SUPPORTING EXPLICIT INTERPRETATION OF STANDARDS AND GUIDANCE

Z. R. Stephenson*, J. A. McDermid*

*Software Systems Engineering Initiative,
University of York,
Heslington, York
YO10 5DD, UK
zoe.stephenson@ssei.org.uk

Keywords: Standards, deliberation, transparency, tool support, consensus.

Abstract

The standards and guidance used in safety-critical systems development are subject to varying degrees of interpretation. This is most apparent when the guidance from one document is used as a means of compliance for another. One such example is Def Stan 00-56; it sets a number of relatively abstract goals and encourages the use of other standards to meet those goals. In this paper, we present a modelling technique that helps the system developer to explain how the use of one standard meets the needs of another by way of explicit items of evidence. We illustrate the model with some examples from recent work on Def Stan 00-56 and IEC 61508, and discuss some of the critical issues in enabling more general use of such explicit representations.

1 Introduction

Safety-critical systems development in the UK Defence context is governed by Def Stan 00-56 [6]. It sets 13 key objectives for the successful acquisition of safe systems, such as:

> d. Tasks that influence safety are carried out by individuals and organisations that are demonstrably competent to perform those tasks [6, p3]

and:

> g. A Safety Case is developed and maintained that demonstrates how safety will be, is being and has been, achieved and maintained. [6, p4]

These objectives lead on to a more detailed set of requirements placed upon the supplier of a system, known as the Contractor. Since the requirements are relatively generic, different Contractors will implement them in different ways. Part 2 of Def Stan 00-56 recognises that Contractors may

> "...adopt alternative safety standards, which have different requirements to this Standard. These will be acceptable where they meet the intent of this Standard." [7, p11]

Our work is typically focused on software products, and in this context an appropriate standard governing an off-the-shelf safety-critical software component might be DO-178B [8] or IEC 61508 [4]. Following such a standard produces a body of evidence which would be called upon in demonstrating that the requirements of Def Stan 00-56 have been met.

This scenario raises two interesting questions:

- Which of the requirements of Def Stan 00-56 can be demonstrated this way?
- What can be done to identify and fill in any remaining gaps?

In this paper, we do not attempt to address these questions directly. Instead, we recognise that differences between individuals, organisations and products will lead to different answers to those questions, making the prospect of using evidence from another software safety approach volatile and risky. Hence, we seek a modelling method that exposes the links between standards, to act both as a guide to the Contractor in arguing that specific requirements are met for a specific product and as a tool for collaborative deliberation about the potential links between standards.

The following section describes the available design choices for linking between standards, and justifies the selection of evidence-based links for the modelling approach. Section 3 describes a model for inter-standard deliberation. In Section 4, we illustrate the use of the model for Def Stan 00-56 and IEC 61508. The use of the model raises some practical concerns, which we highlight in Section 5 before summarising in Section 6.

2 The links between standards

A standard or guidance document for a safety-critical development process potentially does 4 things:

- It conveys a set of guiding principles. In some cases these principles will be explicit; in others they will drive choices but remain tacit. If the committee behind the document changes frequently compared to revisions of the document, understanding and use of tacit principles may change.
- It conveys rationale to describe why particular requirements are placed on those following the standard, or why particular recommendations are made for those

following guidance documents. Different documents convey different amounts of rationale, and sometimes use a separate document to do so [9].

- It suggests or requires that certain processes are followed in certain ways. For example, DO-178B suggests that, at software development assurance levels A and B, executable object code is checked against low-level requirements and that the check is performed independently from the creation of the object code. [8, p98]
- It causes the generation of evidence. For example, the check of object code against low-level requirements should give rise to a report that shows which part of the object code relates to which part of the requirements, and details the checks made for that requirement and the success of the comparisons.

Since the exposition of principles and rationale varies greatly between standards, it is unrealistic at this stage to provide support for comparisons through those channels. Even if such a comparison could be convincingly drawn, it is unlikely to directly result in detailed practical guidance on what to do to address any gaps that arise.

