CER

The Voice of European Railways

POSITION PAPER

RAC Way forward

14 March 2014

COMMUNITY OF EUROPEAN RAILWAY AND INFRASTRUCTURE COMPANIES - COMMUNAUTÉ EUROPÉENNE DU RAIL ET DES COMPAGNIES D'INFRASTRUCTURE - GEMEINSCHAFT DER EUROPÄISCHEN BAHNEN UND INFRASTRUKTURGESELLSCHAFTEN

CER aisbl Avenue des Arts, 53 B-1000 Bruxelles Tel: +32 2 213 08 70 Fax: +32 2 512 52 31 contact@cer.be www.cer.be

1. Executive summary

This Position Paper makes public the official CER position on and for the way forward for the development of explicit harmonised RAC. It recommends changes and amendments to be done, ensuring the deployment of a safe, sustainable, cost-efficient and reliable railway system with all its subsystems included.

The application conditions of ERA proposal are not yet precise enough to achieve a common understanding for an appropriate use as intended by the CSM-RA (see sections 3 and 4). Therefore mutual recognition is currently not sufficiently supported by the application of the concept as domestic interpretations vary. In the main body of this paper (sections 5 to 8, Annex 1) an attempt to answer the questions posed in the ERAs plan of work and some suggestions for improving and clarifying ERA proposals has been made, with the objective of minimising the potential for misapplication or misuse of the proposed concept. Therefore, CER position covers the following items:

- Amendment of ERA proposed text for the regulation (sections 5 to 7, Annex 1) presenting new or improved definitions (*directly, barrier, potential, typically, technical system, operating hours*) and clarifying the scope and application cases of the proposed concept. In particular, to avoid any misinterpretation, CER believe that the term '*RAC-TS*' should be renamed into '*CSM Design Target*' (see section 6).
- Inputs for the application guide (examples, CER common understanding on application cases and method to be applied : see section 8)

However it has not yet been possible to provide a comprehensive CER endorsed validation of the ERA's proposed severity classes and related values for CSM design target. This is because many fundamental questions concerning the use of the proposal remain. In order to provide constructive feedback, and start discussions about a longer term piece of work to develop a coherent approach, a number of further actions for CER and the Agency are proposed (see section 9):

- The workshop organised in April 2014 should allow to agree on the main principles (concept and definitions to be included in the regulatory text, topics to be developed in the application guide, concept for handling barriers).
- Once the principles are defined, CER will give their position on severity classes and related target.
- A meeting might be necessary to finalise a recommendation.
- Working party need to be organised to write the guidance.

Currently CER cannot support ERA's proposal for the following reason. Only in a very few cases a failure of a function of a technical system leads immediately to accidents. Therefore it is essential that the handling of barriers is included in the proposal (see Annex 2). Furthermore, other uncertainties of the proposal lead to the conclusion that additional clarification is necessary in order to make CER able to provide a validated position on the proposed classes.

2. Reference document

Information note about ERA's plan for the way forward for the *development of explicit harmonised risk acceptance criteria for failures of functions of technical systems*
Reference: ERA/INF/02-2012/SAF document version 0.1, dated 16/01/2013

3. CER-EIM understanding of the "RAC-TS / CSM design targets'" intended purpose

CER believe that the term RAC-TS should be renamed into CSM Design Target. The term 'Risk Acceptance Criteria for Technical Systems' provides many indirect questions which are not core about the subject at hand:

- Is it a 'risk' (combination of severity & frequency) that we must evaluate? Or simply the frequency? This could lead people to evaluate frequency through an expert judgment instead of a safety study. Risk is dealt in the 'broadly acceptable' phase, and then only frequency is to be considered.
- The term 'criteria' is a generic one, but the values proposed are only numeric. This could lead to translation of these values in qualitative criteria, thus losing the homogeneity of treatment of the Explicit Risk Estimation principle
- 'acceptance for technical system' remains very unclear, and does not describe the true goal, that is, to have a proper design. This could lead people to concentrate on an appropriate acceptance criteria, instead on focusing on the design. The consideration of systematic causes could be neglected as the risk acceptance is understood as a comprehensive requirement.

The CSM design target defines the safety requirements for the design process of technical systems in specification phase. The criteria are safety design targets for purely technical functions of these systems where a prospective demonstration of a functional failure rate follows processes according to established and harmonized standards like EN 50128, EN 50129 or IEC 61508.

