"Reasonable application of the EN 50 126 for the modification of an electrical and mechanical Safety System"

Dr. Stefan Pöting, Senior Safety Expert and Site RAMS Manager for Alstom Transport Deutschland

Abstract
The application of risk based safety analysis has been introduced to the Railway system with the publication of the dedicated standard EN 50 126 in 1999. In the railway sector the application of these standard is more and more enforced by European Regulations such as the Railway Safety Directive 2004/49/EC and Commission Regulation (EC) No 352/2009 Common Safety Methods on Risk Acceptance (CSM-RA) [11]. This provides a special challenge for modification of existing systems which were engineered when these standards were not in place and relevant documentation is not available.

In a project for a safety relevant modification of the automatic train control (ATC) system integration this challenge was accomplished with the combined effort of the operator, national safety authority, independent safety assessors, designers, RAMS-engineers and quality inspectors in a professional but reasonable manner. This modification project demonstrates for a small but critical significant change that a trustful application of the process, methods and tools of EN 50 126 is practical. It is demonstrated that the significant change according to CSM Commission Regulation (EC) No 352/2009 [1] on the signalling integration was managed safely and has reduced the previously existing technical risk further to a tolerable and acceptable level.

Key aspects for the success of the project in a critical environment will be pointed out. It will be highlighted that the reasonable application of the standard for the demonstration of the compliance to the CSM has to be performed in a team effort of all involved participants to the project and in an open minded and trustful environment. This approach will bring such difficult projects to a safe and trusted solution.

Introduction
In the past a safety relevant failure of an unperformed emergency braking function occurred during service operation of a multiple unit train. This incident was carefully investigated and analysed in order to understand the root cause of the incident and to be able to determine if the incident is in line with the operational requirements (which it obviously could not be), the safety principles and requirements were correct or if the incident was due to the failure of one or more components.

The investigations identified the three major failures which needed to be corrected to ensure a safe operation in the future preventing a reoccurrence:

- The SIFA-valve responsible for activating an emergency braking has been stuck half way.
- The stuck SIFA-valve was not detected during tests for such events.
- The activation of the emergency braking was only done on a non redundant path.

Following the clear identification of the failures, the implementation of interim mitigation was set up and the development of the solution was started. During the first approach the design engineers worked on a new solution. When finished they presented the result to the RAMS-engineers and they provided a safety demonstration for the solution. At the end a safety case was presented to an independent assessor who did not agree on the solution and who questioned the weaknesses at the beginning and finally the total system integration and gave some idea of further enhancements to be respected.

Looking back at the situation it was totally unsatisfactory:

- Money had been spend on the development of the solution, the safety case and the assessment,
- The result was the solution was rejected,
- The implementation needed to be postponed,
- More money needed to be spend for a new approach,
- The interim mitigation measures needed to be extended.

The obvious question was how could such a situation be avoided and the successful development and assessment be better controlled and achieved?
The successful modification, its planning and achievement are described on the basis of the example. This example clearly showed that a reasonable and trustful team work in a concurrent engineering process and a successful collaboration of operator, developer, manufacturer, ISA and NSA can be the way for a successful application of the process according to EN 50126.

**Project Implementation**

1. **Risk Based Safety Demonstration in line with EN 50126, EN 50129 and CSM-RA 352/2009**

   The project was a multiple challenge as new standards such as EN 50 126, new rules and guidelines needed to be respected for an old existing system designed to different target values. Therefore all participants:
   - operator,
   - national safety authorities,
   - independent safety assessors,
   - designers,
   - RAMS-engineers and
   - quality inspectors

   need to agree on a reasonable way to apply the standard.

   The one of the main focuses was to demonstrate
   - that the limited change does not have any negative effect on other systems and
   - that it increases the level of safety to a reasonable level.
   - As there were limited analysis existing for the old design the challenge was to demonstrate the reasonable increase and the non degradation.

