Available online at www.sciencedirect.com

ScienceDirect

Electronic Notes in Theoretical Computer Science 238 (2009) 27–39

Electronic Notes in Theoretical Computer Science

www.elsevier.com/locate/entcs

A Generic Goal-Based Certification Argument for the Justification of Formal Analysis

Ibrahim Habli, Tim Kelly[1,2]

Department of Computer Science
University of York
York, UK

Abstract

Formal methods are powerful specification and verification techniques for establishing high confidence in safety-critical systems. However, there are a number of concerns about the use of evidence generated from formal methods, when used in place of conventional testing, for satisfying certain certification objectives. In this paper, we address this issue by reviewing two certification documents, DO-178B and the UK Defence Standard 00-56, focusing on their approach to accepting formal analytical evidence. We also present a generic goal-based safety case that can be instantiated to facilitate the justification and presentation of formal analysis to the certification authorities. The safety case is based on claims about (1) the achievement of the intents of the certification objectives, (2) the demonstration of the trustworthiness of formal analysis and (3) the practical feasibility of deploying formal methods within a specific project.

Keywords: Formal Methods, safety cases, safety arguments, certification, GSN.

1 Introduction

Formal methods have emerged as a potential technique for improving the assurance and cost-effectiveness of the specification and assessment of safety-critical systems. However, prescription in safety standards has hindered and complicated the adoption of formal analytical techniques. The development of safety-critical systems, particularly in the aerospace domain, is regulated according to strict certification guidelines. It is necessary to evaluate any new Validation and Verification (V&V) analytical approach, prior to employment, against applicable certification requirements. Many standards, particularly the DO-178B guidance [2], consider testing to be the preferred V&V technique for compliance.

[1] The authors would like to thank the DTI and our industrial partners, Rolls-Royce plc., Jaguar Cars and Goodrich Engine Control Systems, for supporting this work under the MOSAIC project (MOdelling, Simulation and Analysis for Incremental Certification). Many thanks also to Zoe Stephenson for reviewing the format of this paper.

[2] Email: Ibrahim.Habli, Tim.Kelly@cs.york.ac.uk

doi:10.1016/j.entcs.2009.09.004

In this paper, we examine two different certification documents, DO-178B and the UK Defence Standard 00-56 [10], and the way each approaches formal analysis. DO-178B is known to give precedence for testing evidence while Defence Stan 00-56 considers analytical methods to offer the strongest form of evidence. However, both standards, regardless of their conservatism or preference towards formal analytical evidence, require the submission of a reasoned justification as to why and how formal analysis achieves the certification goals. To this end, we present a generic safety case argument that can be instantiated to facilitate the justification and presentation of formal analysis to the certification authorities. A safety case is defined in UK Defence Standard 00-56 as [2]:

> *"A structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given operating environment."*

The safety case that we present is based upon claims concerning (1) the achievement of the intents of the certification objectives, (2) the demonstration of the trustworthiness of formal analysis and (3) the practical feasibility of deploying formal methods within a specific project. The safety case is documented using the Goal Structuring Notation (GSN) [7] — a graphical argumentation notation which explicitly represents the individual elements of any assurance argument (requirements, claims, evidence and context) and the relationships that exist between these elements.

The remainder of this paper is organised as follows. Sections 2 and 3 examine the consideration of formal analytical evidence in DO-178B and Defence Standard 00-56. The safety case concept is introduced in Section 4. Section 5 explores the role of GSN in communicating safety case arguments. In Section 6, we present a generic GSN argument for the justification of formal analysis. The paper concludes with a summary in Section 7.

2 Formal Analysis in DO-178B

The use of formal methods is addressed in DO-178B in Section 12 — "Additional Considerations". DO-178B acknowledges the strength of formal methods in producing "*an implementation whose operational behavior is known with confidence to be within a defined domain*" [2]. It even goes further to declare that the deployment of formality is equivalent to thorough analysis, as it not only detects requirements, design and code errors but also eliminates them. However, it subsequently undermines the aforementioned statements by declaring that formal methods are complementary to testing, and hence indirectly implying that evidence generated from formal methods cannot be used as the sole means for compliance with verification objectives, specifically those objectives concerning the verification of the executable object code.

