

The HEAT/ACT Preliminary Safety Case: A case study in the use of Goal Structuring Notation

Paul Chinneck

Safety & Airworthiness Department
Westland Helicopters, Yeovil, BA20 2YB, UK

chinnecp@whl.co.uk

David Pumfrey, John McDermid

Department of Computer Science
University of York, York, YO10 5DD, UK

david.pumfrey|john.mcdermid@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. The project therefore chose to adopt a phased approach to safety case development, beginning with a Preliminary Safety Case (PSC). Goal Structuring Notation (GSN) was chosen as the development method for the PSC, because of its perceived merits of ease of construction and clarity of review.

This work was first reported in a presentation at the UK Safety Critical Systems Symposium (SSS'04), which described the initial development of the PSC argument structure, and investigated some of the practical issues identified in using GSN.

This paper revisits the HEAT/ACT project. It reprises the original construction of the GSN argument, and goes on to show how the PSC has developed and evolved since that initial development phase. It examines how the GSN argument has been used in the interaction with other partners and sub-system suppliers involved in the HEAT/ACT project, and considers whether the effort expended in developing the PSC has lived up to expectations in its contribution to safety process management.

1 Background to the HEAT/ACT project

The HEAT/ACT project consists of replacing the conventional mechanical flight control system on a medium-lift helicopter with a fly-by-wire system (Juggins et. al. 2004, Staple and 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 electromechanical 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.

2 Safety case approach

With such a project, the safety concerns are obvious, and therefore a convincing and thorough Safety Case is paramount. UK Defence Standard 00-56 (UK Ministry of Defence 1996b), which defines the safety management requirements for defence projects “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).

Through a process of review with airworthiness authorities, the PSC would provide initial confidence that the design of the HEAT/ACT system was such that acceptable safety could be demonstrated. 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, so the scope of the Safety Case was to include an assessment of the impact of the modification on the safety of the whole aircraft.

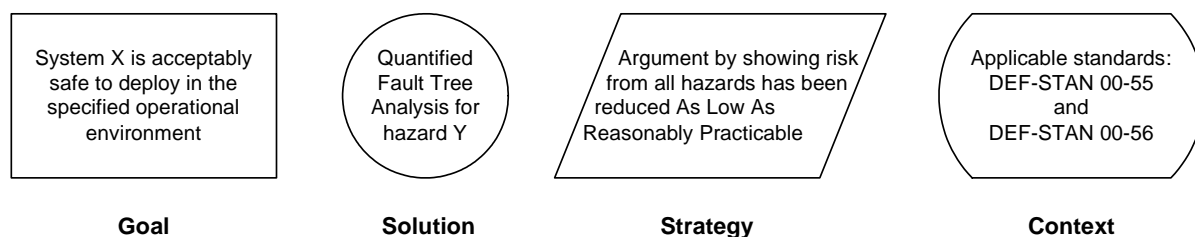


Figure 1 – Notation for principal GSN elements, with text showing example instances of each

Further safety case phases will follow to support major project milestones, such as hardware production and commissioning, and commencement of test flying (initially on a single aircraft). Each phase will use the preceding phase as a basis, refining and adapting the argument structure as the design evolves, and adding more complete evidence to support the argument. It was therefore vital that the safety argument presented in the PSC should be developed and presented in a way that would facilitate its future evolution. It must also support the engineering process by providing a structure in which to document safety activities and processes. 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.

GSN explicitly represents the individual elements of any safety argument (requirements, claims, evidence and context) and (perhaps more significantly) the relationships that exist between these elements (i.e. how individual requirements are supported by specific claims, how claims are supported by evidence and the assumed context that is defined for the argument). The principal symbols of the notation are shown in figure 1.

When these elements are linked together in a network they are described as a ‘goal structure’. The principal purpose of any goal structure is to show how goals (claims about the system) are successively broken down into sub-goals until a point is reached where the claims can be supported by direct reference to available evidence (solutions). The notation is also used to make clear the argument strategies adopted (e.g. selecting a quantitative or qualitative approach), the rationale for the approach, and the context in which goals are stated (e.g. the system scope or the assumed operational role).

Many different views exist on how (or even whether) GSN diagrams should be shown within delivered safety case documents. The approach chosen for HEAT/ACT was to present 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 subsequent phases of Safety Case development. As an aid to readers who are not familiar with the use of GSN, the PSC starts with an introduction to GSN notation, along with the more conventional description of the HEAT/ACT system.

