This paper is published in a supplemental volume to DSN-2004, the proceedings of the 2004 International Conference on Dependable Systems and Networks 2004

Assurance Cases: how assured are you?

Samantha Lautieri, David Cooper, David Jackson, Trevor Cockram
Praxis Critical Systems
{samantha.lautieri, david.cooper, david.jackson, trevor.cockram}@praxis-cs.co.uk

Abstract

This paper proposes an approach to system assurance that acknowledges the commonality between the different threads of safety, security and reliability, reduces duplicated work, and can be supported by web-enabled tools. It provides assurance that systems will meet with regulators and budget holders' approval.

We discuss some of the problems with the current means of proving assurance, and how the best practices in the safety, security, and reliability domains could benefit from being brought together within a suitable framework to achieve a single, unified assurance case.

We offer up a solution by way of an eDependabilityCase (eDC) tool, working within a single, integrated framework, to develop and present an assurance case.

1. Introduction

Overall system assurance will often encompass safety, and security, and business and legal aspects of your system. It is larger than the traditional safety case, or security argument. Reliability appears as a critical aspect of all of these (Figure 1).

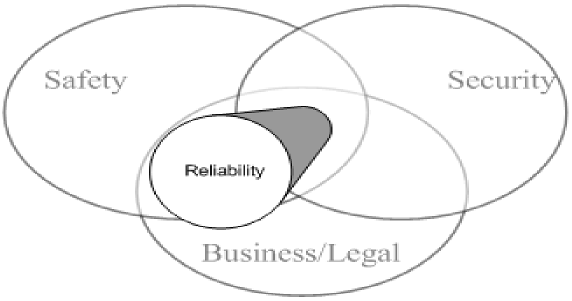


Figure 1: Aspects of Assurance

Traditionally, assurance is separated into individual safety, security and reliability assurance cases [3, 4, 5]. But this can lose the bigger picture. We will argue here that there are benefits in taking a view of systems assurance across *all* aspects, while still following the industry's best practice in the individual domains. There are obstacles, but there is a way forward that will

- reduce the effort required;
- reduce the reluctance in producing integrated assurance cases; and
- show that tools exist to assist in the integration.

2. The Hard Copy vs. the Soft Copy

The traditional medium for safety, security or reliability cases has been paper, but there are many aspects to this that inherently make it cumbersome. Making the change from the hard copy to the soft copy is a natural decision, but in order to reap the advantages that a soft copy can provide it has to be correctly thought out and is an engineering exercise in itself.

2.1 Ease of navigation

A paper-based assurance case for a system can be many inches thick. Having to read so much is not an enticement, and knowing where to find the relevant information is not always easy.

A PC-based alternative would seem a natural step. If the assurance case were collated appropriately, it should be less cumbersome, and its navigation would be less complicated and easier.

2.2 Ease of drilling down

A paper based assurance case will not inherently have clear traceability, yet showing traceability provides a simple means of justifying decisions. For example, tracing from part of an assurance argument to the person constructing that argument can support accountability and identify the competency of the person making the decision.

A soft copy of an assurance case can more easily have traceability built in. Through the use of automatically generated hyperlinks, the assurance case could be traversed in whatever order the user wishes.

2.3 Configuration Management

The documentation that makes up the assurance case generally comes from many applications, organisations, departments and processes. Document management is no easy task and base lining can be difficult and unwieldy. Issues include:

- unique identification;
- accessibility;
- version control;
- organisation of the information
- indexing and referencing.

Configuration control can be made easier and less of a burden if soft copies are used. When configuration control is an inherent part of working practice the implementation overhead is reduced. Sensible incorporation of source documents within the soft copy of an assurance case is a further means of reducing the overhead.

2.4 Diversity of Information Packaging

Producing a consistent presentation of an assurance case can be difficult due to the differing sources of many of the input documents. However, if consistency of presentation can be enforced by the tool that pulls all the information together into the soft copy version, then effort savings can be made.

