

Qualitative analysis of dependability argument structure (Extract)

Mark A. Sujan¹, Shamus P. Smith², Michael D. Harrison³

¹University of York, ²University of Durham, ³University of Newcastle upon Tyne

1 Introduction

Structure is key to understanding the strength of a dependability argument. It can be used to analyse such arguments, highlighting properties that are indicative of weak arguments. Generic mechanisms can be developed for strengthening arguments based on structure that can be applied to specific arguments. Within this structure, appeal may be made to barriers or defences to demonstrate that unacceptable consequences can be protected against or prevented. This chapter explores the role that structure can play, using as an example the public domain Reduced Vertical Separation Minimum analysis published by EATMP (the EUROCONTROL Programme for Performance Enhancement in European Air Traffic Management). In order to perform the analysis the structure of the argument, and the use of barriers, is modelled explicitly with the aid of Goal Structuring Notation (GSN). The chapter also considers how confidence in the validity of an argument may be gained by a variety of means including operational feedback if the system (or a previous version of it) is already in service, or from specific design documents and stakeholder interviews.

Sections 2 and 3 discuss the general structure of dependability arguments and the role of barriers in these arguments. Section 4 reflects on the quality of an argument and presents generic ways of strengthening arguments. Section 5 further explores these structural aspects in relation to the Functional Hazard Analysis for the introduction of Reduced Vertical Separation Minimum (RVSM) within European airspace. Section 6 summarises and discusses the principal findings of this study.

2 The role of structure in descriptive arguments

Well-formed dependability arguments that support the assessment of their validity should have a structure that consists (to a first approximation) of claim, argument and evidence. The *claim* is the property or statement which we would like to assert (and argue for), and may be structured for example as a safety requirement, a safety objective, a target level of safety, or a derived sub-goal. To support this claim, specific *evidence* is produced that should relate to the claim.

The *argument* explains how evidence supports the claim. The relationship between claim and evidence is made explicit as rules, principles, inferences and so on. Both evidence and argument are therefore crucial elements of the overall dependability argument. Poor evidence will weaken confidence that a claim can be supported. Strong or true evidence will not support a claim if the evidence is not sufficiently related to the claim, or if the assumption of their relationship is shown to be wrong.

3 The structure of barriers in arguments

References to barriers (for the concept of barriers see for example [8; 7]) commonly form part of the evidence intended to demonstrate that either a hazard's probability of occurrence is reduced (preventive barrier), or that the severity of the consequences of the hazard is contained (protective barrier).

The dependability argument defines a structure for describing how these barriers are used in mitigation. This structure can describe relationships between barriers both temporal and logical. Temporal order can describe whether a barrier is intended to prevent a hazard or protect from its consequences (and it can describe temporal order within these categories). Order can also describe different degrees of mutual dependence, including simple logical relationships. Barriers may prevent a hazard or protect from its consequences interdependently by forming a logical AND-relationship. They may also perform the function of prevention or protection independently (thus forming an OR-relationship). It is also possible that a barrier is the only preventive or protective obstacle for a particular hazard. These idealised relationships ignore the different degrees of dependence and relevance of each barrier. This kind of reasoning can serve as the basis for analysis.

Structure may focus on the identification of weak spots by highlighting single barriers for high-risk hazards, or by enabling a more comprehensive understanding of potential dependencies. These observations and understandings can feed back into the design and into the dependability argument. The analysis can also focus on validating assumptions made about performance and independence of barriers through operational feedback.

4 The Quality of an Argument

Uncertainty within a dependability argument can arise from:

- uncertainty attached to the evidence
- uncertainty attached to the argument
- the degree of coverage of the evidence

Dependence of the pieces of supporting evidence on one another is also an important aspect of the structure of an argument that can be analysed. Evidence can support a claim by itself (single support), or a number of pieces of evidence may support together a claim (linked support), or they may support independently of one another a claim (diverse support).

The general structure of arguments may be used to derive generic ways of strengthening specific arguments or to increase confidence in their validity.

One approach relies on increasing the depth of the argument pattern. The type of uncertainty addressed is related to the rigour demanded by the third party, and not to the uncertainty inherent in the evidence or warrant itself. Depth-approaches ‘explain better’ (or in more detail) the argument, thereby increasing our confidence, and potentially also pointing out hidden assumptions or other problems.