3 Initiation and development of the Preliminary Safety Case

When work on the PSC began, preliminary safety planning and preliminary hazard identification and risk assessment activities had been completed for the project, but detailed specification, design and analysis had not been commenced. The timing of PSC initiation was therefore ideal, meeting both guidance (e.g. Kelly 2003) and the project requirements. In the programme of a typical project, this would 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 initial issue of the PSC.

The definition of the top goals of the GSN structure was relatively easy, building directly on commonly-described high-level arguments. However, developing the lower-level argument structures required to support these top goals initially proved problematic. Obstacles included concerns over how to manage the integration of existing safety evidence (e.g. for existing components being re-used in the HEAT/ACT system), as well as simple lack of inspiration in identifying suitable strategies for developing the argument.

These obstacles were largely overcome by a combination of the use of patterns (Kelly and McDermid 1997) – generic argument structures which must be *instantiated* for a specific system – and, even more effectively, by “borrowing and modifying” from a range of existing safety cases. The Pre-Implementation Safety Case for reduced vertical separation minima in European airspace (Eurocontrol 2001) was particularly useful for this activity. Ideas were also borrowed from an MSc thesis (Graham 2002), which developed a generic safety argument for modifications to existing aircraft; this provided some useful suggestions for how to tackle the arguments about integration of HEAT/ACT into the development helicopter. Examining how the authors of these and other safety arguments had solved the problems of instantiating patterns provided the inspiration to assist development of the argument, 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 could be adopted and adapted. The authors also found that reading and review of other safety cases were significant in building confidence in our own ability to recognise – and subsequently produce – well-structured and robust arguments.

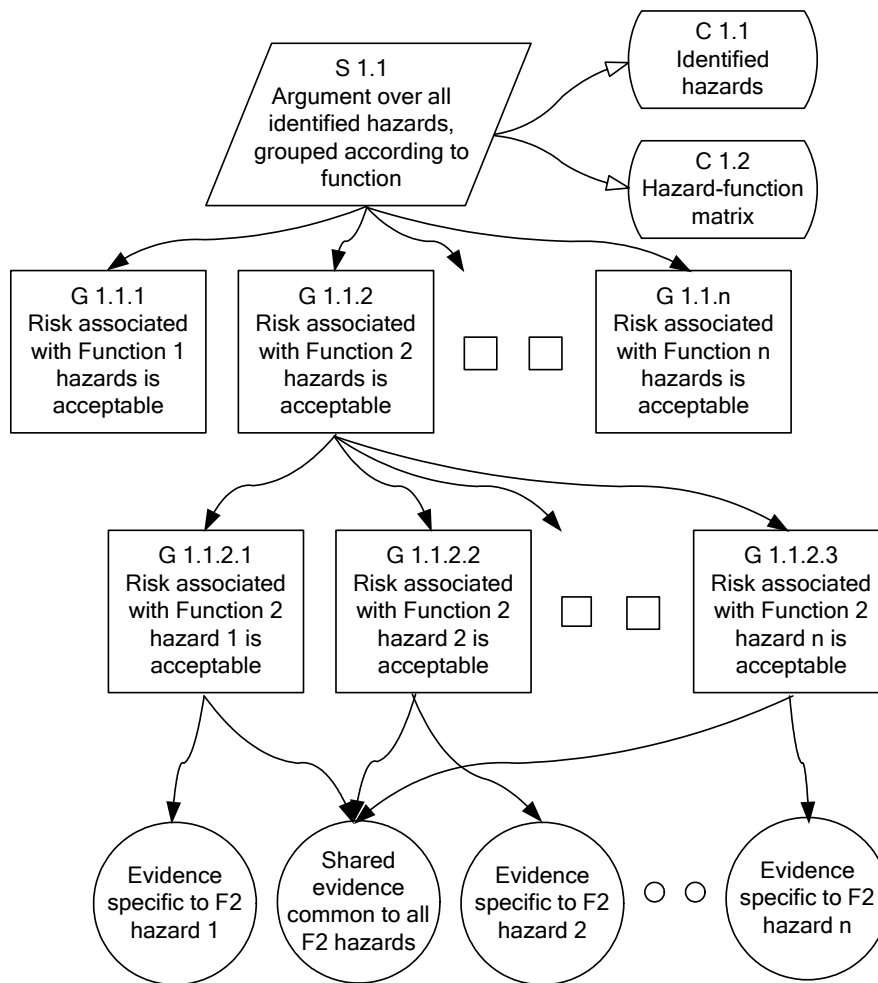


Figure 2 – Fragment of GSN showing the use of functional breakdown to organise identified hazards

Development of the PSC by the primary author began in mid-April 2003, and by the project Preliminary Design Review (PDR) at the end of May, the argument comprised 26 substantial pages of GSN structures. A further three weeks' work saw the document ready for signatory approval. To reach this stage, a number of substantive issues in both the structuring of the argument, and in its presentation in GSN, had been tackled and overcome, and (as we reported in Chinneck, Pumfrey and Kelly 2004) the authors were excited and encouraged by the progress made, and by the generally positive response of those who read and reviewed the PSC.