The quantitative design targets define the design safety requirements to control random causes of failures of purely technical functions.

The design targets are linked with severity classes, describing typical outcomes of accidents in terms of fatality and/or injury, which could arise out of at least a single failure of a purely technical function.

The quantitative design target and the linked severity class represent an acceptable level for the design safety under the precondition that additional safety measures of

established and harmonized standards can be demonstrated (e.g. qualitative measures to control systematic causes of failures, adequate maintenance and operation, …).

The link to these safety measures is provided (e.g. in EN 50128, EN 50129, IEC 61508) to control systematic causes of failures of purely technical functions (mostly electronic and software).

The CSM design target shall support mutual recognition between the Member States. In all cases where the application conditions of the CSM design target are fulfilled, mutual recognition is given for the hazards controlled by applying the CSM design target.

The CSM design target does not necessarily consider all specific safety requirements of a railway system in the European Union. The specific needs of RUs/IMs to ensure a safe integration and to maintain the safety level of a Member State are outside of the objective of the current ERA's proposal for CSM design targets, as it deals only with technical systems.

For the technical system considered in the CSM RA and the severity chosen, the CSM design targets focus on the harmonization of the safety performance of technical products, which will allow using them all over Europe, where the necessary requirements are fulfilled to extend its area of use.

The third risk acceptance principle encompasses human and operational elements which are currently not covered by the CSM design target as it is proposed by ERA.

The CSM design targets do not represent a level of safety at railway system level/ Member State level but a level of design safety.

4. CER approach to the development of explicit design target

In general, the needs of RUs/IMs are not sufficiently covered by the current proposed concept, as the railway system usually includes safety barriers linked with technical systems. Nevertheless, the CSM design target could become a useful tool in the context of the Regulation (EC) 402/2013 (CSM-RA) for facilitating risk analysis if:

- the scope of the concept is unambiguous and
- the targets are set at a level that support maintaining or improving the level of safety in the European Union and
- it is not too costly for the sector to avoid disadvantages in intermodal competition.

The concept behind the CSM design target is therefore important to be clear for railway safety and competitiveness of the sector. This requires high precision for the definition of the scope, the criteria and the methodology for the application of the CSM design target, in order to ensure that a practical solution for the European Railways will be created.

In the view of CER, the current ERA proposal has a number of shortcomings and should be further developed with respect to the following items:

- A methodology how to demonstrate that a design target is met would support the application of the CSM design target. Therefore, the competence of the manufacturer to apply the CSM design target concept has also to be further investigated (i.e. open issue to be solved in the application guide). The concept of design safety must be compatible with the Safety Integrity concept of EN 50126-50128-50129 in order to ensure consistency between the new concept and well-established approaches in the sector for demonstration of safety.
- Further recommendations on how to develop application guidance which supports a harmonized application of the CSM design target is presented in the following sections. The regulatory text and the proposed text comprise several assumptions and unspecific terms (directly, barriers, technical system, operating hours) which will certainly lead to discussions, (mis-)interpretations and/or wrong applications of the concept.

A multiple step approach is required for a successful development and implementation of the CSM design target. After all relevant parties involved in the development of the CSM design target have the same understanding on what the CSM design target covers, the different classes of typical outcomes could be agreed together with an explicit target.

a) **Agree on application conditions of the existing approach**: therefore we propose clearer definitions of the concepts included in ERA proposal.
b) **Assess the benefit of ERA proposal**: The way to handle barriers from that concept is a major open issue, not only to allow a system safety approach, but also to cover the safe integration aspects as well. We fear that the application cases matching ERA CSM design target definition is too reduced to be used as the basis for a validated support of the proposal. We provide proposals to fill that gap in a simple way, as we believe the barrier concept can be easily achieved (see Annex 2).
c) **Finalize the severity classes**, specify the design targets and verify the new classes

5. Definitions to be included in the regulation

Before presenting severity classes, the terminology should be defined:

- The definition of "Barriers" and "Directly" shall be clearer
- The term "technical system" (as well as functional failure) shall be defined in the regulation more precisely
- "operating hours" shall be defined.

CER propose to introduce the definition (see proposal in annex 1).

These definitions should be accompanied by examples and further explanation in the Application Guide (see Section 8 of this paper).

The 'technical systems' to which functions relate shall be defined and clarified according to good practice safety engineering principles.

