM-DT classes) available at that moment. The original intention of that impact assessment was not only to evaluate the impact on the safety and cost of technical systems but also to use it as a mean for validating the Agency and RAC taskforce proposal for harmonised CSM-DT for lower risk consequence severities.

5.2. The impact assessment requested the railway actors to explain their current practices for accepting risks related to functional failures of technical systems :

(a) What requirements do railway undertakings and infrastructure managers specify in their contracts for functions of technical systems similar to those that should be proposed in the revised CSM-RA?

(b) What do manufacturers receive as requirements whenever they sign a contract with a customer?

5.3. Based on the answers provided by the Representative Bodies to those questions, the Agency expected to get assurance that the CSM-DT proposal reflects correctly the current practices for the acceptance of risk and, if necessary, to adapt the CSM-DT proposal.

5.4. The inputs received on these questions did not enable to achieve all expected objectives.

5.5. The main difficulties with this validation exercise in the scope of the impact assessment were due to the fact that:

(a) most of the companies did not carry out the requested analysis of their contracts and did not provide any data on the related questions.
(b) the NSAs often either left empty the fields asking about the CSM-DT values or answered only on a general basis, without really looking at what they really observe and experience as current practice, e.g. within the authorisations for placing into service structural sub-systems and vehicles.

5.6. The impact assessment showed the need to give more time to the railway actors, in order to allow them to work further on the respective questions and to provide commonly agreed results. As a consequence, in the period July 2013 to September 2014, the Agency, the sector and the NSAs followed a consistent step wise approach to validate the proposal.

5.7. The Agency CSM-DT proposal was published on the Agency web site and communicated to all relevant actors. Special cooperation work was done with the NSAs to clarify how they handle the CSM-DT within APIS and which NSAs are able to submit validation of the legal text.

5.8. As described in the sections above, the validation inputs were discussed in the framework of a series of workshops until a consensus (unfortunately not unanimity) was reached. The agreed wording of the legal text fits to the present practice of the sector and of the majority of NSAs, for whom the CSM-DT subject is relevant.

5.9. **Main conclusions of the impact assessment report:**

(a) The final report of the CSM-DT impact assessment gives in a concise form the most important conclusions and discussions of the replies received from the European railways. In order to avoid repeating those conclusions in detail in the present report, reference is made to the original impact assessment report for more information : see {Ref. 6.}.

(b) Basically, the impact assessment shows a strong qualitative indication that :

(1) harmonised CSM-DT will lower the amount of explicit risk estimations to be redone due to the use of different CSM-DT requirements. Less redesigns of technical systems, as well as less paper work for safety cases are expected;
(2) harmonised CSM-DT will improve cross-acceptance of technical systems.

(c) The impact assessment received very limited information on the question of costs related to the use of harmonised CSM-DT. The main identified costs are related to the process of defining appropriate CSM-DT-values and getting them validated. Further costs could not be predicted by the railways. The impact assessment shows nevertheless that including harmonised CSM-DT in the CSM-RA will further increase transparency on safety requirements and if set at appropriate level will improve cross-acceptance of technical systems for explicit risk estimations.

(d) The following three main points were contained in the scope of that impact assessment :

(1) Estimation of the impact in terms of the necessity to include in the CSM-RA further harmonised CSM-DT;
(2) Estimation of the impact in terms costs (unchanged or increased development cost of technical systems);
(3) Estimation of the impact in terms of safety (validation of the appropriateness of the proposal and neither increase nor decrease of the safety requirements).

(e) As explained above, for each of those 3 main points, the impact assessment shows that:

(1) the railway actors (railway undertakings, infrastructure managers and NSAs) clearly see the need and require the harmonisation of further CSM-DT (for further types of risk consequences severities).

(2) the railway actors (railway undertakings, infrastructure managers and NSAs) are not able to provide precise data on the actual impact in terms of costs. The CSM-DT's are deeply incorporated within the design and development process for technical systems. It is therefore almost impossible for the companies to extract and attribute a precise percentage of the overall cost to the compliance with CSM-DT. It is thus expected that even if the same question was asked more times to the same actors, the answer would not change too much. In overall, a more reliable estimation in terms of costs, than the one already available, could not be delivered.

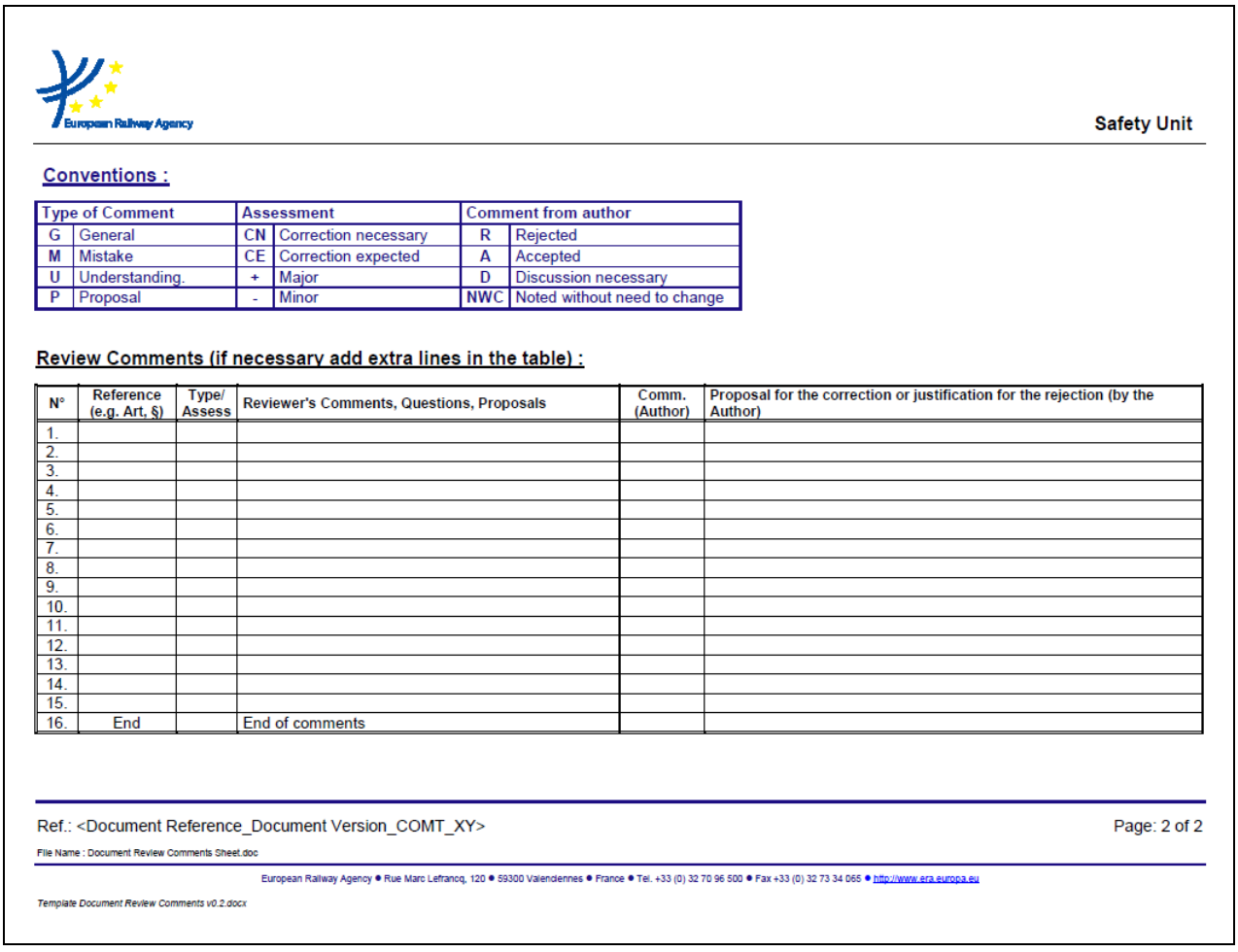
(3) the estimation of the impact assessment in terms of safety (validation of the proposal) was not possible for the sector by February 2012. For this reason, extra time was taken until September 2014 in order to work further and gain assurance on this important point.
The railway actors had more than 2 additional years to reconsider the CSM-DT proposal and gain confidence that the suggested CSM-DT categories correspond to the present practice and experience in the railway domain. This goal has been achieved with a wide majority amongst the European railway community.

5.10. Based on this summary of results of the initial impact assessment on CSM-DT, it can be concluded that the aims and the need of an impact assessment to support the Agency recommendation to EC is fulfilled by the impact assessment delivered in February 2012 : see {Ref. 6.}. The initial impact assessment, complemented by the work done in the period 2012-2014, gives sufficient visibility of the impact of the proposal for harmonised CSM-DT. See also http://www.era.europa.eu/Document-Register/Pages/Recommendation-on-the-revision-of-the-CSM-on-risk-evaluation-and-assessment-.aspx

6. PUBLIC CONSULTATION

6.1. In compliance with Article 4 of the Agency Regulation {Ref. 3.}, on 3rd November 2015 the Agency sent the CSM-DT amendment of Regulation 402/2013 for Public Consultation by the trade unions, social partners, NSA network, railway sector organisations, including ETF and EPF, European Commission, as well as by the other units and the legal adviser of the Agency.

6.2. The Agency applied a "formal review process". The reviewers were asked to send their comments to the Agency using the "comments sheet template" represented in Figure 1. The Agency provided a formal answer to all received comments and returned by e-mail the completed comment sheets to the reviewer for further discussion and agreement. Where agreement could not be reached with the reviewer by e-mail, a phone call took place to discuss and, if possible to find an agreement.



European Railway Agency — Safety Unit

Conventions :

Type of Comment		Assessment		Comment from author	
G	General	CN	Correction necessary	R	Rejected
M	Mistake	CE	Correction expected	A	Accepted
U	Understanding.	+	Major	D	Discussion necessary
P	Proposal	-	Minor	NWC	Noted without need to change

Review Comments (if necessary add extra lines in the table) :

N°	Reference (e.g. Art, §)	Type/ Assess	Reviewer's Comments, Questions, Proposals	Comm. (Author)	Proposal for the correction or justification for the rejection (by the Author)
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					
15.					
16.	End		End of comments		

Ref.: <Document Reference_Document Version_COMT_XY> Page: 2 of 2

File Name : Document Review Comments Sheet.doc

European Railway Agency ● Rue Marc Lefrancq, 120 ● 59300 Valenciennes ● France ● Tel. +33 (0) 32 70 96 500 ● Fax +33 (0) 32 73 34 065 ● http://www.era.europa.eu

Template Document Review Comments v0.2.docx

Figure 1 : Example of comment sheet used for the formal review process.