4 Moving on

With the top-level safety argument established in Issue 1 of the Preliminary Safety Case, work began on the compilation of Issue 2. The main purpose of this issue was to reflect project progress since Issue 1, especially the increased level of detail available about the system architecture. This would effectively be the first test of the appropriateness and extensibility of the high level argument structure that had been developed, and would give a good indication of whether it genuinely provided the capability for development throughout the life of the project. A further purpose of the up-issue was to incorporate the (minor, if numerous) comments received from interested parties.

To cope with the enormous amounts of design detail now available, a single document was no longer sufficient; separate Safety Cases were required for the major sub-systems. These documents would support and extend the overall system-level safety case, while also performing a stand-alone function for the particular system.

4.1 Sub-system safety cases

In structuring the HEAT/ACT PSC, a key approach to managing the “explosion” of complexity in the safety argument was grouping the identified hazards by system function. This made it possible to present information about related hazards in a logical progression, and to make it clear where there was commonality between the evidence presented for the hazards within a group, as sketched in figure 2. To help readers navigate this 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 to function and function to hazard relationships.

Once the system-level PSC had been issued, attention turned to these functions, and the required safety argument to show adequate safety for the equipment concerned. As we explained in our first paper (Chinneck, Pumfrey and Kelly 2004), the initial approach we tried

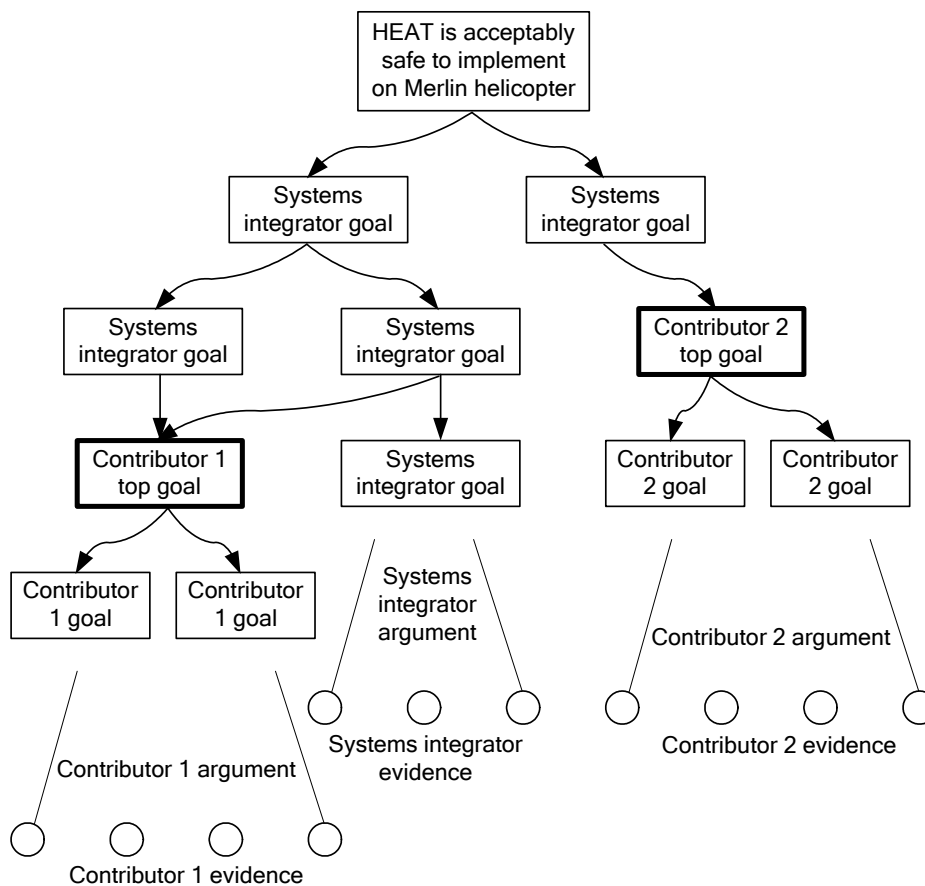


Figure 3 - Initial (unsatisfactory) attempt at integrating supplier contributions to the safety case, with single “interface points” for each contributor

was to structure the argument 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 3.