6. Scope of CSM design targets

The scope and application cases of the CSM *design target* could be clearer in particular to avoid unnecessary costs. In general, ERA recommendation shall allow a common understanding of all stakeholders, including NSAs. Operators shall be free to use one of the three risk acceptance principles as according to Section 2.1.4 in Annex I of CSM Regulation 352/2009 those principles are equivalent.

CER propose to determine the scope and application cases of CSM design target (see annex 1).

7. Severity classes / values of CSM design targets

The severity classes shall be defined to ensure that no interpretation is possible and no overlap between the classes exists. Severity classes shall be defined as a typology of failures (not only a single event).

The design target has to be applied at that level of a technical system, where at least one failure or a combination of failures has a credible potential to lead directly to an accident.

CER propose to define the targets (see Annex 1).

ERA has explicitly chosen (there were other possible choices) to express the CSM Design target requirement as a maximum of "failures per operating hour". This approach fits many systems, but not all. Thus, the "failures per operating hour" unit will have often to be translated in other units relevant to the systems under consideration, for example:

- probability per unit of time (may be other than per operating hour): occurrence probability of an unwanted event during a given duration (the profile of which has to be defined, e.g. powered time, time under stress …),
- probability per unit of anything else describing the relevant conditions of use, according to the failure mechanism: distance, load, number of cycles,
- probability of failure on demand (or "per solicitation"),
- probability without dimension: e.g. percentage of time a function is available,
- rate: conditional probability to experience an unwanted event during a time interval [t;t+dt] knowing it has not happened before "t". e.g. Failure Rate = -1/R*(dR/dt), R being the probability (no dimension) of no failure occurring during a [0;t] time interval,
- qualitative, e.g. SIL (safety integrity level) for programmed systems,
- etc…

The "translation" has to be done particularly when designing the system's architecture and when apportioning the CSM design target requirement to its components. If the underlying safety demonstration is to be mutually recognised, a harmonised approach is required. Therefore, for systems for which quantitative requirements are not relevant, the legal text has to give the possibility to translate the quantitative targets into qualitative requirements (e.g. SIL, number of independent failures, intrinsic safety …). Today SIL are described in EN 50128, EN 50129, standards and future EN 50126 standards covering random and systematic aspects of design.

A major fear for CER would be that a NSA does not accept dealing with systematic failures through a SIL development for software or dealing with mechanical parts through a recognised code of practice arguing that, since the CSM design target is expressed as a failure rate, a failure rate has to be calculated anyway for the systematic failures as well.

8. Application guide

CER generally agree with ERA's list of items proposed to be developed in the application guide, but stress that the scope and the means to demonstrate the achievements of design target are major open issues to be solved. This could be solved through a working party, which should cover:

- The method to be applied (link with existing standards / concepts like SIL, ALARP, system safety approaches defined in the CSM regulations)
- The link with the overall safety architecture and the way to define quantitative target depending on additional safety measures in place (e.g. when the failure does not directly lead to injuries).

a) Using CSM design targets

The guide should make clear that a railway actor may apply on a voluntary basis CSM design target on a technical system on which external barriers apply. This could allow the automatic mutual recognition of the technical system but might lead to increased costs.

- This should not allow a NSA to refuse a barrier accepted by an assessment body (if a NSA does not accept such a barrier, it has to demonstrate that the barrier is not appropriate).
- This possible voluntary application of CSM design targets should not lead to a general use of CSM design targets out of their scope (and leading to have fully interoperable system but not affordable)
- However, if a barrier approach is taken (the CSM design target is not entirely allocated to the system under consideration), mutual recognition is no longer automatic (unless a method presented in the guide is applied).

The CSM design targets are not supposed to be used on a mandatory basis, since:

- According to Section 2.1.4 in Annex I of CSM Regulation 352/2009 the three risk acceptance principles are equivalent. There is no requirement to prefer one principle. The proposer can choose the principle which is the most beneficial for the system under assessment to demonstrate the control of hazards.
- The CSM design targets are only the most demanding values that can be asked for, unless NSA proves – and notifies – that more stringent targets are necessary to keep current national

safety level. Mutual recognition is still reachable without conformity to these values, it is only no longer 'automatic': an NSA has to accept the reached value if an assessment body recognised them as appropriate, while conformity to *CSM design target* provides automatic acceptance of the target.
Note: 'automatic' does not mean that it is forbidden for the NSA to check the safety demonstration, only that the target is accepted by the NSA.

