

Reuse of Safety Case Claims - An Initial Investigation

David Bush[†] and Anthony Finkelstein[‡]

[†] National Air Traffic Services Ltd & UCL, [‡] University College London

Abstract: Many of the industries involved in safety related or safety critical systems development use Safety Cases to record and present their rationale for believing that their system is acceptably safe. Such Safety Cases are costly to produce and represent a significant investment of effort. Increasing trends to reuse components - evident strongly in the communications domain - has prompted practitioners to consider the reuse of relevant Safety Case claims previously. This paper reports the results of a case study examining the pre-requisites of, and scope for, industrial and corporate reuse strategies and whether current tools and techniques would support such an approach.

1 Introduction.

Organisations responsible for developing safety critical and safety related systems have a legal and moral responsibility for satisfying themselves (and often their regulators) that the system to be put into operation is sufficiently safe. It is increasingly frequent for them to discharge this responsibility through the production of a Safety Case. While the structure, content and format of safety cases varies across industries and even between industries, the intent remains the same. A Safety Case is intended to present a convincing argument that the system will be acceptably safe in operation.

In spite of the variations between and within industries, there is an increasing convergence of opinion on what the elements that make up a Safety Case should be. Bishop and Bloomfield [¹] describe these elements as:

- **Claim** about a property of the system or some subsystem.
- **Evidence** which is used as the basis of the safety argument. This can be either facts, (e.g. based on established scientific principles and prior research), assumptions, or sub-claims, derived from a lower-level sub-argument.
- **Argument** linking the evidence to the claim, which can be deterministic, probabilistic or qualitative.
- **Inference** the mechanism that provides the transformational rules for the argument.

The requirement to satisfy oneself as to the safety of a system applies no less where that system has been developed with re-used or Commercial-Off-The-Shelf components. This is a practice strongly followed by both vendors and systems integrators in the procurement of communications components for safety related systems. Both purchasers and vendors can see the potential for economies if evidence can be reused, as the production of safety cases is an expensive and time consuming process. It is therefore natural to enquire whether an increased application of reuse may well be able to benefit from the reuse of claims from other safety cases where the reused artefact has been applied. Some of the arguments advanced for such reuse seem to be particularly relevant to developers of safety related systems^φ:

- **Error rates will be lower:** Reused components can often be used in more diverse situations than specifically written code. This means that more of the residual errors will have been identified and removed.
- **Better statistical evidence is available:** Reused components can typically accrue more running time, offering a chance for valid statistical evidence of reliability to be achieved, even at high reliability levels.

^φ Such benefits clearly require a metrics system and a defect reporting and corrective action scheme (DRACAS).

2. Issues in Assuring Reused Components

Addressing the issue of assurance of COTS components, Lindsay & Smith [2], suggest three areas developers need to consider when seeking to reuse components in safety related and safety critical systems:

- Verifying the specified behaviour, and eliminating or being robust to unspecified behaviour.
- Validating the safety of specified behaviour in the new operational context.
- Continuing to ensure safety as the re-used component changes.

These are often not trivial problems in using COTS components, where the end user often has no access to development artefacts such as design documentation and source code, nor control over the fault reporting and corrective actions undertaken by the supplier. They also mean that the benefits of reusing Safety Case claims or evidence, even in the case of internal reuse only come at some cost.

3. Issues in Safety Case Reuse

Kelly & McDermid[3] assert that

It is not uncommon for an engineer, having recognised a similarity, to plunder a previously developed safety case to help in the development of a safety case in a new project. In some cases, the engineer may believe certain elements of the two projects to be sufficiently similar to actually "cut-and-paste" parts of the original documentation and subject them only to minor review and modification.

Anecdotal evidence across a range of industries would seem to support the existence of this informal form of reuse. Such reuse is not necessarily wrong, but suggests potential problems both in the process of Safety Engineering and its product (the new Safety Case). The problems in the process arise because practise is ad-hoc and inconsistent in the organisation. Problems may arise in the product because the new context of the component may not be taken into account and no link is established between the original and reused safety evidence - if the former were to be found in error, how would the latter find out about it?

