IRSE INTERNATIONAL TECHNICAL COMMITTEE

OPTIMISING COST AND SAFETY BY APPROPRIATE USE OF EUROPEAN NORMS

Written and edited by Peter Stanley and Joachim Stutzbach, IRSE-ITC on behalf of the International Technical Committee of the IRSE

_____

It has been found that risk analyses carried out in accordance with the European Standards and reflecting the specific detail of each application has led to a great escalation of cost of safety approval. Producing a separate risk analysis for each installation in a country increases the costs without discernable benefit. There is scope for making substantial cost reduction through new approaches to generic risk analysis.

The use of formal procedures in accordance with the European Standards may not lead to better quality of developments – on the contrary quality could be lost as resources are applied to the expanded needs of risk quantification and documentation at the expense of other quality related activities that depend on highly experienced railway signalling engineers to deliver assured system reliability and availability.

1 Introduction

The International Technical Committee (ITC) of the IRSE has reviewed the application of ENs to actual developments carried out in the European railway sector/industry. This document is a summary of its review and recommendations.

The national rules that have existed in most countries for many years covering the design, application and implementation of signalling and safety systems in a fail-safe manner were implicitly based on tolerable risk assumptions and have generally been interpreted as defining a system or equipment that is sufficiently safe provided the rules were obeyed, i.e. safety levels were defined for a country.

Such a definition of apparently absolute safety does not serve as a basis for the ongoing realisation of a safety culture that nowadays demands a risk analysis.

As part of European harmonisation, a series of pan-European standards was produced in the 1990s for the entire railway operation; the standards define a safety graded system based upon

the elements of risk, together with certain technical requirements and processes for establishing and observing sufficient safety throughout the entire life cycle of a railway installation or a vehicle.

In the field of control and communications these aspects are covered principally by the standards EN 50126, EN 50128 and EN 50129.

2 Basic Scope of EN 50126, EN 50128 and EN 50129

2.1 EN 50126

EN 50126 is the core standard which relates to the RAMS aspects of a system and the entire life cycle of each technical component and system within the context of railway transport.

The system definition, risk analysis and necessary development process are defined, albeit risk analysis is covered by an outline procedure with the objective of establishing tolerable hazard rates for system operation. Safety is defined as “freedom from unacceptable levels of risk of harm”.

There is hardly any distinction made in the standard between the definition of an individual system and that of a generic system, analysis options that are very important for the application of this and other standards.

The annex to the standard proposes risk tolerability criteria and definitions by which an established risk can be graded and judged, an example being demonstration that the safety level of a new system is at least equal to that of its predecessor system.

It is anticipated that changes may be made in the future, since the new European safety directive envisages that safety objectives are specified.

2.2 EN 50129

This standard describes in detail what action and documentation has to be provided for the purpose of preparing the safety case. The annexes to this standard contain further details about certain steps involved in the safety case production. Its scope is clearly restricted to the development phase of railway signalling and in contrast to EN 50126, distinguishes between generic and specific safety cases and introduces a requirement for the use of exact tolerable hazard rates according to allocated Safety Integrity Levels (SIL 1-4) derived from IEC 65108.

2.3 EN 50128

This standard is based on a conventional V model for software development processes. Today iterative processes are more common

3 Experience with the present standards

3.1 Experiences with risk analyses

A number of examples of risk analyses are considered.

3.1.1 The introduction of axle counters in the United Kingdom

To avoid unnecessary repetition of safety assessment it was decided to develop a Concept Safety Case which compares axle counters with the single rail d.c. track circuits that would have been the usual alternative and to address all generic issues associated with large scale use of axle counters on 25 kV electrified lines.

As part of this, a risk and hazard analysis was performed to establish the tolerable risk associated with existing track circuit systems. The Concept Safety Case included a template to be followed by all individual projects that ensured that local conditions were fully considered. Potential benefits were increased reliability and a reduction in broken rails due to the removal of insulated rail joints. Potential disadvantages include the reset requirements and the requirement for emergency communications from the driving cab.

The Concept Safety Case notes the mitigations that can be included in project designs and the template indicates how the mitigations can be shown to reduce risk to a level as low as reasonably practical, (the UK legal requirement).

Consideration of axle counters as a complete system including operational factors, communications, cabling and power supplies provides an excellent example of an application of the EN procedures with the maximum use of a generic approach.