After some experimentation, however, it became clear that a single point interface like this led to unacceptable distortion of the argument structure. To produce a clear and comprehensible argument, it is essential to honour the logical relationships between goals – for example, keeping all sub-goals related to management of a single hazard together. In the HEAT/ACT system (and, we suspect, in most other large systems), these logical relationships do not follow sub-system or contractual boundaries (e.g. there may be causes of, or contributors to, a single hazard in many different subsystems). This was particularly true where there were both “product” and “process” elements to the information required from a supplier. We were therefore forced to think again.

This problem was solved when we realised that we had already constructed an “ideal” argument structure in the system-level PSC. By using this same structure as a self-imposed “pattern” to start the sub-system safety cases, we would ensure consistency with the system level argument, and suppliers would be able to see how their contributions “fitted in” to the whole. This breakthrough led to very quick construction of these lower-level safety cases.

Integrating these sub-system safety cases with the system-level safety case enabled previously unavailable detail to be shown. Issue 1 of the PSC contained suggested patterns, outlining how important arguments (such as showing how risks associated with each of the hazards had been reduced As Low As Reasonably Practicable) should be developed. Since each sub-system PSC now contains a development of this argument, the patterns are no longer required, and the hazard “leg” of the argument in the revised system-level PSC now stops at the functional split.

As well as meeting the requirements of UK Defence Standard 00-56, the HEAT/ACT system is being developed in accordance with Defence Standard 00-54 (UK Ministry of Defence 1999). (This standard – “Requirements for Safety Related Electronic Hardware in Defence Equipment” – is the hardware partner to the more widely-known software standard 00-55 (UK Ministry of Defence 1996a)). Annex B of Defence Standard 00-54 contains very clear guidelines for safety case contents. A flash of inspiration saw these guidelines turned into a generic GSN argument, which was then tailored for each function within the HEAT system. As well as providing a structure for the argument, a further benefit of this is that it will be easy to compile a compliance matrix (not yet implemented) against the 00-54 requirements, to show how the equipment safety case

complies with the standard. This will further reduce the time required to assess the final document.

One area on which 00-54 particularly focuses is the requirement to include “*a description of any outstanding issues that may affect the safety integrity of the [Safety-Related Electronic Hardware]*”. One of the first equipment safety cases to be written was for the Electrical Generation & Distribution System – clearly a fundamental requirement for a wholly electrically-powered primary flight control system. Following the issue of this safety case, various design reviews were held, with recommendations for potential changes to improve system integrity, required by the introduction of HEAT. The nature of the safety case allowed these “outstanding issues” to act as drivers for these recommendations, lending considerable weight to the resultant outcome. This in turn acts as good evidence to show the two-fold aspects of the design-safety relationship – safety should clearly drive design, but conversely no design change should ever be incorporated before suitably rigorous safety analysis has been carried out.

4.2 Supplier safety cases

Of the eight HEAT system functions required to have their own safety case, two are the responsibility of other HEAT consortium companies. These companies have taken the GSN methodology and expanded the information content at each level by their more textual approach. The resultant documents are similar to the reduced vertical separation minima Pre-Implementation Safety Case (Eurocontrol 2001), where the actual GSN breakdown is only 2 or 3 levels deep, with reference to textual paragraphs elsewhere in the document to act as solutions to the final sub-goals. For instance, one company has chosen to include a snapshot of the hazard log (perhaps more properly an issues/causes log, due to the sub-system level at which they are working) to which reference can be made within solution nodes in the goal structures. The resultant documents work well, with the singular reservation that the GSN and textual parts of the document appear less integrated than perhaps is desirable, making review not quite as straightforward as where the GSN “leads” the safety argument. That said, the very fact that the top-level structure is so similar to the HEAT PSC makes any correlation between the two effortless.

Of the sub-system safety arguments, some of the most challenging are those concerning parts of the design and implementation processes that have the potential to give rise to systematic errors. Here, no argument can ever be constructed to prove absolute freedom from such errors. Instead, process becomes paramount in arguing that the probability of any error (having catastrophic consequences) is beyond credence. There are many ways of approaching this argument, and providing sufficient evidence to support it. One method used for the HEAT programme is that of a process FMEA. This details the processes used, examines any potential shortfalls in those processes, and either explains why those shortfalls cannot happen, or identifies mitigation that ensures that they are benign should they occur.

