국제규격에 기반한 철도종합안전대책기술서 개발에 관한 연구

A Study on the Development of Safety Cases Based on International Standards

알란 카스키*	왕종배**	맹희영***	김영상****
Alan Caskie	Wang, Jong Bae	Maeng, Hee-Young	Kim, Young-Sang

ABSTRACT

새로운 시스템이나 제품이 철도운영환경에서 이용할 수 있을 만큼 안전하다는 것은 체계적인 문서화를 통해 입증해야 한다. 이러한 적정성을 제공하기 위해서는 안전성 관련 사항들은 논의에 대한 유효성을 판단하기에 앞서 독립적인 검증기관이나 자체적인 전문 평가를 수행하는 기관(또는 관리기관)에 제시되어져야 한다. 이러한 유효성은 종합안전대책기술서 형태로 제공되어지며 이는 사실에 대한 단순한 열거가 아니라 해당 시스템이나 제품의 실제 사용시 안전하다는 확신을 해당 기관에게 줄 수 있도록 고안되어 있는 일련의 논의들이다. 종합안전대책기술서는 관계자가 시스템 및 제품의 신규도입으로부터 발생되는 모든 리스크에 대한 분석 및 평가 수행여부와 이러한 리스크를 어떻게 관리하고 개선시켜 왔는지를 나타내주는 문서이다. 또한 관리가 효과적이고 지속적으로 적용되었음을 확인하기 위한 관리 시스템을 제시해 주기도 한다. 본 연구는 유럽의 철도산업 범주내에서 종합안전대책기술서 그 자체의 특성과 시스템의 형태 및 적용 가능한 제품에 대해 정의를 내리는데 그 목적이 있으며 기술서의 취지와 구조, 보조문서 및 관련법규에 관한 사항에 초점을 맞출 것이다.

1. Introduction

With ever-increasing complexity and reliance on technology in the railway environment, it is no surprise that the assessment and certification of new or modified systems should also become more complex. Due to the international implementation of these systems, the need for common principles and procedures was essential to ensure that assessments and certifications performed in one country could be adopted by other countries.

In order to achieve this Europe created numerous standards via CENELEC, most notably EN 50126, EN 50128 and EN 50129, describing processes to be followed in order to provide assurance of the safety of all railway operators. In this context, "railway operators" consists of infrastructure controllers and the operators of both trains and stations (this includes suppliers of systems used by these operators). Of the standards mentioned, EN 50126 is the top-level document that covers the overall process, based on the system lifecycle, to enable the implementation of a consistent approach to the management of reliability, availability, maintainability and safety (RAMS) for the total railway system. Activities that are to be conducted by developers and manufacturers are defined in EN 50129. EN 50128 is the software specific "subset" of EN 50129.

In 2002, the International Electrotechnical Commission (IEC) adapted CENELEC standards EN 50126 and EN 51028, which are now recognised in the form of IEC 62278 and IEC 62279 respectively. These standards are now virtually identical to the CENELEC versions but are now more applicable for worldwide usage. The International Electrotechnical Commission (IEC) is the leading global organisation that prepares and publishes international standards for all electrical, electronic and related technologies. The standards published by the IEC serve as a basis for national standardisation and as references when drafting international tenders and contracts. More recently in Korea, the Ministry of Commerce, Industry and Energy has adapted IEC 62278. Although compliance with this standard is not mandatory, it is becoming increasingly common for RAMS requirements to be included in contractual negotiations for new systems and equipment.

* 로이드 레지스터 레일, 비회원, 주저자
** 한국철도기술연구원, 회원
*** 서울산업대학교, 기계설계자동화, 비회원
**** 로이드 레지스터 레일, 비회원
E-mail :young-sang.kim@lr.org TEL : (02)3703-7565 FAX : (02)782-1659

Compliance with the CENELEC standards is mandatory within the European Union and for safety related issues, this is demonstrated via the submission of a Safety Case.

2. Safety Cases

A Safety Case is required for all safety related railway applications, from complete systems down to individual sub-systems and their components, and serves two main purposes. Firstly, it gives confidence to the regulatory authority that the operator has the ability, commitment and resources to properly assess and effectively control risks to the health & safety of staff, contractors, passengers and the public. An example of the regulatory structure within the UK is shown in Figure 1. Secondly, it provides a comprehensive core document, with links to other more specific documents and rules and procedures, against which an organisation and regulatory authority can ensure that accepted risk control measures and health & safety management systems have been properly implemented and continue to be operated in the way originally intended.

