# Chapter 14

# Qualitative analysis of dependability argument structure

Mark A. Sujan[1], Shamus P. Smith[2], Michael D. Harrison[3]

[1]University of York, [2]University of Durham, [3]University 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.

Argumentation communicates and thereby assures a system's dependability to a third party. In addition to the value of the argument as a demonstration of dependability itself, the process of providing such arguments can improve the dependability of a system. This is particularly so when incremental approaches to safety or assurance case development [10] are employed, as mandated by an increasing number of standards, such as the UK Def-Stan 00-56 [14] or the Eurocontrol Safety Regulatory Requirement 4 [4] as expressed in the best practices description of the Eurocontrol Air Navigation System Safety Assessment Methodology [5]. Convincing the third party that an argument of dependability is adequate is a difficult task, and for this reason quantifiable arguments that can be repeated are preferred to descriptive arguments that convince through their clarity, exhaustiveness and depth. These are all qualities that are difficult to measure. In practice it is often impossible to quantify the likelihood of undependability of a system that is yet to be fielded and has only been tested in a limited, possibly simulated set of conditions. The chapter is concerned

with the adequacy of descriptive arguments. It makes two claims, both claims using the structure of a descriptive argument.

The first claim is that general structural characteristics of arguments may be used as a basis for reflection on a specific argument's adequacy based on notions such as depth, coverage and strength of mitigation. Structural characteristics can be used to derive generic mechanisms for strengthening arguments which can be instantiated within the context of a specific argument. Previous work was concerned with the reuse of arguments [11]. The second claim is concerned with the implicit structure of defences or barriers. Appeal to barriers [8; 7] typically forms part of the mitigation argument, intended to demonstrate that either a hazard's likelihood of occurrence or the severity of its consequences have been sufficiently reduced. Making this use of barriers explicit within the structure of the argument can be helpful in analysing and assessing how the barriers are implemented in the actual system (or a previous version of the system), and whether there are any potentially weak spots, such as single barriers for high-risk hazards, or independent barriers for which operational feedback provides evidence of common failure behaviour. This develops previous work that began to establish an agenda for assessing the use of barriers in dependability arguments [12].

The use of diverse or multi-legged arguments as a means of increasing the confidence to be attached to dependability arguments is a frequent practice in safety-critical industries. For example, one leg may contain an argument about the dependability of the system backed by direct evidence, such as operational testing. The other leg may then be concerned with the demonstration that the evidence produced in the first leg is trustworthy, or that the overall design process followed has adhered to some industry-specific and relevant standard. This second type of evidence is indirect in that it does not make any direct claim about product quality. Whether assumptions of diversity can be made in a specific argument is not thoroughly understood (an issue that is considered in more detail in Chapter 13 by Bloomfield and Littlewood). This chapter is mainly concerned with *exploring qualitatively the structure of dependability arguments*, in particular direct arguments which include references to barriers. Chapter 13 presents an attempt to address the issue of multi-legged arguments formally.

In this chapter, 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. It may be claimed for example that a computer program achieves its required safety objective perhaps described as a certain probability of failure on demand (pfd). It may be assumed that in order to ensure that adequate levels of software reliability have been achieved, statistical testing has been performed on consecutive versions of the program. In order to support the claim, reference may be made to testing results that are provided as evidence.

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. The argument above claims that statistical testing performed on a representative operational profile is indicative of the reliability that the software will exhibit in actual operation.