4.3 Integration

Arguing the safety of the unfamiliar, novel technology of HEAT equipment has been challenging enough. But of equal importance is to ensure that the impact of this new equipment on the legacy platform and its associated systems is adequately analysed for safety. This analysis process is complicated because of differing safety management standards in use. The target aircraft (Merlin) is certified to British Civil Airworthiness Requirements (BCAR), largely civil-based, to satisfy which each system has independent Hazard Assessment, Detailed Analysis and Safety Assessment Report documents to argue its safety. The HEAT system, as explained earlier, is using Defence Standard 00-56 as its safety management standard, which results in a different approach to safety argument, and resultant document suite.

This potential mismatch between new equipment and legacy host platform has been very carefully managed and scrutinised. The logical approach has been to list all aircraft systems requiring the BCAR suite of safety documents (some 46 in total), and then to separate them into those completely unaffected, those physically changed by the introduction of HEAT (e.g. hydraulic power system) and those indirectly affected (e.g. where one or more of that system’s inputs or outputs is changed by HEAT installation). A further analysis has been carried out to identify situations where previously non-catastrophic failure conditions (e.g. total loss of AC power) are now catastrophic following the introduction of HEAT. This inevitably raises the question of “what if benign failure conditions were never noted in the extant safety analysis?” - an inherent problem with “reporting by exception”. This problem is an example of the “completeness argument” issue discussed in section 5.1 below. As with any such argument, the solution must rely on evidence about the quality of the safety process and the calibre of the staff conducting the analysis. In this respect, the relatively radical nature of the HEAT system is probably an advantage, in that it is obvious that it engenders new safety issues, and the focus of the design staff on the safety aspects of HEAT and its effects is beyond reproach in this instance.

The complex, inter-dependent nature of the HEAT system (and its host platform) hinges on the satisfactory (and safe) functional interaction between various parts of the systems. As the hazards have been allocated to functions and addressed in these groups, there is always a risk of missing hazards that cannot be allocated to any one function. To combat this, a further sub-system safety case is being created, entitled “Functional Interactions”. This will build on the work mentioned above (the list of impacted systems) and develop it to provide what some within the project are hailing an “aircraft-level” FMEA. This will bridge the potential gap between the sub-system safety cases and the overall system-level safety case, which is peculiar to the functional breakdown of hazards adopted.