   With the help of a system analysis based on systematic structured old design documentation the system architecture and its impacted interfaces were clearly identified. The main milestones of the project were:
   - The existing and the new requirements (especially for safety) were clearly identified and listed.
   - The identified requirements were openly reviewed with participants.
   - Based on the agreed requirements the existing design was reviewed to identify needed changes, changes to interfaces and systems.
   - As a result the safety concept for the modification was set up and updated detailing the functional changes required and the safety requirements.
   - Based on these results the designer and the RAMS-engineer developed together a choice of three solutions on a system design basis.
   - These solutions were evaluated and presented to the participants.
   - The best solution was selected and the safety concept and design were developed and detailed
   - while the design was continuously reviewed and the safety demonstration was performed.
   - The review of the changes included the check of the modified systems, circuits as well as the fulfilment of the safety requirements.

2. **Effective Project Setup**

   Taking the experiences of the first modification solution into account a new project approach had been set up. The following key items have had a special focus right from the beginning:
   - The full team of all participants: operator, the NSA, ISA, quality inspector, validator and design and RAMS-engineer and manager have been involved and have agreed on the approach.
   - An open and free discussion and communication between all parties had been agreed right from the beginning.
   - System and sub system definitions were agreed at the start between all participants.
   - The existence of a safe system has not been challenged.
   - The existing documentation and demonstration has been considered to be still valid, even though it is not fully in line with today’s interpretation of the requirements of EN 50126.
   - The existing solution, its principals for system architectures are considered to be proven in use systems except for the items which have been identified to have contributed to the safety incident.
   - Safety targets and requirements were agreed at the start between all parties.
• Design and safety demonstration and review have been managed in a collaborative concurrent engineering way of working in parallel for the whole project.
• The application of the standard EN 50 126, the quantitative methods and the reliability values for existing components as listed in the data sheets and international standards have been accepted and agreed to be relevant for demonstration.
• The solution has been presented and demonstrated to the train operators and reviewed with them in order to ensure it is in line with the working environment.

Even though many of these items appear to be trivial and standard for the concurrent engineering approach and the application of the standard it helped to focus the mindset for the project.

3 Project safety plan
The above principles have been agreed and were put into the safety plan to set a well defined reference baseline for assessments. It is even an advantage for the concentration on the work, to agree on the scope without unidentified risk for the involved participants. Especially for the NSA and the ISA this document identified the limitation of this project and its safety demonstration ensuring that no additional risk for the project was identified and left an open responsibility for themselves. As the safety management plan is normally seen as a non beneficial document only for the management purpose, approach has turned the safety plan into a very beneficial document. It was used as a reference, a project scope definition and a limitation of activities. It turned into a reasonable cost reduction tool. The safety plan contained the following essential information and was shared with NSA, ISA, and operator during the start-up phase [8]:
• the safety
• management structure,
• safety-related activities,
• approval mile-stones throughout the life-cycle, and
• include the requirements for review of the Safety Plan at appropriate intervals.

4 System definition and analysis
Key success for the limitation of the work of this modification is the clear system definition and interface description. The better the system and the sub systems are defined by their functions, their components and their interfaces, the easier the concentration on the key systems can be achieved. Such systematic approach makes the concentration on the key elements of the system and the key functional targets clearer and easier to implement and follow. Other items need to be followed as well, but from an other focus and attention.

The benefit of the systematic approach is further that requirements and functional responsibilities can be clearly identified, allocated and distributed in a hierarchical manner with clear targets and functional expectation.

The key information to be provided in this system definition and analysis is:
• Identification of system
• Identification of sub systems
• Identification of interfaces
  o Inputs and their limits
  o Outputs and their limits
• Identification of function and mal function behaviour

Beneficial for this modification project was that a clear systematic approach was followed for the initial design and it builds a good baseline for the system definition in this modification project. As a positive consequence system and sub system interfaces could be analysed effectively.

The root causes were identified from root cause analysis and various incident reports. The linked systems and functions involved were identified. The functional system behaviour was checked and the unwanted behaviour identified in the test procedure for the system start-up test. Under certain conditions interim test results could be misinterpreted as if a test procedure had been applied successful giving the feedback of safe system and therefore the test was passed successful.