This general structure of arguments is analysed in [13]. Here Toulmin distinguishes six different components, four of which form the basis for the analysis of this chapter. The claim or conclusion has already been discussed. Toulmin further refers to the evidence produced in support of the claim as *data*. The general rule or principle explaining the relationship between data and claim is referred to as a *warrant*. Toulmin also distinguishes the evidence produced to support the claim from the evidence produced to explain the authority of the warrant. This latter type of evidence is referred to as *backing*. The two kinds of evidence are substantially different since, while data is usually specific to the particular claim and is derived from the system or object under consideration, backing is specific to the general warrant, and can be derived from any number of domains, such as an underlying taxonomy, legal statutes and so on. Furthermore, the explicit distinction between a warrant and its backing also illustrates their difference in practical function. While the warrant is general and applies to all appropriate arguments, the backing is factual and specific in nature. In the computer program example the warrant would be backed by providing exact references to authorative studies in software dependability which have shown that the error in the prediction of the reliability of specific software systems was below some small threshold $\varepsilon$ when operational profiles were used during testing which deviated from the actual profile during operation by no more than a small measure $\delta$. This backing used to support the warrant consists of concrete, factual information. The warrant, on the other hand, posits a general and practical rule for how, given these facts, certain evidence may be used within an argument to support specific claims.

It is common practice to abbreviate the terminology and the corresponding structures. This results in an imprecise use of the terms, and blurs the distinction originally intended by Toulmin. For example, often the explicit distinction between warrant and backing is not represented. The warrant-backing structure is treated instead under the single heading ‘argument’. The term ‘argument’, on the other hand, also

refers to the overall data-warrant-backing-claim structure. It may be more appropriate to refer to the overall argument as 'argument structure', and to the warrant-backing structure as 'argument' to avoid confusion. For the sake of simplicity, the term 'argument' in its dual meaning is used in this chapter on occasions where the exact meaning should be clear from the context.

The general structure of arguments (i.e. argument structures) and a further hypothetical example from aviation are shown in Figs. 1 and 2.

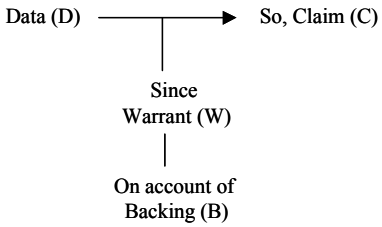


**Fig. 1.** Toulmin's original argument structure (excluding Qualifiers and Rebuttals)

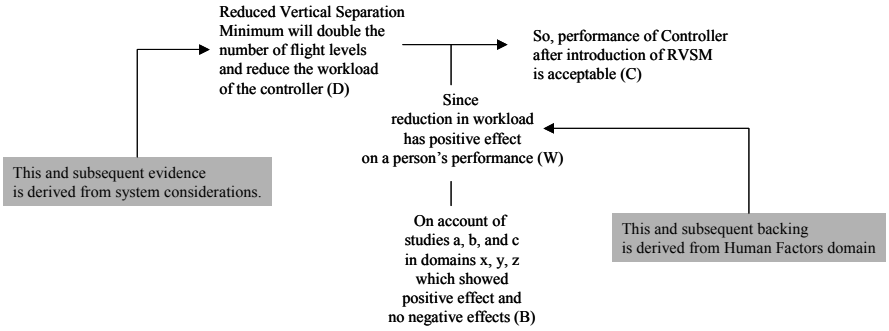


**Fig. 2.** Argument structure example set in aviation[1]

In the hypothetical aviation example of Fig. 2 it is claimed that the performance of the Air Traffic Controller (ATCO), after the introduction of a modification to the European airspace (RVSM), is acceptable. The evidence offered states that the number of flight levels available to the ATCO will double as a result of the introduction of RVSM, thus reducing the controller's workload. More flight levels will allow a more flexible assignment of aircraft to different flight levels. This supporting evi-

[1] It is very unlikely that this argument would be acceptable as it currently stands. The evidence does not provide sufficient grounds to move to the conclusion even if it were true. The quality of an argument is discussed further in Section 4.

dence derives from considerations about the specifics of the airspace layout and of the air traffic management. The warrant, in turn, explains why this data supports the initial claim. It is stated that in general a reduction in workload may have positive effects on a person's performance. It is assumed therefore that an intervention that leads to a reduction in controller workload will *presumably* have positive effects on the operator's performance, and *probably*[2] lead to acceptable controller performance. This is based on the assumption that it had been acceptable before the intervention. The warrant is not derived from a specific air traffic control environment, but from the more general human factors (or aviation psychology) data. The backing of the warrant in this case is a reference to authoritative studies, which apparently found that a reduction in workload had only positive and no negative effects on the operator's workload in the systems under consideration. As a note of caution it should be added, that this example of a hypothetical argument has been constructed deliberately in a weak way, as it illustrates not only the general structure of an argument, but also considerations of the quality of an argument (see Section 4 for a more thorough discussion).

