



Electronic Safety Case: Challenges and Opportunities

Trevor Cockram, Ben Lockwood

Publication notes

Copyright © 2003 Praxis Critical Systems Limited and Raytheon Systems Limited

Electronic Safety Cases: Challenges and Opportunities

Trevor Cockram Ben Lockwood
Praxis Critical Systems Limited Raytheon Systems Limited

Abstract

This paper describes the use of electronic formats for safety cases to meet the requirements of a number of military and civil standards. The challenge to safety engineers is to produce safety cases that are quickly readable, intelligible and auditable even when a large amount of material is required. We describe the problems in developing complex safety cases using traditional development methods and the opportunities to address these problems by the development of an electronic safety case. We then describe an example eSafety Case and how this can be used to manage a safety programme and to produce a safety case that will meet the requirements of the certification authorities.

1 Introduction

The provision of a safety case is a requirement of many standards [HMSO 1992, MoD 1997, MoD 1996, HSE 2000]. A Safety Case presents the argument for the safety of a system and summarises and justifies the supporting evidence. A Safety Case is an input to the safety approval process for a system. The body responsible for safety approval will consider all relevant safety submissions, primarily the Safety Case and supporting documentation such as reports of Safety Audits and Assessments, in order to satisfy themselves that the system is adequately safe and conforms to the relevant international, national and industry safety standards.

The detailed content of a safety case can vary, but in this paper I am referring to the body of information that makes the case that the system is safe. This includes:

- defining the system, including the system boundary and the system architecture and functionality;
- identifying the development and safety management plans;
- providing the logical argument that shows that the system is safe based on the evidence available;
- detailing the hazard and accident identification, causal and consequence analysis;
- demonstrating that risk reduction has been carried out to an acceptable level, with resultant closure of hazards;
- defining safety requirements and methods of verification; and
- describing any limitations and caveats; and the final conclusion on the safety of the system.

The provision of safety cases has resulted in an ever increasing workload for equipment producers (to produce the safety cases and manage their contents), and also for independent assessors and regulators (who are required to assess safety cases). Typically a safety case for a moderately sized system, along with the reports that constitute the primary supporting evidence, can result in a pile of paper several inches thick (larger systems safety cases have filled library shelves).

The challenge to safety engineers is to produce safety cases that are quickly readable, understandable and auditable even when a large amount of material is required. Fortunately opportunities exist to de-risk the safety case development process by presenting the safety argument for review early in the programme and building up evidence incrementally throughout the development and use of the system.

2 Safety Case Problems

The problems of developing and using a safety case, apart from the obvious one of carrying out adequate safety analysis and hazard mitigation, include the following:

2.1 Paper-based Safety Cases

2.1.1 Ease of Navigation

A typical safety case for a single piece of equipment is of the order of six inches thick and starts with hundreds of pages of system description. This can have the effect of immediately switching off the reader, as it is not clear where the relevant safety information can be found.

2.1.2 Ease of Drilling Down

Another issue in paper safety cases is the difficulty of finding a trace through the information provided, for example the accountability and competency for the safety decisions made.

2.1.3 Configuration Management/Control

It is often the case that the material with the safety case comes from a number of different processes and tools. This can lead to a major document management task and difficulty in generating and maintaining a common baseline for the material. The issues include unique identification of, and access to, documents (including specific versions of them). There is also a potential problem with organising the information with sufficient indexing and referencing mechanisms to allow the reader to find all the relevant information.

2.1.4 Diversity of Information Packaging

It is also difficult (or even impossible) to maintain a consistency of presentation. A problem often comes with the use of a proprietary hazard log tool that is only capable of producing reports in a single format that is impossible to embed within

another document. This often results in additional summary hazard reports being written to overcome these shortcomings, but result in an amount of nugatory work.

2.1.5 Ease of Packaging and Delivery

Large paper-based safety cases are unwieldy, which results in large volumes of paper being generated, collated and being sent to the interested parties. The resulting safety case is bulky, not in an easily readable form and difficult to modify.

2.2 Clarity of safety argument

With many safety cases there is a problem with the clarity of the safety argument and links to the rest of the content of the safety case. The safety argument is often buried in sections of the detailed text and not easily traceable to the supporting evidence. The individual threads of the safety argument may also be dispersed through the levels of documentation provided.

2.3 Multiple certification standards and processes

Many systems are developed with the intention of dual or multiple uses. The consequence is that a system is certified for one use and there is a large translation task to make the safety certification and information acceptable to another certification body. In practice, the safety data required for different certification bodies is similar, i.e. to show that the likelihood of hazards has been reduced to an acceptable level and that the processes used for development are appropriate. The differences in certification compliance therefore can be addressed through the development of a cross-reference index for compliance to each standard.