Comparisons of processes are troublesome because Def Stan 00-56 gives very few constraints on processes. It effectively requires the creation of a demonstrably acceptably safe system. The difference in levels of process abstraction makes a process-by-process comparison difficult to produce in a consistent and repeatable manner.

The final option is a comparison based on evidence. With evidence, there are two questions that can be asked of a standard or guidance document:

- What evidence will be generated by following the requirements or recommendations?
- What evidence is sufficient to show that the requirements or recommendations have been met?

For the evidence to be appropriate, it should be sufficient to demonstrate that the requirements or recommendations have been followed. This concept of sufficiency is not absolute; it depends on the exact requirement or recommendation in question and the judgement of engineers and other stakeholders. For example, the nature of sufficiency to show that people in safety roles have appropriate skills and training is rather different to the type of sufficiency that shows that object code conforms to low-level requirements.

Given the difficulties with process, rationale and principle-based comparisons, our model is based on comparisons through evidence. The following section details the modelling approach and how that approach helps with the problem of varying judgements across the different parts of a standards or guidance document.

3 Modelling inter-standard deliberation

3.1 Analysis of evidence-based linking

The evidence link between two different process documents is based on the two evidence questions from section 2, as follows:

1. If document 1 is followed, what evidence is produced?
2. If an appeal is made against fulfilment of the needs of document 2, what evidence is sufficient?
3. How well does the evidence from document 1 meet the needs of document 2?

In each of these questions there is the potential for variation in the answer and hence uncertainty in arriving at a definitive answer. Our modelling method must be able to handle uncertainty and variation to allow participants to qualify their opinions.

For the first question, the generated evidence will depend on which parts of the document are relevant to the particular product being developed. If the document is structured around a number of levels of assurance or integrity, it will also depend on what has been chosen. If particular tools are used for parts of the process, then the evidence will sometimes be distributed between the generic evidence about the behaviour of the tool and the specific evidence about its use within the process. Nevertheless, it should be relatively easy to characterise the evidence produced from each part of the process outlined in a standards or guidance document. The fundamental issue here is the exposure of the underlying variation in some explicitly-documented form.

For the second question, the sufficiency of evidence will depend on the particular need of the standards or guidance document. For example, the following requirement appears as part of Def Stan 00-56 [6,p8]:

> 7.4.1 The Contractor shall establish a **safety committee** that allows participation of all relevant stakeholders.

What constitutes sufficient evidence to show that this requirement has been met? One view is that the membership of such a committee should be documented, and a diary of meeting dates should be provided. This is useful, but it does not necessarily demonstrate that all relevant stakeholders are able to participate. It may be felt necessary to also publish agendas and detailed minutes, define criteria for relevance of stakeholders, validate those criteria, show that the committee membership meets the criteria and demonstrate through logs of meeting arrangements that reasonable means are employed (teleconferencing, videoconferencing, online meeting software) to enable inclusion in committee meetings. In practice, a common understanding of sufficiency in this case is likely to fall between these extremes. In some cases there will be broad consensus on the sufficiency of evidence for a particular question, in others there will be variation on a case-by-case basis. It may be necessary to record sufficiency criteria that are qualified with contextual information.

For the third question, there are even fewer opportunities for consensus. It is likely that convincing comparisons will either be very general and highly qualified or specific to particular uses of the standards or guidance. With this in mind, it is appropriate for a comparison model to support a number of different positions on the degree of compatibility between the two documents.

3.2 Comparison model

The proposed static structure model for comparisons between standards or guidance documents is shown in Figure 1. It provides elements for document modelling, evidence linking and the deliberation of assertions.