## 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). A barrier may be an individual physical component of the system realising a specific safety function. Generally speaking however a barrier is a socio-technical system involving a combination of technical, human and organisational measures. Examples of barriers include physical interlocks preventing critical actions from being carried out at inappropriate times, guards preventing people making contact with dangerous parts of the system (physical obstructions, warning signs, procedures and so on), or a combination of a person (or people) interacting with equipment or advisory systems and relying on procedures. An aviation example of such a combination is the Lost Communication Procedure that is used when an aircraft is not fulfilling the required equipment standard in the RVSM space because of a communication equipment failure. This procedure defines actions to be carried out by the air traffic controller, as well as by the aircraft crew with their respective supporting technology. Hence the barrier, abbreviated as Lost Communication Procedure, comprises many socio-technical aspects (and many further barriers at lower levels of abstraction). Hollnagel [8] distinguishes between the function that a barrier fulfils and the system providing this function (barrier system). Barrier functions could involve the prevention of a particular hazard or the protection from the

[2] The qualifiers *presumably* and *probably* form an important part of Toulmin's argument structure (Toulmin, 1956) that are not elaborated here. They provide an indication of the degree of strength that the data confer on the claim given the specific authority of the warrant.

hazard's consequences. Barrier systems, on the other hand, can be classified in the following way:

- *Material barrier:* A barrier which prevents a hazard or protects from a hazard through its physical characteristics, e.g. a physical containment protecting against the release of toxic liquid.
- *Functional barrier:* A barrier that prevents a hazard or protects from a hazard by setting up certain pre-conditions which have to be met before a specific action can be carried out or before a specific event can take place, e.g. a door lock requiring a key, or a logical lock requiring a password.
- *Symbolic barrier:* A symbolic barrier requires an interpretation by an agent to achieve its purpose. Examples include all kinds of signs and signals.
- *Immaterial barrier:* A barrier which has no physical manifestation, but rather depends on the knowledge of people. Examples include rules or expected types of behaviour with respect to a safety culture.

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. The structural model derived from the dependability argument could then be used to analyse assumptions made when an older system or parts of the new system are already in place based on this feedback.

## 4 The Quality of an Argument

Confidence in an argument can be increased by ensuring that the evidence [6]:

- is acceptable or true
- is relevant to the claim
- taken together, provides sufficient grounds to move to the conclusion.

Conversely uncertainty can arise from:

- uncertainty attached to the evidence (for example, experimental assessments of workload levels)

- uncertainty attached to the warrant or argument (for example, the basic rule that a reduction in workload results in improved system safety)
- the coverage of the evidence (for example, is a reduction in workload by itself sufficient to claim that controller performance is acceptable?)

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. Govier, when describing "Support Pattern Types" ([6], see also [15]), makes a distinction between single, linked and convergent argument support. The means by which evidence can support a particular claim are distinguished. Structures can be used to mirror the logical structures discussed in relation to barriers. A *single support* type implies that a claim is supported by a single argument (i.e. a single evidence-warrant-backing structure). A claim may also be supported interdependently by a number of arguments, where each argument's support rests on the validity of the other arguments (*linked support*). Finally, a number of arguments may also support a claim independently of one another (*convergent support*). Convergent support corresponds to a fully diverse argument form.

These structures can be used to identify whether evidence is independent of one another or whether pieces of evidence exhibit dependencies (to varying degrees). It is possible for example to have convergent argument support, where the evidence may exhibit some dependencies. This would be indicative of weak argument construction. It is also possible that an argument exhibits linked argument support where each individual argument is none the less independent of the other.