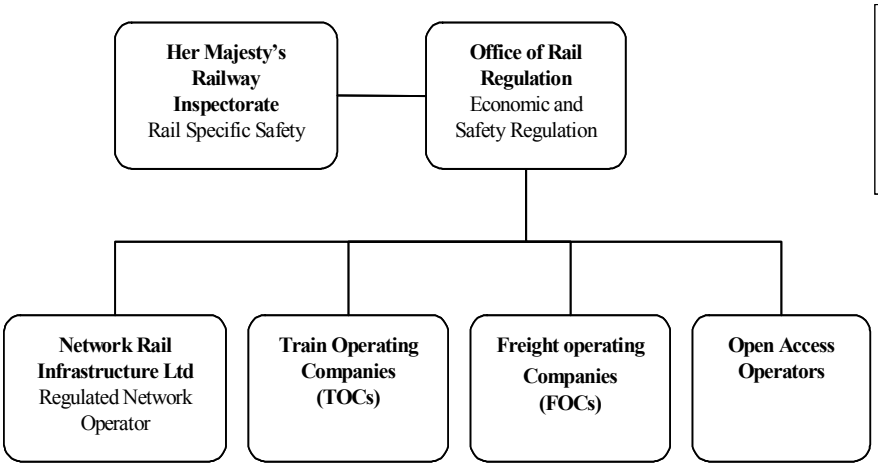

Figure 1 − Regulatory Structure in the UK

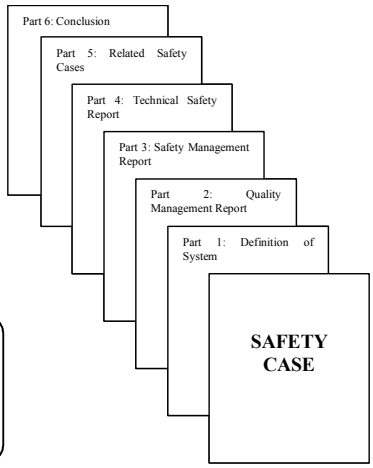

Figure 2 − Safety Case Structure

The preparation of a Safety Case and keeping it up to date requires a systematic approach to managing health & safety, which is essential if risks are to be properly and consistently identified, controlled and minimised as required by legislation.

The Safety Case is a line of argumentation, not just a collection of facts. It aims at convincing a regulatory authority, who does not necessarily have a deep knowledge of the specific technological issues involved, that a given product or system is safe enough to be taken into use. This line of argument will demonstrate that all risks are analysed and assessed and determine show they will be eliminated or controlled as necessary. Alternatively, the Safety Case may be used as evidence in genuine legal proceedings years after the system was authorised and commissioned to demonstrate that adequate analysis was conducted.

Prior to submission to a regulatory authority, each Safety Case should be assessed by an independent third party to verify compliance with all relevant requirements, whether they are contractual, legal or functional. The regulatory authority will then accept or reject the submission based upon their own assessment and the opinions of the third party assessment.

One of the most common problems with Safety Cases is that they are too concise. It is essential that they don't simply just refer to dozens of documents, leaving it up to the assessor to read through them all and extract all the necessary facts and information. The Safety Case must in itself contain enough information to give a clear impression of the system or component's safety properties and indicate where the detailed analysis can be found if required. Therefore, the Safety Case sections that are described in this paper must contain descriptive text rather than just a list of references.

Although EN 50126 defines the process for managing safety, EN 50129 provides guidance on the structure of a Safety Case. Similar guidance can also be found in "Engineering Safety Management" (see Section 4 for further details). The Safety Case sections outlined below are taken from EN 50129.

2.1 The Contents of a Safety Case

EN 50129 provides an extensive description of how Safety Cases should be structured and although the standard is aimed at safety related electronic systems for signalling, the structure is used extensively for the vast majority of submissions. In the following, each section is briefly described. It should be noted that it is perfectly acceptable to let each section be a freestanding document, provided it has the right contents. The main sections of a Safety Case are illustrated in Figure 2 and defined in the following sections.

2.1.1 Definition of System

The first section in the Safety Case is the "Definition of System". It should give a complete and detailed description of the system for which the Safety Case is being presented. EN 50129 states:

"This shall precisely define or reference the system/subsystem/equipment to which the Safety Case refers, including version numbers and modification status of all requirements, design and application documentation."

This means that the definition of system shall contain:

- A description of what the system is, its functionality and purpose, with references to the requirements' specification and other descriptive documents.
- The system or product structure. This is a document that identifies the components of the system and the way they are related to each other and the overall system.
- Descriptions of all interfaces, both external and internal, with references to the corresponding documentation. The interfaces should be traceable to the product structure.
- Issue, revision and date of all applicable documentation and/or versions of components or modules.

It should be noted that this section is a definition of the system, not just a description. Any modification of a component or module will necessitate a new - or at least updated - Safety Case. This also applies to any referenced documents that are updated.