2.4 Dealing with multiple variants

Much of our work is associated with the development of safety cases for equipment that is used in the rail industry, civil and military aviation (both on the ground and airborne), and the finance sector. The equipment is often characterised by large numbers of variants and applications. The safety management for the project needs to take account of the high degree of re-use within the equipment and functional designs to provide a consistent and cost effective means of conducting the safety management and the delivery of safety cases.

3 Overview of the eSafety Case Approach

With a large amount of material to manage, the intuitive approach is to treat the safety case as an intranet and to manage and link the material together by means of hypertext. The idea of using hypertext to link information with a safety case is not new, see for example [Brown R 1998], however, the challenge is to address the issues of complex safety cases in an efficient manner to provide a safety case which is manageable, auditable and acceptable to the certification authorities.

The overall approach is based on the use of an electronic presentation of the safety case using standard PC browsers and plug-ins. This provides a readily available and common platform for presentation – removing the need for bespoke tools.

3.1 The single document approach

One of the problems with current safety cases is that the information is generated throughout the system development; it is often diverse and presented in various formats. In addition, standards require that various safety documents be produced at stages of the development without necessarily a view to the ultimate goal of an acceptable safety case. The approach we have used is to use an electronic safety case that provides a single electronic document that presents the safety information for the system at various points during the programme lifecycle. This performs the traditional function of a safety case, but also contains each of the documents required during the safety lifecycle. By using a single evolving document like this, the consistency of safety information is maintained with a view of reaching the ultimate goal of an acceptable safety case. One of the benefits of a safety case with electronic links to the key supporting information during the development process is that the readers can see how the safety case is developing and take steps to plug any gaps which become apparent. By making the intentions of the safety case clear early in the system development programme, the risk of substantial rework to obtain certification at the end of the process is considerably reduced.

In this way the eSafety Case can perform the functions of the following documents:

- Safety Case, including safety argument and supporting evidence
- Safety Plan
- Preliminary Hazard Analysis
- System Hazard Analysis
- Hazard Log Report
- Safety Requirements

3.2 The Electronic Safety Case

The key navigational elements of the electronic safety case are:

- The overall presentational structure (chapters/sections of the safety case) presented through a menu bar.
- The safety argument (presented in Goal Structured Notation), which provides a means of navigating from a specific safety argument goal to the assumptions, strategy/justification and the supporting evidence.
- The hazard log (included in the safety case structure) that provides a traceable route to the individual assessments, mitigation approaches, safety requirements and evidence related to the specific hazards.
- Other hyperlinks used as appropriate from the detailed pages.

Information is generated in one of the following ways:

- General Textual or Graphical Information: produced using standard office tools and incorporated into HTML pages.
- Database or other Tool Outputs: many tools allow reports to be generated in an HTML format and these can be easily incorporated or massaged by standard scripts into usable components of the safety case.
- Reference to PDF documents: most systems using browsers are set up with the Acrobat Reader plug-in which allows reports to be easily included in the safety case format.

A particular safety case is based on:

- Common Skeleton: which includes all pages that can be reused for all variants and/or views (much of the common skeleton can actually be common to different programmes in our experience).
- Variant Specific pages: which address issues, methods or items which are only applicable to a particular variant of the system .
- View Specific pages: which address presentational issues with respect to a given safety case view (reflecting for example Def Stan 00-56 [Mod 1996] format, or a JSP 430 safety case format [MoD 1996-2]).

Clearly there is benefit in maintaining a significant amount of re-use through the common skeleton if variants or views are required. The development of our safety case is based on an incremental approach where:

- A skeletal safety case framework is built early on (partly off-the-shelf).
- A hazard log database is developed and maintained.
- An initial safety argument is developed.
- 'Builds' of the safety case are carried out at appropriate times during the programme to reflect the current snapshot of the safety case.

3.3 Improving the safety argument

Electronic Safety Cases provide improved safety arguments in several ways. The argument can be represented graphically in the form of a goal structured notation argument, which can be structured into a number of linked hypertext pages so that each section of the argument can be clearly seen. Supporting text can be provided on each page to provide a commentary on the graphical argument. Safety case navigation can also be improved by making the graphics hypertext sensitive so that the user can link directly to the evidence and data that support the argument.