6.3. The public consultation did not generate new comments or views which were not already expressed by members of the Workshop involved in the CSM DT validation. The following comments are the main outcomes from Public Consultation and those meetings:

(a) the majority of returned replies support the definition of additional categories of CSM design targets in the CSM for risk assessment;

(b) with the exception of the German and Swiss NSAs, none questions the sufficiency of the validation of the proposed categories of CSM-DT and none disagrees that they correspond to current practices or requirements for design of technical systems that are referred to in national legislation or in applicable standards;

(c) CSM-DT's are necessary for the mutual recognition of safety demonstrations and the associated results from risk assessment of structural sub-systems and vehicles. The use of CSM-DT should prevent other conformity assessment bodies to request unjustified additional risk assessments and demonstrations and consequently, CSM-DT should limit additional undue costs for technical systems;

(d) the use of CSM-DT shall be restricted to the design of electrical, electronic and programmable electronic technical systems whereas clarifications are expected to be provided concerning their use for the whole railway system, purely mechanical and mixed technical systems;

(e) a change of the wording of the two CSM-DT categories is expected to enable an easier distinction between the two categories;

(f) most of the reviewers ask for an application guideline to describe the way the CSM-DT can be used and to contain examples of demonstration of compliance with the CSM-DT;

(g) a small minority of reviewers estimate that:

(1) the wording of the two CSM-DT categories is not sufficiently clear and specific (e.g. *whole train* or only *a part of the train affected by the considered failure*, *fatalities, at least one fatality*) and does not enable a clear distinction of the two categories;

(2) because there is no upper limit ("*at least one fatality*") there is an overlap between the two categories. This may lead to assignment of a less demanding design target to a function with a higher dimension of the risk;

(3) some readers interpret the wording "*affecting the whole train*" as CSM-DT being applicable only to trainborne technical systems, excluding their usability for infrastructure systems. This thus requires clarification in the proposed amendment rather than only in the application guideline;

(4) different interpretations of the CSM-DT wording are possible which makes the mutual recognition of the results of quantitative risk assessments impossible. This is in contradiction with Article 1(2)(c) of Regulation 402/2013;

(5) the use of CSM-DT should be limited either to functions defined in TSIs (when relevant for the interoperability) or to a list of functions contained in a legal text separate from the CSM-RA or in some kind of technical document discussed in RISC;

(6) if the use of CSM-DT is not limited to such a list, there is a fear that the proposer does not allocate correctly the right CSM-DT for the functions that are not validated. This could lead to an incorrect use of the CSM Regulation and would jeopardising the achievement of mutual recognition of the results of the risk assessment;

(7) German and Swiss NSAs propose to apply a step wise approach, i.e.:

(i) use the CSM-DT for the functions contained in the list of a legal text;

(ii) an Agency group of experts should meet regularly for discussing which new functions can be added to the list in the agreed legal text;

(iii) after getting sufficient experience with the CSM-DT and getting confidence on a correct use of the two categories, Swiss NSA suggests abandoning the mandatory

use of the list whereas the German NSA suggests extending the list in the legal text to new functions for which the usability of CSM-DT has been agreed with the group of experts;

The process for setting up the list of functions in the legal text with the associated CSM-DT (e.g. in an annex of the CSM-DT application guide or a separate technical note) shall be managed by the Agency and comparable to the one used for setting up equivalent requirements in TSI's. The annex of the CSM application guide with the list of permitted functions and associated CSM-DT shall be regularly revised by the Agency based on representative expert discussions.

(h) when using CSM-DT, the obligation to deal with both random hardware failures, systematic failures and systematic faults of the technical system is accepted by everyone. Controlling only the hardware failure part is not sufficient as this would lead a big part of risk not properly managed;

(i) there is expectation that the use of barriers will be described in the application on how they can be used to allocate less demanding design targets;

(j) finally there were proposals to change some existing text of the CSM-RA which was not object of the current amendment.

6.4. The results from Public Consultation were presented and discussed in the 72nd RISC Committee on 10th February 2015 and NSA Network meeting of 24th-25th February 2015.

6.5. The modifications were also presented, discussed and agreed with the representative bodies (CER-EIM-UNIFE) on a bilateral meeting on 3rd March 2015.

6.6. The comment sheet template represented in Figure 1 was used to process the received comments and remarks.

6.7. The points on which consensus could not be reached at the workshop or during Public Consultation are summarised in section 9.2.

7. DESIGN TRAGETS IN THE AVIATION FIELD

7.1. Introduction

7.1.1. At the 71st RISC meeting on 6th November 2014, the Agency presented the results of the validation of the proposed CSM design targets (CSM-DT).

7.1.2. In order to get assurance that the proposed values are reasonable, the Danish representative in RISC suggested the Agency to verify whether experience could not be learnt from the aviation field.

7.1.3. The Agency explained to RISC that similar quantitative requirements are applied also for the design of big aircrafts. Indeed, in 2009, the Agency contracted a study for analysing the use of risk acceptance criteria for technical systems and operational procedures in different fields of industry, including the aviation. The results of that study were published in 2010. They are uploaded on the Agency web page under the following link :

http://www.era.europa.eu/Document-Register/Documents/risk-acceptance-criteria-for-technical-systems.pdf

7.2. Comparison of railway and aviation requirements and practices

7.2.1. Following the 71st RISC meeting, the Agency decided to check again the experience from the aviation domain and to verify whether there was not a risk to introduce too permissive safety requirements for technical systems used in the railway domain.

7.2.2. The Agency read and analysed on its own the following reference documents retrieved from the study referred to here above :

(a) AC-AMJ N°25.1309 on the system design and analysis;
(b) DO-178b on software development assurance;
(c) DO-254 on hardware development assurance;
(d) SAE ARP 4754 on system integration requirements;
(e) SAE ARP 4761 “Guidelines and methods for conducting Safety Assessment process on civil airborne systems and equipment”

7.2.3. In order to cross check whether those documents have correctly been understood, the Agency contacted also a representative of the Italian national safety authority from the aviation domain.

7.2.4. Based on this analysis and the bilateral discussions with a representative of the Italian national safety authority from aviation, the Agency arrives at the conclusion contained in Table 3.

Table 3 : Similarities between aviation and railways.

AVIATION	RAILWAYS
In aircrafts, safety critical functions are performed by complex technical systems	Railways use also complex technical systems to achieve safety-related functions
Failures of technical systems used in aircrafts have an effect on the safety of the airplane and/or its occupants	Failures of technical systems used in railways have an effect on the safety of the train and/or its occupants and/or on persons outside the train

Table 3 : Similarities between aviation and railways.

AVIATION	RAILWAYS
Failures of technical systems can result in catastrophic consequences with hull loss and multiple fatalities. The aviation literature uses the "Failure Condition" terminology.	Failures of technical systems can result in a catastrophic consequence with damage to rolling stock or infrastructure and multiple fatalities either inside or outside the train. The CSM for risk assessment uses the terminology hazards arising from a failure of a function of a technical system.
Failure Conditions related to technical systems are covered by quantitative targets	Failures related technical systems are covered by quantitative design targets (CSM-DT)
Risks/Failure Conditions arising from human actions are controlled by operational and organisational safety arrangements	Risks arising from human actions are controlled by operational and organisations provisions of the SMS
Safety requirements for Failure Conditions related to technical systems are **based on historical data** For **design of new airplane** it is reasonable that serious accidents caused by technical systems should not be allowed a higher probability than the safety performance achieved till there.	Safety requirements introduced by CSM-DT are **based on the current practice** reflected by national legislation and relevant safety standards
• ***For big airplane**, historical evidence indicated that that the probability of a serious accident due to operational and airframe-related causes was approximately one per million hours of flight [10^{-6} per flight hour]*	A rigorous reporting of accident and incident data for railways does not exist in all Member States. Therefore this does not enable to setup quantitative requirements for the design of technical systems based on historical data
• *About 10 percent of the total figure **were attributed** to Failure Conditions caused by the airplane's systems → serious accident from all Failure Conditions shall not be greater than 10^{-7} per flight hour*	In railways, **there is no yet formal evidence** of the overall apportionment of failures between causes related to technical systems and those due to human interactions. Nevertheless, the already available statistics at some railway organisations seem to show that the contribution of technical systems is smaller than 10% and even closer to 1%.
• *Arbitrarily assumption : there are about 100 potential Failure Conditions in an airplane which could be catastrophic → allowable target apportioned equally among all Failure Conditions* ***Catastrophic Failure Conditions shall not be greater than 10^{-9} per flight hour***	There is no arbitrary assumption on the number of safety-critical functions in a technical system used in railways. The same CSM-DT requirement has to be applied for the design of the whole technical system
Units used for quantitative requirements: **frequency of occurrence per flight hour**	Units used for quantitative requirements: **frequency of occurrence per operating hour**
Further accident reporting and monitoring in aviation confirms that those targets are achieved in practice also by the design of new airplanes	The use of CSM-DT needs to be monitored in order to verify whether the safety performance actually achieved is at least as good as the one specified in the proposed amendment of CSM-RA
Catastrophic Failure Conditions shall not be greater than 10^{-9} per flight hour	**The failure of a function of a technical system with catastrophic consequences shall not be greater than 10^{-9} per operating hour**

Table 3 : Similarities between aviation and railways.