To address *uncertainty inherent in the evidence or in the warrant* the breadth of an argument should be increased. Breadth-approaches are needed that provide diversity to the evidence.

A common approach to arguing for the dependability of a system in the context of a breadth-approaches by means of a ‘product-leg’ and a ‘process-leg’. It is often the case that different argument legs are not independent or fully diverse, and this poses a problem in determining the confidence that can be placed in the argument (for a discussion about this particular problem see Chapter 13 by Littlewood and Bloomfield).

A final aspect of argument quality illustrated in this chapter is the *provision of sufficient grounds* to draw a conclusion or claim. Diverse evidence, for example through the introduction of a second argument leg is required to ensure sufficient coverage.

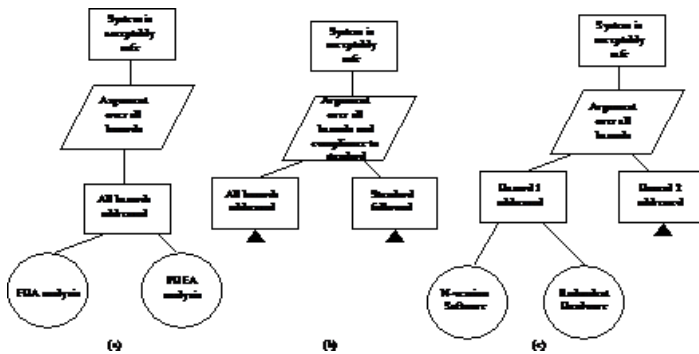


Fig. 1. Examples of using breadth to increase the confidence of arguments by reducing uncertainty. (a) diverse evidence (b) diverse argument (c) diverse barriers

Figure 1 provides generic examples of different ways to strengthen arguments by increasing their breadth in order to reduce uncertainty (using a notation that derives from GSN [9]).

5 Case study: RVSM functional hazard analysis

The Functional Hazard Analysis (FHA) which provided evidence for the Eurocontrol Reduced Vertical Separation Minimum (RVSM) pre-implementation safety case was analysed.

In the analysis below nineteen hazards are analysed out of a total number of 72. The FHA arguments in the document are provided in textual form. This makes it difficult to analyse and describe structure and dependencies precisely. These difficulties have been pointed out in other papers [9; 1]. Arguments were transformed post-hoc into GSN, see figs. 2 and 3 for an example. For the sake of clarity, essential GSN elements such as context have been deleted.

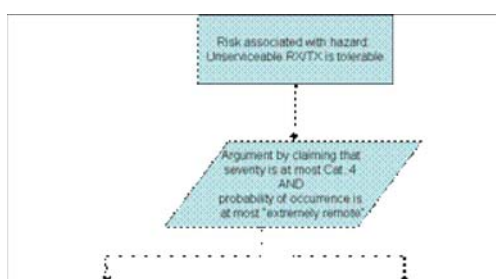




Fig. 2. Detail from Hazard Mitigation Argument Ref. 1.15: Top-level and probability branch (not showing context etc.)

Figures 2 and 3 show the structure of the argument demonstrating that the risk arising from a failure of the airborne communication equipment (RX/TX) is tolerable. All arguments follow the same top-level structure: the claim that the risk arising from a hazard is tolerable is broken down into a claim that the severity is at most x , and a second linked claim that the probability of occurrence of this hazard is not greater than y .

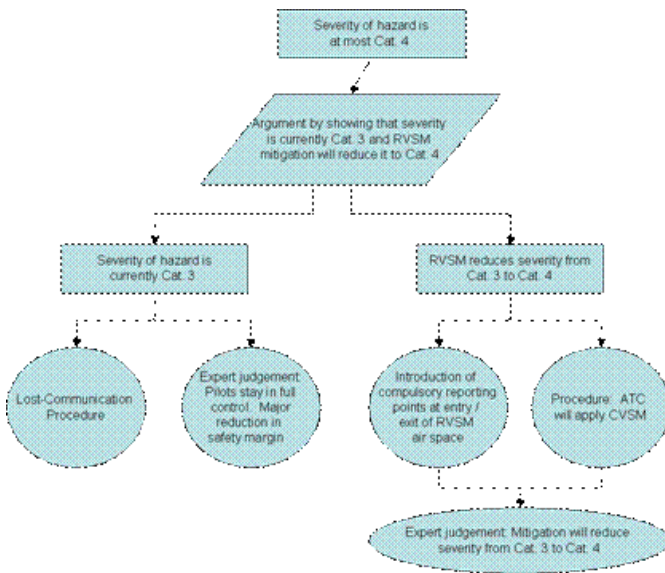


Fig. 3. Detail from Hazard Mitigation Argument Ref. 1.15: Severity branch (not showing context etc.)