The high level of prescription in DO-178B is a key hurdle for obtaining certification credit with the use of formal methods, specifically with regard to the verification process. DO-178B explicitly requires the performance of three levels of 'tests' (Fig-

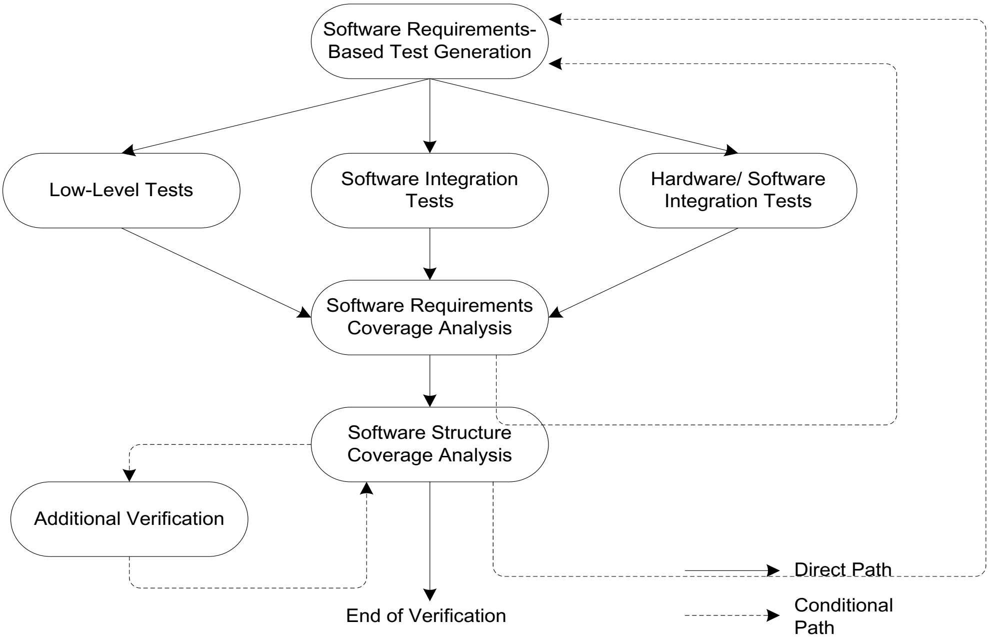

Software Requirements-Based Test Generation
Low-Level Tests
Software Integration Tests
Hardware/ Software Integration Tests
Software Requirements Coverage Analysis
Software Structure Coverage Analysis
Additional Verification
End of Verification
Direct Path
Conditional Path

Fig. 1. Testing Process in DO-178B[2]

ure 1): low-level tests, software integration tests and hardware/software integration tests — rather than 'verification'. Normal-range and robustness test cases should be developed for each requirement addressed by these tests. All test cases should be generated from the requirements. The quality of testing is judged against two coverage measures: requirements coverage and structural coverage. While the first type of coverage determines which requirements were not tested, the latter determines how well the test cases exercised the code structure.

Testing is a powerful method of verification. In particular, testing is the dominant technique for software/hardware integration verification due to the need to exercise the software on the target platform. However, formal analytical techniques are now well established and proven and can replace testing for certain applications, at least for the verification of the software at the unit and software integration level. Current DO-178B objectives make it difficult to claim credit for the use of formal methods, as the objectives are very specific to testing (e.g. because of objectives formulated as "**Test** coverage of high-level requirements is achieved" rather than "**Verification** coverage of high-level requirements is achieved"). One aim of Sub-Group 6 in the EUROCAE WG71 and RTCA SC205 committees developing DO-178C is to try to abstract the verification objectives [9]. If successful, formal analysis would become a possible means for compliance as long as it can be shown to be trustworthy and directly targeting the certification objectives.

3 Formal Analysis in UK Defence Standard 00-56

The UK Defence Standard 00-56, Issue 4 [2], adopts a different approach to safety certification. Def Stan 00-56 is both evidence-based and goal-oriented and focuses on the strength, rigour and coverage of evidence with regard to safety requirements. Defence Stan 00-56 lists the following types of evidence as acceptable [2]:

a. *Direct evidence from analysis*

b. *Direct evidence from demonstration (testing and/or operation), including quantitative evidence*

c. *Direct evidence extracted from the review process*

d. *Process evidence showing good practice in development, maintenance and operation*

e. *Qualitative evidence for good design, including expert testimony.*

Unlike DO-178B, where testing evidence takes the front seat, Def Stan 00-56 gives precedence to analytical evidence. Nonetheless, in order to obtain credit for the use of analysis as the primary means for compliance, the analytical methods should be accompanied with supporting backing information, including:

Reasoned justification — addressing the use of analysis in the context of a specific application, including known limitations

Full documentation — addressing the configuration consistency, repeatability and verifiability of analysis

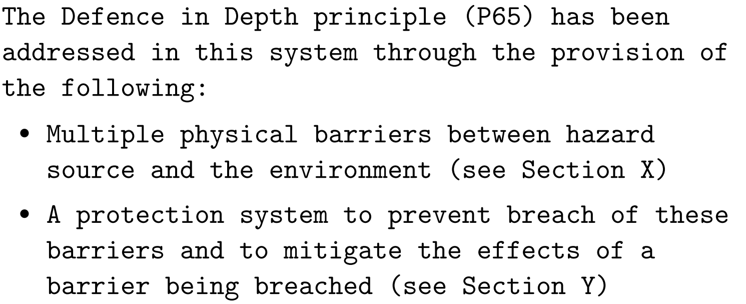
Tool qualification — addressing the rigour of analysis through automation and tool support

Personnel competency — justifying staff competency with regard to performing analysis and using tools, if available

Suitability of models — addressing the correctness and the justification of the selection of models, specifically the ability of the models to represent certain aspects of the actual system such as timing, resource usage, run-time errors and functional properties.

Analytical evidence therefore takes precedence in Def Stan 00-56 as long as it is accompanied with a reasoned justification regarding the analytical method's trustworthiness and practicality. In DO-178B, analytical evidence may be considered a means for compliance if the certification authorities are provided with a compelling argument concerning its effectiveness in satisfying the verification objectives — traditionally achieved by testing. This can only be achieved after agreement with the certification authorities. Gaining such agreement can have the potential to prolong the process of obtaining approval.

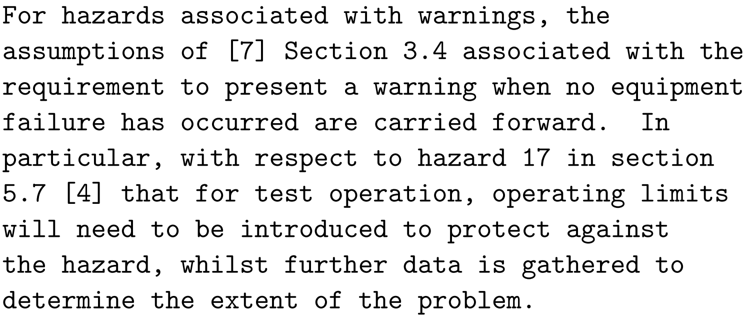
In short, the use of analysis as a means for compliance, in both DO-178B and Def Stand 00-56, involves the submission of an argument and evidence to substantiate any claims about the integrity and effectiveness of the analytical methods. In essence, the safety engineers are required to submit a safety case in support of



The Defence in Depth principle (P65) has been addressed in this system through the provision of the following:

- Multiple physical barriers between hazard source and the environment (see Section X)
- A protection system to prevent breach of these barriers and to mitigate the effects of a barrier being breached (see Section Y)

Fig. 2. An Example Textual Argument



For hazards associated with warnings, the assumptions of [7] Section 3.4 associated with the requirement to present a warning when no equipment failure has occurred are carried forward. In particular, with respect to hazard 17 in section 5.7 [4] that for test operation, operating limits will need to be introduced to protect against the hazard, whilst further data is gathered to determine the extent of the problem.

Fig. 3. The Problems of Textual Safety Arguments

analysis. In the next two sections, we introduce the safety case concept, exploring the role of the Goal Structuring Notation (GSN) in communicating safety case arguments.

4 Safety Case Arguments

Safety arguments are typically communicated in existing safety cases through free text. Figure 2 shows a fragment of a safety argument communicated using free text. The text describes clearly how a safety requirement (P65) has been interpreted and achieved in the system. It also clearly provides references to where the evidence supporting the lower level statements can be found.

Well-structured approaches to expressing safety arguments in text can be effective. However, there are problems experienced when text is the only medium available for expressing complex arguments. The text shown in Figure 3, taken from a real industrial safety case (with identification of the target application hidden), illustrates some of these problems.

The text shown in Figure 3 is unclear and is poorly structured. Not all engineers responsible for producing safety cases write clear, well-structured English. Consequently, the meaning of the text, and therefore the structure of the safety argument, can be ambiguous and unclear. Cross-references, of the type shown in Figure 3, are often necessary given the role of the safety case as an integrator of evidence. However, multiple cross-references in text can be awkward and can disrupt the flow of the main argument.