AVIATION	RAILWAYS
Failure Conditions with less severe effects can be more likely to occur than 10^{-9} per flight hour	Risks arising from failures of technical systems with a less severe consequence severity are acceptable at a frequency of occurrence not greater than 10^{-7} per operating hour
Comparison of quantitative requirements	
AVIATION : see {Ref. 14.}	**RAILWAYS : Agency recommendation**
Catastrophic Failure Conditions resulting in multiple fatalities usually with the loss of the airplane (thus impacting all occupants) ≤ 10^{-9} per flight hour **[Extremely improbable Failure Condition]**	Failures of functions having possibility to affect whole train (thus all train occupants) and resulting in multiple fatalities ≤ 10–9 per operating hour **[≈Catastrophic consequences]** **[Highly improbable as defined in CENELEC]**
Hazardous Failure Conditions reducing the capability of the airplane, with a large reduction in safety margins, physical distress to crew or excessive workload on crew and impacting a relatively small number of occupants ≤ 10^{-7} per flight hour. **[Extremely remote FC]** **Requirement applicable also for a single fatality**	Failures of functions having possibility to affect a limited area of train (thus a relatively small number of occupants) and resulting in at least one fatality ≤ 10^{-7} per operating hour **Requirement applicable also for a single fatality** **[≈Critical consequences]** **[Improbable as defined in CENELEC]**
Major Failure Condition ≤ 10^{-5} per flight hour **[Remote]**	Light injuries ≤ 10^{-5} per operating hour **[≈major consequences]** **[Rare as defined in CENELEC]** As it is not necessary for mutual recognition, on request of all stakeholders it was not included in the amendment of 402/2013
Minor Failure Condition ≤ 10^{-3} per flight hour **[Probable]**	"10^{-3} per operating hour" existed as a result of the taskforce on the development of risk acceptance criteria. But as it is not necessary for mutual recognition, on request of all stakeholders, it was not considered at all in the amendment of 402/2013
Equivalence or similarities of quality and safety assurance processes	
Standards with similar requirements are used for designing technical systems. It can thus be presumed that the technical systems in both fields are expected to achieve equivalent levels of safety performance	
Equivalent processes are used for the Safety Assessments, Hardware and Software Development, Verification & Validation & Management of Systematic Failures and Systematic Faults	
Similar requirements and standards are applicable in both fields for the demonstration of the achievement of quantitative requirements, including the use and modelling of safety barriers external to the technical system under assessment. This includes among others: • Use of Qualitative and Quantitative demonstrations; • Use of Top Down [Fault Tree Analyses – FTA – analysing the combination of failures] and Bottom-Up [e.g. Failure Mode Effect (and Criticality) Analysis – FME(C)A – analysing the effect of individual failures] approaches	

7.3. Should railway technical systems be safer than the aviation ones?

7.3.1. It is important to underline that contrary to the aviation, where the availability of the aircraft core functions must be maintained for a safe landing, "**in railways the fail-safe state corresponds to the train at standstill**", much easier to achieve. Taking that into account, and these similarities with the aviation field, there is thus a great confidence that the proposed quantitative design targets (CSM-DT) will not decrease the existing safety levels in EU railways. For each consequence severity of a failure of a railway technical system, the same quantitative design target (CSM-DT) is specified as for the corresponding consequence severity for big aircraft.

7.3.2. There is no justification for defining more severe and more demanding design targets for railway than those used in aviation. The validation by the representative bodies shows that neither the safety performance would be decreased nor the cost for implementing the CSM-DT would be increased compared to the current practice. On the contrary, imposing different values for the same categories would be too much penalising for railways and, compared to the current experience, it would lead to an unjustified increase of safety requirements, and therefore of the associated costs, for the development of the technical systems in railways.

8. CONTENT OF THE RECOMMENDATION

8.1. Existing CSM-DT in regulation 352/2009 and 402/2013

8.1.1. The CSM-RA enables the evaluation of the risk acceptability of a significant change to the railway system by using one or a combination of the following so-called "risk acceptance principles", without giving priority to any of them:

(a) the application of codes of practice;
(b) the comparison with similar reference systems;
(c) the use of explicit risk estimation.

8.1.2. The risks, which are controlled by the application of codes of practice or by the safety requirements derived by a comparison with a similar reference system, are considered as acceptable provided that the conditions of application of these two risk acceptance principles are fulfilled and sufficiently documented as defined in the CSM-RA. Additionally, whenever the third risk acceptance principle – *the explicit risk estimation* – is used and in order to be able to determine whether the residual risk is sufficiently low so that it is not necessary to take any immediate action to reduce it further, risk acceptance criteria (RAC) are used.

8.1.3. One harmonised RAC (of the type called CSM Design Target) for explicit risk estimations is included already in point 2.5.4 in Annex I of the CSM-RA. It says the following:

"*Where hazards arise from failures of technical systems not covered by codes of practice or the use of a reference system, the following risk acceptance criterion shall apply for the design of the technical system:*

For technical systems where a functional failure has credible direct potential for a catastrophic consequence*, the associated risk does not have to be reduced further if the rate of that failure is less than or equal to* 10^{-9} *per operating hour.*" [CSM-RA, Annex I, point 2.5.4]

8.1.4. As mentioned earlier, already by the time when developing the Regulation N° 352/2009, it was clear that further harmonised RAC (for lower severity consequences and further types of risks) will have to be provided. This was the aim of the consequent work, to which the present recommendation is related.

8.2. Different types of RAC

8.2.1. It is crucial to underline that the present recommendation covers only the very particular type of RAC for failures of functions of technical systems. It does not cover all types of other RAC, although the railway sector starts indicating now that a big part of them should be worth harmonising.

8.2.2. Generally in 2007, the work on the harmonisation of further RAC suggested the harmonisation of criteria related to all types of risks. Later on, during the development it became clear that for the sector it is too demanding to work on all types of risks simultaneously. This is why the development had to be split in parts and the efforts to be focused on a step-by-step approach. The following general high-level types of RAC have been identified:

(a) RAC related to failures of functions of technical systems with different types of direct consequences:

(1) catastrophic consequences measured in terms of reflection on "human life" as a "measurement unit" – addressed by the current CSM-RA – Regulation 402/2013;
(2) other consequences, again measured in terms of reflection on "human life" as a "measurement unit"– open for definition / harmonisation;
(3) other consequences, measured in terms of reflection on "damages to the environment", or similar – appropriate for freight traffic (and not only) – open for definition / harmonisation;

(b) RAC related to failures of functions of technical systems with different types of non-direct consequences (where barriers are present), and

(c) RAC for risks related to human errors within the railway system (covering the design of the technical systems, their integration into the railway system, the "operational changes", the "organisational changes", introduced by the railway companies, etc.).

8.2.3. The above proposed "hierarchy" has not been strictly defined. It only gives to the reader of this report a sense of feeling of the wide variety and types of risks and RAC, which may be experienced and may need to be harmonised in practice. It was the initial aim of this development (as well as within the original scope of the mandate for this work) to harmonise all of these RAC, however in the scope of a few years' work, it became clear that it was not realistic to do this at once. The work needed to be done at smaller steps.

8.2.4. The present recommendation covers only the RAC for failures of functions of technical systems with certain direct consequences measured in terms of influence/degradation of human life. As described in the accompanying report for the revision of Regulation 352/2009 {Ref. 10.}, a considerable amount of further work has been done to prepare the basis for harmonisation of further types of RAC (i.e. RAC for risks related to human errors within the railway system). However, these could not have been the scope of the present recommendation.

8.2.5. Additionally, it is important to underline that both the proposer of a change according to the CSM-RA and the national safety authority or any other "accepting or requiring party" need to clearly distinguish between the design targets for the technical system itself (such as the existing harmonised CSM-DT from Regulation 352/2009), and any other (national or not) requirement for the acceptable safety performance of the technical system while it is being integrated, maintained and operated as a part of the railway system (like Common Safety Targets -CSTs, national safety levels - NRVs, company safety targets, etc.).

8.2.6. The currently existing RAC (CSM-DT) in the CSM-RA considers hazards arising from failures of functions of a technical system that have potential to lead *directly* to particular unwanted consequences. This RAC is a *design target* for the assessed function of the technical system. The design target specifies the requirements to be fulfilled by the design of the considered technical system. It cannot be compared to:

(a) any statistical performance of existing technical systems which is based on data collected taking into account that these technical systems are integrated in the railway system. This type of statistical data is generally not a reflection of the mere performance of the technical system itself, but is a reflection also of many other "barriers" and factors like the way the technical system is integrated, operated and maintained by its owners and users;

(b) any national safety levels and targets, which may principally be defined at the level of a Member State level, but where in practice the safety is based on the combination of several barriers of different natures (operational, organisational and technical). For such targets,

technical systems are not the unique mean to prevent accidents, irrespective of the safety performance of such systems.

8.2.7. The CSM-DT shall thus not be confused with any target of a type similar to those defined within the Common Safety Targets or the Common Safety Indicators. A solid understanding of this fact is a basis for the correct application of the present recommendation for harmonisation. Further information about the differences will be given within the application guideline document supporting this recommendation.

8.3. Recommendation for further CSM-DT

8.3.1. Based on the work performed in the period 2007-2014 on the development and validation of CSM design targets for technical systems, it is possible to make a proposal for the harmonisation of further RAC, renamed into "harmonised CSM Design Targets", for risks arising from failures of functions of technical systems. Compared to the single CSM-DT defined in Regulations 352/2009 and 402/2013, these CSM-DTs are altogether covering an additional consequence severity of risks that have a credible potential to lead directly to the considered accident.

8.3.2. The main following requirements are proposed. The precise text regarding the CSM-DT can be found in the recommendation that the present report accompanies.

2.5.5. If hazards arise from failures of functions of a technical system, …the following requirements 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 failures of the associated function is 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 failures of the associated function is demonstrated to be improbable.

2.5.6.… the requirements in point 2.5.5. shall be referred to as the harmonised design targets. They 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.

The design targets … shall neither be used as overall quantitative targets for the whole railway system of a 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, the hazard identification shall be carried out in accordance with point 2.2.5. in Annex I. The hazards arising from the purely mechanical part shall not be controlled by the use of the design targets…

2.5.7. The risks arising from failures of functions of technical systems … shall be considered as acceptable if the following requirements are fulfilled:

(a) The compliance with the applicable harmonised design target is demonstrated;

(b) The associated systematic failures and systematic faults are controlled in compliance 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 are identified and registered in the hazard

record in accordance with point 4 of Annex I. In accordance with point 1.2.2. of Annex I, these application conditions shall be transferred to the actor responsible for the demonstration of the safe integration.

8.3.3. It is important to note is that the text of the recommendation simultaneously:

(a) adds one harmonised CSM-DT more for a lower severity of the consequence of risks. This enables to target the development costs of technical systems proportionately to the risk introduced by that system;

(b) helps the mutual recognition of risk assessments results for the two categories of consequence severities of risks;

(c) enables the use of explicit risk estimation for innovative technical solutions;

(d) helps to close and achieve mutual recognition of safety-related open points within the LOC&PAS TSI;

(e) keeps the flexibility of the railway actors to choose the most appropriate design targets for the design of their technical systems.

Depending on the safety performance actually to be achieved, the two existing provisions in Regulation 402/2013 (points 2.5.5. and 2.5.6 in annex II renumbered into point 2.5.10 and 2.5.11 in the proposed amendment) may still be used either to request a more demanding design target, if this is necessary to maintain the existing safety level, or to permit the use of a less demanding design target, if the existing national safety level can still be maintained with that less demanding design target.

8.3.4. The monitoring of the use of the points 2.5.10 and 2.5.11 in Annex II of the proposed amendment of Regulation 402/2013 will allow collecting information on whether in future the proposed CSM-DT do not need to be adapted to fit to the values actually used in the railway business.