A further problem arising from the various document sources is duplication of work. Duplication of effort can result when information is necessary to fulfil the requirements of more than one application or methodology. However, this can be reduced when the more integrated view is adopted, giving concurrent visibility of requirements within all applications or methodologies.

2.5 Ease of packaging and delivery

A paper-based case, generating large volumes of paper, has to be collated and sent to stakeholders.

The size and bulk of a soft version of an assurance case is not an issue.

3. Gaps and Conflicts

When the assurance of a system is divided into requirements for a safe, secure and reliable system, each of them being addressed separately, then gaps and conflicts can arise. The gaps and conflicts may

- not be evident;
- be dealt with too late in the lifecycle;
- not be resolved even when evident.

These gaps and conflicts can compromise the assurance of the system and they may not apparent until the systems is in use.

When sound engineering principles are used as part of an integrated view then it becomes easier to identify the gaps and conflicts. Figure 2 illustrates how Safety, Security and Reliability can be coordinated, enabling easier identification and therefore faster resolution of gaps and conflicts.

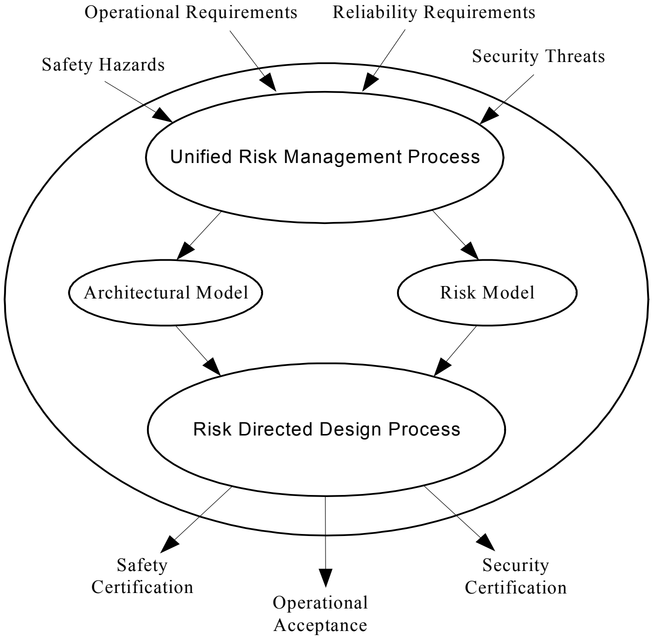


Figure 2: Coordinated Safety, Security and Reliability

4. Clarity of the argument

Clarity of the assurance argument is key in convincing the regulators that assurance has been achieved. In practice, burying the argument in sections of detailed text with a lack of mapping to the supporting evidence is common. The individual threads of the argument may also be dispersed through the levels of documentation.

The tools to provide clarity in the argument are available. Tools combined with a sound framework provide further assurance of clarity—the framework defines a clear direction for the argument and helps it to remain clear as it is created. However, every domain is different, and the framework must work with the domain standards in force.

5. Multiple standards and processes

Many systems are developed with the expectation reuse in other contexts. Providing assurance in one context of operation for one regulator and then translating it to another context of operation and another regulator can require significant rework. In practice, the data required by different regulators or certification bodies is not that dissimilar, but the structure and organisation of the data can seem to imply otherwise. Ideally, one would like to develop the analysis and evidence once, and re-present it as appropriate for each context and each regulator's standards. Communications between the safety, security and reliability communities, between the civil and military areas, along with the adoption of an integrated view will help to address the issues of system assurance in contexts.

6. Best Practice

Standards do not always reflect industry best practice. Best practice evolves as the industry better understands the issues, but prescriptive standards lag behind. SafSec (a research program on integrating safety and security certification) [1] has proposed a framework for achieving safety and security certification without mandating the specific means of achieving the requirements. By concentrating more on the goals of certification rather than the detailed steps SafSec can stay relevant for longer. SafSec has so far been mapped to the requirements of the Common Criteria [4] and DefStan 00-56 [5] but it is expected to be suitable for DO-178B [6], SW01 [7] and other standards also.

