Turning Up the HEAT on Safety Case Construction

Paul Chinneck
Safety & Airworthiness Department
Westland Helicopters, Yeovil, BA20 2YB, UK
chinnecp@whl.co.uk

David Pumfrey, Tim Kelly
Department of Computer Science
University of York, York, YO10 5DD, UK
david.pumfrey|tim.kelly@cs.york.ac.uk

Abstract

The HEAT/ACT project consists of replacing the conventional mechanical flight control system of a helicopter with a fly-by-wire system. With such a project, the safety concerns are obvious, and therefore the development of a thorough and convincing Safety Case is paramount. Goal Structuring Notation was chosen as the method for this, on its perceived merits of ease of construction and clarity of review. This paper outlines the work conducted, and appraises these perceived merits against experience during and following the construction of the Preliminary Safety Case.

1 Background to the HEAT/ACT project

The HEAT/ACT project consists of replacing the conventional mechanical flight control system on a helicopter with a fly-by-wire system (see Staple & Handcock 2002). It involves extensive re-engineering of the aircraft systems, including:

- removal of two out of three hydraulic systems
- replacement of the main and tail rotor hydraulic actuators with electro-mechanical actuators
- removal of mechanical flying controls.

The major new items include:

- adding another electrical generator
- installing actuator control units
- adding two new fly-by-wire (FBW) flight control computers.

1.1 Safety case approach

With such a project, the safety concerns are obvious, and therefore a convincing and thorough Safety Case is paramount. Def Stan 00-56 (Ministry of Defence 1996) Part 2 “encourages the concept of an evolving Safety Case” in order to “[initiate the Safety Case] at the earliest possible stage…so that hazards are

identified and dealt with *while the opportunities for their exclusion exist*." The HEAT/ACT project recognised the benefit of constructing the safety argument as early as possible, for this precise reason. Any change to the architecture, for safety reasons or otherwise, becomes dramatically more difficult and expensive once designs are frozen and components are in manufacture. The project therefore chose to adopt a phased approach to safety case development, beginning with a Preliminary Safety Case (PSC).

The ultimate intent of the Safety Case was to show, by clear argument, that the HEAT/ACT system, when fitted to a Merlin helicopter, will be acceptably safe for operational use. The PSC was required to contain a complete argument, showing all of the important claims that would have to be made and demonstrated in order to satisfy the safety requirement. Goal Structuring Notation (GSN) (Kelly 1999) was chosen as the method for representing this argument on its perceived merits of ease of construction and clarity of review. Early proposals for evidence to support this argument were also required as part of the PSC development.

Through a process of review with airworthiness authorities, the PSC would provide confidence that the design of the HEAT/ACT system was such that acceptable safety could be demonstrated. It would support the engineering process by providing a structure in which to document safety activities and processes until the system has been fully designed and final safety analysis has been completed. Before the system hardware is produced and commissioned, an Interim Safety Case will be required. This will use the PSC as a basis, refining and adapting it to suit the final system design, and adding more complete evidence to support the argument.

The scope of the Safety Case is to include an assessment of the impact of the modification on the safety of the whole aircraft. It is of course of no benefit to show that the new system is acceptably safe without also considering the effects it has on the platform into which it is integrated.

1.2 Timeline

Guidance (Kelly et. al. 2003) shows that the pre-requisites for preparation of a PSC are:

1. The initial Safety Programme Plan (SPP) for the project (though note that this will develop as the PSC is constructed, as evidence requirements will generate new tasks that will have to be incorporated in the SPP)
2. A Preliminary Hazard Identification (PHI), together with initial hazard analysis and Risk Estimation
3. Identification of key safety requirements

This guidance also states that the PSC should be constructed before:

1. Detailed specifications are produced
2. Detailed design and implementation work (and any related analysis and testing) has commenced

3. System Safety Analysis (following on from Preliminary Hazard Analysis) is conducted

A stated requirement of the HEAT/ACT project SPP was that the PSC should be prepared to support Preliminary and Critical Design Reviews (PDR and CDR). Producing the PSC would also ensure that the Interim Safety Case could be prepared in time to support first flight.

The timing of the request for HEAT/ACT PSC production met both the above guidance and the project requirements. In the programme of a typical project, this should have allowed many months in which to draft, develop and finalise the PSC. However, the HEAT/ACT project has very challenging timescales, giving no more than two months for construction and issue of the PSC.

1.3 PSC development and presentation

The HEAT/ACT PSC was largely written by a single person. Throughout the development process, however, the expertise of others was called upon to review the argument. Several individuals read and commented on the document as work progressed, and there were also more formal meetings in which the primary author worked through the structure of the argument with a group.

The GSN diagrams form a key part of the delivered PSC document. The PSC starts with preliminary material, including an outline description of the HEAT/ACT system, and an introduction to GSN notation to help readers who are not familiar with its use. The majority of the document then presents a small section of the argument in GSN on each page, followed by textual discussion. The text explains the intent of the argument fragment, with justification where necessary, and describes how it is intended that the fragment will be developed (including an outline of evidence requirements) in the Interim and subsequent phases of Safety Case development.