9. STAKEHOLDERS' OPINIONS ON THE RECOMMENDATION

9.1. General opinions of the stakeholders

9.1.1. CER, EIM, UNIFE and all national safety authorities, except the German and Swiss ones, which were involved in the development and validation of CSM-DTs support the proposed legal text. These design targets are a valuable and significant step forward for the railway sector in the application of the CSM RA regulation and for the achievement of mutual recognition of structural sub-systems and vehicles.

9.1.2. The sector organisations and most of the NSAs expect the additional CSM-DT to enhance the mutual recognition of the application of the CSM and of the results of the risk management process specified therein, leading to less paper work and less additional demonstrations when applying for operation in other Member States.

9.1.3. The stakeholders did not request for any transition period before the entry into force and application of the new requirements. However, to help the sector with the application of the CSM-DT, all involved experts unanimously agree on the necessity to produce an application guideline. The application guide should support the legal text with additional explanations. It should be available at the stage when the recommendation will be put to vote by the Member States. At present, the following structure is proposed for the application guide:

(a) introduction;

(b) explanations and principles (definitions);

  (1) links/relationships with standards;
  (2) relevance of using/not using CSM-DT;

(c) description of the steps for applying the CSM design targets;
(d) level of application of CSM DTs;
(e) explanation regarding the use of internal and external barriers;
(f) examples for assigning severity categories

  (1) include a list of examples of functions of technical systems;
  (2) include a list of examples that are out of scope of CSM-DT;

(g) use of design targets for mechanical systems: clarify that it is primarily for use of electrical/electronic systems;

9.1.4. CER, UNIFE and EIM are ready to provide support in the development of this guideline and welcome the involvement of the Member States in the development and review of the guideline.

9.2. Minority opinions of German and Swiss NSAs

9.2.1. German NSA position

9.2.1.1. The German NSA has the following two main issues on the text proposed by the Agency after the Public Consultation.

9.2.1.2. **German NSA position concerning categories/definitions**

Some changes to the Agency recommendation are proposed in order to eliminate; from its point of view, the "overlap between the two CSM DT categories". In addition to that, it is suggested to

use the EN CELENEC definitions (e.g. "*catastrophic*" and "*critical*" accidents) instead of "similar" definitions. If specific definitions are needed, clarify their use for the needs of "explicit risk estimation" in order to avoid mistakes with respect to standards.

9.2.1.3. **Agency reply :**

(a) The Agency agrees that, as far as possible, consistency shall be kept with the CENELEC standards which are relevant to the railways. However, the use of CENELEC standards shall not change the scope of the Safety Directive 2004/49. For example:

(1) CENELEC defines a "*'catastrophic accident' as an accident typically resulting in fatalities, multiple severe injuries or major damage to the environment*", whereas;

(2) the amendment defines a "*'catastrophic accident' as an accident typically affecting a large number of persons and resulting in multiple fatalities*";

(b) Although the SMS must ensure the control of all risks associated with the activities of the infrastructure manager or railway undertaking, the scope of Directive 2004/49 does not include any explicit requirement for the protection of the environment. Other national and EU legislation deal with the environmental protection. Refer for example to "*Directive 2004/35/CE of the European parliament and of the Council of 21 April 2004 on environmental liability with regard to the prevention and remedying of environmental damage*". See also the following link : http://ec.europa.eu/environment/legal/liability/. Redundant EU legislation shall therefore be avoided.

In addition to that the protection of the environment shall not only be requested when CSM-DT are used during quantitative explicit risk estimation. The proposed change would thus only impose the consideration of environmental risks when CSM DT's are used and not in all cases where CSM-RA is used.

Finally, this would not be consistent with the requirements on the national safety authority for the assessment of the RU/IM SMS. The CSM-RA would setup requirements for the environment whereas there is not any reference in the CSM for conformity assessment (Regulations 1158/2010 and 1169/2010) to any criterion that the NSA shall use for verifying in practice that the RU/IM SMS has measures in place to protect against damage to the environment.

(c) Concerning the consideration of "multiple severe injuries", as explained during the work-shops (see section § 4.2.6.), the German NeGSt project has demonstrated there are many failures of technical functions (at least 50% of the validated functions – more or less 60 functions) which do not lead to fatalities at all. Consequently, including "injuries" in the CSM-DT categories, would be too penalising and, compared to the current experience and practice, would lead to unjustified increase of safety requirements, and therefore of the associated costs, for the development of the associated technical systems. So, the definitions of "catastrophic"[(1)] and "critical"[(2)] accidents does not need to be changed.

(d) Considering the definitions of "catastrophic"[(1)] and "critical"[(2)], it is difficult to understand the German NSA perception of "overlap between the two categories". The two categories refer to different types of accidents. The first one refers to "big accidents" whereas the

(1) *'Definition (23) 'catastrophic accident' means an accident typically affecting a large number of persons and resulting in multiple fatalities'.*

(2) *'Definition (35) 'critical accident' means an accident typically affecting a small number of persons and resulting in at least one fatality'.*

second one refers to "small accidents". They are distinct and do not present overlap. They affect either a large number of persons or a small number of persons. Furthermore, they correspond exactly to same concepts used in the aviation domain : refer to section § 7..

Based on those explanations, it is not necessary to modify the proposed text for the amendment of Regulation 402/2013.

9.2.1.4. **German NSA position concerning categories/definitions**

From the German NSA point of view, the wording of the two CSM-DT categories is not sufficiently clear and specific (e.g. *a large number of persons* or only *a small number of persons affected by the considered failure, fatalities, at least one fatality*). As there is no upper limit ("*at least one fatality*") the distinction between the two categories is not clear; there is thus an overlap between the two categories. This may lead to assignment of a less demanding design target to a function with a higher dimension of the risk.

9.2.1.5. **Agency reply:** refer also to the explanations in point here above.

Concerning the incorrect allocation of the CSM-DT to the considered failure of a function of the technical system, according to Regulation 402/2013 the proposer's risk assessment and appropriateness of the results (i.e. including the allocation of CSM-DT and demonstration of their achievement) shall be checked by a competent CSM assessment body accredited or recognised according to the requirements and criteria contained in Annex II of Regulation 402/2013. This provides assurance that the errors of possible incorrect allocation of CSM-DT are detected by the safeguards put in place by the EU railway legislation.

9.2.1.6. **German NSA position concerning scope/missing validation**

(a) The German NSA proposes changes to clarify the scope and solve the issue of the missing (or insufficient) validation of the proposed CSM-DT. In addition to that, the German NSA proposes to introduce a process for extending the use of explicit risk estimation according to the actual state of play in the sector via an annex of the guideline. That should support the sector activities.

(b) The German NSA proposes that the CSM design targets, referred to as harmonised design targets, shall apply to those failures listed either in:

(1) relevant TSIs, for those functions that are sufficiently validated and which are relevant for interoperability, or;
(2) an annex to the CSM application guide for the remaining harmonised and sufficiently validated functions.

(c) The German NSA requires also an Agency group of experts meets regularly for discussing which new functions can be added to the list in the agreed legal text. This process leading to the definition of the list of functions, and of the associated CSM design target values, to be included in the annex of the CSM application guide needs to be designed by the Agency and to be comparable to the one leading to the identification of such functions contained in relevant TSI's. From the German NSA point of view, the purpose of this request is to ensure that the responsibility for the safety of the railway system is not changed. The annex of the CSM application guide with the list of functions and associated design target values shall then be regularly revised by the Agency based on those representative expert discussions.

9.2.1.7. **Agency reply:**

(a) The proposed text introduces new concepts [e.g. validation, sufficiently, guide, annex to the guide, processes leading to a list of functions, design of the guide, different concept of responsibility for the railway safety and expert discussions] that would need to be defined in the legal text whereas in practice, on one side such text is not necessary and on the other side, it would be deleted by the juridical services of the Commission.

(b) The TSIs and the CSM-DT defined in the CSM for risk assessment are complementary. If the amendment of Regulation 402/2013 is adopted, the CSM will provide the ceiling values for hazards that have a credible potential to result directly in either "catastrophic" (i.e. big) or "critical" (i.e. small) accidents. There would thus be two harmonised consequence severities of accidents.

(c) The acceptable quantitative requirements for those consequence severities can only be discussed and agreed by a competent group of experts and dealing with Risk Assessment and Risk Management. Such a discussion cannot take place in the TSI Working Groups as they do not necessarily contain experts in risk assessment and risk management. This is the reason for including the CSM DT values in Regulation 402/2013.

(d) As the CSM does not have the ambition, and does not need, to identify exhaustively all railway functions to which CSM-DT could be applied [especially taking in to account the freedom for the proposer to use any of the three risk acceptance principles for controlling the identified hazards], it is not necessary to incorporate such provisions in the legal text of the CSM. Where relevant, the TSIs will refer to the CSM for the use of the correct category of CSM-DT. The CSM does not supersede and cannot modify the requirements already set up in TSIs.

(e) In addition to that, the proposed text would move the responsibility for the safety of the railway system into the CSM instead of laying it down on those which operate and maintain the railway system, i.e. RUs and IMs. That is contradictory with Article 4 of the Safety Directive 2004/19.

(f) For those reasons, it would be a wrong approach to narrow the usability of CSM-DT through the proposed text only to a list of functions contained in TSIs or in an annex of the guideline.

(g) Concerning the "process for defining the list of functions", it would automatically exclude the possibility to use the Explicit Risk Estimation (3rd RAP). Accepting the change would impose implicitly the use of Codes of Practice and would also fix an order of priority among the three risk acceptance principles. This was categorically rejected by the large majority of experts of the Workshop on CSM DT.

(h) The Agency Regulation 881/2004 already specifies the working method of the Agency for developing TSIs. There is thus no need to create redundant legislation. As explained in the lines above, it is not the purpose of the CSM to carry out an exhaustive functional identification, and subsequent allocation of requirements, for all functions of the railway system. The CSM only sets out the acceptable frequencies of failure for the identified two categories: "catastrophic" and "critical". When relevant functions are used, at that moment and based on results from the risk assessment, the user/proposer is responsible to specify which of the two categories of the CSM fits to the change under assessment. That work will then be assessed by the independent CSM assessment body. Furthermore, the CSM cannot know in advance all possible cases where those CSM DT values could be applicable. Whenever necessary, a TSI will make reference to the CSM DT categories.

(i) The list of functions for which quantification is possible cannot be exhaustive in the legal text. As written above, it is not the purpose of the CSM to carry out such a functional identification, and subsequent allocation of quantitative requirements, of the railway system. Consequently restricting the use of CSM-DT only to a limited list of functions of TSIs or of the guide will make illegal the use of the CSM-DT for functions which are not in the list and that might be known by experts outside the working group.