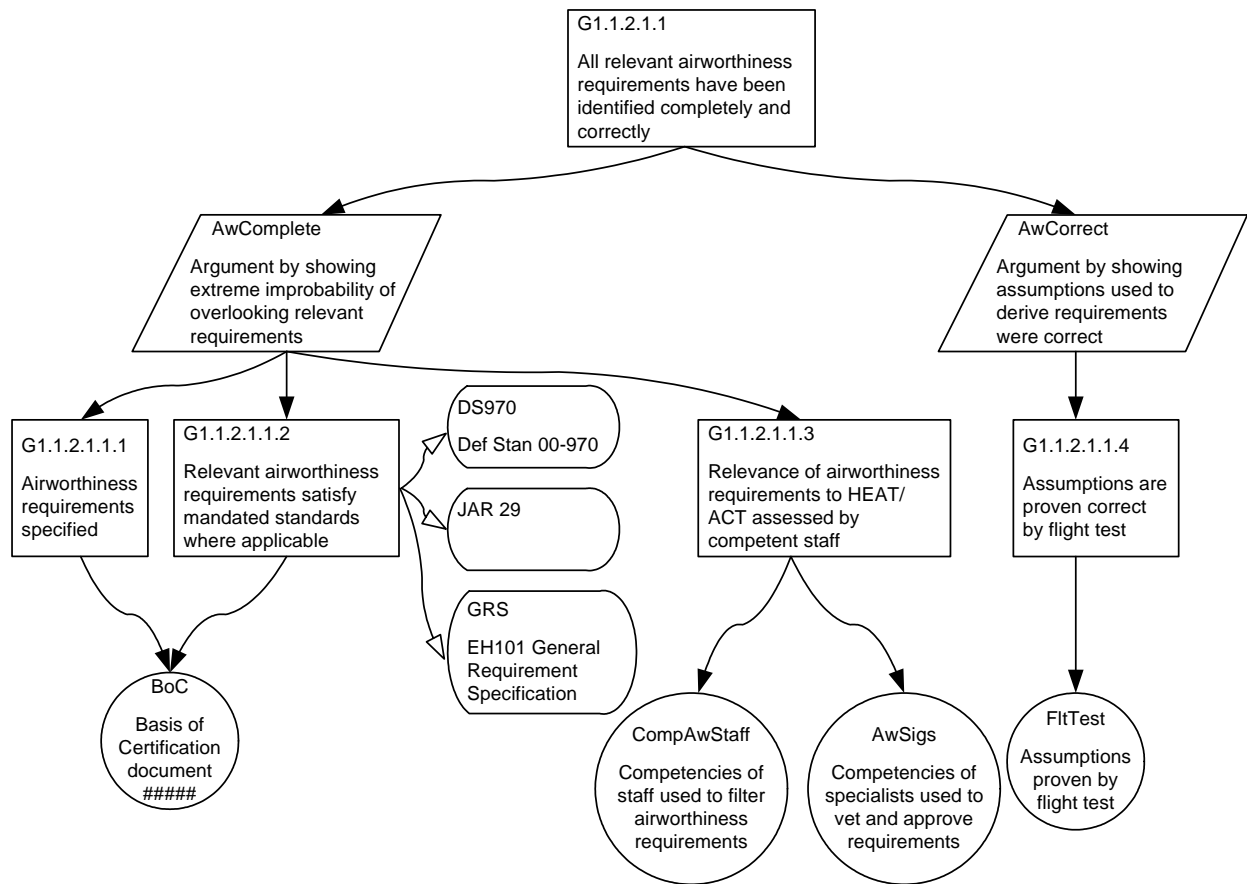


Figure 4 – Example of goal requiring argument of completeness

5 Meeting the challenges of argument evolution

Our previous paper described some of the challenges that had to be overcome in development of the top-level safety argument in the PSC. Inevitably, as the argument has evolved, a number of new issues have arisen, and this section considers some of the “generic” problems (i.e. those not specific to the HEAT system / Merlin integration) that we have tackled.

5.1 Completeness

One of the most challenging issues encountered in completing the goal structures was how to satisfy goals such as “All hazards addressed in accordance with ALARP principle” and “All applicable requirements and standards are satisfied”. The problem with these is that discharging them requires an argument of completeness, i.e. that all hazards or requirements have actually been identified. All that is required for such a goal to fail, as with any universal assertion, is a single counter-example.

In general, it is impossible to absolutely guarantee completeness of an activity such as hazard identification. There always remains the possibility that something has been overlooked, or that a hitherto unknown problem will be encountered with new technology. One possible approach to arguing safety in these circumstances would be to show that any such omission would be benign. This would, perhaps, be feasible for systems of low criticality, or for individual components within a highly-redundant

configuration, where external mitigation can be shown to prevent an unforeseen condition having critical consequences. However, such an approach is clearly not acceptable for system-level arguments about a high-consequence system such as HEAT.

In effect, since proof of completeness is impossible, the best that is possible in a safety case is to provide robust evidence that a significant omission is incredibly unlikely. The arguments presented must appeal to the engineering process to deliver this evidence. This was the general approach that was taken for the HEAT system and subsystem PSCs. The development of these goals followed a general pattern of identifying the *product* of the activity (the hazard log, or the list of requirements), backed up by a *process* argument supporting the claim that items had not been overlooked. Wherever possible, this process argument contains evidence of diversity within the process, e.g. an independent review of the primary activity, as well as supporting evidence such as the calibre and qualifications of the staff undertaking the activity.

An example of the development of such a goal (that all relevant airworthiness requirements have been captured completely and correctly) is shown in figure 4. Note that this argument is a little unusual, in that the process here is essentially a filtering exercise; the airworthiness requirements are collated from a variety of standards, and the critical activity is identifying those that are relevant to the HEAT project.

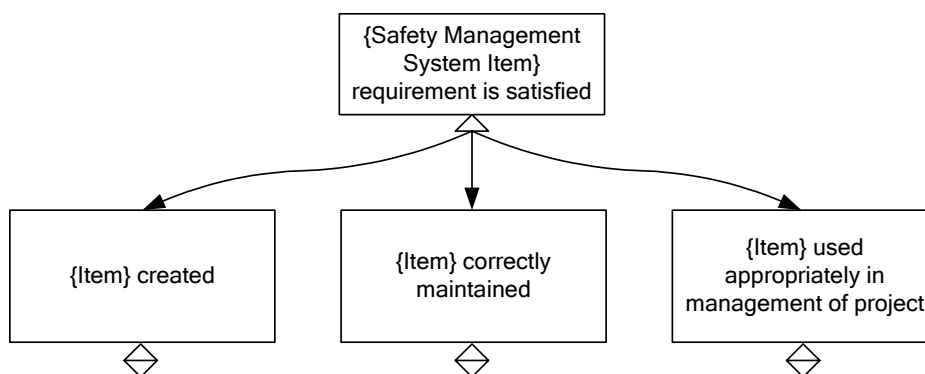


Figure 5 – Pattern for arguing correct use of safety management documents in the safety process