In the guide it should be clear that *CSM design target* should not be applied to purely mechanical / hydraulic system before a harmonised standard exist and it is demonstrated that CSM design target can apply to such a system. A technical system where the CSM design target applies is: a collection of components, products and/or subsystem required to deliver the function for the railway *for which the* prospective demonstration of a functional failure rate follows processes according to established and harmonized standards.

b) Examples for CSM design target concepts

The guide shall include examples illustrating the key concepts defined in the regulation. In general, the guide should make clear which domains do CSM design target apply in the context of IMs, RUs, ECMs, manufacturers, NSAs; which application cases are representative. We propose the following examples related to directly / no barriers:

- *The door opens in a non-authorized situation (at speed, on the track side, …). This can result in the fall of a passenger. The fact that a passenger has to be in front of the door is not a failure (it is a normal situation, nothing forbids passengers to be in front of the door outside of stations). In this case directly applies*
- *Absence of braking can lead to a collision with another train (or derailment). The fact that another train is present at a specific location is not a failure, as nothing prevents two trains to be in a close distance (except the braking system which has failed)*

The word 'Typically' need to be illustrated. As an example, the sentence "failure that has a credible potential to lead directly to an accident where typically an individual person is affected" means that:

- the failure will lead to a situation where no additional failure is necessary (no barriers exist) to lead to the accident
- this accident (e.g. collision, fall of passenger, …) when present, will in most case concern an individual person. This means that in most cases only an individual person will be injured or die (which can be in total more than one).

A way of differentiating accidents where typically an individual person is concerned from those where typically a group of people is concerned can be the following:

- If the failure exposes passengers of the train wherever they are placed in the train, then the 'typically a group of people' will be chosen.
- If the failure exposes passengers of the train only if they are placed in a particular place of the train, then the 'typically an individual person' will be chosen.

9. Conclusion / next steps

CER call the Agency to ensure that the recommendation on CSM design target will not lead to any misinterpretation. Therefore, a multiple step approach has to be considered to finalise the recommendation and further develop and harmonise method for risk acceptance.

The workshop organised by ERA beginning of April should allow achieving a common understanding on the framework. The main principles to be developed in the regulation and the guide should be agreed:

- Rename 'RAC-TS' as 'CSM Design Target' (see section 6)
- Provide clear definitions (see justifications in section 5 and proposals in Annex 1) of the terms Directly, Barrier, Potential, Typically, Technical system, Operating hours
- Define a non-ambiguous scope (see justification in sections 5, 6, 7 and proposals in Annex 1)
- Application guide should be developed to provide relevant example of CSM design target and avoid any misinterpretation or wrong application (see section 8).
- Define how the concept could allow to handle Barriers

The workshop should also be the place to agree on the next steps (schedule, meeting to be organised).

If these elements are agreed, based on examples, CER will be entitled to give their final position on severity classes and related target.

The final text of the recommendation should be prepared in a dedicated meeting (task force) according to the workshop outcomes.

A Working party will be necessary, in particular to develop the guidance document:

- Examples to support the application of the concept
- method to be applied (link with existing standards / concepts like SIL, ALARP, system safety approaches defined in the CSM regulations)
- The link with the overall safety architecture and the way to define quantitative target depending on additional safety measures in place (e.g. when the failure does not directly lead to injuries).
- and continue the work to define the conditions for ensuring automatic mutual recognition in the presence of barriers (see Annex 2).

Only if all aspects are solved the concept will become a successful implementation. The handling of parts is not sufficient.

ANNEX 1 ELEMENT TO BE PRESENT IN THE REGULATION

Following text is proposed to replace ERA's proposal for adding an article 2.5 in the CSM-RA regulation (main changes regarding ERA's proposal are marked in red).

2.5.4.1 Definitions

Design targets apply to failures of functions of technical systems that have a credible potential to lead directly to an accident.

The term "directly" means that the failure of the function has the potential to lead to the unwanted consequences without the need for additional failures to occur (i.e. failure external to the system under consideration).

The term 'potential' means that there is no implication that the failure of the function will inevitably lead to the unwanted consequence; there may be circumstances external to the function (e.g. presence of a train), but as these are not failures, the "directly" still applies. No 'barrier' exists between the failed function and the unwanted consequence.

The term "credible" means that in the majority of the cases "the potential accident" will lead to the chosen severity class consequences. This does not mean, that an experienced accident resulting in e.g. 4 fatalities, which was defined as an accident usually leading to one fatality leads to reclassify in a higher severity class.