(j) In addition to that, allocating a requirement to a function without knowing how the function is achieved/architectured in the railway system might lead either to over specification or under specification of the safety requirements. Consequently, implementing the proposed comment would create a risk because of the legal text.

(k) A legal text cannot specify a clear list of completely defined functions, outside their operational context, and cannot setup safely the associated frequencies of failures without knowing how these functions are going to be actually implemented by the architecture of the railway system. A guideline is also not a legally binding text.

(l) Finally, Article 18 of Regulation 402/2013 already requires the Agency to collect all information on the experience of the application of Regulation 402/2013 and to make recommendations to the Commission with a view to improving the Regulation or guidance documents.

Based on all those explanations, the comment cannot be taken into account.

9.2.2. Swiss NSA position

9.2.2.1. The Swiss NSA has the following two crucial concerns on the text proposed by the Agency.

9.2.2.2. The differentiation between the two categories of CSM-DT in point §2.5.5 before Public Consultation was not enough clear for the proposer to be able to distinguish the two categories.

The Agency proposal after Public Consultation is satisfactory for the Swiss NSA;

9.2.2.3. The validation of the CSM design targets has not been done for a large spectrum of functions.

In order to enable the use of the proposed CSM-DT, the Swiss NSA proposes to limit the application of the CSM design targets to a list of functions. The reasons are the following:

(a) even if the representative bodies (CER, UNIFE, EIM) confirm they have validated the design targets (CSM-DT), the NSAs have never received the detailed information about how this has been carried out (the access was denied for confidentiality reasons), and;

(b) the validation was done by the representative bodies only for a specific set of functions of technical systems.

From the Swiss NSA point of view, because of that there is no guaranty that the allocation of the CSM design targets to other relevant but not validated functions of European railway system can actually work. Too many different opinions from the sector have been heard during the discussions in the workshop on CSM-DT. This raises concerns to the Swiss NSA about the possibility of an incorrect use of the CSM Regulation. This concern is even higher taking into account the future limited role of the NSAs on mutual recognitions of results from the application of Regulation 402/2013.

9.2.2.4. **Agency reply :**

(a) It is true that for the reasons explained in section § 4.2.6. different opinions were raised during the different workshops. However, with the exception of the German and Swiss NSAs, at the last workshop all experts have agreed on the proposed text. They estimate acceptable to include in the application guideline on CSM-DT all additional and necessary explanations on the use of and on the demonstration of compliance with the CSM-DT.

(b) Concerning the incorrect allocation of the CSM-DT to the considered failure of a function of the technical system, according to Regulation 402/2013 the proposer's risk assessment and appropriateness of the results (i.e. including the allocation of CSM-DT and demonstration of their achievement) shall be checked by a competent CSM assessment body accredited or recognised according to the requirements and criteria contained in Annex II of Regulation 402/2013. This provides assurance that the errors of possible incorrect allocation of CSM-DT are detected by the safeguards put in place by the EU railway legislation.

(c) It is not necessary that the CSM-RA changes the responsibility for the safe operation and safe maintenance of the railway system. Neither the CSM assessment body nor the national safety authority is responsible for the safety of the railway system. The Safety Directive 2004/49/EC clearly sets that responsibility on the railway undertakings and infrastructure managers for the part of the railway system they are responsible for.

9.2.2.5. The Swiss NSA proposes the following solution:

(a) limit the use of CSM-DT at a first stage to a list of functions that have been **validated by an explicit risk analysis** and where a consensus on the appropriate CSM-DT has been reached. As a basis, the validated functions from the workshop can be taken. The Swiss NSA would appreciate a lot, if the corresponding validation documents could be made available also to NSA's.

For the Swiss NSA, only the functions with the failure rate of 10^{-7} per operating hour [second CSM-DT category] are concerned by this limitation. Such a list of validated functions would be a good basis for mutual recognition among different states.

(b) The Swiss NSA sees three application cases of the CSM design targets:

(1) full mutual recognition for all functions with failure rates lower than 10^{-9} per operating hour [first CSM-DT category] (state today).

(2) full mutual recognition for functions with failure rates lower than 10^{-7} (but higher then 10^{-9}) per operating hour provided it is on the list of functions;

(3) for functions with failure rates lower than 10^{-7} (but higher then 10^{-9}) per operating hour that are not on the accepted list, mutual recognition is only possible if an explicit risk analysis is available.

(c) although during Public Consultation the Swiss NSA agreed to include such a list of functions in the application guideline on CSM-DT, recently the Swiss NSA expressed that a more binding form (kind of legally binding technical document) would be preferable.

(d) after getting experience on CSM-DT with a practical application of the amended regulation, the limitations expressed in the second and third points above (bullet points (2) and (3)) can be abandoned.

9.2.2.6. **Agency reply :**

(a) As replied here above to the German NSA concerns, the list of functions for which quantification is possible cannot be exhaustive in the legal text. It is not the purpose of the CSM RA to carry out such a functional identification, and subsequent allocation of quantitative requirements, for all functions of the railway system. Consequently restricting the use of CSM-DT only to a limited list of functions will make illegal the use of the CSM-DT for functions which are not on that list and that might be known by experts outside the working group.

(b) In addition to that, allocating a requirement to a function without knowing how the function is achieved/architectured in its operational context of the railway system might lead either to over specification or under specification of the safety requirements for the function. Consequently, implementing the proposed comment would create a risk because of the legal text.

(c) A legal text cannot thus specify safely a clear list of completely defined functions, outside their operational context, and the associated frequencies of failures. A guideline is also not a legally binding text. A list in the guideline can only be indicative.

(d) Finally, Article 18 of Regulation 402/2013 already requires the Agency to collect all information on the experience of the application of Regulation 402/2013 and to make recommendations to the Commission with a view to improving the Regulation or guidance documents.

Based on all those explanations, the comment cannot be taken into account.

9.2.3. Concerns of German and Swiss NSAs

9.2.3.1. Because of insufficient validation, and of the overlap between the two categories as perceived only by the German NSA, different interpretations of the CSM-DT wording are possible. This might make the mutual recognition of the results of quantitative risk assessments impossible.

9.2.3.2. The use of CSM-DT should be limited either to functions defined in TSIs (when relevant for the interoperability) or to a list of functions contained in a legal text separate from the CSM-RA or in some kind of technical document agreed by representative experts;

9.2.3.3. If the use of CSM-DT is not limited to such a list, there is a fear that the proposer does not allocate correctly the right CSM-DT for the functions that are not validated. In addition to jeopardising the mutual recognition of results from risk assessments, this could lead to an incorrect use of the CSM Regulation and thus to a decrease of the safety level in EU.

9.2.3.4. **Agency reply :** according to Regulation 402/2013 the proposer's risk assessment and appropriateness of the results (i.e. including the allocation of CSM-DT and the demonstration of their achievement) shall be checked by a competent CSM assessment body accredited or recognised according to the requirements and criteria contained in Annex II of Regulation 402/2013. This provides assurance that the errors of possible incorrect allocation of CSM-DT are detected by the safeguards put in place by the EU railway legislation

9.2.4. Agency replies to German and Swiss NSAs concerns

9.2.4.1. As explained in the sections above, the Agency has provided an argumentation to the German and Swiss NSAs of the reasons for not taking their comments into account.

9.2.4.2. As the changes suggested by those two NSAs diverge significantly from the agreement reached with the representative bodies (CER, EIM, UNIFE) and all the other national safety authorities which estimate, it is not possible to take them into account without breaking the consensus reached at a large majority among all other involved experts. Indeed, all other experts of the workshop estimate that the validation of CSM-DT is sufficient and that the proposed amendment corresponds to the quantitative requirements either presently specified by national legislation/rules or contained in the applicable EN standards. The German and Swiss NSAs did not accept the Agency justifications.

10. CONCLUSIONS

10.1. Amendment of Regulation 402/2013 with CSM-DT

10.1.1. The interests and benefits for defining harmonised risk acceptance criteria for technical systems, renamed into design targets (CSM-DT), has already been expressed by the railway stakeholders in 2007, during the development of the first CSM for risk assessment (Regulation 352/2009). Such criteria are useful for technical systems when carrying out quantitative risk assessment with the Explicit Risk Estimation (3rd risk acceptance principle). Harmonised criteria for the design of technical systems enables to assess in a harmonised way the acceptability of risks arising from failures of the technical systems.

10.1.2. Since 2007, the Agency has been working intensively with the NSAs and representative bodies on the development and validation of those harmonised design targets for technical systems. The validation of the proposed CSM-DT took place between 2012 and 2014. Compared to the current practice, the use of CSM-DT for the design of technical systems would neither decrease the safety performance in the EU railways nor increase the development costs of technical systems. The proposed "CSM-DT categories and values" correspond thoroughly to the present reality, experience and practice in EU railways. From the representative body point of view, and the majority of the involved NSAs, the CSM-DTs are usable for their purpose.

This point of view could not be shared entirely by the German and Swiss NSAs; their comments are given in section § 9.2.. Basically, they estimate that : the validation is insufficient, the two categories are overlapping and the use of the CSM-DT should be limited to a list of functions previously **validated by an explicit risk analysis** and based on a consensus on the appropriate CSM-DT among representative experts. Without this limitation, there is a fear of different interpretations of the CSM-DT wording and incorrect allocation of the CSM-DT categories. This might make the mutual recognition of the results of quantitative risk assessments impossible if the use of CSM-DT is not limited to a list. In addition to jeopardising the mutual recognition of results from risk assessments, this could lead to an incorrect use of the CSM Regulation and thus to a decrease of the safety level in EU.

10.1.3. The Agency provided the argumentation to the German and Swiss NSAs on the reasons for not taking their comments into account (see section § 9.2.). As on one side the changes they suggest diverge significantly from the agreement reached with the representative bodies (CER, EIM, UNIFE) and all the other national safety authorities, and on the other side introduce other risks and problems, it is not possible to take their comments into account without breaking the consensus reached at a large majority among all other involved experts. All other experts of the workshop estimate that the validation of CSM-DT is sufficient and that the proposed amendment corresponds to the quantitative requirements either presently specified by national legislation/rules or contained in the applicable CEN/CENELEC 5012x standards.

10.1.4. According to Regulation 402/2013, the proposer's risk assessment and appropriateness of the results (i.e. including the allocation of CSM-DT and demonstration of their achievement) shall be checked by a competent CSM assessment body accredited or recognised according to the requirements in Annex II of Regulation 402/2013. This provides the assurance that the errors of possible incorrect allocation of CSM-DT are detected by the safeguards put in place by the EU railway legislation. The German and Swiss NSAs did not accept the Agency explanations.

