A Harmonised Risk Acceptance Criterion for Technical Systems on European Railways

Braunschweig, June 2007
Prof. Dr. Jens Braband

Siemens Transportation Systems
Background on European Railway Agency

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 railway safety. These measures concern common safety targets and common safety methods, the definition of common safety indicators and the harmonisation of documents related to safety certification.

Common safety methods describe how safety levels, achievement of safety targets and compliance with other safety requirements are assessed in the different member states.

In this context, UNIFE has agreed on a proposal which contains a risk acceptance criterion for technical systems.
Scope: UNIFE Proposal for Technical Systems
UNIFE has agreed on the Risk Acceptance Criterion for Technical Systems (RAC-TS) reference value:

Any failure mode of a function resulting in a hazard that has a **credible immediate** potential for **catastrophic consequences** shall not occur with an occurrence rate of 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 results in an accident with catastrophic consequences.
- **Immediate** in this context means that no credible barriers exist that may prevent an accident.
- The purpose of this criterion is to define a **design target** from which risk analysis methods can be calibrated.
Concerning risk analysis and in particular risk apportionment, ERA has recently come to 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 level of 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 subsystems 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 $10^{-9} / \text{hour}$ …”.

- The Euro-Interlocking project has proposed the same target for all safety-critical functions of electronic interlockings. This requirement is very similar to particular risk analysis results for electronic interlockings which have been assessed and approved by the EBA.

- This approach is similar to the approach and target 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 for large aircraft fleets, e.g. Boeing 737, that the overall safety level has actually been met in practice.
For a programmable electronic control system implementing the corresponding safety function, this would, in IEC 61508-1 (the basic safety publication for programmable electronic systems in all sectors) or EN 50129, equate to a requirement falling into category SIL 4.

It also represents the highest level of integrity that may be required 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 in civil aviation.
Justification: Economic Arguments

- Accident investigation and statistics demonstrate that human errors with organisational factors or flaws in the safety culture are more, not to say the most, important factors contributing to accidents. The contribution from technical system failures becomes negligible for systems such as signalling systems (credible estimates range far below 1%). This has been demonstrated theoretically as well as empirically.

- Generally, the safety level of existing technical systems is sufficient.

- Due to its negligible contribution to the overall risk, an increase in the technical safety level is not cost-effective (e.g. SAMNet, IRSE).

- If this high safety level of technical systems were harmonised and standardised, the competitiveness of the European railway industry would increase.
### Application Example: Risk Matrix Calibration

<table>
<thead>
<tr>
<th>Frequency of occurrence of a hazardous event</th>
<th>Risk Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequent</td>
<td></td>
</tr>
<tr>
<td>Probable</td>
<td></td>
</tr>
<tr>
<td>Occasional</td>
<td></td>
</tr>
<tr>
<td>Remote</td>
<td></td>
</tr>
<tr>
<td>Improbable</td>
<td>Intolerable</td>
</tr>
<tr>
<td>Incredible</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Severity Levels of Hazard Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insignificant</td>
</tr>
<tr>
<td>Marginal</td>
</tr>
<tr>
<td>Critical</td>
</tr>
<tr>
<td>Catastrophic</td>
</tr>
</tbody>
</table>

- Typically an accident
- Guiding examples to be developed
- RAC-TS

© Siemens AG 2007
Conclusions

- UNIFE has proposed a pan-European harmonised risk acceptance criterion for technical systems (RAC-TS).

- RAC-TS has been justified by several arguments, including normative, legal and economic arguments.

- It has also been outlined how it can be applied as a reference point for the calibration of particular risk analysis methods.

- It can be expected that RAC-TS will simplify discussions on the appropriate safety requirements and thus save time and money in railway projects.

- Last but not least, a harmonised criterion would increase standardisation and thus the competitiveness of the entire railway sector.
Thank you for your attention!
References

- Braband, J.: Risikoanalysen in der Eisenbahn-Automatisierung, Eurailpress, 2005


- SAMNet: Common Safety Targets and Common Safety Indicators, Position Paper D1.2.3, Handouts at Final User Group Meeting, December 2005
References

- ERA: Feasibility study “Apportionment of Safety Targets (to TSI Subsystems) and Consolidation of TSIs from a Safety Point of View” WP1.1 Assessment of the Feasibility to Apportion Common Safety Targets, Version 1.0, February 2007

- Society of Automotive Engineers: Certification Considerations for Highly Integrated or Complex Aircraft Systems. Aerospace Recommended Practice 4754, 1996