2 Outline of the experience

2.1 Starting out

The definition of the top goals of the GSN structure was relatively easy, as much guidance exists for starting safety arguments. The system and its integration into the aircraft would be treated as separate concerns. For the system argument, the common “product/process” argument approach was taken. In the “product” argument strand, the identified system hazards are addressed, and developed until direct evidence can be presented to show that the risks from these hazards have been adequately controlled. The “process” strand demonstrates how all applicable standards and requirements are satisfied.

However, after quickly sketching out the top few levels of the argument structure, it became increasingly difficult to extend the argument structure into lower levels of sub-goals. A number of different situations were evident. In some cases, it was already obvious what the solution (evidence) nodes at the bottom of the argument should be; the difficulty here was in "reaching" existing evidence, i.e. breaking down high-level goals to sub-goals at a level where it could be shown that the evidence directly and sufficiently satisfied specific goals. In other parts of the structure, the problem was effectively lack of inspiration; some of the goals clearly required significant decomposition, but no obvious strategy could be seen. A third problem was how to resolve obviously related goals in different branches of the argument structure.

2.2 Developing the argument

At this point in the development of the PSC, advice was sought, and both safety case patterns (Kelly & McDermid 1997) and a number of existing safety cases were considered as potential sources of inspiration and guidance.

2.2.1 The patterns approach

Safety case patterns represent sections of argument to satisfy specific goals. They require "instantiation" to suit the context into which they are introduced; that is, they contain elements such as alternatives from which the appropriate selection must be made, and incomplete structures, which must be extended. In applying patterns in the context of the HEAT/ACT PSC it was found that, at the top levels of the safety case structure, they generally yielded good guidance and suggestions for the expansion of specific goals. Specific patterns incorporated into the argument included Functional Decomposition, and the commonly used (but possibly not fully understood) ALARP.

As the project progressed, however, it was found that patterns were of more limited use in developing the argument to a sufficient degree to complete any part of the GSN. This may be because patterns are, by their very nature, "skeleton" structures, which require tailoring to be properly used. Without experience of identifying appropriate relationships between the "reality" of the system or process that is to be represented, and the library of available patterns, it can be difficult and time-consuming to make appropriate choices. Also, considerable expertise is required in deciding when a pattern has been fully instantiated, and a branch of the argument can really be considered complete.

What proved more useful at this low level was actual safety case material. This yielded the ability to examine how other authors had "solved the problems" of instantiating patterns, and also suggested "micro-patterns" – often a very small number of GSN elements, or even just well-chosen wording of a goal or strategy – which provided the inspiration to assist development of the argument to the very lowest level.

2.2.2 Borrowing and modifying

In investigating how to complete the HEAT/ACT PSC argument structure, the authors examined a number of published safety cases that have used GSN. Two specific safety cases were found to be extremely helpful; the European Reduced Vertical Separation Minimum Pre-Implementation Safety Case (EUR-RVSM PISC) (Eurocontrol 2001) and the safety argument for integration of new technology on to older platforms proposed in Kenneth Graham's MSc project report (Graham 2002). Examples of ideas adopted from these documents included:

EUR-RVSM PISC:

- Proving that any requirements were firstly complete and correct, and then showing that those correct requirements were satisfied.
- Variants on the "direct evidence supported by backing evidence" pattern. (A similar pattern is also used extensively in the UK Civil Aviation Authority's standard for Software Safety Assurance (Civil Aviation Authority 2001).)
- Stating Safety Objectives at the beginning of the Safety Case, proving they are addressed within the safety argument, then showing compliance in a summary at the end.

Kenneth Graham's MSc project report:

- Integrating a system under fault-free conditions, then assessing the fault tolerance or failure management following installation.
- The key assertion that a system can only be safe after modification provided that the parts of the system not affected by the modification were acceptably safe in the original state.

All of these ideas provided important "building blocks" for the safety argument. The authors also found that reading and review of these and other safety cases were significant in building confidence in our own ability to recognise – and subsequently produce – well-structured and robust arguments.

3 Successes

3.1 Speed of construction

The request for the PSC was made in early April 2003. Development of the argument by the primary author began in mid-April, but quickly reached an impasse. In mid-May other expertise was drawn in to review the work so far, and the approach described above using patterns and drawing on other safety cases was adopted. From this point, the rate of progress dramatically increased. Within a further two weeks, the document had grown from just 8 very basic GSN diagrams to 26 much more comprehensive ones, for presentation at project PDR. A further three weeks' work saw the document ready for signatory approval. From this state to the final issued version, only very minor changes were required, despite requiring four different people to check and sign the PSC as approved.

3.2 Development and discussion

As the document progressed, it became clear that using GSN had some huge advantages over a textual document:

- Many of the revisions required during the development were merely expansions of earlier work, rather than complete re-writes of sections. This is illustrated in the sequence of Figures 1 to 3, where three stages in the expansion of the Hazard Log goal can be seen. The final expansion of this goal in Figure 3 actually forms a very satisfactory pattern, which could be used in other safety cases where maintenance of a hazard log is an important aspect of safety management.