10.1.5. The Agency verified also the experience and practice in aviation. This cross-check demonstrates the equivalence or similarity for the aviation and railways of the use of quantitative requirements and of the quality and safety assurance processes recommended by relevant standards :

(a) in the same way as for railways, for big aircraft design and for the same types of accidents or consequence severities, the same categories of design targets are used;

(b) in aviation the "single fatality" is included in "relatively small number of persons" category;

(c) standards with similar requirements are used for the design of technical systems. This presumes that the technical systems in both fields are expected to achieve equivalent levels of safety performance;

(d) equivalent processes are used for the safety assessments, hardware & software development, verification & validation & management of systematic failures and systematic faults;

(e) similar requirements and standards are applicable in both fields for the demonstration of the achievement of quantitative requirements, including the use and modelling of safety barriers external to the technical system under assessment. This includes among others :

(1) use of qualitative and quantitative demonstrations;
(2) use of top down [Fault Tree Analyses – FTA – analysing the combination of failures] and bottom-up [e.g. Failure Mode Effect (and Criticality) Analysis – FME(C)A – analysing the effect of individual failures] approaches

10.1.6. Consequently, despite diverging opinions of a minority of experts, the Agency believes the amendment of Regulation 402/2013 on the CSM for risk assessment is a harmonised tool :

(a) to lower the amount of explicit risk estimations to be redone due to the use of different quantitative requirements for the design of technical systems. There should thus be less redesigns of technical systems, as well as less paper work for safety cases;

(b) to decrease the number of additional unnecessary administrative, risk assessments and safety demonstration work, as well as inappropriate cost, time and resources investments for the railway undertaking, infrastructure manager and national safety authority;

(c) to improve the mutual recognition of structural sub-systems and vehicles in compliance with Article 5 of Regulation 402/2013 and in particular to facilitate the authorisations for placing into service structural sub-systems and vehicles.

10.1.7. For the sustainability of EU railways, it is important to permit a safe railway competition with other modes of transport. So, it is crucial that the development costs of technical systems (including structural sub-systems and vehicles) are proportionate to the risk associated with their failures. Technical systems shall be safe enough, but shall not be safer and more expensive than actually needed. There is no acceptable justification for setting up more severe and more demanding design targets for railways than those currently used in the aviation. **The aviation includes the "single fatality" in the "relatively small number of persons" category**.

10.1.8. Similarly to the aviation, for the design of railway technical systems it is important to enable the distinction between :

(a) failures having the possibility to result in accidents with **catastrophic consequences** (e.g. collisions and derailments) not limited to an area of the train. Such accidents **affect a large number of persons**, either inside or outside the train, and **can result in multiple fatalities**.

*The frequency of occurrence of catastrophic accidents shall be **highly improbable [10^{-9} h^{-1}]**.*

(b) failures having the possibility to result in less severe consequences such as **critical accidents** (e.g. unintended opening of an individual door) limited to an area of the train. Such accidents **affect a relatively small number of persons**, either inside or outside the train,

and **can result in at least one fatality**. The upper limit is the "relatively small number" setup as objective for the considered type of accidents.

The frequency of occurrence of critical accidents shall be ***improbable [10^{-7} h^{-1}]****.*

10.1.9. The proposed categories are based on the existing experience and practice in railways. Despite the current railway statistics may show relatively small numbers of fatalities for most of the observed railway accidents (accidents with many fatalities are fortunately exceptional), the setting up of the CSM-DT is based on the "most reasonable or typical outcome of the failure". This means that the wording of the CSM-DT invites the proposer to consider "what could be the credible potential of the failure of the technical system?". If it could affect a large number of persons, category 1 must be used; if could affect a relatively small number of persons, category 2 must be used.

10.1.10. As explained in this report, it is not possible allocate safely a CSM-DT to a function outside its operational context and making abstraction of how the function is architectured in the railway system. Consequently, including in a legal text a mandatory list of functions might either result in the under-specification [*i.e. risk to decrease the safety performance of the EU railways*] or in the over-specification [*i.e. unjustified increase of the development costs of the technical system*] of the safety requirements of the functions included in the list. This would not only be dangerous but would also be counterproductive and heavy to maintain through the update of a legal text. It should therefore be quite acceptable to include in the application guideline on CSM-DT an indicative list of examples of functions of technical systems for which CSM-DT are usable.

Furthermore, if a function is not included in the list of the legal text, the use of CSM-DT would not be permitted. This would then prevent the innovation in railways and make later impossible the update of the list with new functions, as experience could not be gathered for new functions

10.1.11. Finally, unjustified too demanding CSM-DTs do not only increase the development costs by a factor 5 to 10 between the 10^{-9} and 10^{-7} categories but also require more complex technical systems, with redundant and fail-safe architectures, to be able to achieve very high safety performance. The disadvantage of too safe and complex railway technical systems is a poor availability performance. The consequences of an increased unavailability of too safe and complex railway technical systems are :

(a) higher maintenance costs during the life-cycle of such technical systems that directly hinder the competitiveness of the EU railway;

(b) the fail-safe state of railway technical systems obliges to continue the operation of the railway system with "operational procedures" where the safety relies entirely on the organisational and operational (i.e. human factors) arrangement in the RU/IM SMS, without the assistance of the unavailable technical system.

10.1.12. Unjustified high development costs (due to unduly high CSM-DT) eat up also the safety budgets of the proposer and generate the risk to divert the risk management efforts from the necessity to mitigate correctly also the Human Factors which are the main contributors to the systematic failures and systematic faults.

10.1.13. In order to help the EU railway sector with the application of the CSM-DT and to provide assurance to the NSAs that the CSM-DT will not be misused, an application guideline on CSM-DT will be written. This guide will be available at the stage when the recommendation will be put to vote by the Member States. It should support the legal text with additional explanations.

10.2. Co-ordination with CEN/CENELEC

10.2.1. The Agency is having regular coordination meetings with the chairman of the working group 21 of CEN/CENELEC in order to share the requirements contained in the CSM for risk assessment. The objective is to permit CENELEC to include in the on-going revision of the EN 50 12x standards tools and techniques that can be applied to address the requirements of the CSM on risk assessment, including the quantitative risk assessments through explicit risk estimation and the modelling of safety barriers to derive the acceptable safety requirements for the system under assessment.

10.2.2. The coordination between the Agency and CEN/CENELEC is an on-going activity. The Agency is taking care that CEN/CENELEC is not only in line with the CSM for risk assessment but that it also provides the necessary help for the full implementation of the CSM. For example, the Agency and CEN/CENELEC agree on the necessity to provide guidance on how to perform operational and organisational risk assessments. These seem to be the most difficult areas where the railway sector would need the greatest help.

10.2.3. Consequently, the coordination with CENELEC must be continued on a regular basis.

Annex 1: Definitions and abbreviations

Definitions

Table 4 : Table of definitions.

Definition	Description
Agency	The European Railway Agency (ERA)
Guide/Guideline	The application guide on CSM-DT

Abbreviations

Table 5 : Table of abbreviations.

Abbreviation	Meaning
APIS	Authorisation for Placing Into Service
CSM	Common Safety Method
CSM-DT	CSM Design Target
CSI	Common Safety Indicator
DT	Design Target
EC	European Commission
ECM	Entity in Charge of Maintenance
ERA	European Railway Agency
IM	Infrastructure Manager
NRB	Network of Representative Bodies
NSA	National Safety Authority
RAC-TS	Risk Acceptance Criteria for Technical Systems
RISC	Railway Safety and Interoperability Committee
RSD	Railway Safety Directive
RU	Railway Undertaking
SMS	Safety Management System

Annex 2: Reference legislation

Table 6 : Table of reference legislation

{Ref. N°}	Title/Description	Reference	Version
{Ref. 1.}	Mandate to the European Railway Agency for the revision of the common safety method on risk evaluation and assessment	C(2010) 6931 final	final
{Ref. 2.}	Directive 2004/49/EC on safety on the Community's railways (Railway Safety Directive)	OJ L220, 21.6.2004, p.16 (Corrigendum)	
{Ref. 3.}	Regulation 881/2004 establishing an European Railway Agency (Agency Regulation)	OJ L220, 21.6.2004, p.3	
{Ref. 4.}	Commission implementing Regulation (EU) N° 402/2013 on the common safety method on risk evaluation and assessment and repealing Regulation (EC) No 352/2009	402/2013	30 April 2013

Annex 3: Reference documents

Table 7 : Table of reference documents

{Ref. N°}	Title/Description	Reference	Version
{Ref. 5.}	Definition of RAC for technical systems		2.0
{Ref. 6.}	Final report of impact assessment http://www.era.europa.eu/Document-Register/Pages/Recommendation-on-the-revision-of-the-CSM-on-risk-evaluation-and-assessment-.aspx		1.3
{Ref. 7.}	Executive Summary concerning the "proposal for risk acceptance criteria to be included in the scope of the revision of regulation 352/2009"		2.0
{Ref. 8.}	Proposal for RAC definition: " definition of RAC for failures of functions of technical systems, which are covered entirely by a technical solution"		3.0 May 2011
{Ref. 9.}	General framework for the risk acceptance criteria within the CSM on risk assessment (Explanatory note on the development of RAC)		2.0, December 2010
{Ref. 10.}	Agency report on the experience with the existing regulation (EC) N° 352/2009 on a common safety method on risk evaluation and assessment and on the revision of that regulation http://www.era.europa.eu/Document-Register/Pages/Recommendation-on-the-revision-of-the-CSM-on-risk-evaluation-and-assessment-.aspx		1.0 13/07/2012
{Ref. 11.}	Information note about “ERA’s plan for the way forward for the development of explicit harmonised RAC-TS” (hereinafter called shortly: “the CSM-DT Way Forward Note”) http://www.era.europa.eu/Document-Register/Pages/RAC-note-1-2013.aspx	ERA/INF/02-2012/SAF	16.01.2013
{Ref. 12.}	Summary note on the inputs received during the validation of the regulatory and guideline proposal for explicit harmonised Risk Acceptance Criteria for failures of functions of Technical Systems (RAC-TS)	ERA-INF-100	1.0 27.03.2014
{Ref. 13.}	RAC-TS proposal resulting from the validation of the proposal laid down within the ”RAC-TS Way Forward Note” (ERA/INF/02-2012/SAF)		1.0 31.03.2014
{Ref. 14.}	Advisory Circular - Advisory Material Joint : System Design and Analysis	AC/AMJ No 25.1309	6/10/2002

Annex 4: More details on the development and validation of CSM-DT

A.4.1. History of development of risk acceptance criteria from 2007 to 2012

[A1] In 2007, during the development of the very first version of the CSM for risk assessment (CSM-RA - Regulation 352/2009), it became clear that harmonised Risk Acceptance Criteria (RAC) needed to be developed for explicit risk estimation (i.e. third branch of the CSM RA flowchart). Therefore, the Agency created in April 2007 a working group called "RAC taskforce". It was a subordinate expert group to the Agency Working Group responsible for the development and revisions of the CSM-RA.