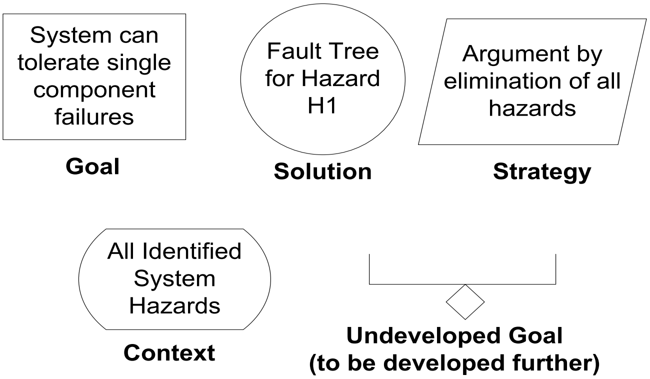

System can tolerate single component failures
Goal
Fault Tree for Hazard H1
Solution
Argument by elimination of all hazards
Strategy
All Identified System Hazards
Context
Undeveloped Goal (to be developed further)

Fig. 4. Principal Symbols of GSN

In the context of developing, agreeing, and maintaining the safety arguments within the safety case, the biggest problem with the use of free text is in ensuring that all stakeholders involved share the same understanding of the argument. Without a clear and shared understanding of the argument, safety case management is often an inefficient and ill-defined activity. The following section describes a structured technique that has been developed to address the problems of clearly expressing and presenting safety arguments.

5 The Goal Structuring Notation (GSN)

The Goal Structuring Notation (GSN) [7] — a graphical argumentation notation — 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 4 (with example instances of each concept).

When the elements of the GSN 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 claims can be supported by direct reference to available evidence (solutions). As part of this decomposition, using the GSN it is also possible to make clear the argument strategies adopted (e.g. adopting 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).

Figure 5 shows an example goal structure. In this structure, as in most, there exist 'top level' goals — statements that the goal structure is designed to support. In this case, "C/S (Control System) Logic is fault free", is the (singular) top level goal. Beneath the top level goal or goals, the structure is broken down into sub-goals,