Even where reuse can be formalised, there are likely to be benefits and concerns. For example

- It means more eyes on evidence - errors are more likely to be found.
- It means a lack of diversity - many people could use erroneous evidence.
- It means building up field service experience evidence.
- It creates implications for responsibility of a developer is applying someone else's evidence

4. Pre-requisites for Reuse

If reuse of safety evidence is going to be achieved in a defensible, structured and repeatable way there are a number of pre-requisites that must be achieved:

- **Taxonomy:** We must be able to classify the information elements that comprise a safety case, so that we have a common understanding of the information it contains, and what that information means.
- **Information Model:** We must define a model of our information, and rules for relating it. We have previously identified the importance of context information in reuse, so our model must support this. Our model must be modular - i.e. it must allow progressively more detailed claims to be described and understood, and therefore be identified and reused. This is important because it is likely that, if reuse of evidence is possible, it is probably at quite a detailed sub-component level - where the restrictions of the context of use are either more easily understood and hence argues about, or where the context is more similar between systems.

- **Standardisation:** Our safety cases must conform to our information model. This will have significant impact on legacy safety cases - and it may not prove worthwhile to convert these into a new format.
- **Storage & Retrieval:** Our safety cases must be stored, be retrievable, searchable and support tracability. Furthermore, reuse will be easiest if we can integrate the editing, storage and searching capabilities into a support tool.
- **Information Availability:** It is axiomatic that safety information must be available if it is to be reused. In the case of internal reuse, such information may be available although for legacy systems whether it is available in a useable form may be an issue. However, in the COTS case it is possible that the vendor would not be willing to make available all their information - particularly at a sub-component level - for use outside of their own systems.

5. Tools and Techniques for Reuse

Some of the pre-requisites described above are beginning to have robust solutions for example Kelly^[4] has used GSN to present safety cases, which provides a comprehensive information model supported by a graphical approach to encoding and relating types on information in a Safety Case. A highly simplified extract of a Safety Case using GSN^φ is shown in Figure 1 below.