3.1.2 The introduction of new electronic interlockings in Germany

A similar procedure to that described above was selected in Germany for producing a risk analysis for interlocking systems. A system definition was determined for an interlocking on a non-proprietary basis. Topological/geographical specifics, timetables and other variable aspects were not part of the system definition. Hence, the resulting values apply to all interlockings installed in Germany and are commensurate with the range of present technical standards as long as the input data for risk analysis is observed.

Based on this system definition, the residual risk was established for existing and operationally tried-and-tested systems and the risk tolerability value for new systems was also determined. The functionality of interlocking systems was not affected by applying this specific procedure. This was due to the exclusive determination of technical safety at the beginning of the analysis.

3.2 Comparison of these two examples

Both examples are based on a comparative analysis. A definition was constructed on a generic level for the system to be assessed. The process requires an operationally tried-and-tested system to be investigated and the consequential determination of the residual risk. This established residual risk constitutes the minimum value for a new system being introduced. Based on the generic system definition, the results can be applied to any installed systems throughout a country.

Both British and German procedures are based on the risk tolerability criterion that at least the same safety level has to be met in the new system as is achieved for an operationally tried-and-tested system (i.e. LSSL or GAMAB, see Section 4.6.3.3 of EN 50126). Similar procedures may be found for assessing the safety of interlocking systems being introduced in the Netherlands, Switzerland and Denmark. Possible changes which could result from the new European safety directive have already been referenced above.

In Germany the procedure for defining the tolerable risk for level-crossing protection systems determined the residual risk on the basis of statistical values for systems in operation based on experience of day to day performance of level crossings on public roads. Here again, the same safety level, based on a defined generic system determined for both existing and new systems, serves as the a risk tolerability criterion.

3.3 Alternative procedure for a risk analysis

A different procedure was selected for establishing the risks associated with the radio-based train operating system (FFB). In this case, the system definition for the signalling and safety system was selected for an entire line including the rolling stock (onboard unit) and operators, based around a defined architecture for the automatic train protection system. Values were also determined for the line topology and train movements (timetable, maximum number of movements requiring operator actions, etc.). Consequently, although the results are generic, they are only applicable to lines where the defined restrictions will apply (restrictions in time table, architecture und line topology). The individual risk to a passenger was established by combining the risks emanating from the hazards with the possible extent of damage in the event of an accident.

3.4 Establishing the system definition for risk analysis and possible consequences for the resulting hazard rates

The above examples are all based on a system definition that covers the safety and integrity of the signalling system and includes a risk analysis of operations where the system is radio-based. It should be noted that the risk analysis only covers parts of the rail transport system and the overall tolerable risk is not used as a basis. The situation might change with the implementation of common safety targets within the new Safety Directive of the European Union.

EN 50126 relates to railways in their entirety. If the present-day risk for a total railway operation is used as the tolerability criterion, it would have to be divided up among the individual subsystems of the railways *(Figure 1)*. The sum total of the tolerable risks of the subsystems has to be less than or equal to the present-day risk of the overall rail transport system.

The production of a risk analysis against a specific system definition must therefore take into account the required overall safety objective and the division of the overall risk among the individual sub-systems.

3.5 Considerations of the implications for Risk Analysis Procedure of the quoted examples and non-harmonised sub – system definitions

3.5.1 Consequence for the risk tolerability criteria

In the absence of a comprehensive railway-wide risk analysis the comparative analysis method, as described in the examples above remains today the only practical means by which the subtotal of risks in the various sub systems is established, based on the implicit existing risk within the installed system.

Comparative analysis has another advantage: A risk analysis has to be approved before it can be used for the development and installation of systems. It is easier for an authorized person to approve a risk analysis based on experience with an existing system than to approve something new.

Overall, this risk tolerability criterion (i.e. at least the same safety level as in the system to be replaced) remains the basic criterion for most situations and is the one most recommended by specialists.

3.5.2 Consequences for the system definition

In the present situation, where risk factors and hazard awareness are all-important, a risk analysis should be undertaken for all existing subsystems, taking into account the technology, human factors, the man-machine interfaces and any other special factors resulting from the system design and application.

Considerations of topology or timetable should be excluded,(a benefit of the generic approach i.e. no analysis of specific systems is required in EN 50129). The additional work needed for analysing the risks in the implementation of specific systems is minimal to zero since evidence of the same safety level can be demonstrated generically.

The generic approach, done once for one railway and not for each installation gives the opportunity to make considerable cost savings. Human factors and other special factors have to be taken into consideration in the generic system definition.