A 'barrier' is a means that is intentionally implemented (thus to be controlled and monitored) and results in the reduction of the frequency and/or the mitigation of the severity of potential accident(s) arising from the functional failure. Barriers may be of different natures. Other factors that may be circumstantial (i.e. not intentional), e.g. the presence or otherwise of another train, the presence or otherwise of a passenger to be exposed to the failure, are not considered to be barriers.

'Technical system' is a collection of components, products and/or subsystem required to deliver the function for the railway. The CSM design target applies for a technical system, which is usually based on electronic and/or software implementations.

'Operating hours' are defined depending on the context in which the system under consideration is functioning. Where the system is part of a train, the appropriate metric is train operating hours. Where the system is not part of a train, the appropriate metric is the number of system operating hours. In the case of a non-train-based system which cannot fail when trains are not running, then the number of system operating hours per day can be reduced to by the proportion of the day for which trains are operational.

2.5.4.2 Use of CSM design target

CSM design target shall be referred to as harmonised safety design requirements for technical systems. The achievement of these design targets are a mean to achieve an acceptable level of safety when appropriate design processes has been demonstrated and the safe integration of the technical system into the railway system has been demonstrated.
The CSM design target are required to be used only where automatic mutual recognition is being sought, or where they are necessary to achieve a national level of safety. They represent the most demanding design targets that can be required. The proposer is also free to use more demanding design targets for his own purposes.
A more demanding target than CSM design target may be notified by a NSA only if it can demonstrate that the more demanding target is justified and necessary to achieve the national safety level.
Meeting design target can be a way to achieve mutual recognition. Mutual recognition can also be achieved by using one of the other risk acceptance principles.
If the proposer can demonstrate that the national safety level in the Member State of application can be maintained with a less demanding design target than the harmonised design target, then this less demanding target can be used instead of the harmonised one. The possibility of mutual recognition is no longer given automatically.
For the case where failures of functions have external barriers affecting the frequency or consequence of the hazard then these can be considered and used to derive less demanding design targets. In this case, the mutual recognition may still be possible, but is not automatic.

2.5.4.2 3 Severity Classes - Values for CSM design target

The following design targets shall apply to failures of functions of technical systems:

[CER position on ERA definition and values reserved – CER will give a final position after a workshop]

When estimating the typical severity of the consequences of the analysed functional failure in order to derive which of those harmonised design targets is applicable for the assessed hazard, the proposer shall apply the following conditions:

(a) If no trustworthy statistical data or expert estimates are available, then a more demanding but credible severity of consequence shall be chosen.

(b) The outcome to consider shall be an outcome greater than the average but not the worst case event.

Typically means that the consequences will in most cases lead to that outcome.

ANNEX 2 HANDLING BARRIERS WITH CSM DESIGN TARGET

It is CER's conviction that barriers are also applicable in the current ERA proposal.

a) Qualitative method to handle barriers

When a barrier is identified, and its efficiency proven (e.g. no situation where the barrier will have no effect), then the severity attached to the function under consideration without the barrier can be considered one class lower than the severity attached to the accident.
Note: though this method can be used outside of technical systems barriers, it provides the following pros & cons:

Pros	Cons
Fast evaluation of new target Safety kept at a high level Can be applied for both technical or operational barriers	Still need to ensure that the barrier reduces the frequency of the accident by at least a factor of 100. Easily reached for a technical system, but has to be ensured proper training & formation for reaching that efficiency for operational barriers Rough estimation, thus can lead to over safety When no maintenance is made (failure is not detected and no restoration is expected during the system's lifetime), the barrier efficiency may be overrated (then this barrier should not have decreased the severity attached to the system under assessment)

b) Quantitative method to handle barriers

When the barrier is a technical system, then its probability of failure can be calculated, the target can then be apportioned between the function under consideration and the barrier.
Note: this method is rarely used outside of technical systems barriers, it provides the following pros & cons:

Pros	Cons
Optimisation of safety vs cost is possible Safety kept at the acceptable level	Maintenance need to be taken into account (unsafe down time for each failure) Safety study can be time-consuming for complex systems with multiple barriers Rarely applicable to non technical barriers

c) Barrier Concept

An approach to incorporate barriers in the application of the CSM design targets is of fundamental importance. To ensure that the barriers are handled in a coherent way,

clear definitions of the types of barriers are necessary. Furthermore, it is essential to describe how the barriers impact the design target.
A barrier is always an action on the system under control of the RU or IM. A barrier can be of technical or operational nature. The safety performance of a barrier must be controlled by the RU / IM. Measures which are not controllable by the RU / IM (e.g. passenger behaviour, probability of car on technically not-protected level crossing) cannot be used as a safety barrier.
To support mutual recognition it is necessary to develop a harmonized list of barriers. Meaning by "Barrier": A physical and/or non-physical barrier means to reduce the frequency and/or the severity of the consequences of potential undesired events. [pr EN 50126-1, Proposal for RAC definition, Version 3.0, 23.05.2011, …].

Generic list of typical kinds of barriers [ROSA]:
- Human attention of railway staff
- Train protection systems
- Measures on guideway for ensuring clearance envelope
- Measure for route safety
- Separation of Road and Track measures
- Protection measures against intrusion of persons into clearance envelope
- Measures for ensuring safe transport of passenger and loading
- Measures for safety passenger exchange
- Maintenance measures

d) Assessing the mitigation quality of barriers

To foster mutual recognition an approach for assessing the effectiveness of barriers is necessary for these harmonized barriers.
If a barrier concept is developed according to the aspects mentioned before, a possible procedure is as follows:

1) The function of a technical system is assumed to fail (neglecting the existence of barriers in this step)
2) The potential accident is analysed.
3) The typical outcome of that accident is assessed.
4) The CSM design target is selected according to the consequences of the expected accident type.
5) Existing barriers (reducing the occurrence or mitigating the consequences of an accident) are identified and their safety performance is analysed.
6) External barriers are taken into account by reducing the acceptable rate of the unwanted consequence by the probability of the failure of barriers.
7) Case validation
   a) The resulting acceptable failure rate is lower than the CSM design target – the safety requirement of the design target can be decreased as far as the level of safety is maintained.
   b) The acceptable failure rate is in the range of the CSM design target (e.g. < factor of 10) – the safety requirement of the design criteria is taken as selected.

c) The acceptable failure rate is higher than the CSM design target – the safety requirement of the design target is taken as selected and additional safety barriers (from the harmonized list) must be implemented. Where this is not possible the safety requirement of the design target must be from the next higher class.

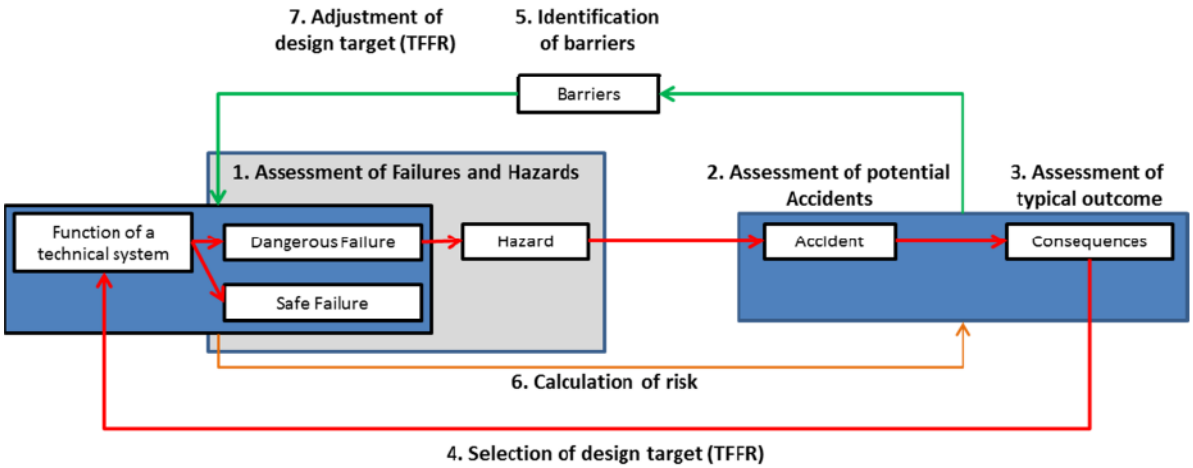

Figure 5: Selection and Adjustment of design target

e) Conclusion

CER thus propose to add the method presented in this annex into the application guide, and to discuss their possible reference in the regulation. The conditions for ensuring automatic mutual recognition in the presence of barriers have to be clearly defined and some principles should be set in the regulation.