The general structure of arguments may be used to derive generic ways of strengthening specific arguments or to increase confidence in their validity. While mechanisms for strengthening an arbitrary argument are generic and thus data independent, their application to a specific argument is context sensitive. In terms of practical use it entails taking a specific argument and testing whether it could be strengthened using a generic mechanism.

An example of how structure can be used to increase confidence is illustrated by the examples of Figs. 2 and 3. Imagine an auditor assessing why the introduction of more flight levels will result in a reduction in controller workload. Providing additional information supporting this evidence (which has now become a claim in itself) may have the effect of strengthening the auditor's confidence in the argument. Additional evidence could be provided, for example reference to an experimental assessment of workload conducted with additional flight levels. The authority for moving from this evidence to the claim that workload will be reduced is given by a warrant positing that, for example, experimental workload assessments are indicative of workload levels experienced in a real-world situation. In the same way, the auditor could demand to be told why it should be believed that a decrease in workload should have positive effects on a person's performance. Further evidence, such as the reference to different studies on the effect of workload on people's performance could back this warrant (see Fig. 2). In terms of structure, both of these approaches rely 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.

An example of this last point can be seen by considering initial evidence expressed as "RVSM will double the number of flight levels and reduce the workload of the controller by as much as one third". Subsequently produced evidence expressed as "Experimental assessment of controller workload with additional flight levels showed a reduction of workload of one third" explains why there is confidence to make this claim. In itself, it does not reduce or eliminate the uncertainty attached to the claim but may increase a third party's confidence in the argument because they have a better understanding of where the data came from.

In summary then depth approaches 'explain better' (or in more detail) the argument, thereby increasing our confidence, and potentially also pointing out hidden assumptions or other problems. This is illustrated in Fig. 3.

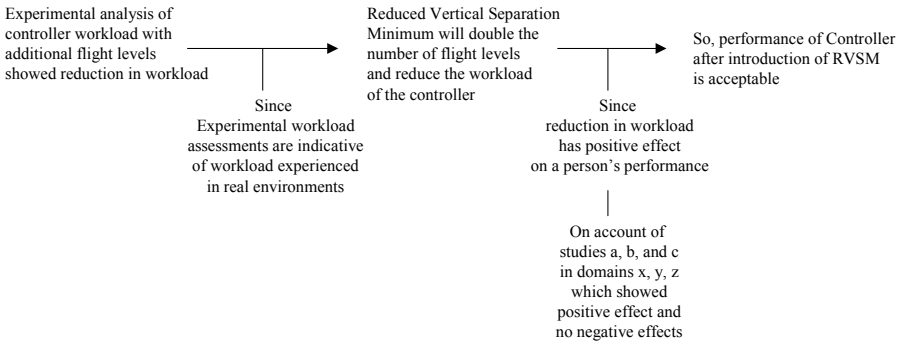


**Fig. 3.** Adding depth to an argument

To address *uncertainty inherent in the evidence or in the warrant* the breadth of an argument should be increased. For example, even though experimental workload assessments may be indicative of workload experienced in real environments, how well these results transfer to the real world might be unclear. There is inherent uncertainty attached to this kind of evidence. For a reason such as this the auditor could, for example, request additional evidence. A response to this might be to explain in greater detail the experimental analysis. The problem is that such a depth approach does not mitigate the uncertainty inherent in the evidence, breadth approaches are needed that give diversity to the evidence. Diverse evidence could consist of the reference to statistics from the experiences of RVSM in the transatlantic airspace, where this mode of separation management has been operational for many years. The characteristics of the transatlantic airspace are different from the characteristics of the European airspace, and may therefore lead to conjecture as to whether these statistics can be transferred. However, in conjunction with the experimental workload assessment, the auditor may now entertain a higher degree of confidence in the overall claim.