[A2] The aim of the "RAC taskforce" was to work on explicit RAC and develop harmonised criteria for the acceptance of technical, operational and organisational risks, including the different types of possible consequences of risk severities. This RAC taskforce was active until May 2011. After a short period of cooperation with the CER/UIC SSMG Working Group and EIM, it was recognised that it would not be possible to cover all types of risks and their acceptance criteria at once. It was therefore decided in the CSM working group to exclude from the scope of the RAC development the harmonisation of the criteria for operational and organisational risks.

[A3] Until May 2011, the RAC taskforce focused its work on the development of a proposal for an extended set of RAC for failures of functions of technical systems (RAC-TS renamed later on into CSM-DT). The objective was to include them in the first revision of Regulation 352/2009 (i.e. into Regulation 402/2013). The proposal suggested the use of different quantitative design targets for hazards arising from failures of functions of technical systems, depending on the expected consequences from the hazard occurrence. The proposal was reviewed formally, agreed and accepted by the organisations represented in the CSM working group (various National Safety Authorities, CER, UNIFE, EIM, and UIP). With these results, the "RAC taskforce" was dismissed and the CSM working group took over the agreed results.

[A4] During the revision of Regulation 352/2009, the whole CSM working group estimated very important of having harmonised CSM-DT for the mutual recognition of structural sub-systems and vehicles. However, before including them in the CSM-RA, it was necessary to verify their usability on a representative set of functions of different railway technical systems, The CSM working group decided to involve the European railway companies and organisations in this validation work by a "RAC Impact Assessment" and a questionnaire.

[A5] The "RAC Impact Assessment" took place between June 2011 and March 2012. It was open for inputs from all railway companies, Representative Bodies (like CER, EIM, UNIFE, UIP, etc.) and National Safety Authorities (NSAs). Within their answers, the European railways confirmed that for various reasons, and in particular for the mutual recognition of structural sub-systems and vehicles; they need further harmonised RAC-TS for explicit risk estimations and for achieving mutual recognition of their risk assessments. Nevertheless, the Impact Assessment could not bring sufficient evidence to give confidence to the railway actors and the Agency that at this stage an agreed proposal for an extended set of harmonised RAC-TS can be made. Consequently, in spite of a series of extended deadlines and further intensive work, meetings and discussions taking place in the period December 2011-May 2012, a common position and proposal for RAC-TS could not be achieved between all involved organisations and national safety authorities.

[A6] For this reason, the CSM Working Group could not include in its final proposal of the revised CSM any common suggestion for an extended set of harmonised RAC or CSM-DT. For more details refer to the report on the revision of Regulation 352/2009 {Ref. 10.} under the following link

http://www.era.europa.eu/Document-Register/Pages/Recommendation-on-the-revision-of-the-CSM-on-risk-evaluation-and-assessment-.aspx

[A7] Consequently, in July 2012 the European Railway Agency sent to the European Commission its final recommendation for the revision of Regulation 352/2009. This recommendation did not include any amendments or changes with respect to the topic of the harmonised Risk Acceptance Criteria. It was decided to continue with this development work also after the submission of that Agency recommendation. The aim was to achieve sufficient validation and agreement by the European railway actors to allow the inclusion of the future results in a consequent amendment of Regulation 402/2013.

A.4.2. Validation of CSM-DT in the period June 2012 – September 2014

A.4.2.1. CSM-DT Way Forward Note – Call for validation

[A1] After the delivery of its recommendation for the revision of Regulation 352/2009, the Agency analysed systematically the work performed so far on the development of CSM-DT. The objective was, based on the work done in the period 2007-2012, to try to learn from the gained experience and to take practical measures for optimising the future work on the discussed subject. As a result of that, in January 2013 the Agency published an information note about the "*ERA's plan for the way forward for the development of explicit harmonised RAC-TS*" {Ref. 11.} (hereinafter called shortly: "*the CSM-DT Way Forward Note*"). Amongst others, this note:

(a) gives an analysis of the work that took place from 2007 to 2012, identifies challenging issues and suggests solutions for them;
(b) makes a proposal for regulatory text for CSM-DT;
(c) gives a proposal for topics to be included in the supporting guidelines;
(d) asks the manufacturers, RUs, IMs, NSAs, etc. to start with their validation of the given proposal and to communicate the results of that validation to the Agency;
(e) explains synergies with the LOC&PAS TSI and the work on the ERTMS DMI.

[A2] After the publication of the "*CSM-DT way forward note*" {Ref. 11.}, its content has been presented and discussed repeatedly in detail at the meetings of the Network of National Safety Authorities and the Network of Representative Bodies.

[A3] During these meetings the concerned actors set themselves the deadline of 15th November 2013 for closing the validation of the regulatory and guideline proposals contained in the note.

A.4.2.2. Rules for sufficiency of the validation

[A1] The Network of NSAs, as well as the Network of Representative Bodies also discussed and defined the rules for the sufficiency of the validation of the proposal. With regards to this, the summary of the received inputs indicated that the validation of the proposal will be sufficient, if :

(a) the validation is logical, consistent, does not have obvious controversies and makes sense.

This refers especially to the fact that in the work before June 2012, during the last decisive phases, the validation presented by some of Representative Bodies included some obvious controversies. It was thus agreed that this type of obvious controversies should be avoided;

(b) the validation is based on examples of what is acceptable at present.

The railway sector need to make their own analysis, based on examples from their real practice;

(c) the validation is validated by manufacturers, RUs and IMs and not only by NSAs;

(d) the validation contains CSM-DTs that do neither reduce the present level of safety, and are thus the "state of art", nor increase the costs of development of corresponding technical systems.

The validation needs to be based on real practice examples from the concerned actors, rather than on general fears, feelings, thoughts and statements.

A.4.2.3. How do NSAs treat the CSM-DT within the authorisation for placing into service (APIS)?

[A1] During the meetings of the Network of NSAs, special attention and very much effort have been laid upon the investigation of the current practice of the NSAs regarding the way they treat the CSM-DT in the scope of the authorisations for placing into service (APIS) they deliver. Three general models of behaviour were identified.

[A2] The collection of information and the discussions on these models allowed the Agency to understand better the current practice of NSAs. It also allowed to gain an overview of the results that could be expected the NSAs to deliver as part of the validation of the CSM-DT proposal. The identified models of behaviour of the NSAs, as well as the respective expectations about the validation are described in the following paragraphs:

[A3] **NSA CSM-DT MODEL 1**:

(a) when the NSA grants an APIS:

(1) the NSA grants the APIS based on:

(i) the report of the notified body (NOBO);
(ii) the report of the independent safety assessor (ISA) (for the cases where the CENELEC EN50129 standard is used) or the CSM assessment body (CSM-AB) (for the cases where the CSM-RA is used);
(iii) the report of the designated body (DeBo) (for the cases where it is involved).

(2) the NSA does not redo/recheck the work of the ISA/CSM-AB;
(3) the NSA neither sees, nor questions, neither the CSM-DT nor any other type of RAC.

NOTE: Such NSAs are normally not able to deliver inputs for the validation of the CSM-DT proposal, based only on their own practice for the CSM-DT acceptance.

(b) **As a result** of the collection of information within the framework of the NSA Network meetings, it became clear that the majority of NSAs [namely 17 NSAs] are presently applying Model 1. Even though, normally these NSAs are not able to deliver themselves inputs for the validation of the CSM-DT proposal, 1 to 3 such NSAs announced their will to possibly validate the CSM-DT proposal by the means of working together with the railway sector within their Member State. The following is the precise view of the results of the inquiry:

(1) 13 NSAs apply Model 1 and could not deliver validation inputs:

(i) IT, HU, LT, AT, PT, RO, GR, BG, NL, SK, LV, SL;
(ii) PL did not submit a final confirmation whether they are using this model and whether it could submit validation.

(2) 1 NSA [NSA CZ] – applies Model 1 but in exceptional cases like disagreements with the applicant, or similar, Model 2 below is applied. NSA CZ announced not being able to validate the CSM-DT proposal.

(3) 3 NSAs apply Model 1 and, in coordination with the railway sector of their country, delivered validation inputs: ES, UK (via the RSSB), BE (via EIM).

Remark: NSA HR stated not applying any model yet.

[A4] **NSA CSM-DT MODEL 2**:

(a) when the NSA grants an APIS:

(1) the NSA accepts the reports of the CSM-AB, the ISA, the NoBo and the DeBo.
(2) the NSA can also check additionally the contents of the risk assessment and the way how the CSM-DT and the other types of RAC have been set.
(3) the NSA sometimes disagrees with the CSM-DT or any other type of RAC and sets new targets.

NOTE: Such NSAs are able to deliver inputs for the validation of the CSM-DT proposal. They need to deliver inputs in order to ensure compliance with their present system.

(c) The collection of information during the NSA Network meetings showed that 7 NSAs are presently applying Model 2 (with slight variations in its performance). Even though, normally these NSAs are able to deliver inputs for the validation of the CSM-DT proposal, only 1 to 4 NSAs announced that they will possibly submit validation of the proposal. Here is the detailed overview of the responses received:

(1) NSA LU applies Model 2.

It sometimes questions the content of the CSM-AB report and the choice of the CSM-DT. For example, if the applicant would have chosen 10^{-7} h^{-1}, the NSA would sometimes ask the applicant why 10^{-9} h^{-1} was not chosen. NSA LU did not deliver validation inputs of the proposed CSM-DT.

(2) NSA IE applies a modified version of Model 2

Normally the NSA follows the work on the project (including the work of the different assessment bodies) from an early project stage. But the NSA IE does not intervene with regards to CSM-DT; it did not deliver validation inputs.

(3) NSA FI applies Model 2; it tried to deliver externally collected inputs.
(4) NSA EE applies Model 2; it tried to deliver validation inputs.
(5) NSA NO applies a modified version of Model 2, which can sometimes be seen as Model 3.

Sometimes the NSA disagrees with the CSM-DT or any other type of RAC and sets, or requires the definition and argumentation of new targets. The NSA NO does not define the CSM-DT but requires the applicant to give the arguments and to demonstrate how the National Safety Level set up in the Norwegian national legislation is maintained. The NSA NO did not deliver validation inputs.

(6) NSA FR applies Model 2

After discussion on the whether NSA FR applies Model 2 or Model 3, NSA FR stated to be applying Model 2. It delivered validation inputs;

(7) NSA Channel Tunnel apples the same Model as FR. It did not deliver validation inputs.