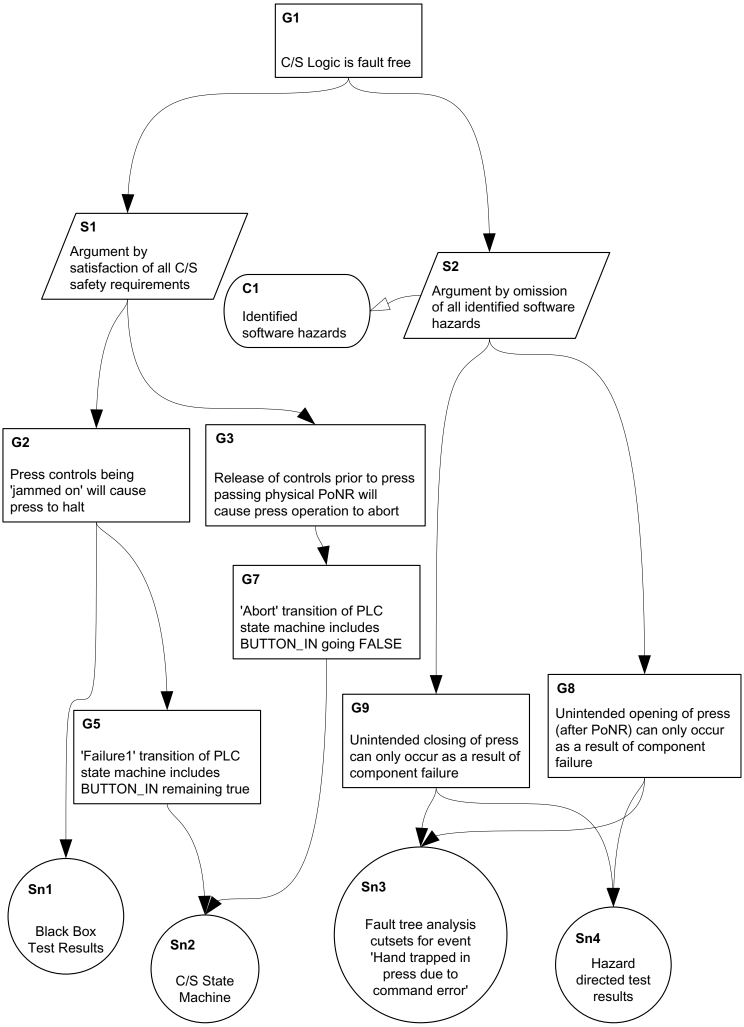

G1
C/S Logic is fault free
S1
Argument by satisfaction of all C/S safety requirements
C1
Identified software hazards
S2
Argument by omission of all identified software hazards
G2
Press controls being 'jammed on' will cause press to halt
G3
Release of controls prior to press passing physical PoNR will cause press operation to abort
G7
'Abort' transition of PLC state machine includes BUTTON_IN going FALSE
G5
'Failure1' transition of PLC state machine includes BUTTON_IN remaining true
G9
Unintended closing of press can only occur as a result of component failure
G8
Unintended opening of press (after PoNR) can only occur as a result of component failure
Sn1
Black Box Test Results
Sn2
C/S State Machine
Sn3
Fault tree analysis cutsets for event 'Hand trapped in press due to command error'
Sn4
Hazard directed test results

Fig. 5. Example Goal Structure

either directly or, as in this case, indirectly through a strategy. The two argument strategies put forward as a means of addressing the top level goal in Figure 5 are “Argument by satisfaction of all C/S (Control System) safety requirements” and “Argument by omission of all identified software hazards”. These strategies are then substantiated by five sub-goals. At some stage in a goal structure, a goal statement is put forward that need not be broken down and can be clearly supported by reference to some evidence. In this case, the goal “Unintended Closing of press after PoNR (Point of No Return) can only occur as a result of component failure”, is supported by direct reference to the solutions “Fault tree cutsets. . . ” and “Hazard Directed Testing Results”. Within Europe, GSN has been adopted by a growing number of companies within safety-critical industries for the presentation of safety arguments within safety cases. The following list includes some of the applications of GSN to date:

- Eurofighter Aircraft Avionics Safety Justification
- Hawk Aircraft Safety Justification
- U.K. Ministry of Defence Site Safety Justifications
- U.K. Dorset Coast Railway Re-signalling Safety Justification
- Submarine Propulsion Safety Justifications
- Safety Justification of UK Military Air Traffic Management Systems
- London Underground Jubilee Line Extension Safety Justification
- Swedish Air Traffic Control Applications.

The key benefit experienced by those companies adopting GSN is that it improves the comprehension of the safety argument amongst all of the key project stakeholders (i.e. system developers, safety engineers, independent assessors and certification authorities). In turn, this has improved the quality of the debate and discussion amongst the stakeholders and has reduced the time taken to reach agreement on the argument approaches being adopted.

6 A Generic Argument for the Justification of Formal Analysis

Unlike traditional means for compliance (e.g. testing), the approval of formal analysis as a primary means for compliance depends on the submission of a compelling safety/certification argument that provides evidence that a formal technique can achieve, and later on has achieved, certain certification objectives. In this section, we explore some fundamental elements of the justification required to provide the context for formal analysis and document the logical dependencies of these elements in a GSN-based argument.

The justification of formal analysis is often carried out by comparison to testing. Arguing that a formal analytical technique is "*at least as convincing as*" testing offers one potential means for generating a compelling safety certification argument [4]. This approach entails the following activities:

(i) Eliciting the objectives and arguments in support of the testing techniques as presented in the standards

(ii) Developing an argument that is "*at least as convincing as*" the testing argument, which demonstrates that the new analytical technique(s) achieve(s) the same objectives as those achieved by testing

(iii) Arguing that it is feasible to implement the proposed analytical technique(s).

However, the main hurdle is extracting the real intent and rationale behind the certification objectives that the argument needs to satisfy. For example, the DO-178B document does not provide a published rationale for the development of the guidance. This is partly because the guidance was developed by the consensus of