At the bottom of the model, a particular standard or guidance document is described as a hierarchical structure of StructureItem elements. For example, the structure of IEC 61508 may be described as having part 1, part 2 and so on, with part 1 containing an Introduction section, a table of contents, a Section 1 titled "Scope" and so on. Particular StructureItem elements live at the same "level", so a list of

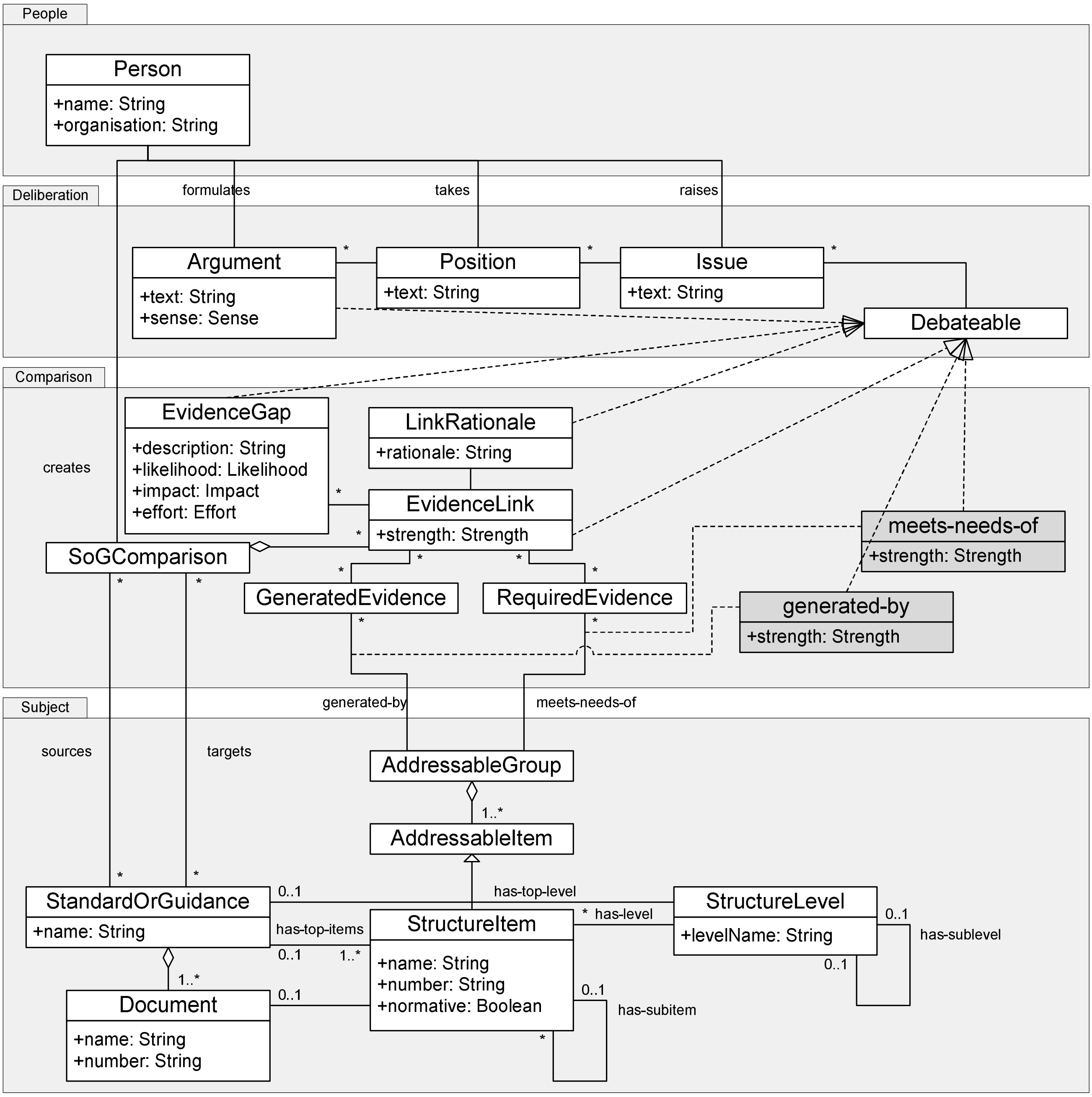

Figure 1 – Class diagram for comparisons between standards or guidance documents

StructureLevel elements is also maintained. It is recognised that standards and guidance are often divided into individual documents, so the model includes the concept of a document relating to a particular StructureLevel. Each StructureItem is an example of an AddressableItem, giving room to add other ways of referring to the parts of standards or guidance. Finally, any number of AddressableGroup elements may be made, each one identifying a particular selection of parts of a standard. This might be used, for example, to pick out the set of paragraphs in DO-178B that produce traceability information at various levels of decomposition.

In the Comparison package, a comparison is drawn between two StandardOrGuidance elements by linking the generated and required evidence. Each piece of generated evidence is associated with a particular AddressableGroup, indicating that following the guidance or requirements of that AddressableGroup *generates* that evidence. Similarly, each piece of required evidence is associated with the particular AddressableGroup whose *needs are met* by that evidence. A link is drawn between the GeneratedEvidence and the RequiredEvidence, and this is assigned a particular strength according to some consistent scheme. The model allows the link to join together a number of different GeneratedEvidence instances to meet a number of different RequiredEvidence instances. Mindful of the need to address the gaps between approaches, the model allows zero multiplicities, e.g. to show that a particular RequiredEvidence is not supported by any GeneratedEvidence. A given SoGComparison shows a particular Person collecting together a number of these EvidenceLink elements. If a particular EvidenceLink has a gap or shortfall in the evidence that needs to be explained, an EvidenceGap element may be added to identify the issue.