In this case the Train Control and Monitoring System (TCMS) then allowed the use of the train system with a non safe and false emergency brake activation system.
Based on these results the systems impacted by the modification could be identified in the System Definition of the TCMS. The functional modifications requirements were allocated to the functions in the identified systems and the impacted interfaces reviewed:

Diagram 2: Systems Impacted by the Modification

When system and sub system relation are clearly identified with their interfaces only the identified key functionalities need to be reviewed, analysed and if necessary adapted. The detailed system functional requirements according to the expected system safety behaviour need to be ensured for a safe system.

5 Safety Concept

The functional expectations from the safety perspective have been detailed and allocated to the relevant systems. For each relevant system and sub system the safety concept describes the expected functionality and their failure behaviour. The relevant safety requirements are identified as such and a possible test for its correct implementation is drafted as indication how the successful implementation can be demonstrated.

For each requirement a detailed description of the requirements is identified in a structured way which should contain the minimum reference information and descriptions as follows:

- Requirement definition – unique identifier of the requirement
- Title – identify the topic of the requirement
• Designation – purpose of the requirement in brief verbal description
• Classification – safety critical in case function fails
• Modifications – anticipated modification for the design during the design change
• FMI – Field Modification Instruction
• Components – relevant systems, sub systems or components
• FMECA- Failure Mode Effect and Criticality Analysis – what kind of failure modes have to be evaluated
• Flowchart/FTA – to which functional flow chart for the processing and / or which fault tree (FTA) is the requirement linked to
• SRIL – Link to Safety Related Item List, a tool to manage aspects of safety with the various aspects of such as design, manufacturing, testing, validation, maintenance, instruction …
• Test Interval – what is the automated system test interval
• Inspection Period – what is the relevant maintenance inspection interval
• MIL – Maintenance Instruction List identifying if an update needs to be considered

Using this way of presenting the planned modification allowed everyone from the team to follow and understand the intended modification and allowed an easy follow up of taken decision and assumption. This was even more important as the project has had participants involved in 4 countries (Germany, Sweden, Norway and Great Britain) and 5 different entities which needed to work and agree together on one solution. Therefore an as much as possible precise description of the expected functionalities has to be transmitted in a clearly structured way. In addition there is the need in the projects that the documentation has to be readable and useful for all different aspects of the project work such as:
• Design
• Safety demonstration
• Validation
• Quality inspection
• Maintenance
• Assessment

The detailed requirements towards their safety functional expectation need to be recorded. This ensures that the requirements are met for the implementation and can be correctly proven in the demonstration to follow. The detailed expectation and functional needs are listed from other related analysis such as FMECA, FTA, event tree or flowchart. The relevant components and the failure modes and expected failure behaviour are detailed to ensure the demonstration will meet all safety requirements. With these information details and a well detailed description a positive assessment is ensured. NSA, customer, validator and ISA can follow the argumentation that the system has been design safely and is safe for operation.

The solution is developed based on the detailed safety requirements described and allocated. Adaptations according to the development have to be made in the concepts as a consequence of the concurrent engineering approach and the joint solution development.

6 Solution Development
The detailed design has been managed by the system engineer who worked closely with the RAMS-engineer. Together they reviewed
• the detailed design documents,
• identified the interfaces of the systems,
• analysed the existing functionalities,
• clarified the relevant components and contacts
• by reviewing the existing functions.

As a result the RAMS-engineer and the design engineer evaluate the solutions and pre-select the preferred solution.
Diagram 3: **Choice of Solutions**

The pre-selection of the solution was briefly discussed with the operator, ISA and NSA to ensure they understand the reasons for the selection and to be fully transparent. To ensure the most stable and straightforward process application for the design and safety management processes, the pre-selected solution is detailed to gain the confidence that this solution can be implemented when finalized.

Diagram 4: **Detailed Design of Pre-Selected Solution**

At the end of this phase, the design is confirmed to fulfill the safety functionalities, the safety requirements, and to be physically installable. In this case, sub functions have been tested, and sub functionalities have been pre-tested to confirm the solution. The safety manager has reviewed his draft safety report in which he has confirmed that all previously detailed safety requirements are confirmed to have been implemented with an appropriate level of confidence and references.