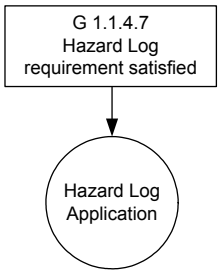

Figure 1 - Stage 1 of evolution of Hazard Log requirement GSN

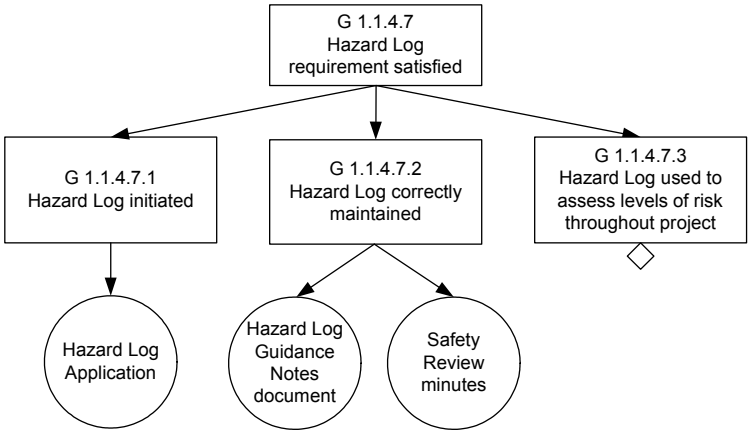

Figure 2 - Stage 2 of evolution of Hazard Log requirement GSN

- It was possible to re-use self-imposed "patterns" from earlier in the document. As a new area came under scrutiny for development, thoughts and methods from earlier on were re-used, dramatically reducing the time required.
- It remained very simple to keep the "big picture" in mind, even when developing the structure to six or seven sub-levels.

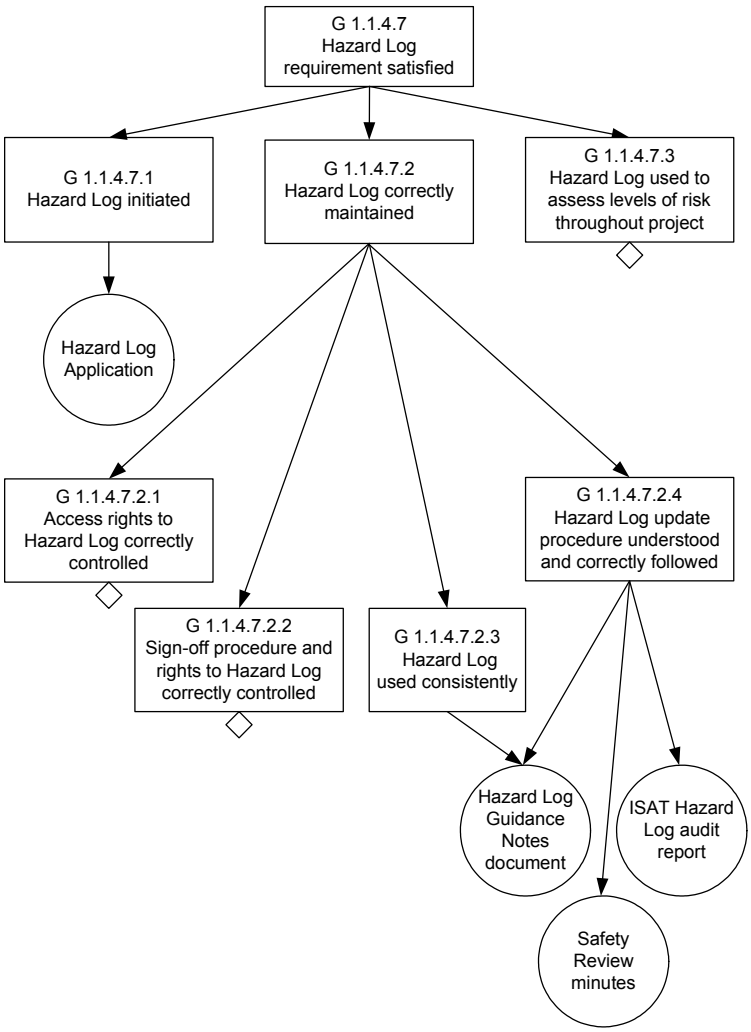

Figure 3 - Stage 3 of evolution of Hazard Log requirement GSN

- It was much less likely that areas of the safety argument would be overlooked. Working with top-level goals before breaking them down into sub-goals helped this enormously.
- Discussion of parts of the document was simplified, as it was easy to use the GSN hierarchy to explain to people the context of the area under discussion.

A further benefit of GSN was realised when it came to asking equipment suppliers for sub-system safety cases. The diagrams showing the breakdown of hazards related to system functions formed an easy starting point for helping each supplier to identify their contributions to the safety case. Various parts of the process argument were also used to show the relationships between different organisations' safety activities.

3.3 Successful reviews

At various stages throughout the creation process, Safety Case reviews were undertaken. Again, the benefits of GSN became clear during these reviews. At one point, the near-complete document (comprising 26 pages of GSN diagrams) was presented to representatives from the MoD at the project PDR. This took just 30 minutes.

The document was also reviewed at the various levels of Project Safety Meetings held. Not only was it relatively quick to review the entire Safety Case, but it was easy to see what had changed or been added since the last review. Conducting these on-line reviews on a text-based document would have been virtually impossible. At a practical level, a single GSN diagram could easily be "lifted" from the document and made into a projection slide as the basis for discussion.

Following issue of the document, the primary author received a number of complements relaying how simple the document was to read and understand. These comments came from both technical and non-technical staff, proving the benefit of GSN in representing the argument in a clear and unambiguous fashion.