In the Deliberation package, the model makes use of a classic issue-based deliberation structure [2]. Certain other elements in the model may be contentious – they represent an opinion rather than an objective fact. These elements are collected together under a single Debateable interface. Any Person may raise an Issue with a Debateable element, and from there a Person may take a particular Position on that Issue. For example, the Issue may be a weak link, with a Position that it should be strengthened by adding further sources of evidence. Argument elements are created in support of or against particular Positions, creating a deliberation tree. Finally, any Argument may in turn raise further Issue elements; it may itself become Debateable. The intent here is to allow multiple parties to collaboratively reach a consensus on the degree to which the activities governed by one approach meet the needs of another. In support of this, the People package at the top of the model provides an independent view of individual Person elements and the organisations that they represent.

4 Illustration: IEC 61508 and Def Stan 00-56

As part of the ongoing work of the SSEI, we manually produced a comparison of the evidence generated through IEC 61508 and the requirements of Def Stan 00-56. The comparison predates and inspires the model given in Section 3, and covers only the Comparison package of that model. Instead of the flexible AddressableItem approach, the paragraph numbering of each standard is used.

As an example of a straightforward evidence link, consider the link diagram in Figure 2. This shows IEC 61508 on the very left, then the generated evidence, then the required evidence and finally the relevant clause of Def Stan 00-56. In this situation, the link is relatively straightforward, and there is little debate. However, the link in Figure 3 is much more debateable. Here, Def Stan 00-56 calls for the establishment of tolerability criteria for risks, so that the categories used in ALARP assessment (broadly acceptable, tolerable and unacceptable) may be objectively determined. In IEC 61508, however, there is very little that would establish these criteria. The closest match found in our analysis was from a particular requirement to establish a target failure rate for each function. The link shows that, while this information could form part of the overall set of tolerability criteria, it is far from complete.

A final illustration of the linking method is given in Figure 4. Here, the diagram shows a complete lack of any evidence from IEC 61508 that would demonstrate that a process for risk acceptance had been agreed.

In our study, we drew up 14 comparison charts to cover the various parts of Def Stan 00-56. These were mapped to the requirements of IEC 61508 and the resulting charts revealed 41 different evidence gaps that could potentially arise. These gaps are the result of analysis from one particular point of view, however, and do not necessarily reflect real-world project experience. To build up a representative data-set, many more parties must be involved in the analysis.