5.2 Purging of Assumptions

A further stage in the development of the safety case was the recognition of the importance of a review of assumptions. The argument presented in the initial release of the PSC did not contain a large number of assumptions, but it was clearly important to check that those that did exist were still valid and acceptable. Many more assumptions were introduced during the elaboration of the system level argument and construction of the subsystem safety cases. As the review process began, it became clear that the assumptions fell into two distinct groups; *external* and *internal*.

External assumptions are those that relate to “the world outside the safety case”, and their effect is generally to define or limit the scope of the safety case. For example, a key external assumption stated in the HEAT safety case relates to the initial phase of test flying; it is assumed that the aircraft to be used as a test platform was acceptably safe before it was modified, and that the safety case therefore need only present argument and evidence relating to the safety of the new systems, and the changes that were made to the aircraft in order to integrate these new systems.

Internal assumptions are those assumptions that relate to items that are within the scope of the safety case, or the activities that it describes. For example, to make progress in developing the argument, it may be necessary to “predict” the results of an activity that is not yet complete. Thus an argument relating to avoidance of single point failures might rely on the assumption that the designers will select a solution incorporating redundancy.

Clearly, these two classes of assumption need to be treated in quite different ways. External assumptions can be viewed as “genuine” assumptions, and there is no reason why they cannot remain in the completed safety case *provided* that their significance is recognised and accepted. For example, an assumption that “there is no need to test function X during initial flight trials” effectively introduces an important limitation, which needs to be respected. Kelly and McDermid (2003) have suggested the use of an explicit “assumption log” as part of the management of the safety critical system development process; it seems that this concept could usefully be extended to track assumptions throughout the life of the safety case.

Internal assumptions, on the other hand, are really “place holders” or unresolved cross-references, and are unacceptable in the completed safety case. In general, they must be converted into goals, and evidence presented to show that they have been discharged like any other goal. We described this process as “purging” of assumptions. What we observed was that internal assumptions frequently represent information that is “non-local”; i.e. where the safety argument that is being developed for one item relies on, or needs to refer to, the argument presented for another item in a different part of the safety case. In discussion of how these assumptions can be managed efficiently in a large, modular safety case, we concluded that it is often appropriate to represent them as “away goals”, as described in Kelly (2003).

5.3 The self-referential safety case

As work progressed, it became clear that the way the PSC was being used was, in itself, an important part of the safety process. This led us to add the various phases of the safety case as explicit evidence documents within the argument structure. Initially, the way this was done was somewhat unsatisfactory; the PSC and intended future phases were simply attached directly as evidence satisfying a single top goal of “safety case developed and maintained”. This did not seem a very “strong” structure, in that it made no real claims about the benefits of the very structured approach being taken to the development of the safety case.

In considering how we could make more use of the PSC in arguing the quality of the safety process, we realised that we had already presented a generic pattern (figure 5) for arguing about items required by the safety management system (SMS) (e.g. the hazard log and the safety programme plan). This pattern essentially recognises that it is not sufficient for a safety management document merely to exist; it must be shown to be being maintained, and being used appropriately in the process. Discharging the third sub-goal in this pattern (“{Item} used appropriately in management of project”) actually implies two things; that the role of the item is correctly defined and understood, and that the item really is being used in the defined role.

We realised that this pattern was more general than we had at first thought. Although developed initially to show

that explicit Defence Standard 00-56 SMS requirements were being discharged, this pattern actually applies to *any* process-related document, including the safety case itself. Thus we were able to significantly expand the argument about the PSC, showing how it has been developed, maintained and (most importantly) actively used to drive the development of the system. [Note, however, that it is not usually necessary to present this sort of argument for *evidence* documents such as safety analysis results; whilst it may be important to show that such documents are kept up-to-date as the design evolves, they have a sufficiently clear and limited role that it is unnecessary to present arguments about their use within the project.]