3.4 Dealing with multiple certification standards

It is possible to generate alternative views in the format of hypertext navigational structures of the safety data held within the safety case to show the information in a form that the certification body finds acceptable. As an example, a system

containing software has been developed to Defence Standard 00-55 [MoD 1995] SIL-2 requirements. One view of the safety case provides all the requirements of a safety case to this standard. Another view of the safety case shows a safety case for certification to RTCA DO178B level C [RTCA 1992]. The mandatory documents for civil certification, i.e. the Plan for Software Aspects of Certification, the Software Accomplishment Summary and the Software Configuration Index, uses the same information as in the Def-Stan 00-55 safety case but rearranged into a form to meet the civil certifiers expectation solely by means of hypertext links. Both the civil and military certification authorities have accepted this approach and noted that the electronic safety case made their jobs easier.

3.5 Dealing with multiple variants and applications

In projects where there are multiple variants and applications it is desirable that a common safety case be developed and modified as required. This implies that safety cases that are based on a re-use model would be the most efficient means of forming the large number of safety cases required for the equipment in the various variants and applications. We have developed a re-use model using the principles of domain analysis applied to the equipment requirements.

This analysis identifies the domains of the requirements, ie whether they are:

- a) Common to all applications;
- b) Specific to equipment variants and options;
- c) Common to a generic application types;
- d) Specific to a single application incidence.

Hypertext technology is used to manage the safety case arguments and supporting data in a configurable form. This approach allows a user of the safety case to browse it for the particular configuration of the equipment that is of interest. The configurable version of the safety case proposed is to be delivered either as a computer file which can be browsed by standard browsing tools such as Internet Explorer, or a printed copy of the output of the specific configuration of the equipment.

The contribution to the platform safety cases will follow a similar approach, i.e. taking a subset of the equipment safety case together with the generic platform and specific platform configuration

4. An example eSafety Case

One of the points about the electronic safety case is that it should be accessed via a computer and therefore in the printed form it is difficult to show its functionality. An example electronic safety case will be demonstrated at the Symposium. More

on-line information about the example electronic safety case can be found at www.esafetycase.com.

4.1 System description

This is an eSafety Case produced for a totally fictitious system: The Totally Imaginary System (TIS) Programme is for the design, production and installation into system platforms of equipment that includes a secure encrypted radio, and to provide in-service support of the TIS equipment. The new equipment, consisting of Communicator and Transmitter products, will replace the existing equipment where fitted. The systems will include Frequency S functionality (selective, data-link mode) and have been designed with the capability to incorporate future technology.

4.2 Management summary

The first page of the electronic safety case shown in Figure 1 is the management summary that gives the background of the system, the standards to which the safety case is being developed, links to system description and argument, the conclusions and any limitation and caveats that apply to the safety case. You will also note in the layout that there is a navigation frame that appears in each safety case page to allow the user direct access to the principal sections of the safety case.



Figure 1. eSafety Case for the TIS Transmitter – Management Summary.

and back it up with evidence. This helps to de-risk the safety case development programme.

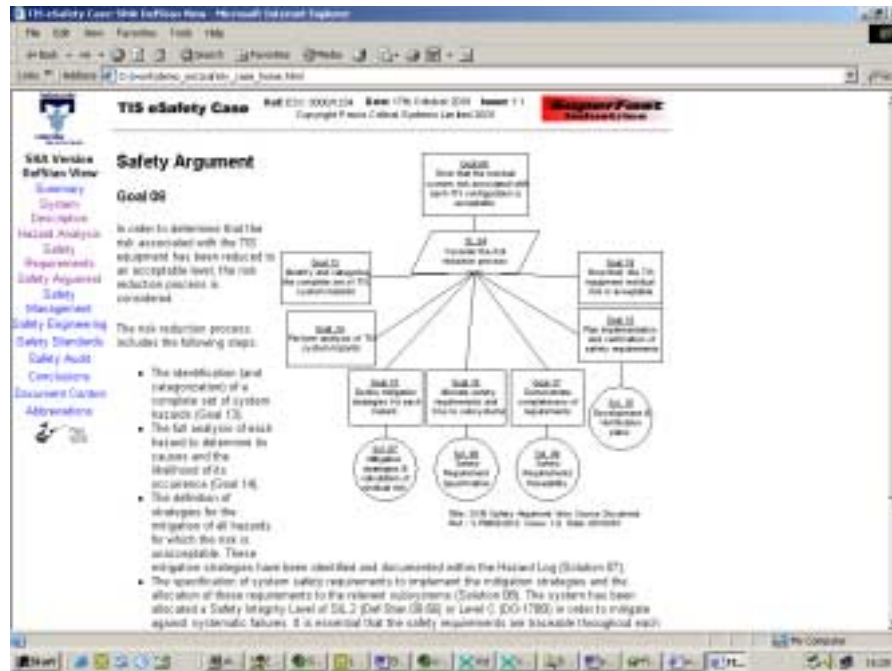


Figure 3. eSafety Case for the TIS Transmitter – Safety Argument.