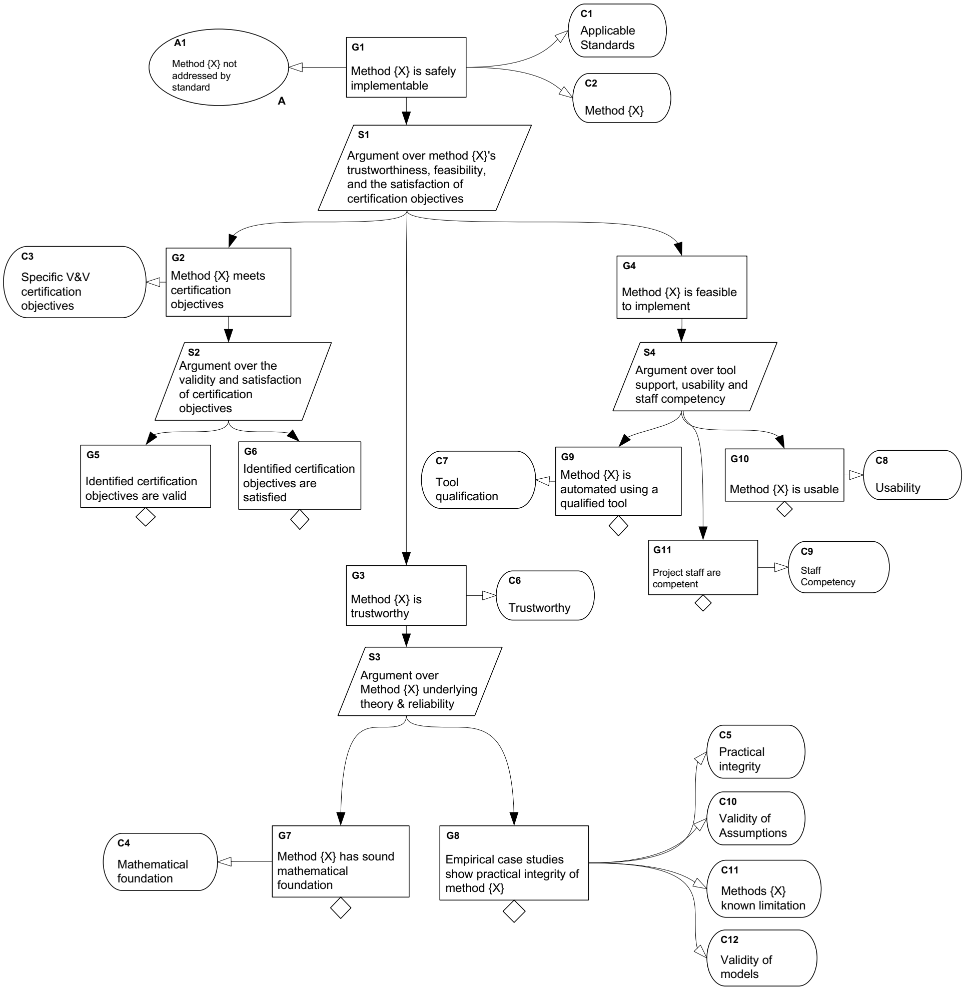

A1
Method {X} not addressed by standard
A
G1
Method {X} is safely implementable
C1
Applicable Standards
C2
Method {X}
S1
Argument over method {X}'s trustworthiness, feasibility, and the satisfaction of certification objectives
C3
Specific V&V certification objectives
G2
Method {X} meets certification objectives
G4
Method {X} is feasible to implement
S2
Argument over the validity and satisfaction of certification objectives
S4
Argument over tool support, usability and staff competency
G5
Identified certification objectives are valid
G6
Identified certification objectives are satisfied
C7
Tool qualification
G9
Method {X} is automated using a qualified tool
G10
Method {X} is usable
C8
Usability
G11
Project staff are competent
C9
Staff Competency
G3
Method {X} is trustworthy
C6
Trustworthy
S3
Argument over Method {X} underlying theory & reliability
C5
Practical integrity
C10
Validity of Assumptions
C4
Mathematical foundation
G7
Method {X} has sound mathematical foundation
G8
Empirical case studies show practical integrity of method {X}
C11
Methods {X} known limitation
C12
Validity of models

Fig. 6. Generic Argument for the Justification of New Analytical Technique

257 companies and organisations, based on industrial best practices.

In this paper we complement the above approach by tackling three fundamental aspects of the justification of formal analysis which should be covered by a certification argument, namely:

- Elicitation of the 'rationale and intent' of V&V objectives, and showing how they can be satisfied by formal analysis
- Demonstration of the trustworthiness of formal analysis
- Demonstration of the feasibility and practicality of employing formal analysis using available project resources, e.g. tools and personnel.