5.1 Structural analysis: depth and breadth of arguments

Structural analysis proceeds by investigating the depth and the breadth of the arguments conducted separately for both the severity and the probability branch.

Table 1 shows that 23 out of 38 arguments possess a depth of 1, while only 15 arguments are developed to a deeper level. A common argument consists of top-level claims that the severity of occurrence of the hazard is at most x , while the probability of occurrence is at most y . This is supported directly by evidence, consisting of a description of operational consequences (severity) and expert judgement (probability). Many of the mitigating factors are not explained to a high level of detail, which makes a thorough analysis of, in particular, potential dependencies or hidden assumptions more difficult.

	Depth = 1	Depth > 1
Probability Branch	9	10
Severity Branch	14	5
Σ	23	15

Table 1: Analysis of the depth of probability and severity branches

The statistical analysis of argument breadth is presented in Table 2. Overall, 77 support patterns have been identified in the 19 arguments. Of these, 36 support patterns were single support, 30 linked support and 11 diverse support. Arguments employing linked/dependent support consist usually of a description of operational consequences intended to demonstrate that the severity of hazard is at most x .

A linked/independent support pattern is employed in the safety case to express an argument scheme of the kind “The probability of occurrence currently is at most z , **and** the RVSM mitigation will reduce it further, **so** the probability of occurrence is at most y ”. Ten out of 12 linked/independent support patterns in the probability branch were of this kind.

Finally, 10 out of the 11 diverse/independent support patterns were found in the probability branch. About half of these are of the type “RVSM mitigation reduces the probability of occurrence to y , **and in addition** any future problems will be dealt with quickly, **so** the probability of occurrence is at most y ” (or comparable phrases with expert judgement and additional

mitigation). While both pieces of supporting evidence are independent of one another, it is obvious that only the first piece of evidence provides sufficient grounds. Assessment of the remaining diverse / independent patterns proved to be difficult because of relatively low elaboration as was discussed in the analysis of the depth of the arguments.

	Single	Linked		Diverse		
		<i>Independent</i>	<i>Dependent</i>	<i>Independent</i>	<i>Dependent</i>	
Probability	24	12	0	10	0	
Severity	12	5	13	1	0	
Overall	36	17	13	11	0	$\Sigma = 77$

Table 2: Analysis of the support pattern types and their dependence

5.2 Barrier Analysis

A final stage in the analysis was to consider the use of barriers in the hazard mitigation arguments. Overall, 26 preventive barriers and 27 protective barriers were referenced. Among preventive barriers, the most common are monitoring programmes, procedures, adaptation of systems to accommodate RVSM, and training. Protective barriers are mainly concerned with the controller managing the situation, often according to some kind of procedure not explained in greater detail. There is little mention of any kind of technological barriers or technological support. As was mentioned in relation to the discussion of argument depth and breadth there seems to be a tendency to simplify complex issues into generic statements such as “*The crew will regain control*”, without explicit reference to how this is achieved and on what kind of support it relies. The feasibility of an approach such as this should be assessed.

6 Conclusions

Operators of safety-critical systems are required to provide a clear and convincing argument that their system is acceptably safe. This chapter has explored the structure of descriptive arguments as they are commonly found in safety and assurance cases. The aim of this chapter has been to provide a conceptual toolset enabling better understanding, construction, and assessment of dependability arguments.

Starting from a general structure of arguments, aspects influencing the quality of an argument have been identified, including the uncertainty inherent in the evidence, uncertainty inherent in the argument (i.e. in the warrant or backing), the coverage of the evidence, as well as the relationship and the dependence of the pieces of supporting evidence on one another. In order to assess the quality of an argument, and to improve confidence, two structural characteristics – depth and breadth – have been presented. The depth of an argument relates to the rigour of the argument, while the breadth of an argument relates to uncertainty and coverage.