A common approach to arguing for the dependability of a system in the context of a breadth approach is 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. The example illustrates the significance of this. It is not sufficient to demonstrate that the controller's performance will be acceptable after the introduction of RVSM, simply by saying that workload will be reduced. Even if true a number of open questions remain to be answered before the overall claim should be accepted (e.g. whether all relevant systems can be updated to support RVSM, what happens in case of computer failures, how the probability of erroneous actions can be reduced and their impact mitigated and so on). To make the overall argument more acceptable and to increase confidence in the claim, additional diverse evidence should be provided thereby increasing the breadth of the argument. For example, in order to support the top-level claim (controller performance is acceptable) a second argument leg could be introduced claiming that all relevant hazards have been reduced as low as reasonably practicable (ALARP). This claim could then, in turn, be supported by reference to a Functional Hazard Analysis. Taken together, the two legs "all hazards being ALARP" and "RVSM reducing operator workload" may provide sufficient grounds to move from the evidence to the claim.

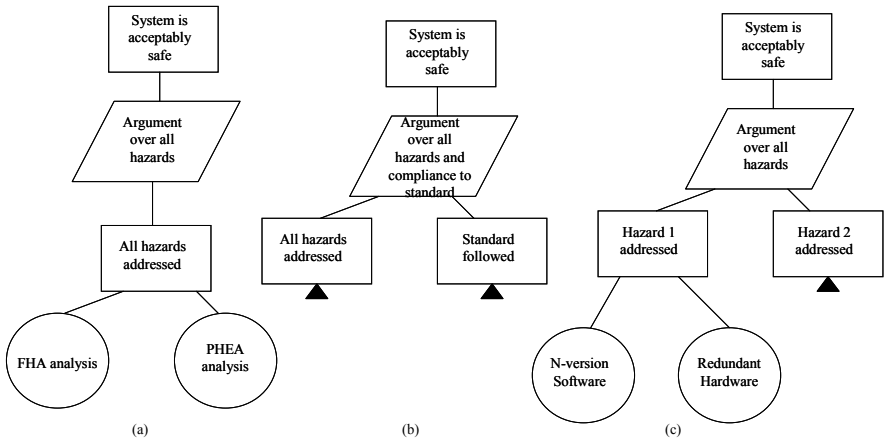


**Fig. 4.** Examples of using breadth to increase the confidence of arguments by reducing uncertainty. (a) diverse evidence (b) diverse argument (c) diverse barriers

Figure 4 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]). Since it is not the purpose of this chapter to provide a tutorial introduction to GSN, the notation is used without further comment. The argument translations presented in GSN are self-explanatory, the process of translation may require further explanation and [9] provides a clear introduction.

In summary, the confidence that can be placed in an argument depends on the rigour of the argument, the uncertainty inherent in the evidence, and the coverage of the evidence. To increase confidence in an argument, additional evidence should be

supplied to make it possible to increase the argument's depth or breadth in the following way:

- Depth Approach:
    - Rigour of the argument

- Breadth Approach:
    - Uncertainty inherent in the evidence
    - Coverage

In the next section the structure of a public domain argument is explored. To carry out this analysis the Eurocontrol RVSM Functional Hazard Analysis (FHA) has been translated into GSN using the ASCE software tool [1]. The analysis investigates the structure of the arguments as well as the use of barriers referenced in these arguments.

## 5 Case study: RVSM functional hazard analysis

RVSM is an EATMP programme established to contribute to the overall objective of enhancing capacity and efficiency while maintaining or improving safety within the European Civil Aviation Conference (ECAC) airspace. The main scope of RVSM is to enhance airspace capacity. The introduction of RVSM will permit the application of a 1000ft vertical separation minimum (VSM) between suitably equipped aircraft in the level band FL290 – FL410 inclusive. Before the introduction of RVSM the VSM was 2000ft (referred to as CVSM).

A prerequisite to the introduction of RVSM was the production of a safety case to ensure that the minimum safety levels were maintained or improved. The Functional Hazard Analysis (FHA) constitutes an essential part of the Pre-Implementation Safety Case (PISC). The FHA document which forms the basis for the study of this section is publicly available [2] as is the Pre-Implementation Safety Case [3]. Three areas have been considered in the FHA:

1. Mature / Core European air traffic region (EUR) RVSM area
2. Mature / Transition space
3. Switchover

For each area a number of scenarios were created for the FHA sessions. In total 72 valid hazards have been analysed during the FHA. For all of these, safety objectives have been established. The report concludes that 70 hazards had achieved their safety objectives, while two hazards were assessed as safety critical and not tolerable.