5 Enabling general use of the approach

One of our goals with this research is to create some common understanding and expectation regarding the use of particular civil standards in meeting the requirements of Def Stan 00-56. We believe that open debate and deliberation about the use of standards is a compelling route to achieving this goal. In this section, we identify a number of steps that we feel are appropriate in achieving this goal.

5.1 Extending the model

We have planned for the extension of the model to accommodate other ways of referencing the content of a standards or guidance document. For example, it may be appropriate to refer to a particular part of a paragraph, a particular word, a particular area of a page or a particular principle embodied in a standard. In addition to this planned extension, we recognise that the model may turn out to be incomplete when used by others. For example, users may find that they wish to raise issues against items that are not currently tagged as debateable, or they may find that they wish to refer to link elements to support an argument about the consistency of a particular position.

5.2 Implementing tool support

Our model is intended for implementation in a collaboration and deliberation tool. In addition to the automated layout of link diagrams and the production of evidence gap documentation, such a tool could also provide summary information such as standards coverage and consistency checks. To support open debate about the use of standards and guidance, the tool support should be as widely-available as possible. The ideal approach would be as a web application, but there are a number of concerns that would need to be addressed:

- Users may refrain from commenting on an evidence link in public, as it could have an impact on liability or expose confidential information. To address this, some mechanism may be available to selectively publish deliberation and allow for separate deliberation stages within the confines of a particular organisation.
- The full text of standards and guidance such as IEC 61508 and DO-178B is only available for a fee, and the licensing terms of those documents do not permit arbitrary use of the text in a web application. The links between the application and the documents must be carefully balanced so that they are useful without infringing upon the rights of the copyright holders.
- There are existing tools that manage the navigation and interrogation of standards and guidance documents, and other tools that allow for document annotation and online deliberation. Integration with these tools would perhaps be of benefit to some of the potential users of the standards / guidance document comparison system. However, it is not clear that a web application would support integration of this sort in a useful manner.

As initial validation of the model as a basis for tool implementation, we prototyped the model using the EuGENia modelling system [5]. The system provides a general-purpose modelling environment which, while not appropriate for the general user, provides an opportunity to detect problems in the model. During this validation exercise, we detected and corrected a missing association in the Subject package and enhanced the ability to deliberate over multiple standards. The validation exercise also revealed key aspects of model usability which will inform further work on a domain-specific comparison environment.

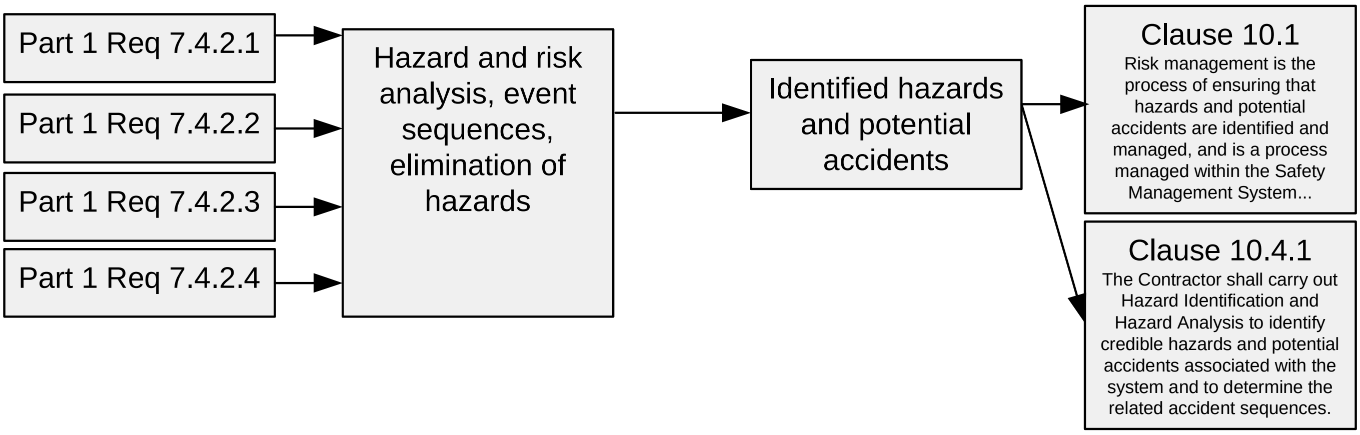
Part 1 Req 7.4.2.1
Part 1 Req 7.4.2.2
Part 1 Req 7.4.2.3
Part 1 Req 7.4.2.4
Hazard and risk analysis, event sequences, elimination of hazards
Identified hazards and potential accidents
Clause 10.1
Risk management is the process of ensuring that hazards and potential accidents are identified and managed, and is a process managed within the Safety Management System...
Clause 10.4.1
The Contractor shall carry out Hazard Identification and Hazard Analysis to identify credible hazards and potential accidents associated with the system and to determine the related accident sequences.