Dependability arguments appeal to barriers in order to demonstrate that the risks arising from particular hazards have been mitigated sufficiently. Within the argument a structure of these barriers is implicitly defined. The chapter has argued that an explicit consideration of these barriers, i.e. of their temporal and logical order as well as of their relationship and dependence on one another, may be useful in the assessment of the quality of an argument.

The case study attempted to demonstrate how this conceptual toolset can be applied, and what kind of reasoning it supports. The results of this analysis were insights into the structure and quality of the arguments, such as the high level of abstraction of the arguments (low depth), and the high ratio of linked versus diverse support patterns. The arguments are not developed in detail and do not provide much diversity to reduce uncertainty or to increase coverage. Possible reasons for this could be the nature of the FHA process, and the nature of the change argued for, as well as the nature of the argument itself.

FHA is usually conducted in brainstorming sessions, bringing together a number of experts and stakeholders from different backgrounds. The views of the people on the system under investigation are distinct to maximise the benefit of the FHA. This, however, may explain the lack of depth in the dependability argument. Hazards are addressed one by one, and immediate mitigation solutions are provided without reference to an ‘overall’ shared safety architecture, and without developing the argument to a greater degree of rigour.

The introduction of RVSM to the European airspace is considered in terms of its safety case as a modification to an already existing system aimed at facilitating the management of increasing levels of air traffic. As such, the argument is concerned with features added to the current system, without concerning itself explicitly to a great extent with the details of the existing system. Therefore, the evidence provided consists of additional procedures and so on without explaining in detail the entirety of the underlying safety principles. As a result, it makes the task of deriving a consistent and coherent safety architecture and of assessing potential dependencies among the mitigation solutions more difficult.

The kind of exercise described in this chapter should be the responsibility of the authors of the dependability argument. The techniques illustrated provide an effective framework within which such analysis can take place. The explicit representation of mitigation solutions (i.e. barriers) provided for each hazard, facilitates the assessment of potential dependencies of these solutions among a number of otherwise unrelated hazards.

References

- [1] Adelard (2005) The assurance and safety case environment – ASCE.
<http://www.adelard.co.uk/software/asce/>
- [2] Eurocontrol (2001a) EUR RSVM programme: Functional hazard assessment. Working Draft 1.0, European Organisation for the Safety of Air Navigation.
- [3] Eurocontrol (2001b) EUR RVSM programme: The EUR RVSM Pre-Implementation Safety Case. Version 2.0
- [4] Eurocontrol (2001c) Eurocontrol Safety Regulatory Requirement 4: Risk Assessment and Mitigation in ATM. Version 1.0
- [5] Eurocontrol (2004) Air Navigation System Assessment Methodology. Version 2.0
- [6] Govier T (1988) A practical study of arguments. Wadsworth.
- [7] Harms-Ringdahl L (2003) Investigation of barriers and safety functions related to accidents, Proceedings of the European Safety and Reliability Conference ESREL 2003, Maastricht, The Netherlands
- [8] Hollnagel E (1999) Accidents and Barriers. In: Hoc J-M, Millot P, Hollnagel E, Cacciabue PC (eds) Proceedings of Lex Valenciennes, Volume 28, Presses Universitaires de Valenciennes, pp. 175-182
- [9] Kelly TP (1999) Arguing Safety – A Systematic Approach to Managing Safety Cases, PhD Thesis, Department of Computer Science, University of York, England.
- [10] Kelly TP, McDermid JA (2001) A Systematic Approach to Safety Case Maintenance, Reliability Engineering and System Safety, volume 71, Elsevier, pp 271-284
- [11] Smith SP, Harrison MD (2005) Measuring Reuse in Hazard Analysis. Reliability Engineering and System Safety, volume 89, Elsevier, pp 93 – 194
- [12] Smith SP, Harrison MD, Schupp BA (2004) How explicit are the barriers to failure in safety arguments? In: Heisel M, Liggesmeyer P, Wittmann S (Eds), Computer Safety, Reliability, and Security (SAFECOMP'04), Lecture Notes in Computer Science Volume 3219 Springer, pp 325-337
- [13] Toulmin SE (1958) The uses of arguments, Cambridge University Press.
- [14] UK Ministry of Defence (2004). Interim Def-Stan 00-56: Safety Management Requirements for Defence Systems
- [15] Weaver R, Fenn J, Kelly T (2003) A pragmatic approach to reasoning about the assurance of safety arguments. In Proceedings 8th Australian Workshop on Safety Critical Systems and Software.