7 **Final Solution Review and Presentation**

The pre-selected solution is presented in an official meeting to all participants (s. 2 **Effective Project Setup**). For this presentation of the modification, the team was extended to the operator's safety experts, safety responsible, and driver's representative. This way, all actors for the future operation and action were at the table, got first-hand information. Everybody on the table was able to raise questions, give concerns, and at the end, was able to understand the selection of the solution. Everybody agreed on the reasonable selection as the best choice and was able to accept the solution when it was implemented as presented.

As the implementation, prototype test, validation, test, and demonstration are related to the operational products in the field, it was also key to set up a common understanding of what needs to be achieved as a whole team. Everybody needed to accept:
that he has to contribute to the full project,
that no short-cuts are acceptable and
that the demonstration and the project
will only be a success, when all planned actions are positively fulfilled.
The successful team building in the project helped to ensure the successful modification for the trains and to deliver together a well founded and structured safety demonstration without deficiencies. The clear and transparent presentation of the solution which is in line with the identified systems affected by the modification, confirm to all team members that the modification is limited to the identified systems. This in detail confirmed with the operational history of the trains that train system can be considered safe in use for all other systems not affected by the modification. For this aspect all not affected system are considered as:
• a reference system for themselves
• proven in use and
• adequately safe.

Diagram 5: Final Selected Solution

8 Safety Report
The safety report summarizes all aspects of the safety demonstration for the modification. The safety report at train system level is making reference to the safety reports of each adapted system. There is always the tendency to go to one document for the full demonstration. Whereas the experience in the past, in current projects and especially also on this modification project has revealed advantages that is much better to handle modification, upgrades, changes and adaptations per system. This way it is much easier to reuse, update or change part of the system without having to reflect the whole system in the safety report.
The content of the safety report is structured in line with the proposed document structure of the EN 50129 [8]. This makes an assessment by an ISA much better, as it is obvious to identify the aspects of the standard to be checked and trace the relevant information.
The safety concepts provide a well structured source of information:
• for the safety requirements to be checked,
• the clear identification of each requirement,
• the link to the validation activity
• the quality test to be performed and
• the instructions (manuals, maintenance information) to be updated.
At this stage the safety report wraps up all information needed for the field approval of the system.

9 Prototype Test
For the modification of this safety critical system it was decided to do a test installation and confirm that the final installation will be successful at the end. It is an additional measure which can be an useful instrument to demonstrate in practice that the solution is correct and no unidentified effect will occur.
This is an important aspect when a modification is applied to systems with very limited redundancies and high needs of availability for the operation. With this preliminary test it was confirmed that the
installation, timing and details can be confirmed on a practical basis. It was an additional step implemented to support any prototype test during a regular system development.

10 Installation and Validation
Installation and validation have been prepared carefully to ensure that all aspects of the
- safety concepts,
- safety requirements,
- adverse repercussions,
- implementation tests for the considered components
- maintenance and release to service tests as well as
- further validation test requirements

could be demonstrated and tested. The results were evaluated by an independent validator who confirmed, based on his project audit and the report of the quality test, that installed solution fulfills all aspects.

11 Solution Approval and Homologation
The detailed assessment report of the ISA and the validation report in combination with the safety documentation provided sufficient evidence for the NSA to give their authorisation to put the trains directly back into service. The trains needed to pass the detailed test of the modification as well as a test run allowing them to return back into service operation with passenger service. The special attention given to the:
- adverse repercussion demonstration,
- demonstration of no single failure will lead to a hazardous undetected situation,
- demonstration of the qualitative safety targets expressed on failure rate,
- the requirement tracing as well as
- the validation efforts performed
showed to all involved participants that the implemented modification is safe and was developed and implemented transparently.

Key Elements of Successful EN 50126 Implementation
With the example of a modification on the Automatic Train Control (ATC) in the train system and its interaction with the brake system has been demonstrated. The transparent and reasonable application of process and methods of the EN 50126 and EN 50129 can be applied on a reasonable, practicable and economic affordable way.

The systematic application of the risk and safety management tools, chosen on a reasonable basis openly discussed and commonly agreed, made the demonstration for the acceptance and homologation efficient, transparent and clear. The application of the methods (FTA, FMECA) and the process for a RAMS management of the standard EN 50126 is not a challenge which can never successfully be reached. In this example it was possible to make the application reasonable and practical as all participants involved openly worked on the subject in a trustful collaboration.