Figure 2 – link diagram excerpt IEC 61508/Def Stan 00-56, full link

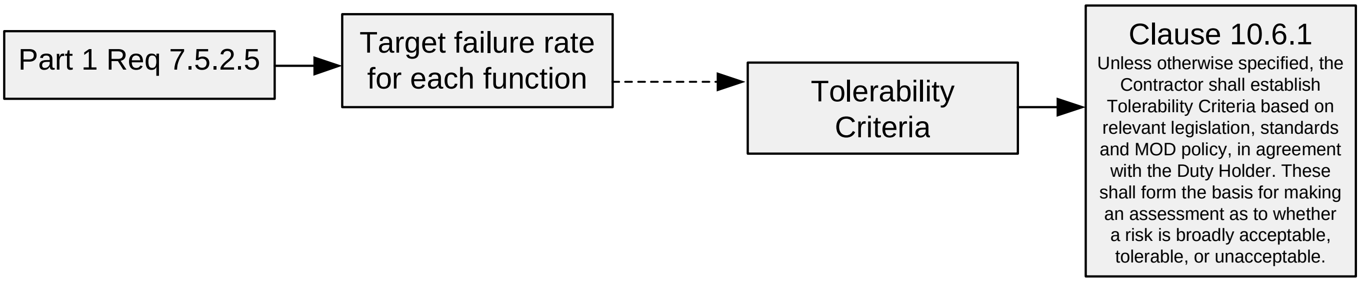
Part 1 Req 7.5.2.5
Target failure rate for each function
Tolerability Criteria
Clause 10.6.1
Unless otherwise specified, the Contractor shall establish Tolerability Criteria based on relevant legislation, standards and MOD policy, in agreement with the Duty Holder. These shall form the basis for making an assessment as to whether a risk is broadly acceptable, tolerable, or unacceptable.

Figure 3 – link diagram excerpt IEC 61508/Def Stan 00-56, partial link

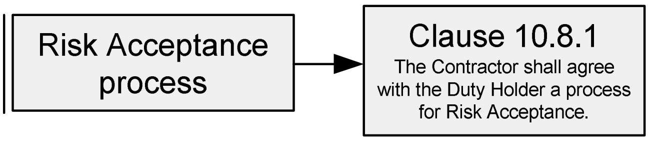
Risk Acceptance process
Clause 10.8.1
The Contractor shall agree with the Duty Holder a process for Risk Acceptance.

Figure 4 – link diagram excerpt IEC 61508/Def Stan 00-56, no link

5.3 Encouraging public deliberation

The recording mechanisms in the Deliberation package of the model in Figure 1 are appropriate for ongoing debate, but their rigid structure provides only a narrow means of expression. To encourage deliberation, there are other technologies such as online conferencing and messaging that could be integrated into the tool. Such technology would also be useful in holding online meetings to review and update the linking model. Such meetings could be focused on particular principles such as ALARP, particular technologies such as object oriented modelling, or particular domains such as engine control.