3.5.3 Risk analysis of specific applications

The present standards are based on the idea that it is possible to develop solutions especially to fit a risk analysis for a specific installation. The lowest cost solution would be an existing technically approved system, but such a system would be most unlikely to fit the results of a risk analysis for a special installation except by sheer chance. Customisation to meet such requirements incurs very high cost and hence the implication is that risk analysis of specific applications will be associated with higher cost solutions.

A further disadvantage in producing a risk analysis for a specific application is that where modifications to the system (e.g. relating to the number of signals, points and routes) or to the operating methodology are made, the risk analysis has to be repeated. This may lead to different results and the specific technical solution may no longer correlate to the results of the new risk analysis.

In summary it is better to use generic system definitions for risk analysis to get generic results. In the system definition it is necessary to take technical factors and environmental factors into consideration. This will lead to the optimum cost saving for risk analysis and for the resulting technical solution.

3.6 Possible revisions of the standards

Is it necessary to perform a risk analysis at all when replacing a technical system with an architecture and safety philosophy that is similar to that of the predecessor system? If the risk analysis were to be based on the criterion of same safety level, a new system, similar to the predecessor one, will fulfil this condition automatically and a risk analysis will increase costs for no additional benefit.

EN 50129 stipulates with regard to electronic components and systems, that risk analyses have to provide quantitative results in order to determine the necessary SIL. The safety objective is not divided and reduced for random failures although a quite considerable percentage of the tolerable safety risk has to take into account systematic hardware and software (program and data) faults.

Given the inaccuracy of a risk analysis generally estimated to be within one or two orders of magnitude and without any consideration of systematic faults, it is unlikely that this standard constitutes a basis for meaningful results.

Thus, the question is raised as to whether a more qualitative analysis is more sensible within the context of risk analysis for electronic components and systems as used in signalling and whether quantitative analyses can be restricted to special situations and critical areas. The comparison between EN 50126 and EN 50129 in their difference in approach and in the work involved to achieve meaningful risk analyses is very marked and should be subjected to a critical review when these standards are revised.

A further question to be discussed for the next review of the standard is the connection of reliability and safety. In case of a break down of a railway safety system (a part or the whole system) normally the operation of the trains goes on. In this situation the safety of train operation can transfer to human operators with a consequential significant decrease in safety. So the safety of train operation is dependant on the reliability and availability of the railway safety system. For reviewing the standard the reliability and availability of a safety system should be defined as a safety requirement for the system.

Regarding validation of safety requirement see chapter 4.2.

4 Experience with the Process Defined in EN 50128

4.1 Volume of documentation as a result of the process

An important finding gained from initial applications of the present standard concerns the volume of documentation required. The scope of work involved increases considerably compared to that required for earlier specifications, a factor that can be detrimental to the cost without any improvement to the quality of the resulting product. This money could be spent on different activities, for example additional testing of the developed system. In this case a better quality system may result from reductions in systematic failures.

The definition of the documentation to be produced during the development process should be revised and the documentation combined as far as possible.

When new systems are to be developed for railway signalling, a requirement specification may already exist for an existing system which can be incorporated into the specification for a new development. Although the development of an existing system would not normally have been implemented on the basis of the present standards, its documentation and operational data over many years will give a quality of information that could not be achieved from analysis of new requirements alone.

4.2 The importance of involving appropriately experienced people in the validation process

The quality of the requirements is of major importance. They constitute the basis for all the development steps and become the basis for all testing. If the requirements are incorrect or incomplete, faults in the resultant system will result and the formal procedure will be flawed.

Hence, in addition to checking the system with respect to the requirements, a check should also be performed to confirm that the validation method is both understood and within the operational and signalling experience level of the person(s) undertaking the validation. On basis this experience a further check of the requirements for the validated system during the validation process is necessary, too. These factors need to be incorporated when the standard is next revised.

This is particularly important when systems are based on newly produced requirements, as it gives a final opportunity to detect and eliminate any existing faults before the system is commissioned and avoids the very high cost of eliminating emerging faults from commissioned installations.

Despite all documentation and prescribed procedures, the quality of the implemented product or system ultimately depends on the knowledge and experience of the persons involved. The substitution of knowledge by prescribed procedures is not tenable.

EN 50128 should be revised to incorporate the features outlined above.