The above aspects are realised in a generic GSN-based safety argument. The argument is presented in Figure 6. The top-level goal (G1) of the argument is that the method is safely implementable. One of the assumptions is that the formal analytical method is not explicitly addressed in the applicable standards (A1). The strategy for justifying the safety of the method depends on three sub-claims:

- The method meets the certification objectives (G2): based on the validity (G5) and satisfaction (G6) of the certification objectives
- The method is trustworthy (G3): based on the mathematical soundness (G7) and practical reliability (G8) of the method
- The method is feasible to implement (G4): based on tool support (G9), staff competency (G11) and usability (G10) of the method.

The symbol '$\diamond$' underneath the sub-goals G5, G6, G7, G8, G9, and G10 indicate that such goals require further decomposition. This decomposition depends on the specific characteristics of each formal analytical method. For example, the sub-goal 'Empirical case studies show practical integrity of methods X' (G8) can be decomposed further based on empirical results obtained from case studies, uncovering both the strengths and limitations of a formal method.

In the subsequent subsections, we discuss ways in which the intent of the certification objectives can be elicited, factors which should be considered to show the trustworthiness of formal analysis, and finally project attributes that should be demonstrated in order to show the practical feasibility of using formal analysis.

6.1 Rationale and Intent of V&V Objectives

In order to substantiate G2 "*Method $\{X\}$ satisfies certification objectives*", it is important to elicit the rationale behind the certification objectives in order to show that formal analysis addresses the intent of the certification objective (i.e. addressing the 'spirit' of the objectives rather than the actual wording). This is particularly important for verification objectives that are specific to testing as it may appear contradictory to claim the satisfaction of a testing objective by formal analytical evidence. A more reasonable approach is to claim the satisfaction of the intent of a testing objective by formal analysis.

However, many standards, particularly DO-178B, do not provide a published rationale for the development of the objectives and means for compliance. Therefore, we recommend that the intent and rationale for the V&V objectives, particularly testing objectives, should be elicited through the following means:

(i) Referring to published 'guidelines' , e.g. DO-248B [3], FAA Advisory Circulars (CA), Frequently Asked Questions (FAQ), and Technical Standard Orders (TSO).

(ii) Developing an argument, based on information revealed in the guidance, which shows the 'logical flow' involved in justifying the significance and contribution of the V&V techniques (i.e. developing an argument for testing on the behalf of the certification authorities or guidance authors [4]).

(iii) Modelling and analysing the 'development and assessment process', as specified in the certification guidance, showing the flow of information, assumptions and dependencies between different activities in the overall lifecycle.

The above three approaches are complementary. For example, DO-178B is not a standalone document. Associated guidelines are continually being updated. DO-178B applicants have to get agreement from the certification authorities on the guidelines to be used. Additional guidelines for the application of DO-178B, for instance, can be obtained from technical certification reports such as DO-248B [3].

A complementary approach to eliciting the intent of the testing objectives is by formulating an argument in support of testing, based solely on information available in the guidelines and guidance. The logical flow of the testing argument should show logical interdependencies between a testing technique and other pre-requisite or post-requisite techniques. The input of the testing technique may depend on the output data and validity of other V&V activities.

Modelling and analysing the lifecycle processes, as specified in the standards, offers another approach to identifying dependencies between testing and the rest of the development activities, and hence potentially inferring the rationale for a recommended or mandated testing technique. In fact, DO-178B insists on evaluating the impact of any alternative means of compliance on the overall development lifecycle process and data:

> *"An alternative method cannot be considered in isolation from the suite of software development processes. The effort for obtaining certification credit of an alternative method is dependent on the software level and the impact of the alternative method on the software life cycle processes."*

6.2 *Arguing about the Trustworthiness of Formal Analysis*

The claim "*Method* $\{X\}$ *is trustworthy*" (G3) in the GSN argument in Figure 6 addresses the integrity of the formal analytical method. The justification of formal analysis should demonstrate both the theoretical soundness and the practical integrity of the formal analytical method. For example, if a formal technique addresses floating-point arithmetic run-time exceptions, the soundness of this technique may be demonstrated against the requirements of the IEEE Standard for Binary Floating-Point Arithmetic (IEEE 754). The soundness of a method may also be undermined by the failure to express, formally, certain properties that are assumed to be addressed by the method (e.g. functional and timing properties).