In the analysis below the FHA Session 1/Scenarios 1 and 2 are considered. Session 1 was concerned with the identification and analysis of hazards relating to the core EUR RVSM airspace focussing on both ground-related and airborne hazards. These two sessions identified 30 valid hazards. For 21 hazards, mitigation arguments were supplied, while for the remaining nine hazards it was assumed that the associated risk was fully acceptable both prior to and after the introduction of RVSM. As a consequence, no mitigation arguments were provided for these hazards. Nineteen hazards are analysed out of a total number of 72. The two safety-critical hazards are not included in the analysis because no mitigation is identified for them.

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. It should be said that this process is not ideal because uncertainties or

ambiguities inherent in the textual description may not be resolved. It would have been better if the GSN goal structures were derived by the people performing the FHA in order to make best use of its capabilities. However, for the current study these uncertainties are acceptable. It should be emphasised, however, that the top-level arguments of the Pre-Implementation Safety Case (PISC), of which this FHA is a part, had been articulated fully in GSN [3]. Figures 5 and 6 illustrate a FHA argument that has been transformed into GSN format. The figures provide close-up views of the top-level argument and the probability branch, and of the severity branch. For the sake of clarity, essential GSN elements such as context have been deleted from the close-up views.

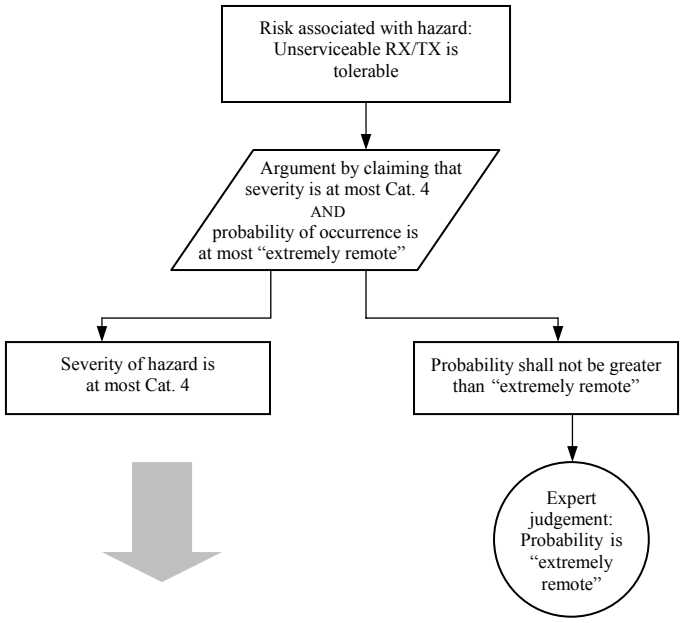


**Fig. 5.** Detail from Hazard Mitigation Argument Ref. 1.15: Top-level and probability branch (not showing context etc.)

Figures 5 and 6 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*. A GSN Pattern [9] has been created from which all the arguments have been instantiated.