The key aspects of the successful implementation of processes and methods of EN 50126 and EN 50129 are:
- Reasonable selection of methods applied
- Trustful application of the demonstration methods
- Selection of quantitative targets for reliability to demonstrated the level of quality for the solution
- Targets demonstrated for reasonable aims such as maintenance intervals and/or quality of selected components
- Reasons selection and combination of quantitative and qualitative demonstration methods (such as FTA, FMECA, ALARP, GAME as described in the Application Guides to EN 50126 [5, 6])

Common Safety Methods on Risk Acceptance (CSM-RA 352/2009)
The above project of a concurrent engineering for the modification of the safety relevant subsystem integration is a positive example for the effective and reasonable application of the safety management process, methods and tools according to EN 50126. As this process aims at the effective
risk management it covers also all aspects of the CSM-RA regulation on risk evaluation and assessment.

The CSM-RA regulation mainly requires an adequate risk management successfully to be implemented. According to the regulation

- the railway operators and
- the infrastructure managers

have to demonstrate that they are managing the risk of their operation. Provider of services (maintenance…) and products (signalling, rolling stock, infrastructure …) for the operation eventually have to deliver the same kind of demonstration for their services and products. As these deliverables are integrated in the operator’s management system it transfers the responsibility of detailed demonstration for the integrated product. The responsibility is cascaded down to the delivering party.

The main aim of the CSM-RA is to ensure that according to the Safety Directive all operators are committed to perform their business at a minimum acceptable level of risk. This level of risk is supposed to be equal for all operators allowing them to freely choose the way it is achieved but to be demonstrated. As of today the railway operations in Europe are considered to be safe. A demonstration only has to be made when a significant change is introduced to the railway system. Each member state of the EU has to identify which need to be considered a significant change for their railway system. In most member states this definition is still missing.

For the modification project the change was considered to be significant as the modification has significantly reduced the probability of the failure to reoccur. Basically the modification fits to a suggested list of aspects to identify a significant change:

- Failure consequence: credible worst-case scenario in the event of failure
- Novelty used in implementing the change: both in the railway sector, and what is new just for the organisation implementing the change
- Complexity of the change;
- Monitoring: the inability to monitor the implemented change throughout the system life-cycle and take appropriate interventions
- Reversibility: the inability to revert to the system before the change;
- Additionally: assessment of the significance of the change taking into account all recent safety-related modifications to the system under assessment and which were not judged as significant.

The guideline to the CSM-RA allows the applicant to concentrate on the major risks of the system. The applicant has to fulfill a risk assessment and identify all risks related to the operation. The risks can be ranked according to the criticality. Broadly acceptable risks without further evaluation are to be considered:

- if the risk is less than a percentage (1-10%) of the Maximum Tolerable Risk for this hazard type. The value of x% could be based on best practice and experience with several risk analysis approaches, e.g. the ratio between broadly acceptable risk and intolerable risk classifications in FN-curves or in risk matrices. This can be represented as shown in Diagram 6;
- or if the loss associated to the risk is so small that it is not reasonable to implement any counter safety measure.
All publications on the CSM-RA show that a demonstration of an effective and acceptable risk management process is based on the expert judgment. A full and exhaustive demonstration is not required, see Diagram 6. Instead a positive assessment of the applied risk management is required [2, 9].

**Quantitative - vs. Qualitative - Demonstrations**

Various methods for the risk management demonstration are provided in [4, 5, 6]. All methods have in common as practical experience shows that one method is more appropriate for a demonstration on a topic than another. As a result the combination of reasonable selected demonstration with the various methods has to be applied:

<table>
<thead>
<tr>
<th>Qualitative Methods:</th>
<th>Quantitative Methods:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Failure Mode And Effect Analysis</td>
<td>• Fault Tree</td>
</tr>
<tr>
<td>• Event Tree</td>
<td>• Event Tree</td>
</tr>
<tr>
<td>• Fault Tree</td>
<td>• Tolerable Hazard Rate</td>
</tr>
<tr>
<td>• Risk Graph</td>
<td>• ...</td>
</tr>
<tr>
<td>• Single / Double Fault Analysis</td>
<td></td>
</tr>
</tbody>
</table>