[A5] **NSA CSM-DT MODEL 3**:

(a) When the NSA grants an APIS, either at the beginning, or at the end of the project:

(1) the NSA derives RAC or CSM-DT from National Reference Values (or similar statistics):
(2) this RAC or CSM-DT shows "how much safety the MS can afford 'loosing with' or 'granting to' the respective project";
(3) the NSA requires the applicant to demonstrate compliance with these RAC or CSM-DT.

NOTE: Such NSAs are able to deliver inputs for the validation of the CSM-DT proposal. They need to deliver them, in order to ensure compliance with their present system.

(d) The work during the NSA Network meetings showed that 3 NSAs are applying Model 3, with some variations in its form. Even though, normally these NSAs would be able to deliver inputs validating the CSM-DT proposal, only 1 to 2 NSAs announced they will possibly submit validation of the proposal. These are more detailed results:

(1) NSA DE applies Model 3

During the discussions of the NSA Network meetings, NSA DE was not able to confirm whether it will validate the suggested regulatory and guideline texts.

(2) NSA SE applies Model 3 and sometimes Model 2 if the NSA SE was not able to define RAC for certain types of functional failures. NSA SE delivered validation inputs for the suggested regulatory and guideline texts.

(3) NSA DK works as follows:

(i) the NSA supervises strictly the competences and the work of the CSM-AB. This can be sometimes seen as Model 2;
(ii) the NSA applies Model 1 for the APIS for changes to the existing infrastructure or to existing trains;
(iii) the NSA applies a modified version of Model 3 when the projects are very complex or consist of building new lines or new types of trains:

In such cases, NSA DK defines a RAC (but not CSM-DT) at the beginning/end of the projects. This RAC refers to the performance of the integrated technical system within its operational context. It is a requirement towards its operator and not directly towards the manufacturer, which works with CSM-DT.

(iv) in the APIS, NSA DK does not see directly the CSM-DT and thus did not deliver validation inputs.

[A6] Further to the above, a bilateral meeting with NSA IT took place. During this meeting it became clear that NSA IT applies Model 1 and cannot deliver validation inputs. This became clear, after the Agency explained and discussed with NSA IT the difference between the CSM-DT and other types of RAC.

[A7] In summary, the underlying table shows the results of the work that investigated the behaviour of the NSAs with regards to the CSM-DT in the scope of the APIS. It shows also a summary of the replies received in the period January - September 2013 to the question whether the respective NSAs would validate the CSM-DT proposal.

Table 8 : Summary NSA behaviour with respect to CSM-DT or other quantitative requirements.

	Model 1	**Model 2**	**Model 3**
How many NSAs apply it?	~ 18 (incl. HR)	~ 7	~ 3
How many NSAs agreed to deliver validation inputs?	1 to 3	1 to 4	1 to 2
Candidates for validation of CSM-DT	ES, UK, BE	FI, NO, FR, EE	SE, DE

A.4.2.4. Workshops on the validation of CSM-DT

A.4.2.4.1. 1st Workshop on validation of CSM-DT : 25th & 26th June 2013

[A1] The Agency launched the validation of CSM-DT in January 2013. As soon as the involved stakeholders set themselves the deadline for closing the validation work (15th November 2013), the Agency decided to organise a mid-term validation workshop in June 2013. The purpose of this workshop was to follow better the progress of the validation work on CSM-DT and to enable pro-active discussions between the stakeholders before the end of the activity.

[A2] The two day workshop (1st workshop on the CSM-DT validation) took place on 25th and 26th June 2013. It included also a general part regarding the experience with the application of the CSM-RA. The workshop was open to anyone who wished to participate. The workshop achieved a participation of more than 50 participants. It included 15 presentations(3), out of which 11 were coming from sector organisations. During this event, various fruitful discussions took place. Additionally, the rules for the sufficiency of the validation were discussed once again. No further complements to them were made.

[A3] During the period January 2013 – April 2014, the stakeholders worked on the validation of the proposed CSM-DT. During that period, the Agency was regularly required to support the sector. Discussions were ensured via e-mails, on the phone, via dedicated meetings, via the provision of dedicated answers to questionnaires on the subject, etc. A list of the meetings held, including a short description of the content, can be seen in chapter 3..

[A4] Although the railway actors had set themselves a deadline for the validation until 15th November 2013, the validation efforts appeared to be challenging and resource-demanding once again. Thus, the intensive work led to further delays in the project. The inputs on the validation of CSM-DT were received until April 2014 included.

[A5] **Results from the validation of CSM-DT:**

(a) Finally, as a result of the validation, dedicated (confidential and data protected) letters or contributions were received on the validation of the proposal for regulatory and guideline texts for CSM-DT outlined in the "*CSM-DT way forward note*" {Ref. 11.}. Inputs were received from 10 actors in total. Out of them there are in total :

(1) 6 NSAs (the inputs of one of the NSAs constituted rather a list of questions);
(2) Representative Bodies (CER, EIM, UNIFE);
(3) 2 independent companies from the railway sector.

(b) NSA IT did not submit validation inputs but made a short-notice presentation of their changed views during the 2nd CSM-DT validation workshop, which took place in April 2014.

(c) Similarly, information in German language has been received by the Agency regarding the work, done in the scope of the German NeGSt project. The contents and relevance of this work have been discussed with representatives of the project team during a dedicated meeting in May 2014.

(d) Within the officially received contribution letters, a few organisations indicate that the inputs they provide are collective inputs and/or representative for a whole sector or a few companies. These are 5 organisations. Out of them there are in total :

(3) http://www.era.europa.eu/Document-Register/Pages/1st-rac-ts-workshop-ppt-dld.aspx

(1) 3 NSAs;
(2) 2 Representative Bodies.

[A6] As a result of the validation of CSM-DT, end of March 2014, the Agency issued the following two papers:

(a) "*Summary note on the inputs received during the validation of the regulatory and guideline proposal for explicit harmonised Risk Acceptance Criteria for failures of functions of Technical Systems (RAC-TS)*" {Ref. 12.} ;
(b) "*RAC-TS proposal resulting from the validation of the proposal laid down within the "RAC-TS Way Forward Note""* (ERA/INF/02-2012/SAF) {Ref. 13.};

[A7] The first of those documents presents an anonymised summary analysis of the validation inputs received by the moment when the report was issued. Shortly after, also the presentation from NSA IT and the information from the NeGSt project were received. The second document lays down the resulting proposal for legal text of CSM-DT to be included in the amendment of the CSM-RA.

A.4.2.4.2. 2nd Workshop on validation of CSM-DT : 1st & 2nd April 2014

[A1] The second workshop on the validation of CSM-DT took place in Lille, in April 2014. It was open to all stakeholders who actively took part to the validation exercise: NSAs, Representative Bodies (CER-EIM-UNIFE), railway undertakings, infrastructure managers, manufacturers, private wagon keepers, as well as all members of the Agency working group on the CSM for risk assessment.

[A2] The objective of the second workshop was to present by the different stakeholders their results of validation of the legislative and guideline texts proposed within the "*CSM-DT way forward note*" {Ref. 11.}. The presentations were followed by an open discussion between the Agency, the stakeholders involved in the validation exercise and the workshop members. The Agency presented the summary and analysis of the inputs received during the validation {Ref. 12.}. It also presented the resulting draft regulatory text of the recommendation {Ref. 13.}. Based on all those inputs, an open discussion took place. It gave the basis for another update of the text proposals. However, it became clear that the wording of the legal text was not yet satisfying enough to be sent for Public Consultation; there was not yet a wide consensus and support within the railway actors and NSAs involved in the CSM-DT validation work.

[A3] As a result of the second workshop, it was decided to make one more workshop on the validation of CSM-DT, as soon as possible. The work to be done until this 3rd validation workshop was split in two parts:

(a) the Agency had to revise and provide an updated version of the legal text in order to reflect the latest received inputs, as well as the discussions and agreements at the 2nd validation workshop;
(b) the Representative Bodies (CER, EIM and UNIFE) took as homework to come back to the next workshop with common views on a list of questions raised at the workshop.

A.4.2.4.3. 3rd Workshop on validation of CSM-DT : 16th July 2014

[A1] The 3rd CSM-DT validation workshop took place on 16th July 2014 in Lille. The discussions were based on the updated legal text. The Representative Bodies presented their common answers to the list of questions defined and agreed at the second workshop.

[A2] Due to difficulties to find the correct wording of the CSM-DT criteria to cover both train-side and infrastructure-side technical systems, it became clear that the Representative Bodies and national safety authorities could not yet agree on a common view on the final definition of the CSM-DT categories. Before sending the amendment of Regulation 402/2013 for public consultation there was a common will within the Representative Bodies to take the legal text and check it once again in order to ensure that it corresponds thoroughly to their present experience and practices.

A.4.2.4.4. 4th Workshop on validation of CSM-DT : 17th September 2014

[A1] It was thus decided to organise a 4th CSM-DT validation workshop. This was the last workshop. It took place in September 2014 in Lille. As usual, also for this workshop the Agency provided an updated draft of the legal text. The Representative Bodies (CER, EIM and UNIFE) checked the workshop whether the latest version of the legal text fits to their current practice and whether the wording is appropriate or may need to be improved in any particular way.

[A2] During the workshop it became clear that all sector organisations were really convinced that the legal text proposal fits for its purpose and reflects the current practice and experience in the railways. This point of view was shared also by UIP and the majority of the participants, although not by the German and Swiss NSAs. With the exception of two points, the legal text was thus widely agreed.

[A3] Due to time limitations and partially to extreme points of view on the side of some actors, it was not possible to achieve a consensus on the following two questions:

(a) Should a list of functions with the associated CSM-DT category be included in a legal text, either in a new annex of the CSM-RA or in an external Technical Document?

The German, Swiss and Croatian NSAs supported this option. After a given period of time, the list might be updated in cooperation with the Representative Bodies and NSAs based on the experience gained by the railway sector with the use of CSM-DT. They requested to specify that process explicitly in the CSM and the European Railway Agency to apply that process for future updates of the CSM and of the list of functions.

Based on technical argumentation, all other members of the workshop agree on including an indicative list of functions and of the associated CSM-DT category a guideline on CSM-DT. They volunteered also to help the Agency for producing the guideline and also for updating later on based on the experience gained with the use of CSM-DT.

(b) How should the exact formulation of legal text be to exclude purely mechanical and purely pneumatic technical systems from the scope of application of the CSM DT?

[A4] For these two points, a “tour de table” was made in order to collect and log all opinions and to enable further work on the legal text before sending it for public consultation in the period November-December 2014. The opinions have been logged in the minutes of the workshop.