2.1.2 Quality Management Report

This section is a report that describes what has been done to ensure that the system has the required quality management system implemented throughout the entire lifecycle. This involves:

- A description of the quality requirements with reference to the corresponding source documents. These are more often than not generic, company internal documents, but there can also be legislation or regulations that define quality requirements.
- A description of the quality management system with references to the corresponding plans and procedures. In other words, a description of what an organisation intends to do in order to ensure the necessary quality. This must also contain a description of the project's organisation and identify by name the people in the various positions and describe their responsibilities and qualifications.
- A description of what actually was done, with references to relevant documentation e.g. audit reports, minutes of meetings and any other documents concerning the performed activities. In addition, any deviations from the plans and procedures should be described and justified.

EN 50129, paragraph 5.2, contains examples of topics (based on ISO 9000) that should be addressed, but the list should not be regarded as being exhaustive - they are examples that are not always applicable. Where a topic is irrelevant it is advisable to explicitly state this fact and provide an explanation rather than just omitting it. Otherwise, it is likely that the independent assessor will assume that it has been overlooked or

ignored. Conversely, there may be other aspects not mentioned in the list that are significant, so thought should be given to as to what else should be included.

2.1.3 Safety Management Report

This is the corresponding report for safety management. As with the quality management report, the safety management report involves:

- A brief summary of the safety requirements with reference to the safety requirements' specification. The safety requirements'specification may be, and often is, a subset of the requirements' specification rather than a separate document. In this case, the relevant parts of the requirements' specification shall be identified. In addition, there will be standards, laws and regulations defining general safety requirements. These must also be identified.
- A description of the safety management system with references to the corresponding plans and procedures. In other words, a description of what the organisation intends to do in order to ensure safety.
- A description of what actually was done, with references to relevant documentation e.g. the hazard log, safety audit reports, test reports, analyses and any other documents containing evidence of the activities that were performed. In particular, the way the hazard log is managed must be described. In addition, any deviations from the plans and procedures should be described and justified.

EN 50129, paragraph 5.3, contains examples of topics that should be addressed. It is worth noting that this standard makes the safety management process described in Section 5.3 mandatory for Safety Integrity Levels (SIL's) 1 to 4. In particular, this means that a hazard log shall be maintained throughout the entire lifecycle of such systems. EN 50126 should be referred to for a description of SIL's and the system lifecycle.

2.1.4 Technical Safety Report

This is the section where the technical safety characteristics of the system are described. It should describe the underlying methodology for achieving safety and identify which safety standards have been applied. The safety relevant properties of the system should be presented and reference made to the corresponding evidence, i.e. test and analysis results, verification and validation reports, certificates etc.

EN 50129, paragraph 5.4 and Annex B identify the topics that should be addressed. Some of the topics may not be relevant for a particular kind of Safety Case, but as in the quality management report, it is wiser to state this explicitly. Annex B also requires that the Technical Safety Report "shall be arranged" under the headings given in the standard but as additional topics may be included, there may be slight deviations from this arrangement.

2.1.5 Related Safety Cases

Any corresponding Safety Cases relating to the safety of the system should also be identified within this section. In such cases, any restrictions or application conditions mentioned in those Safety Cases should be summarised for clarification.

It should be noted that this also applies when there is a previous version of the system for which a Safety Case already exists. By doing this, the production of a Safety Case for an upgraded system can be considerably simplified. Since the previous version's Safety Case contains all the relevant information for that version, only the changes from the previous to the new version need to be described. In addition, evidence must be provided that the modifications have not adversely affected the safety properties of the rest of the system that has not been modified.

"Related Safety Cases" can also refer to certificates for parts or components, since such certificates will themselves be based on documentary evidence of the relevant safety properties.

2.1.6 The Conclusion

This section should be more than just a statement that the product is sufficiently safe. EN 50129 states:

"This shall summarise the evidence presented in the previous parts of the Safety Case, and argue that the relevant system/subsystem/equipment is adequately safe, subject to compliance with the specified application conditions."

The conclusion is fundamentally the summary of the evidence presented in the previous sections and the argument for the system's safety. This is where the justification shall be given that the quality and safety management activities were adequate, that the technical properties satisfy the safety requirements and that the conditions imposed by any related Safety Cases have been adequately taken into account. Any restrictions, limitations or assumptions that were made should also be stated here.

2.2 Producing a Safety Case

The volume of documentary evidence that the CENELEC standards requires is substantial, and producing a Safety Case can be a daunting task. However, it should be remembered that a Safety Case is really a line of argumentation, and most of the necessary information should already exist. For example, the "Definition of System" contains the information that has already been included in other documentation. Specifications, interface descriptions and similar facts are part of normal engineering work, and producing and maintaining the list of applicable documents is a typical configuration management task.