5 Recommendations

5.1 Application of the Standards

1. The LSSC risk tolerability criterion (i.e. at least the same safety level as in the system to be replaced) is the basic criterion for most situations and is the one most recommended by specialists
2. The use of Risk Analysis should be based on generic system definitions enabling the results to be used for a wide range of applications. The generic approach, supplemented by any necessary application specific analysis, will lead to the optimum costs and resource requirement for risk analysis and for the resulting technical solution.
3. Redeployment of resources from procedures and reports to checking and testing will improve the quality (including safety) of the commissioned system.
4. When replacing existing systems, the requirements for such systems should be incorporated into the requirements for the replacement system.
5. System validation against the requirements and integration information does not guarantee an error free system. Validation should be undertaken only by people with knowledge and experience in developing or checking fail-safe systems and who are able to identify deficiencies in the base information.

5.2 Review and Amendment of the Standards

6. The quantitative risk assessment requirements of EN 50129 take no account of systematic failures which experience suggests are predominant. This should be payed attention of when reviewing the standard.
7. EN 50128 should be amended to include reference to iterative processes in addition to the “V” model.
8. Consider whether it is necessary to perform a risk analysis when replacing a technical system with an architecture and safety philosophy that is similar to that of the predecessor system.
9. The marked difference of approach between EN 50126 and EN 50129 and the work involved to arrive at meaningful risk analysis should be critically examined. The achievable accuracy and relevance of the quantitative analysis as per EN 50129 are questionable and should be reviewed.
10. The reliability and availability of a safety system should be payed attention of as a requirement for a safety system.
11. The definition of the documentation to be produced during the development process should be revised, with the aim of combining reports and reducing the volume of paper.

12. A check should be introduced into the validation process to confirm that the validation method is both understood and within the operational and signalling experience level of the person(s) undertaking the validation.
13. EN 50128 should incorporate a requirement for people with appropriate system knowledge and experience to be involved in the validation process. Competence in understanding the requirements and processes is not enough.

5.3 Consequences of the European Safety Directive

14. System safety objectives must be set as an apportioned part of railway safety objectives within a particular railway administration.
15. It is the responsibility of each railway undertaking and infrastructure manager to define the safety related requirements for new equipment and systems.

Advice:
If there are questions please contact by email the ITC member Peter Stanley:
Ingenica@btinternet.com

Zusammenfassung

Optimierung von Kosten und Sicherheit durch angemessene Nutzen der EN

Es hat sich gezeigt, dass Risikoanalysen, die in Übereinstimmung mit den Europäischen Normen und unter Berücksichtigung der spezifischen Details einer jeden Anwendung ausgeführt wurden, zu einer großen Kostensteigerung für Sicherheitsgenehmigungen geführt haben. Die Durchführung von separaten Risikoanalysen für jede einzelne Installation in einem Land erhöht die Kosten ohne erkennbare Vorteile. Es besteht die Möglichkeit zu beträchtlichen Kostenreduzierungen bei Einführung generischer Analysen.

Formale Prozeduren in Übereinstimmung mit den Europäischen Normen dürften nicht zu einer besseren Qualität der Entwicklung führen. Im Gegenteil könnte die Qualität darunter leiden, dass Ressourcen für umfangreiche Risikoquantifizierungen und deren Dokumentation zulasten anderer qualitätsbezogener Aktivitäten aufgewendet werden, für die hochqualifizierte Signalingenieure erforderlich sind, um eine gesicherte Systemzuverlässigkeit und Verfügbarkeit zu erzielen.

The Authors

The Institution of Railway Signal Engineers (IRSE), is the professional body for all those engaged in, or associated with, railway signalling, telecommunications and allied professions. Founded in 1912, the Institution aims to advance, for the public benefit, the science and practice of signalling

and telecommunications engineering within the industry. It also works to maintain high standards of applicable knowledge and competence amongst the membership.

The IRSE International Technical Committee (ITC) is a forum for development of critical thinking on key technical issues and opportunities within the industry. ITC comprises around twenty senior participants drawn from very diverse national and industry backgrounds, and also benefits from the written input of several extra corresponding members.

ITC communicates with the industry and interested parties through the publication of reports and of technical articles available to the specialist press and published in several languages.

While every care is taken to ensure the accuracy of the content of such publications, some topics are by their nature controversial, and the views expressed are necessarily those of the committee and not of the IRSE as an Institution with charitable status, and the user is responsible for any reliance that he may place on such information.