

Questions, Answers, Ideas concerning Technical Issues of Harmonisation of Safety Assessment

1. Scope

The following short paper is dedicated to collect questions, answers and ideas regarding harmonisation of safety assessment. The paper is thought as a starting point from which experience shall be gathered. In coincidence with the role of a thematic network, solutions to open questions first will be searched from experts. For those questions, where this will not be possible, separate research and/or development projects will be proposed.

2. Safety Case

The structure of a safety case is prescribed for signalling and control systems in EN 50129. Which shall be the structure of the Safety Case for other technical systems (not signalling and control). Can the structure from EN 50129 be applied? This structure can be recommended, is logical, but cannot be required. Therefore, different authors may deviate from this structure.

Can EN 50129 also be used for other electric / electronic sub-systems? From a pragmatic point of view this can be done, however it is not mandatory.

3. Design measures

A safety integrity level consists of two main requirements. The first one is that the function of the object in regard shall not exceed a target value for dangerous failures. Second, certain design requirements have to be fulfilled. EN 50129 presents design requirements for signalling and control. Can these requirements be adopted for other electrical and electronic subsystems? Where shall design requirements be taken from for other (non-electrical) sub-systems?

Especially, which standards can be used for mechanical and civil engineering when design methods for SIL1...SIL4 are to be used or checked ?

4. Safety Targets

How shall safety targets be set up: for the entire system or by apportionment to sub-systems? The question is especially interesting, when already existing systems are changed and a new subsystem is installed. If only an overall system target is present, the entire system would have to be evaluated in order to find out the target for the new sub-system.

Harmonized risk acceptance criteria are needed in this regard.

5. National Safety Standards

Often additional, national safety related standards have to be used (EMC, fire protection, etc.).

Are there countries that do not require the use of additional safety standards (EN 50126 / 50129 is sufficient)?

Example: The German EBA allows the use of EN 50129 , or alternatively Mü8004 (national standards) for signalling and control.

In France, additional requirements exist concerning fire protection.

Are there overview lists of such standards for several countries or persons / institutions that can give information?

6. Quality assurance system

EN 50126 / EN 50129 require the existence and application of a quality management system. By which criteria has a quality assurance system to be judged to be sufficient for a

safety relevant (sub-)system? Is an ISO 9001 certificate sufficient? Which additional requirements have to be made? Are there requirements for the qualification of the personnel?

7. Assessment methods

In which phase of the development / manufacturing process are the methods “evaluation” and “audit” appropriate? Can the evaluation of an object be replaced by an audit of the underlying process?

8. Rail Competence criteria for Notified Bodies / Competent bodies

The new approach framework requirements for certification (Notified) bodies have no Rail specific competence requirements for Notified Bodies. How can we have confidence in their certification if there is no requirement for specific knowledge of Railway technical systems or operations.

The TSIs deal with Interoperable Trains interfacing to Interoperable Infrastructure. How will notified bodies deal with Interoperable trains that need to operate with national infrastructure? Also how will they deal with infrastructure systems that need to interface with existing infrastructure? On operational issues: how can NBs have knowledge of all countries operating rules?. The ideal way to overcome these issues is through an all encompassing safety case (see above).

Analogous problems are expected for other competent bodies.

9. Practical problems regarding Notified bodies

In some countries, notified bodies will not exist within the next 1-3 years. Then, assessment has to be carried out abroad. This implies a need for harmonisation of assessment rules.

In the harmonised area, an assessment from a notified body from another country must be accepted from a legal point of view. However, how much confidence is in such an assessment? How much can harmonised assessment rules enhance confidence?

10. Responsibility

What responsibilities remain with the contracting company to ensure all the assessed systems work with existing systems and what remains with the competent body?

Also, what responsibility lies within the state (governmental institution)?

11. Cross-certification

Which schemes for cross certification are currently proposed? Is there already practical experience with these different conceptions? Which obstacles have been identified?

12. European Projects

Is the Generalised Assessment Method (GAM) (CASCADE) known and used?
Are the results of AcruDa known and used?

Do you know persons, texts, sources of information

- for solutions,
- related problems,
- experience.

Thank you for your collaboration.

Contact:

Dr. Hendrik Schäbe

Phone: +49 221 806 2466

Fax: +49 221 806 3940

e-mail: schaebe@tuv.net