4 Problems and suggestions

4.1 Giving the right impression

The regular reviews of the GSNs in the development of the project drew attention to a number of issues of presentation. One of the most important of these was the relationship between "reading order", and the impression of the overall argument being made. At a fairly early stage in developing part of the argument, a relevant pattern with the structure shown in Figure 4 was identified in one of the sources, and instantiated into the safety case. When this part of the safety case was discussed in review, one of the participants objected, as he had perceived the argument to be primarily about safe behaviour following a single failure, whereas he felt that safe behaviour in normal circumstances was more important.

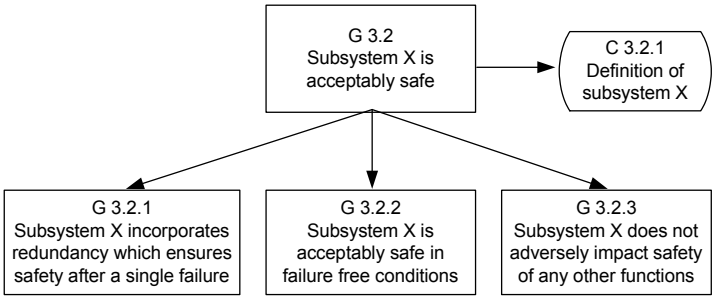

Figure 4 - GSN showing "perverse" ordering of goals

In GSN, layout of items on the page does not imply any order of importance or precedence. Thus, the sub-goals in the pattern above should all be considered to have equal importance in the argument. However, it is worth bearing in mind that the reader's natural tendency is to consider the sub-goals in "normal" reading order, i.e. left to right across the page. Particularly in the mind of readers who are not familiar with GSN concepts, the order in which sub-goals are encountered will inevitably form an impression about their relative importance. In this case, although the components of the argument are all correct and acceptable, the goal relating to safe behaviour following a single failure is encountered before the goal relating to safe behaviour in normal circumstances, giving the incorrect impression that the former is a more important component of the argument.

Pragmatically, therefore, when laying out arguments in GSN form, it is necessary to think about the way in which a reader will approach the document, and perhaps adjust the presentation accordingly. If it really is the case that some sub-goals are more important, then consideration should be given to using a strategy element to identify this ordering. For example, in building the HEAT/ACT safety case, there were a large number of instances where a generic pattern of satisfying a goal through a combination of direct evidence supported by "backing" evidence was used. In these instances, it could be seen that the direct evidence was "spinal", i.e. the safety case would collapse without it, whereas the backing evidence was of lesser importance; inability to provide one of these items of evidence might weaken the argument, but not fundamentally destroy it. In these cases, we considered it might be beneficial to incorporate an explicit strategy element into the GSN, as shown in Figure 5. A similar structuring effect could alternatively be achieved through the use of appropriately worded sub-goals to explicitly differentiate direct and supporting evidence.

In discussing the presentation / reading order of GSN elements, it is also worth considering the way in which the GSN will be "flattened" to transform it into the structure of a full textual safety case. Here, even more than in the diagrammatic form, the order in which items are presented will form a strong impression with the reader. Careful consideration must therefore be given to the order in which the GSN tree is traversed to construct the contents list for the text. We note that at least one of the commercially available GSN tools (Adelard's ASCE (Adelard 2003)) allows this sequence to be specified.

4.2 Representing process

At a high level, the HEAT/ACT safety case made use of the classic "product / process" argument pattern. However, as the argument was refined and developed, we encountered a number of areas where this split proved problematic to develop completely.

At first sight it would appear that, provided the "product" side of the argument is satisfactory, there should be little difficulty in completing the "process" branch. Intuitively, since following the defined safety process produces the evidence