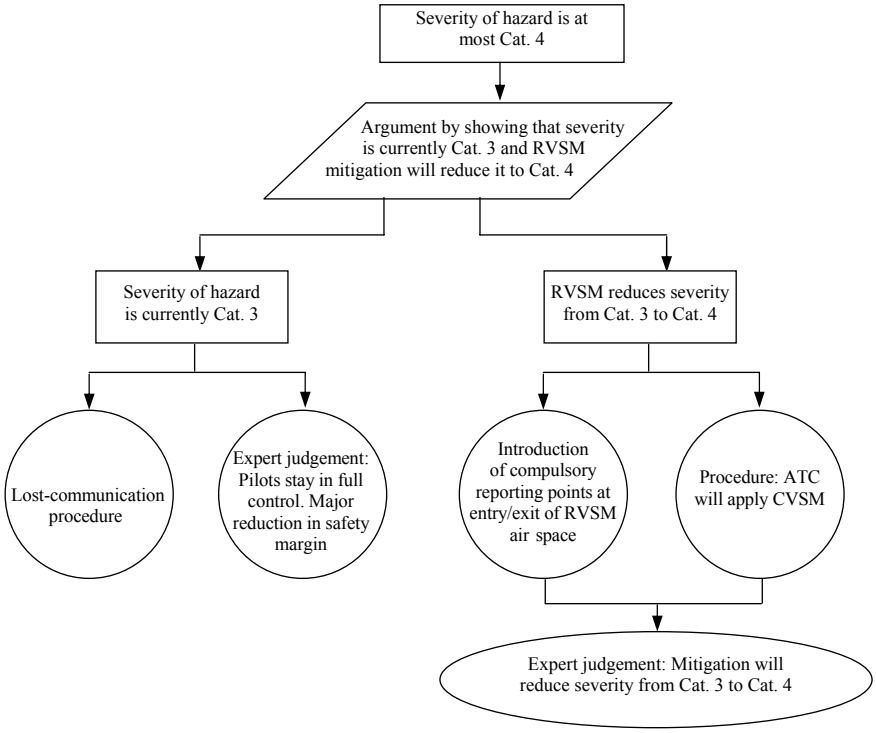


**Fig. 6.** Detail from Hazard Mitigation Argument Ref. 1.15: Severity branch (not showing context etc.)

## 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. Different support pattern types were identified to consider breadth, as well as the dependence or independence of the individual pieces of evidence. For convergent arguments their strength was investigated.

Table 1 shows that 23 out of 38 arguments (i.e. 19 arguments each consisting of a severity and a probability branch) 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). Specific RVSM considerations may increase the depth of the argument, but usually only through the auxiliary construct, which claims that the probability (or severity) is currently at most *z* and that the RVSM mitigation will reduce it to *y* (or *x*). This is then followed by the presentation of evidence as in the earlier case. This type of

analysis reveals that the FHA consists predominantly of simple arguments at a very high level of abstraction. For example, 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. A further issue complicating the analysis is the fact that the FHA was concerned specifically with RVSM mitigation, which leads to an argument lacking details as far as other aspects are concerned, even when these would have increased the comprehensiveness of the argument.

| | 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 convergent 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*. For example, a typical linked/dependent support pattern is *"Only a minor increase in workload will result"* and *"The crew remains in full control"*. Such evidence can be treated singly.

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 convergent/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 convergent / independent patterns proved to be difficult because of relatively low elaboration as was discussed in the analysis of the depth of the arguments. For example, the probability of occurrence of an intolerable situation due to incompatibilities between STCA (Short-Term Conflict Alert) and RVSM is mitigated by adapting existing STCA implementations and by providing training to the controllers. An assessment of their respective relevance, and of whether they are, in fact, convergent or rather linked is difficult given the data available.

The high ratio of linked support patterns to convergent support patterns may have several causes or explanations. In the severity branch the claim of a particular severity is usually supported by linking together a description of worst-case operational consequences. However, it can be argued that the lack of truly convergent arguments is a result of the goal-based approach to safety case development. It may be that such an approach discourages considerations which go beyond demonstrating that a particular goal has been achieved. As already discussed the confidence in the argument may be increased, by providing diverse evidence and increasing the breadth of the argument. This approach was obviously not followed in this particular case study.

| | Single | Linked | | Convergent | | |
|---|---|---|---|---|---|---|
| | | *Independent* | *Dependent* | *Independent* | *Dependent* | |
| 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. The list of barriers identified is illustrated in Appendix A. 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 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.

The mitigation argument in Fig. 6 makes reference to four barriers in the severity claim branch. At least two of these are references to procedures (Lost Communication Procedure, CVSM Application Procedure), while a third can be interpreted as being a procedure, a tool, or a combination of both (compulsory entry points for later calculation). Finally, the fourth barrier refers to the pilot (or crew).