Table 1: Table of Qualitative and Quantitative Methods

Qualitative methods have the advantage to demonstrate logical causes and consequences which can be shared and assessed. The advantage on the one hand side can also be seen as a disadvantage as not all possibly combined effects of the causes and consequences can be evaluated in a single argumentation. Whereas quantitative methods allow an assessment of risk from various causes and therefore can evaluate a combined risk. In addition quantitative methods can be measured by values and seem to be more objective for this reason.

Multiple experiences in this project as well as in several other projects have confirmed that:

- based on the evaluated risk
- based on the evaluated system / function and
- based on the needed demonstration for the safety principle of target

A meaning and reasonable strategy for the demonstration needs to be agreed for a successful safety demonstration and its assessment.

**Quantitative Target Indicators vs. Field data Statistics as Quantitative Targets**

Quantitative targets appear to be more objective and practically oriented. Therefore Tolerable Hazard Rates (THR) are often considered to be measurable and objective targets for demonstrations in a safety case. In many cases today one has to admit that the publicly discussed safety targets are based on accident statistics. Whereas Tolerable Hazard Rates (THR) indicate the probability of a system to fail when in addition the system is in a situation or environment where this failed function can lead to an accident. The accident observed and measured by the field experience combines the
probability of the system to have failed and in which the failed function is relevant to prevent an accident in its environment, Diagram 7. This kind of conditioned probability is difficult to estimate, as in most cases the required probability assumptions are not available.

Diagram 7: Figure A.4 of EN 50 129: Definition of hazards with respect to the system boundary [8]

Internal analysis to calibrate quantitative safety targets based on field data have demonstrated that a logical, mathematical and probabilistic link can be made between
- statistical field observations as quantitative targets based on EUROSTAT [10] and
- quantitative Tolerable Hazard Rates
and is at a reasonable level compared to the THR for a major system provided by [1, 9].
Even though the approach was successful it demonstrated the sensitivity of the mathematical modelling to the choice of parameters describing the accident environment in which the failure might occur.
Quantitative Target Indicators describing the level of reliability of the provided system can help to demonstrate and compare different solutions of different architectures or inspection and maintenance strategies. Quantitative calculations are a tool to value and compare precautionary measures and can help to describe functionally a level of reliability and safety function are expected to have.
Obviously a quantitative target indicator is only needed in such cases, where the risk evaluation needs to be performed explicitly according to CSM-RA when no reference system and no code of practice covering the evaluated risk can be applied.

Conclusion
The principles of the risk evaluation and assessment process are covered with a product development or modification based on EN 50126 [4]. This standard requires that a system is managed and an acceptable level of risk is demonstrated to be achieved. The CSM regulation (EC) No 352/2009 with its three principles to demonstrate the system risk acceptance aims the risk evaluation [3] which is full covered.
The European Regulation CSM-RA (EC) No 352/2009 proposes 3 ways to demonstrate that a system at an acceptable level of risk. The guideline to the CSM-RA details the application and proposes that hazards associated to broadly acceptable level of risk can be neglected for the demonstration. Especially for proven in use systems which are not affected by any modification change the system is considered by itself as reference system to justify that a system can be considered adequately safe.
A reasonable and practicable implementation of EN 50126 process can be performed successful and economical efficient. This efficient way is based on an open, transparent development of a well founded and trusted demonstration for a railway system. As a result all participants finally consider the system safe for use.
The demonstrated implementation of a parallel design and RAMS process has been successfully applied in new design projects as well as modification projects. The joint team approach has secured the risk of the assessment and homologation for all projects and fulfills the requirements of the risk evaluation and assessment of the CSM-RA.
Challenge H: For an even safer and more secure railway

References

[4] EN 50126-1, Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS), CENELEC, 1999
[9] Collection of examples of risk assessments and of some possible tools supporting the CSM Regulation, ERA/GUI/02-2008/SAF, Rev. 1.1, 06.01.2009