This should be the case for most sections within a Safety Case with the possible exception of the Technical Safety Report. This is the section where all the technical data has to be adequately assessed using appropriate modelling and analysis techniques. Some of this information will be available from suppliers and manufacturers but will have to be inserted into the context relative to the safety argument.

The section on related Safety Cases is fundamentally part of the design documentation. If previously approved systems or components are used, the corresponding documentation should be easily identifiable.

Finally, the conclusion is something that needs be developed but is merely a summary of the argument that is made throughout the Safety Case and shouldn't include any data or information that hasn't been included in previous sections.

2.3 Different kinds of Safety Cases

It is possible to re-use many parts of a Safety Case for multiple projects, systems or components. Generic descriptions are often included in some sections (e.g. Quality Management Report) which will not change substantially and will require minimum effort to amend.

Additionally, complex technical systems consist of less complex sub-systems, which in turn will consist of components that are even less complex. Hence, this inevitably leads to a hierarchical structure within a system. When Safety Cases have been produced for the components and sub-systems in the lower levels of a hierarchical system, they can be used on multiple occasions, in all higher level combinations. The same will apply to the products on the next hierarchical level, all the way up to the final product or system. The higher up the hierarchy you get, the less you have to prove, because most of the proof is already contained in the lower level Safety Cases.

Similarly, if a product, for which a Safety Case already exists, is modified, the new Safety Case can be based on the existing one. Acceptance would only be required for amendments made and their effects on the system or product. This is evidently considerably less work than producing a whole Safety Case every time.

3. The benefits of using a Safety Case approach

The CENELEC standards provide a clear and uniform way of presenting the evidence that a given product or application is safe to use. For the assessor, a well-structured and complete Safety Case will greatly simplify his task, shortening the time he needs to produce his report.

Similarly, gaining approval from the safety authority will also be simplified. When the Safety Case is clear and easy to understand, all they need to look for is the independent assessment report confirming that what is included in the main body of the Safety Case is, in fact, true. Hence, it is unlikely that they will require

further documentation in order to become convinced of the product's safety.

For specific applications and products, a single Safety Case can be used in numerous systems and projects as approval would have been provided on other systems. This also has the benefit that operational data can also be taken into account in order to justify the safety arguments contained with the Safety Case.

4. Supplementary Guidance

Engineering Safety Management (commonly known as "The Yellow Book") was originally produced by Railtrack (now Network Rail) in the UK to assist individuals involved in making changes to the railway environment to ensure that these contributed to improved safety. Although the book is not recognised as a regulatory document, the principles and guidance contained within it will help ensure that good practice is adhered to and, if followed, will typically result in compliance with relevant safety standards.

Furthermore, several European countries have now adopted a similar approach based upon the "The Yellow Book" in order to implement and manage processes in a logical manner. These processes provide an element of confidence that legal responsibilities are addressed and documented evidence is available to substantiate this claim.

5. Conclusion

A Safety Case should be viewed as an integral part of the safety management process and be the pivotal basis for the safety argument. It is vital that the document is not regarded as a list of references and clearly sets out, in a logical structure, a summary of the detailed analysis undertaken throughout the lifecycle of the project.

The CENELEC approach (and adopted by the IEC) enforces a transparent and effective means of producing and documenting safety related systems and components. However, this in turn leads to more efficient and consistent approval processes that are often widely applicable.

It is probable through the progression of time that a Safety Case regime, if adopted, will become increasingly simpler as they will be based upon already existing and approved Safety Cases. In theory, this should facilitate and accelerate both the production and the authorisation processes.

From July 2007, the Korean Railway Safety Act will require that all railway operators in Korea perform risk management in order to effectively and systematically manage risk within the railway environment. Hence, it will be essential that safety documentation is developed to help demonstrate compliance with The Act. To assist with compliance it is recommended that the processes and procedures contained within these standards are adopted and implemented on all changes affecting the safety on the Korean railway network.

References

1. Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS), CENELEC EN 50126, September 1999.
2. Railway applications - Communications, signalling and processing systems. Software for railway control and protection systems, CENELEC EN 50128, March 2001.
3. Railway applications - Communication, signalling and processing systems. Safety related electronic systems for signalling, CENELEC EN 50129, 2003.
4. Engineering Safety Management, Issue 4, 2005.
5. Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS), IEC 62278, 2002
6. Railway applications - Communications, signalling and processing systems - Software for railway control and protection systems, IEC 62279, 2002
7. Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS), KSC IEC 62278, September 2004
8. "What is a Railway Safety Case?", HSE Seminar: Railways (Safety Case) Regulations 2000
9. "Undertaking a Safety Case in a Rail Environment", Odd Nordland, SignalComm Europe
10. Railway Safety Principles and Guidance, Part 1, Her Majesty's Railway Inspectorate
11. Korea Railway Safety Act, Ministry of Construction and Transportation, December 2005