6 Acceptability of the GSN approach

A key requirement of the PSC was that it must be accessible (and acceptable) to all of the engineering and management disciplines involved in the project.

At various stages throughout the process of creating the PSC, a range of reviews was undertaken, and the benefits of GSN became clear during these reviews. At one point, the near-complete draft of Issue 1 (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.

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.

7 Looking to the future

As with any major project, HEAT/ACT is expected to have a long lifecycle, from the current development phase through to eventual deployment and use in service. It is important, therefore, that possible changes in the physical, operational and legal context of the safety case

are considered during its development. In fact, it is already clear that there will shortly be a major revision to one of the primary standards applied in the project – Defence Standard 00-56 – and the authors have considered how this will impact the argument and evidence presented in the Preliminary Safety Case.

The revised version of Defence Standard 00-56 (Issue 3) is intended to reflect the MoD policy that standards should be “as civil as possible, and only as military as necessary”. Thus the new standard sets goals, rather than prescribing processes. However, it is intended that good practice established under the current issue (Issue 2) of the standard (or possibly other standards) will meet the requirements of Issue 3. Thus, the authors believe that the argument presented in the PSC can be readily converted to a DS 00-56 Issue 3 form. The main changes required will be to explain the principles applied in constructing the argument, rather than referring to prescriptive clauses contained in Issue 2. In other words, the “spine” of the argument will remain the same, but some of the context and justification will change. Further, we believe it would be a good test of the wording of Issue 3 to check that this can be done, meeting all the goals, and without any core arguments becoming redundant

8 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.

Particular successes noted during the writing of the safety argument included:

- The structure of the PSC document, with GSN fragments introducing and explaining the safety argument in small sections, has proved very successful in breaking the (inevitably large) safety argument down into fragments that can be readily grasped by reviewers and readers alike. This structure was developed for HEAT/ACT without experience of alternative approaches, although it has since been found to be similar to the approach taken by authors of a number of other large safety cases.
- The structured approach helped in significantly reducing re-work, as many of the revisions required during the development were merely expansions of earlier work, rather than the complete re-writes of sections that would be required in a purely textual document.
- 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.

- 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. To date, no question has ever been raised for which the questioner could not be directed to some part of the Safety Case – an impressive testament to the completeness, validity and robustness of the argument.
- 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.

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.

9 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.

10 References

- Chinneck, P., Pumfrey, D.J. and Kelly, T.P. (2004): Turning up the HEAT on Safety Case Construction. In *Practical Elements of Safety: Proceedings of the Twelfth Safety-critical Systems Symposium*. 223-240. REDMILL, F. and ANDERSON, T. (eds). Birmingham, UK, Springer.
- Eurocontrol (2001): The EUR RVSM Pre-Implementation Safety Case. <http://www.eur-rvsm.com/safety.htm#precase>. Accessed 1 Jun 2004.
- Graham, K. (2002): Heavy Modifications: A Three Stage Safety Process for Modification of Undocumented Legacy Systems. MSc Project Report. Department of Computer Science, University of York, York, UK.
- Juggins, P., Handcock, A., Gilmour, J. and Chinneck, P. (2004): Design and Qualification Requirements for a HEAT Fly-by-Wire System for the EH101. *American Helicopter Society 60th Annual Forum*. Baltimore, MD, USA.
- Kelly, T.P. and McDermid, J.A. (1997): Safety Case Construction and Reuse Using Patterns. *Proc. 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, York, UK.
- Kelly, T.P. (2003): Managing Complex Safety Cases. In *Current Issues in Safety Critical Systems: Proceedings of the Eleventh Safety-critical Systems Symposium*. 99-115. REDMILL, F. and ANDERSON, T. (eds). Bristol, UK, Springer.
- Kelly, T.P. and McDermid, J.A. (2003): Hazard and Risk Management & Safety Cases. MSc SCSE module notes. Department of Computer Science, University of York, York, UK.
- Staple, A. and Handcock, A. (2002): The All-Electric Rotorcraft – Challenges and Opportunities. *28th European Rotorcraft Forum*. Bristol, UK.
- UK Ministry of Defence (1996a): Defence Standard 00-55: Requirements for Safety Related Software in Defence Equipment. Glasgow, UK.
- UK Ministry of Defence (1996b): Defence Standard 00-56 Issue 2: Safety Management Requirements for Defence Systems. Glasgow, UK.
- UK Ministry of Defence (1999): Interim Defence Standard 00-54 Issue 1: Requirements for Safety Related Electronic Hardware in Defence Equipment. Glasgow, UK.