5 Further considerations

Using an eSafety Case is not a silver bullet to solve safety issues. The following issues need to be considered before using the eSafety Case approach.

1. Only as good as the underlying SMS process.
2. Configuration and quality of data.
3. Review and user testing.
4. Tools and Build Automation.

5.1 The safety management process

An eSafety Case helps with the presentation of the safety argument and supporting information. It does not provide the means of generating the contents of the safety case. Applying an adequate safety management process is necessary to develop any safety case. The eSafety Case can have the effect of quickly and clearly identifying

any weakness in the hazard identification process, the safety analysis and in the material that supports the safety argument.

5.2 Data Management

The material that makes up the eSafety Case requires careful configuration management to ensure that the links within the case point to the correct version of the data. Data within a developing project will change and the eSafety Case must reflect this. A suitable configuration management tool is essential to hold and control the data.

As data is used its quality must be assessed to ensure that the safety argument remains valid and correct.

5.3 Review and User Testing

Before an eSafety Case is released the safety case developer must comprehensively and systematically review it. The nature of an eSafety Case makes this difficult, however it is easy for the eSafety Case user to “drill” down through the links to follow a specific trail. A systematic process is therefore required to review the content of every page contained within the eSafety Case and testing needs to be undertaken to confirm that the case is readable and that the links are made to the correct place.

5.4 Tools and Build Automation

One of the philosophies behind the eSafety Case is to reduce the number of tools required to use the safety case to a minimum set which will normally be readily available on all PCs (for example Adobe Acrobat Reader and HTML browsers).

The developers may have preferences for certain tools (e.g. database and analysis tools). We have tried to separate out the management of items such as a hazard log database from the safety case build process by utilising HTML export and other filters to ensure that the main build and test process is not constrained by the underlying toolset.

We have extended this idea as far as possible in the generation of the eSafety Case, however, it is necessary to link the data from a number of different tools together. We also know that users will have preferences for particular proprietary databases, analysis tools etc.. The approach we have used is to automate the eSafety Case build process and to make it possible to tailor this build process as much as possible.

6. Conclusions

We have used this approach for the development of safety cases on a number of projects most notably the Successor Identification Friend or Foe programme where eSafety Cases have been produced and accepted by both the military and civil certification authorities against a number of different standards including Defence Standards 00-55 and 00-56, JSP430 and RTCA DO178B.

The response of both the certification authorities and system development teams to the eSafetyCase has been very positive. They have welcomed both the physical ease of use and the content presentation as a major advance.

The initial experiences using this approach have been encouraging. We expect to develop our supporting tools further to streamline build and test processes. We expect to continue learning from the feedback received on the current safety cases from both our immediate clients (developers) and their customers. In particular, we have received feedback suggesting:

- A rolling safety case (living as a document) could support the programme safety management activity as a planning and monitoring tool.
- Much of the structure and content of the safety case is generic and can be re-used for new programmes
- A similar approach could be adopted for other system documentation.

Acknowledgements

The authors would like to thank Ross Wintle for writing the software to allow many of these ideas to be implemented and John Harvey for helpful comments on the process and content of the paper.

References:

[Brown R 1998] - Improving the production and presentation of safety cases through the use of Intranet Technology R Brown in Industrial Perspectives of Safety-critical Systems ed Redmill and Anderson Springer 1998

[HMSO 1992] Offshore Installations (Safety Case) Regulations 1992.

[HSE 2000] Railways (Safety Case) Regulations 2000 Health and Safety Executive.

[MoD 1997] Ministry of Defence Directorate of Standardization. Defence Standard 00-55 Issue 2: The procurement of safety critical software in defence systems.

[MoD1996] Ministry of Defence Directorate of Standardization Defence Standard 00-56 Issue 2: Safety Management Requirements for Defence Systems.

[MoD 1996-2] Ministry of Defence Ship Safety Management Office JSP 430 Ship Safety Management System Handbook Volume 1 Issue 1

[RTCA 1992] Software Considerations in Airborne Systems and Equipment Certification RTCA DO178B Requirements and Technical Concepts for Aviation.