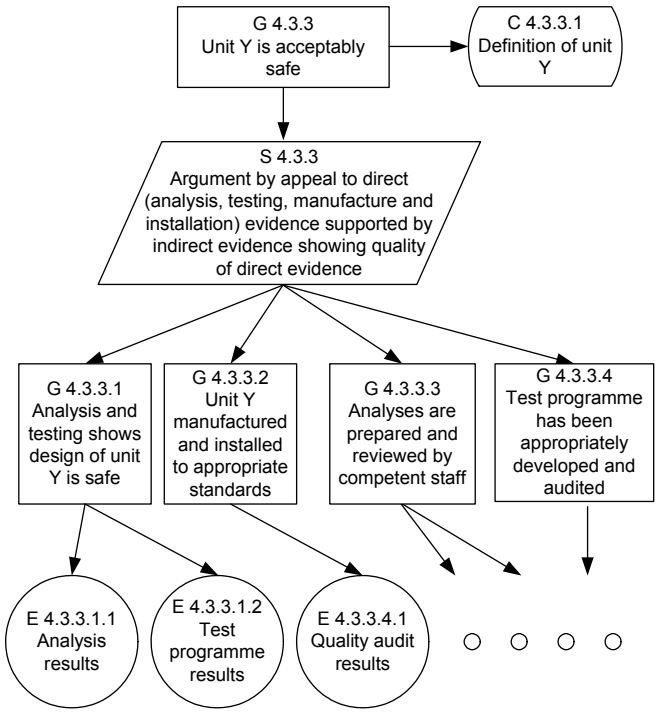

Figure 5 - Using a strategy to highlight the use of direct and backing evidence

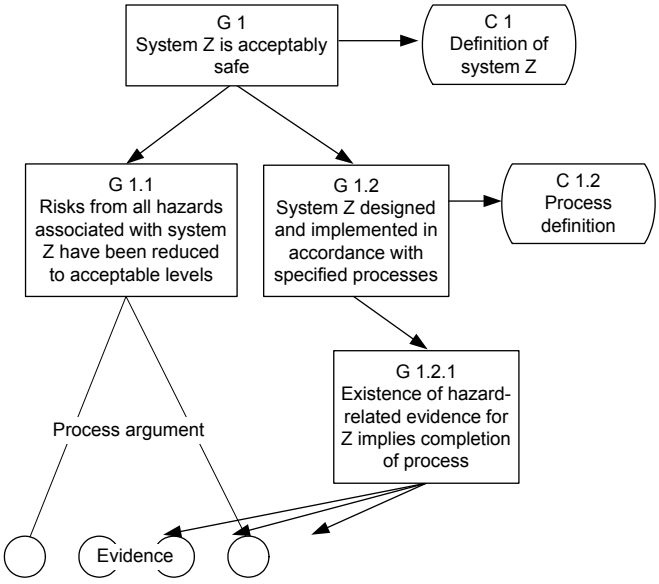

Figure 6 - Naive product / process structure

required to argue product safety, the existence of the product evidence should imply satisfactory completion of the process. In GSN notation, we might expect an argument with the structure shown in Figure 6, where the same evidence is used to satisfy both product and process argument strands.

In practice, however, we found a number of difficulties with this structure. The first is that a safety process is complex, involving many stages. Unless it is very carefully captured and maintained, product-structured evidence may not provide sufficient information to demonstrate that all the steps of the process have been followed. Consider, for example, a "product" safety argument that the risks presented by all identified hazards have been reduced to an acceptable level. The top few levels of such an argument structure are shown in Figure 7. If we also want to demonstrate that a classical safety process has been followed, we may want to complete a structure such as that shown in Figure 8.

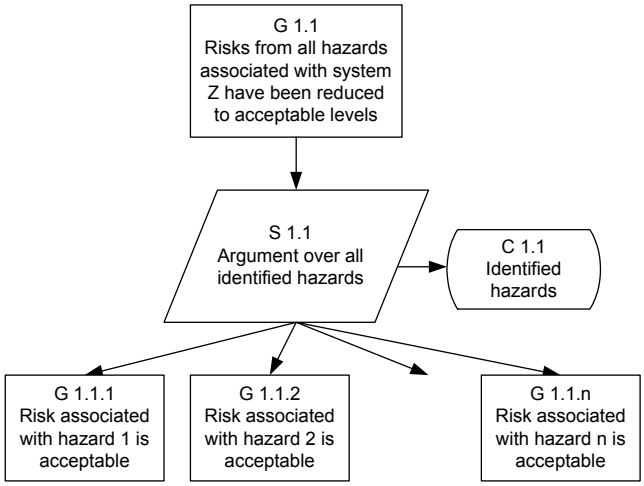

Figure 7 - Hazard-directed argument fragment

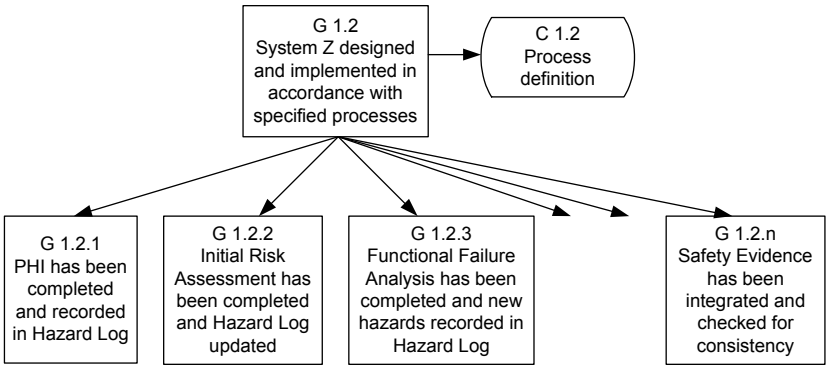

Figure 8 - Process steps argument fragment

The problem in reconciling these two argument approaches is that, as the hazard log is a dynamic document, work done in later parts of the process might update, obscure, or even totally replace, work done at early stages such as PHI. Thus, unless we ensure that a complete change history is available for the hazard log, its final state is unlikely to reflect all of the work that has actually been done. This is a real problem; one of the authors was involved in reviewing a safety case for another project in which exactly this problem was encountered; the safety case claimed that the final hazard log for the project was sufficient evidence that the defined process had been followed; in reality, so many changes had been made during the project that it was impossible to gauge the quality and completeness of the early work.

The benefit of identifying and considering this issue in developing the PSC is that decisions can be made about how to ensure complete process evidence is available. The GSN argument fragment in Figure 9 shows the general approach used in HEAT/ACT, based upon means of compliance matrices. For each part of the process, a choice has to be made whether to ensure complete history is retained in the final state of each item of evidence, or whether "baseline" versions will be retained at key process points.