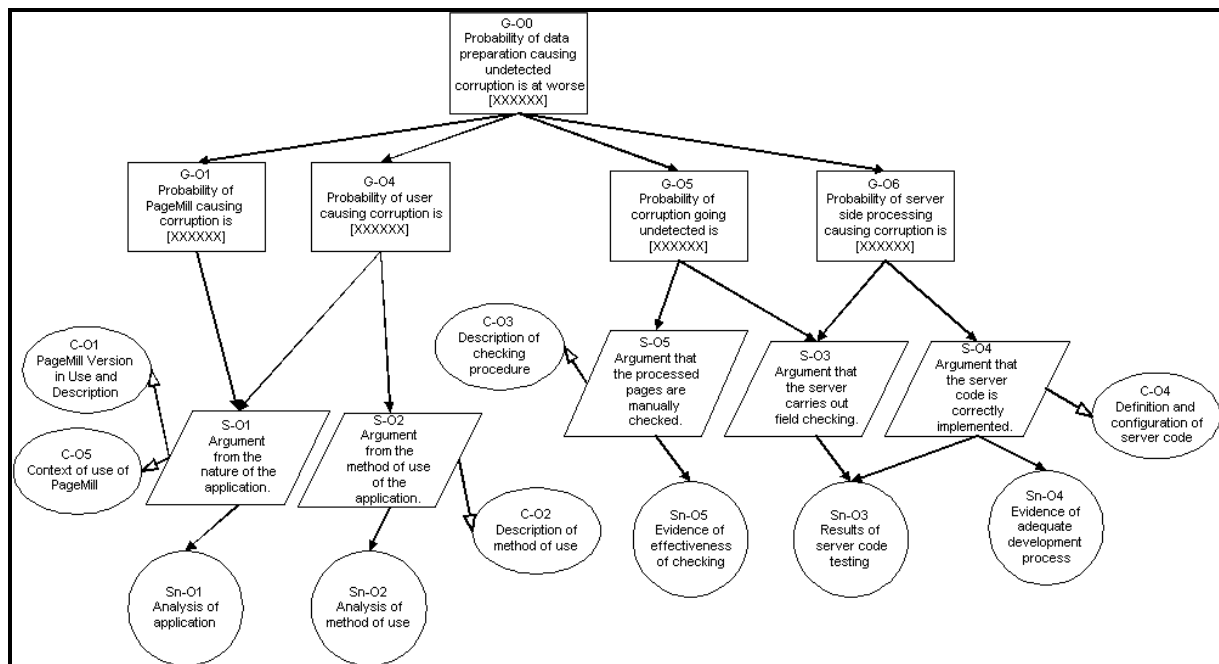


Figure 1 - Extract of GSN Safety Case

This illustrates how reuse might be possible using such a notation. The top-level goal (G-00) shown states one of the requirements on the system - to have a worse case probability of data corruption. This goal is (in this case) refined to sub goals (G-01 to G-06) based on a decomposition of the goal.

The system in question allows an operator to use the 'PageMill'[®] application to create a page of information, which is then checked and processed on the server before being published. In this case it is evident that it may be possible to reuse a number of the claims (Goals) made about the parts of this process.

^φ In the interests of readability, some goals have been omitted from the extract (G-02,G-03). In the interests of brevity, arguments (e.g. S-01) have been linked directly to evidence e.g. (Sn-01) - which is not normally best practice. In the interests of confidentiality, some information has been replaced by [XXXXXX].

For example the claim in G-01 may be reusable in any system using PageMill®, provided that the version is the same (C-01); the context of use is the same (C-05) - or that evidence can be presented in the new Safety Case that differences in these areas are not relevant. This would be an example of reusing evidence based on a COTS product. Similarly in the case of internal component reuse, reuse of claims about server side processing may be possible.

Tool support for notations such as GSN is becoming increasingly mature. Two leading tools for this have been examined. The Adelard Safety Case Editor (ASCE)⁵ supports the ASCAD notation as well as GSN and YSE's Safety Argument Manager (SAM)⁶ provides similar support. However, the degree of support that such tools provide is currently a little too limited for them to fully support corporate reuse of Safety Case claims. In particular the following functionality is needed:

- **Network Support:** Tools will need to be capable of being used in a corporate network setting - with multiple users capable of accessing and editing information.
- **Tracability Support:** Tools will need to provide tracability from Safety Cases to the instances of reusable claims on which they call, audit trails of changes to claims and the connections made to them and comprehensive change notification mechanisms when referenced claims are changed.
- **Search and Retrieval:** Users will need to be able to search and retrieve claims stored in the tool in order to assess their relevance and veracity.

Such functionality is readily available in tools supporting more mature areas of systems engineering, such as Requirements Management tools, and as Safety Case presentation, and the associated editing tools become more mature it is possible that vendors will seek to implement such capabilities if the demand exists.

6. Conclusions

This case study has identified significant benefits likely to accrue if corporate reuse of safety case claims can be made to work. Not only could it result in less costly Safety Cases, but the quality of the claims, and the significance of Field Service Experience evidence called up would also improve. However the practicality of reuse is called into question by: the fact that evidence at the appropriate level of detail may not be available for COTS; legacy safety cases may not be correctly structured to provide reusable claims and, while recent tool support moves a long way towards providing the necessary taxonomy and graphical editing capability, some of the more specialist support required for reuse is not yet available.

Nonetheless, the case study did identify a number of types of safety claims that were candidates for reuse in other projects - particularly in the case of families of similar systems, and highly prominent among these were communications systems components. Whether such benefits merit either industry wide or company wide reuse in general remains to be ascertained!

References

¹ A Methodology for Safety Case Development, Peter Bishop & Robin Bloomfield, Safety-Critical Systems Symposium, Birmingham, UK, Feb 1998.

² Safety Assurance of Commercial-Off-The-Shelf Software, The University Of Queensland, Technical Report No. 00-17, Peter Lindsay and Graeme Smith, May 2000

³ Safety Case Construction and Reuse using Patterns, Kelly & McDermid, Proc 16th Int Conf on Computer Safety, Reliability and Security (Safecomp '97)

⁴ Arguing Safety - A systematic approach to managing safety cases, TP Kelly, YCST 99/05, Sep 98.

⁵ <http://www.adelard.co.uk/software/asce>

⁶ <http://www.yse-ltd.co.uk/index.html>