5.4 Encouraging modelling of context

A key area lacking in the current approach is a way to consistently model the context within which EvidenceLink entities are situated. For example, the EvidenceLink for the link diagram in Figure 3 could be a strong, direct link in a situation where functions interactions are straightforward, correct behaviour of the functions cannot lead to a hazard and hence safety risk can be based solely on function failure rates. Representing different links in different contexts would require some additional modelling support:

- The links, link strength and rationale should all be linked to Boolean combinations of the presence of contextual elements.
- The contextual elements should be drawn from a common contextual model that is itself the subject of deliberation.
- The contextual model should be structured using either feature modelling [3] or ontological concepts [1] to ensure consistency.

5.5 Providing a way to record answers

Our current model is aimed at encouraging practitioners to think about gaps that exist between standards. To appeal to a wide audience, any programme of work that makes use of this technique should also provide for constructive advice on how to address those gaps. This could include particular techniques for avoiding a shortfall in the strength of evidence produced or the use of a complementary standard to provide evidence that would otherwise be missing. Industry consensus in these areas has the potential to greatly reduce the risks associated with the procurement and operation of safety-critical and safety-related systems.

6 Conclusions

In this paper, we described a situation where one guidance document or standard is used as the basis for meeting the needs of another, in particular for meeting the requirements of Def Stan 00-56. The possible links between guidance or standards were investigated, and a model was drawn up in Section 3.2 to help capture the relationships between the different approaches in an explicit form for further deliberation and action. We briefly described the application of the model to the comparison of IEC 61508 and Def Stan 00-56 and identified a number of avenues to investigate for further exploitation of these ideas.

Our aim with future work is to implement tool support for capturing the relationships between guidance and standards and allow wider collaboration, deliberation and consensus on best-practice methods for dealing with the gaps between approaches. A secondary aim is to investigate the use of the model for comparisons between different versions of the same standard. Our final aim is to encourage wider participation in deliberation of this form both as a way to foster understanding within the safety-critical community and as a way to evaluate the model against other means of discussing standards documents.

Acknowledgements

The authors would like to thank the UK Ministry of Defence for their support and funding. This work is undertaken as part of the research activity within the Software Systems Engineering Initiative (SSEI), www.ssei.org.uk.

References

[1] Bao, J. and Honavar, V. "Collaborative Ontology Building with Wiki@nt", Proceedings of the 3rd International Workshop on Evaluation of Ontology-based Tools, 2004

[2] Conklin, J. and Begeman, M. "GIBIS: A Tool for All Reasons", *Journal of the American Society for Information Science*, **40(5)**, pp200-213, 1989

[3] Czarnecki, K.; Kim, C. H .P. and Kalleberg, K. T. "Feature Models are Views on Ontologies", *Proceedings of the Software Product Lines Conference*, 2006

[4] IEC. "Functional safety of electrical / electronic / programmable electronic safety-related systems". IEC 61508, 1998

[5] Kolovos, D. S.; Rose, L. M.; Paige. R. F. and Polack, F. A. C. "Raising the level of abstraction in the development of GMF-based graphical model editors", *2009 ICSE Workshop on Modeling in Software Engineering*, 2009

[6] Ministry of Defence. "Safety Management Requirements for Defence Systems: Part 1: Requirements". Def Stan 00-56, Issue 4, 2007

[7] Ministry of Defence. "Safety Management Requirements for Defence Systems: Part 2: Guidance on Establishing a Means of Complying with Part 1". Def Stan 00-56, Issue 4, 2007

[8] RTCA/EUROCAE. "Software Considerations in Airborne Systems and Equipment Certification". DO-178B/ED-12B, 1992

[9] RTCA/EUROCAE. "Final Report for Clarification of DO-178B "Software Considerations in Airborne Systems and Equipment Certification"". DO-248B/ED-94B, 2001