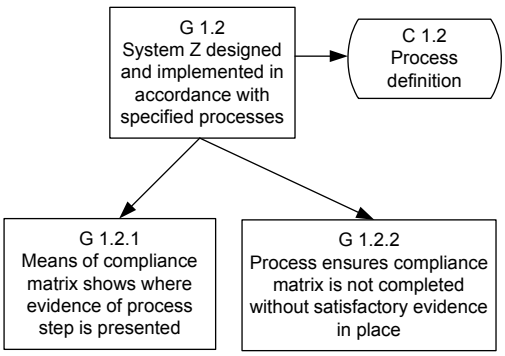

Figure 9 - Argument fragment showing how product evidence is used to support a process argument

Another process-related issue that was encountered in outlining the HEAT/ACT PSC was the occasional temptation to include too much process information in the safety case outline. This was evident, for example, in the first attempt to show how explicit top-level safety requirements would be satisfied. This divided the requirements into two classes – those that could be satisfied directly by compliance with airworthiness directives, and those that were more complex and would require exceptional activities or the involvement of specialists. As the argument structures for these two classes of requirement were developed, it became clear that their evidence requirements were essentially identical. The split had been introduced because of the strong perception that they would be satisfied in fundamentally different ways; whilst this was true from a process management perspective, it was an unnecessary complication in the safety case.

A key element of the "process" strand in the HEAT/ACT PSC is showing compliance with appropriate standards – notably Def Stan 00-56. Attempting to demonstrate this in the GSN presented a number of problems, foremost among which was a direct conflict between easy "read-across" (i.e. presenting a structure that closely reflected relevant sections of the standard), and following a "natural" breakdown (i.e. presenting a structure which reflects the actual organisation of the project). The chosen solution is something of a compromise. Major process elements, such as the key activities shown in Figure 8, which are fundamental to achieving safety and would have been implemented whichever standard was being followed, have been developed in a natural structure. However, where additional arguments and evidence have been included specifically to satisfy particular requirements of the standard (e.g. the elements of the Safety Management System required by chapter 5), these have been presented in a structure (Figure 10) that directly reflects the organization of the standard.

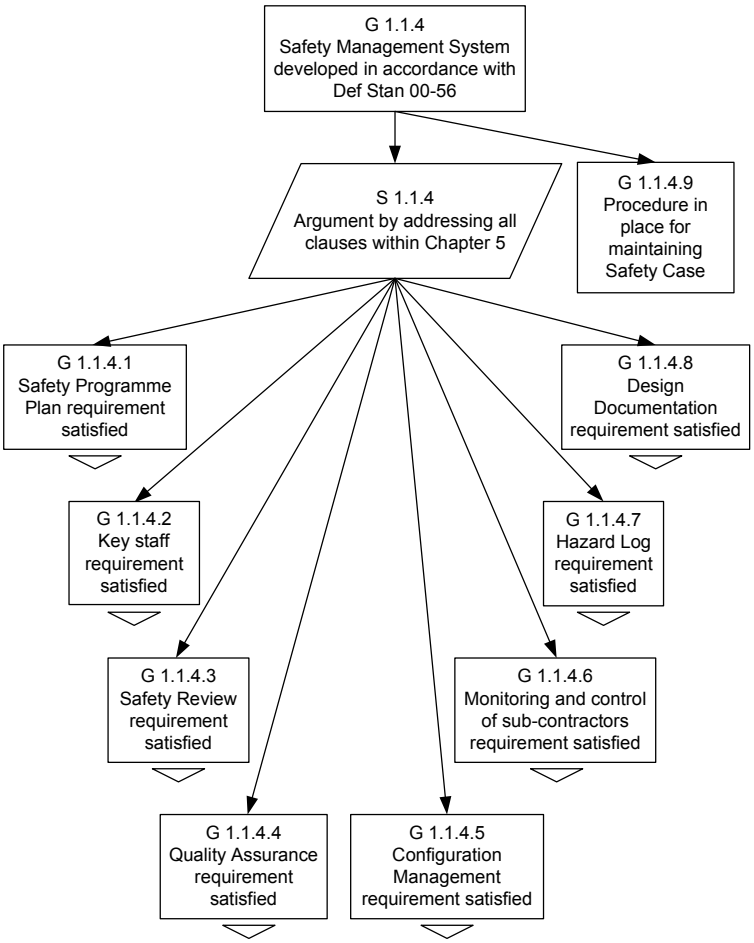

Figure 10 - Satisfaction of SMS requirements from Def Stan 00-56 chapter 5

We discovered that, in addressing the Safety Management System (SMS) requirements of Def Stan 00-56 chapter 5, we needed to create and instantiate another small pattern. The paragraphs in this chapter require various management documents and controls, such as the preparation of a system safety programme plan and the implementation of a system of independent audit. In considering how to show satisfaction of these requirements, we recognised that it would be possible to show that the "letter" of Def Stan 00-56 had been followed merely by pointing to the existence of the relevant items. However, to satisfy the "spirit" of the standard actually requires three separate elements; demonstration that the SMS item has been created, that it has been maintained (i.e. reviewed and updated as the project evolves), and that it has actually been followed. We therefore created the pattern shown in Figure 11 to show satisfaction of each of the paragraphs. An example of the instantiation of this pattern can be seen in the Hazard Log requirement argument in Figure 3.