Successful industrial case studies are also important as they have the potential to demonstrate the effectiveness of formal analysis through generating empirical data. It is necessary for the case studies to show how the formal technique integrates consistently with other design and assessment techniques. These case studies should be based on real safety-critical systems. Further, the case studies should be carried out in the context of the assumed authenticity of the selected formal models. Any known limitations of the formal analytical technique should also be communicated, which may be specific to the context of a project. For example, the ability to demonstrate correspondence between the mathematical model and the software behaviour at run-time is critical [5]. Otherwise, confidence in formal analysis would be seriously undermined. Any formal model will not be useful, and may even be misleading and dangerous, unless its representation provides a satisfactory reflection of the actual system. The actual system encompasses a large number of concepts, assumptions and relationships. However, generally only a small portion of these elements controls the structure and behaviour of the actual system. As a result, a formal model should focus on capturing these prevailing elements in order to reduce the gap between the assumed and the actual system. The validation of the authenticity of a model is undeniably a universal concept, applying to most techniques, regardless of whether they are formal or not. However, this is of a particular importance for formal analysis as the resulting analyses may be used as the sole means for compliance, without the need to exercise the software at runtime. Therefore, unless a high level of confidence can be achieved regarding the faithfulness of the formal model, some testing may still be required.

6.3 Demonstrating the Feasibility of Formal Analysis

The previous sections address the need to formulate a compelling certification argument which can provide strong, relevant and sufficient evidence that a formal analytical technique satisfies the certification objectives. However, there are always concerns about the practicality of applying formal analytical approaches. There is a misconception that formal specification and analysis are a pure theoretical exercise despite the many successful industrial implementations [6].

The certification authorities need to be assured that the deployment of an alternative formal analytical technique overcomes the practical limitations that have been traditionally associated with the implementation of formal methods in large-scale and critical systems, such as [1], [5], [6], [8] :

- Poor tool support
- Poor integration with other techniques
- Inadequate formal mathematical skills and training
- Insufficient industrial examples
- Focus on cost reduction rather than safety improvement.

The safety case argument in support of an alternative formal analytical technique should rebut known misconceptions about formal analysis (G4 "*Method* $\{X\}$ *is feasible to implement*"). The claim about the feasibility of implementing an analysis method is important in order to show that the method is correctly used, given the resources allocated to the project. For example, the first three concerns above can be tackled by the development of a qualified tool that (1) automates the formal analysis process and (2) integrates well with other development and verification tools. It is necessary for the tool to automate and hide formality, as much as possible, and hence minimise the level of formal mathematical skills expected to be exhibited by the developers.

7 Summary

In this paper, we have reviewed two certification documents, DO-178B and the UK Defence Standard 00-56, focusing on their approach to accepting formal analytical evidence. We have also presented a generic safety case that can be instantiated to facilitate the presentation and justification of formal analysis. The safety case is based on claims about (1) the achievement of the intents of the certification objectives, (2) the demonstration of the trustworthiness of formal analysis and (3) the practical feasibility of deploying formal methods within a specific project.

References

[1] Dill D., J. Rushby, *Acceptance of formal methods: Lessons from hardware design*, IEEE Computer, 29(4), Hampton**1** (1996).

[2] EUROCAE (European Organisation for Civil Aviation equipment), *ED-12B/DO-178B: Software Considerations in Airborne Systems and Equipment Certification*, EUROCAE **9** (1994).

[3] EUROCAE WG71 and RTCA SC205, URL: http://ultra.pr.erau.edu/SCAS.

[4] Galloway, A., R.F. Paige, N.J. Tudor, R.A. Weaver, I. Toyn and J.A. McDermid, "Proof vs Testing in the Context of Safety Standards," Digital Avionics Systems Conference (DASC), IEEE Press, Washington, USA, October 2005.

[5] Hall, A., *Seven Myths of Formal Methods*, IEEE Software archive, Volume 7, Issue 5, Hampton**1** (1990).

[6] Holloway C. H., R.W. Butler, *Impediments to Industrial Use of Formal Methods*, IEEE Computer **1** (1996).

[7] Kelly, T. P., "Arguing Safety — A Systematic Approach to Safety Case Management, "Ph.D. thesis, University of York, York, 1998.

[8] Knight J.C., C.L. DeJong, M.S. Gibble, L.G. Nakano, *Why Are Formal Methods Not Used More Widely*, Fourth NASA Formal Methods Workshop, Hampton**1** (1997).

[9] SC-190/EUROCAE WG-52, *Final Annual Report For Clarification Of DO-178B: Software Considerations In Airborne Systems And Equipment Certification*, EUROCAE **9** (2001).

[10] UK Ministry of Defence, *00-56 Safety Management Requirements for Defence Systems*, UK Ministry of Defence, Issue 4 **9** (2007).