

# Ein einheitliches Risikoakzeptanzkriterium für Technische Systeme

Siemens Transportation Systems

Braunschweig, Oktober 2007  
Prof. Dr. Jens Braband

© Siemens AG 2007

## The European Railway Agency (ERA)

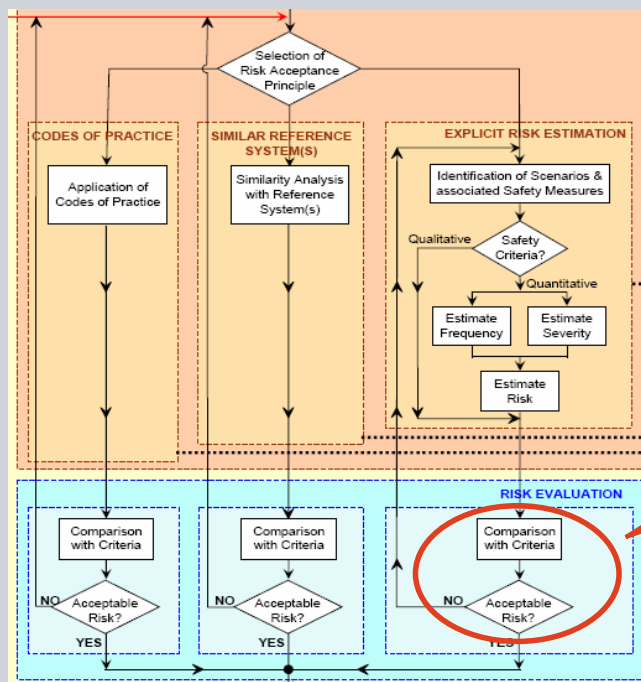
The European Railway Agency (<http://www.era.eu.int>), established by European Regulation 881/2004, has the mission of reinforcing railway safety and interoperability throughout Europe.

The European Railway Agency develops harmonised measures for rail safety. These measures concern common safety targets and common safety methods (CSMs), the definition of common safety indicators and the harmonisation of documents relating to safety certification.

Common safety methods describe how safety levels, the achievement of safety targets and compliance with other safety requirements are assessed in the various Member States.

In this context, UNIFE (Union of European Railway Industries) has agreed on a proposal which includes a risk acceptance criterion for technical systems.

## Scope of Presentation within CSM Recommendation



This presentation deals only with explicit risk analysis and risk acceptance criteria for it

## Definition of Technical System

### A technical system

is a product developed by a supplier including its design, implementation and support documentation.

#### Notes:

- The development of a technical system starts with its System Requirements Specification and ends with its safety approval.
- Human operators and their actions are not part of a technical system.
- Maintenance is not included in the definition, although maintenance manuals are.

## Definition of Function

### A function

is defined in this context as a specific purpose or objective to be accomplished that can be specified or described without reference to the physical means of achieving it (IEC 61226:2005).

Note:

- A function transfers (considered as a black-box) input parameters (material, energy, information) into aim related output parameters (material, energy, information).

## Risk Acceptance Criterion for Technical Systems

UNIFE has agreed on the risk acceptance criterion for technical systems (RAC-TS):

Any failure mode of a function resulting in a hazard that has a **credible immediate** potential for **catastrophic consequences** shall not occur with a rate of occurrence higher than  $10^{-9}$  per operating hour.

- **Catastrophic consequences** are defined by EN 50126 as “Fatalities and/or multiple severe injuries and/or major damage to the environment”.
- **Credible** potential means that it must be likely that the particular failure mode will result in an accident with catastrophic consequences.
- **Immediate** in this context means that no credible barriers exist that could prevent an accident.
- The purpose of this criterion is to define a **design target** against which risk analysis methods can be calibrated.

## FAQ:

### How is RAC-TS Related to the Overall Railway Risk?

It is only indirectly related, as **RAC-TS is a semi-quantitative criterion and the focus is on the avoidance of potentially catastrophic events.**

If a scenario as described by RAC-TS occurs, only rarely is the outcome a catastrophic accident. For example, although some derailments have a catastrophic potential, only 2 fatalities resulted from 529 cases in 2005 in EU-25 (EUROSTAT data).

**Thus, simple approaches** such as multiplying the number of functions by the quantitative RAC-TS design target **will yield meaningless risk estimates.**

## FAQ:

### Is RAC-TS a Risk Assessment Method?

Or, in other words: **Is RAC-TS directly applicable?**

**Yes, but only if**

- the failure relates to a function of a technical system
- the potential is catastrophic and
- there are no credible barriers to prevent an accident.

Such functions are rare in railways, but there are examples:

- failure of an ATP system in high-speed or automated operation
- undetected wrong setting of points in main-line operation
- complete loss of braking capability

However, **in most cases RAC-TS is not directly applicable.**

## FAQ: What Functions is RAC-TS Applicable to?

### prEN 0015380-4

Railway applications – Classification system for rail vehicles – Part 4:  
Function groups

The normative section of prEN 0015380-4 defines three hierarchical function levels (extended in informative annexes to five). In total, prEN 0015380-4 defines several hundred functions relating to trains.