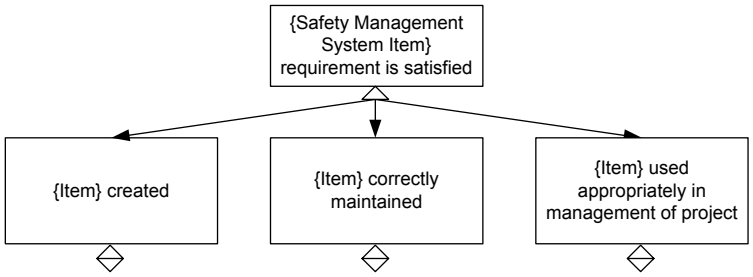

Figure 11 - Pattern to demonstrate satisfaction of SMS Item requirement

4.3 Managing size and complexity

As might be expected, the HEAT/ACT PSC is already a substantial document. The actual size of a safety case cannot be limited – it would be completely unacceptable to exclude information simply on the grounds that "it's already too big" – and elaborate argument structures are unavoidable when examining complex systems. Consideration therefore has to be given to practical means for managing size and complexity. In the HEAT/ACT project, we used two related mechanisms that we believe have been successful in making the safety case simpler to navigate. A particular problem area in the classic hazard-structured GSN argument has always been the point where the argument is split into branches for each individual hazard (as in Figure 7), as this causes an "explosion" in the width of the structure. In the HEAT/ACT PSC, it was recognised that the hazards could be grouped by system function, and this organisation was therefore used as an intermediate step in expanding the argument over all the identified hazards. One of the key benefits we expect to obtain from this structure in making the full safety argument is that there will be significant commonality between the evidence presented for the hazards within a group, as sketched in Figure 12.

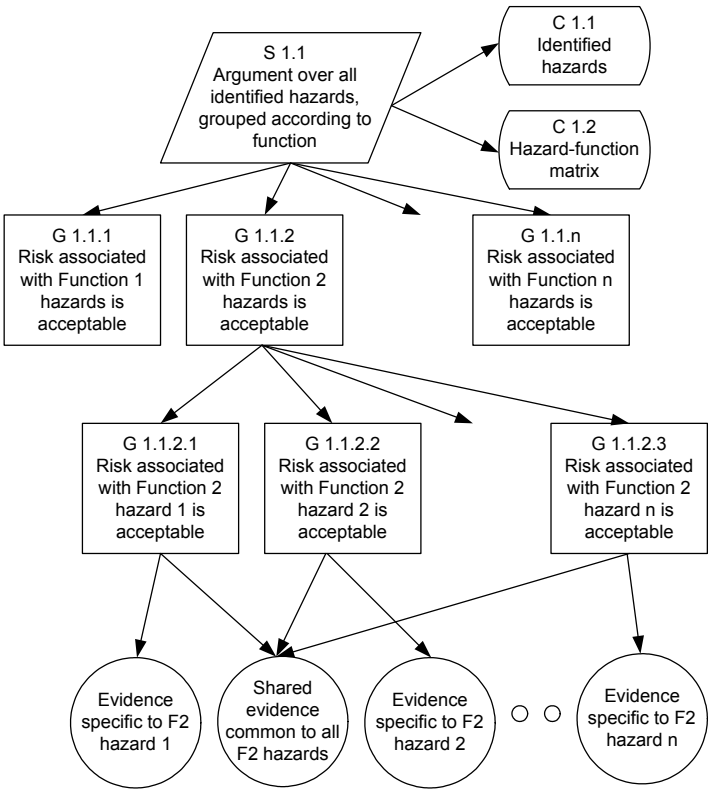

Figure 12 - Using functional breakdown to organise identified hazards

To further ease navigation of the hazard-directed argument, the GSN in the HEAT/ACT PSC document is supported by a matrix showing the functional breakdown of system hazards; this allows readers to quickly identify hazard ⇨ function and function ⇨ hazard relationships.

4.4 Incorporating supplier contributions

A final area where the structure of the HEAT/ACT safety case posed challenges was in deciding how best to incorporate evidence, or sub-arguments, provided by suppliers of subsystems and software. The first thought was to provide a single, clean "interface point", where a section of argument and evidence provided by a supplier could simply be "plugged in", as shown in Figure 13. The hope was that suppliers could very simply be shown how their work would contribute to the overall safety case, and that this would simplify the process of contracting for safety-related work.

After some experimentation, however, it became clear that a single point interface like this simply would not work. Even though a supplier might be working on a