The way barriers are used (or left to be inferred) may be shaped by the type of argument which is constructed. The RVSM safety case argues that air traffic management will *remain* safe after a *modification* to the *existing* air space. This is a special type of argument, which argues the safety of a new system by strongly referring to or relying on an already existing system and that system's safety. In the case of the

introduction of RVSM to the European air space this implies that the FHA does not make reference to or mention existing barriers. Also, it does not provide a comprehensive account of how system safety is achieved. Rather, it focuses on added features such as procedures which will be introduced with RVSM. This makes the assessment more difficult, in particular, since the dependence of certain barriers on other already existing barriers cannot be assessed.

The use of diverse barriers would be recognised as a convergent/independent support pattern type during the analysis. As has been discussed these support patterns are employed almost exclusively to demonstrate that the probability of occurrence of a particular hazard has been sufficiently mitigated, i.e. examples of diverse preventive barriers are used, but hardly any examples of diverse protective barriers are to be found. There are six examples of the use of diverse preventive barriers. These refer to issues such as information about the RVSM status of an aircraft being displayed on different media, e.g. on the radar screen display as well as on the paper flight strips. One example refers to intolerable situations that might arise through wrong RVSM approval status information as a result of training provided to the controllers as well as a specific change message being distributed in case of a late change of RVSM approval status. In cases such as these, as has been discussed, it is difficult to assess without ambiguity the independence (or dependence) of these barriers and their specific relationship to one another given the level of detail provided in the FHA document.

## 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 in-

sights 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 convergent 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.

## Appendix A: Barriers identified in the RVSM FHA document

**(**http://www.ecacnav.com/rvsm/documents/safety/RVSM%20FHA%20V10%2012FEB2001.pdf**)**

**RVSM FHA Session 1 - Scenarios I/II/III**

72 valid hazards identified

2 safety-critical

19 non safety-critical

9 not analysed, as risk was fully tolerable

| **Prevention** | **RVSM Mitigation** | **Haz. ID Reference** |
|---|---|---|
| Monitoring Programme | x | 1.1 |
| Strong encouragement | x | 1.1 |
| Monitoring Programme | x | 1.3 |
| Approval Certification Procedure | x | 1.3 |
| Awareness / Experience | x | 1.6 |
| ACC can suspend RVSM | x | 1.9 |
| 2000 ft. separation for a/c in trail | | 1.11 |
| Awareness Programme | x | 2.2 |
| Change Message | x | 2.2 |
| Flight planning procedure | x | 2.5 |
| Radar screen display | x | 2.5 & 2.17 |
| Special info on flight strips | x | 2.5 & 2.17 |
| Coordination procedure | x | 2.5 & 2.17 |
| Communication procedure | x | 2.5 & 2.17 |
| Ensure STCA is adapted | x | 2.6 |
| Training | x | 2.6 |
| Radar labels | x | 2.7 |
| Specific coordination procedure | x | 2.7 |
| Adapt IFPS to RVSM | x | 2.8 |
| Adapt local systems | x | 2.10 & 2.11 |
| IFPS should check/reject Flight Plan | x | 2.13 |

| Protection | RVSM Mitigation | Reference |
|---|---|---|
| Pilot/controller in control | | 1.1 |
| Procedure: RVSM downgrade | x | 1.3 |
| Procedure: Application of CVSM | x | 1.3 |
| Procedure: Pilot does not deviate | x | 1.3 |
| Pilot / Crew | | 1.9 & 1.11 & 1.14 & 1.15 & 2.5 |
| a/c leaves RVSM airspace | x | 1.14 |
| Procedure: lost communication | | 1.15 |
| Compulsory reporting points | x | 1.15 |
| CVSM | x | 1.15 |
| Procedure: RSM approval status upgrade | x | 2.4 |
| Procedure: how to update data in general | | 2.4 |
| ATCO | | 2.7 & 2.10 & 2.11 & 2.13 & 2.17 & 2.27 |
| Set capacity figures appropriately | x | 2.10 & 2.11 & 2.13 |
| Back-up system with RVSM functions | x | 2.27 |
| ATFM measures | | 2.27 |