In general, the **recommendation is to select the functions from the first three levels of prEN 0015380-4 (but not below)**, taking into account the product breakdown structure. For functions outside the scope of prEN 0015380-4, the **appropriate functional level shall be decided by comparison, based on expert judgment.**

## Example: Functions (based on prEN 0015380-4)

Code	Function Description	Remarks
=BED	Manage signalling of fire	Management of fire alert
=CFD	Manage emergency alarm from passengers	
=CLB	Control tilting	
=DB	Provide external access	Functions associated with the management of the external doors
=EBF	Ensure adequate reaction on unintended uncoupling	
=FB	Provide electrical energy for traction	
=GB	Provide acceleration and dynamic brake force	
=GC	Provide deceleration and keep the train at standstill	
=JBP	Provide Detection of Non Rotating Axle	
=KEB	ATC On-board	
=KF	Automatic train operation	
=KGB	Control Switches	
=KGC	Control Signals	

## FAQ:

### How can RAC-TS be Applied to Other Scenarios?

RAC-TS can **easily be applied to scenarios which differ only with respect to a few independent parameters** from RAC-TS reference conditions.

- We assume that for a particular parameter  $p$  the relationship to risk is multiplicative.
- We assume that in the reference condition  $p^*$  applies and in the alternative scenario  $p'$ .

In this case, only the parameter ratio  $p^*/p'$  is relevant and the rate of occurrence can be reduced. This procedure can be iterated if the parameters are independent.

## FAQ:

### How can RAC-TS be Applied to Other Scenarios?

Example:

- We assume that the actual potential of the consequence (e.g. critical) is ten times less than the potential under reference conditions (which is catastrophic).

Then the requirement is  $10^{-8}/h$ .

- We assume that an additional barrier (independent of the consequences) is identified which is effective in 50% of cases.

Then the requirement is  $5 \times 10^{-7}/h$ .

## FAQ: How can RAC-TS be Used with Common Risk Assessment Methods?

RAC-TS can be **used to calibrate risk assessment methods** (see the simple example below for a risk matrix).

Depending on the particular method, trade-offs can be made (e.g. lower consequences resulting in a lower design target).

Frequency of occurrence of a hazardous event	Risk Levels			
Frequent				
Probable			<b>Intolerable</b>	
Occasional				
Remote				
Improbable		<b>Tolerable</b>		
Incredible				
	Insignificant	Marginal	Critical	Catastrophic
	<b>Severity Levels of Hazard Consequence</b>			

## Justification: Necessity

Concerning risk analysis, and in particular risk apportionment, ERA recently reached the following conclusions:

- **Apportionment of CST** to define common safety requirements ... **is not feasible** in the first set of CSTs nor in the second set of CSTs due to insufficient official data on accident causation
- Even if such data were available, **top down apportionment** of a high-level CST expressed in terms of fatalities in order to derive common safety requirements **is anyway not recommended** due to the high uncertainty and variability ...
- To define such quantitative safety requirements, in particular within the TSIs, it is rather suggested **to agree on common risk acceptance criteria directly** applicable to the sub-systems or constituents being assessed.

## Justification: Technical Arguments

- In the European **TSI-CCS**, a reference for a tolerable risk is given which could be generally applied to new functions or systems: “For the safety-related part of one onboard unit as well as for one trackside unit, the safety requirement for ETCS Level 2 is a tolerable hazard rate of  $10^{-9}$  / hour ...”.
- Several projects have proposed the same target for all safety-critical functions, e.g. Euro-Interlocking for electronic interlockings. This requirement is very **similar to specific risk analysis results** already assessed and approved by the EBA.
- This approach is similar to that in **civil aviation** (see SAE ARP 4754), where this criterion has been successfully used for more than 20 years. It has been shown from operational experience with large aircraft fleets of, e.g. Boeing 737s, that the overall safety level has actually been met in practice.

## Justification: Normative and Legal Arguments

- For a programmable electronic control system implementing the corresponding safety function, this would, according to **IEC 61508-1** (the basic safety publication for programmable electronic systems in all sectors) or **EN 50129**, equate to a requirement of level SIL 4.
- It also constitutes the **highest integrity level that can be demanded** according to the CENELEC and IEC standards. It is also known that higher levels of integrity for complex systems cannot credibly be claimed.
- The target level of risk behind RAC-TS **is already tolerated** in TSI-CCS and civil aviation.

## Justification: Economic Arguments

- Accident investigation and statistics demonstrate that human errors with organisational factors or flaws in the safety culture are very, not to say the most, important factors contributing to accidents. The **contribution from technical system failures becomes negligible** for signalling systems and the like (credible estimates put it at well below 1%). This has been demonstrated both theoretically and empirically.
- Generally, the safety level of existing technical systems is sufficient.
- Due to its negligible contribution to the overall risk, **increasing the technical safety level is not cost-effective** (e.g. SAMNet, IRSE).
- Harmonising and standardising the existing high safety level of technical systems would enhance **the competitiveness of the European rail industry**.

## Conclusions

- UNIFE has proposed a pan-European **harmonised risk acceptance criterion for technical systems (RAC-TS)**.
- A **wide range of arguments** were presented **justifying** RAC-TS on normative, legal and economic grounds.
- An outline was also given showing how it can be **applied per se or as a reference point** for the calibration of certain risk analysis methods.
- It is to be expected that RAC-TS will simplify discussions on the appropriate safety requirements and so **save time and money in railway projects without reducing the level of safety**.
- Last but not least, a harmonised criterion promises to **increase standardisation and hence the competitiveness** of the entire rail sector.