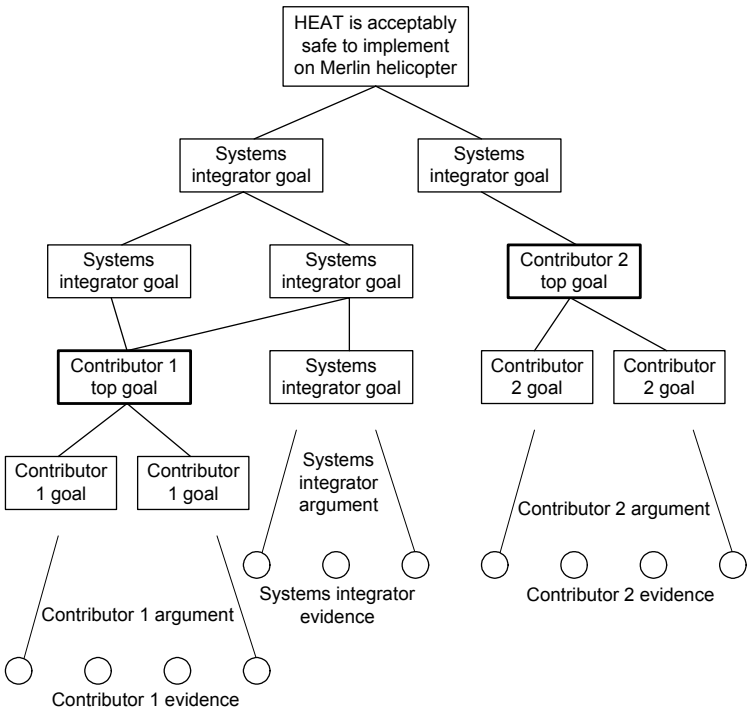

Figure 13 - Initial attempt at integrating supplier contributions to the safety case

relatively small item in terms of development, it was found that trying to pull all of their evidence contributions under a single goal led to unacceptable distortion of the argument structure. This was particularly true where there were both "product" and "process" elements to the information required from a supplier. Eventually, it was concluded that it was better to construct an "ideal" argument structure, without considering who would be responsible for sourcing each item of evidence. Provided that the PSC structure is in place sufficiently early in the project, it is possible to use this to show suppliers what they will be required to contribute, and how their contributions fit into the "big picture". Where a supplier is found responsible for supporting multiple safety case objectives, we recognised that their contributions to the overall safety case should be captured by means of an explicit safety case 'contract' between the top-level and supplier safety arguments – as discussed in (Kelly 2003).

5 Conclusions

This project has provided a convincing demonstration of the advantages of using GSN in safety case construction in an industrial setting. All of the participants in the project were impressed with how much the technique assisted in the

development and, especially, the review and acceptance of the Preliminary Safety Case. Although a lot of safety work remains to be done on the HEAT/ACT project, we are confident that the argument structuring work done on the PSC will provide a solid foundation for completion of the Interim and subsequent Safety Case phases.

It was particularly impressive to discover just how powerful the use of argument patterns could be. Not only did it permit very rapid progress, but we believe that this approach has helped to create a safety case which is more thorough and robust than that which might have resulted had the whole argument been constructed from scratch. A particularly significant feature of this project has been the reuse of ideas from other safety cases, and this is an approach we would strongly recommend to anyone starting work on a new safety case. Again, the use of GSN was extremely helpful here; it was easy to review existing material, and identify argument structures that were particularly compelling, or elegantly expressed.

The project encountered a number of practical issues, which have been discussed in section 5 above. None of these were especially difficult to resolve, but it is clear that, as with writing text, it is important to think carefully about the impression that is being conveyed through the way the GSN diagrams are structured.

A practical suggestion that we would like to make outside the scope of this project is that a discussion forum – perhaps a web site – where users of GSN, and specific GSN tools, could share pattern libraries and help each other out, would be beneficial to the safety community.

Our overall conclusion is that the use of GSN and a pattern library was of huge benefit to this project, and is an approach we would recommend.

6 Acknowledgements

The authors would like to thank Westland Helicopters Ltd for the opportunity to present this work. We would also like to acknowledge the support provided by the EPSRC-funded MATISSE project (grant no. GR/R/70590/01) for some of the work presented in this paper.

7 References

Adelard, 2003, *The Adelard Safety Case Editor – ASCE,* http://www.adelard.co.uk /software/asce/index.htm

Civil Aviation Authority, 2001, *SW01 – Regulatory Objectives for Software Safety Assurance in ATS Equipment* in Part B (Generic Requirements and Guidance) of CAP670 – Air Traffic Services Safety Requirements, London, UK.

Eurocontrol, 2001, *The EUR RVSM Pre-Implementation Safety Case*, http://www. eur-rvsm.com/safety.htm#precase.

Graham, K., 2002, *Heavy Modifications: A Three Stage Safety Process for Modification of Undocumented Legacy Systems*, MSc SCSE Project Report, Department of Computer Science, University of York, UK.

Kelly, T.P. & McDermid, J.A., 1997, *Safety Case Construction and Reuse Using Patterns* in Proceedings of 16th International Conference on Computer Safety, Reliability and Security (SAFECOMP'97), Springer-Verlag.

Kelly, T.P., 1999, *Arguing Safety - A Systematic Approach to Safety Case Management*, DPhil Thesis, Green Report YCST 99/05, Department of Computer Science, University of York, UK.

Kelly, T.P., 2003, *Managing Complex Safety Cases* in Current Issues in Safety Critical Systems: Proceedings of the 11th Safety Critical Systems Symposium, Springer-Verlag.

Kelly, T.P., et al., 2003, *Hazard and Risk Management & Safety Cases,* MSc SCSE module notes, Department of Computer Science, University of York, UK.

Ministry of Defence, 1996, *Defence Standard 00-56 Issue 2: Safety Management Requirements for Defence Systems*, Glasgow, UK.

Staple, A. & Handcock, A., 2002, *The All-Electric Rotorcraft – Challenges and Opportunities*, 28th European Rotorcraft Forum, Bristol, UK.