Developers, assessors, accreditors and certification bodies all need to buy into proposed standards, and this requires communication between all parties. The development of the SafSec methodology has involved and had contributions from many types of stakeholders.

7. Product vs. Process

Some standards put an emphasis on the *processes* used to achieve assurance. Unfortunately, each standard puts slightly different constraints on the processes, making it difficult to use the results obtained from one process to support the arguments for another process.

SafSec emphasises the need to concentrate on the *product*, not the *processes,* and uses an assurance case to structure the evidence such that the emphasis remains on the product. Justification of the means or processes by which the system is assured is less important than justifying that the system itself is assured.

8. Correct Information

The production, collation and presentation of the correct evidence is necessary for useful understanding and production of the assurance case. Gaining the correct evidence to show assurance is essential for minimising costs and meeting milestones. Careful interpretation of standard compliance will help to produce the correct information. Subsequently collation and presentation of the correct information will enable a claim of assurance for the system to be made.

Incorrect interpretation of the standards and the applicability of the evidence generated will place barriers in claiming assurance. The dependability case can be structured around claiming assurance against many standards and the applicability of the evidence should be explicitly structured around the argument.

9. Stakeholder Buy-In

Stakeholder buy-in is essential to the successfulness of an integrated approach to demonstrating assurance. Each community has their own needs and while education of the stakeholders on the commonalities that exist between their domains is beneficial, their buy-in increases the uptake of a new approach.

SafSec has actively sought stakeholder involvement, and has attained a good level of buy-in from those involved. The cooperation by stakeholders in formulating SafSec has been encouraging. The inclusion of Reliability in SafSec will provide further opportunities to gain buy-in from the stakeholders.

10. Satisfaction in the Whole

The assurance that all aspects of safety, security and reliability are addressed would be grounds for claiming assurance of the whole system. An approach that illustrated compliance with all standards, making coherent and clear claims with supporting evidence at hand and obtainable, would be an improvement over the current means of making such claims.

If an eDependabilityCase (eDC) does not provide the 'satisfaction in the whole', then it is still a work in progress.

11. A Way forward: SafSec with Reliability into an eDC

The framework and method developed within SafSec for safety and security, combined with reliability, is a workable approach for obtaining assurance in an integrated framework. It is a natural progression for discovering the commonalities between domains when taking the integrated view.

An electronic Dependability Case is one means of making claims of assurance according to the SafSec framework.

11.1 A good foundation

Approaching the claim of system assurance by adopting an integrated view is necessary to:

- reduce duplication of effort;
- address the need for a product emphasis;
- make the argument as succinct as possible.

SafSec currently integrates safety and security. The inclusion of Reliability and Maintainability, such as that required by Def Stan 00-42 [3], will ensure all aspects of assurance are addressed.

Following a SafSec with Reliability approach is going to reduce the duplication of effort since evidence that is suitable for safety and reliability need only be generated once. The integrated view will take account of the requirements on all aspects of assurance. Rather than safety, security and reliability converging only within the accreditors world (during the later stages of a program), the convergence will occur earlier and benefit everyone involved.

The focus of assurance should be on the *product,* not the *process*. An emphasis on the product, as encouraged by SafSec, nevertheless does demand a rigorous process in support of the assurance argument.

A succinct argument is desirable. SafSec sets out a means of providing a succinct argument for assurance. By taking a risk directed approach to ensure design has built-in risk mitigation, rather than bolted on, then the argument for assurance will be more succinct and less complicated, reducing the work required to make claims of assurance.

11.2 eDC: the smart answer

The eDependabilityCase structures the information on which the claims of assurance of a system relies. At the high level, compliance is shown against applicable standards. At the lowest level is a repository of evidence to support the claims. Evidence may be used to support multiple aspects of the arguments, and may support safety, security and reliability arguments simultaneously.

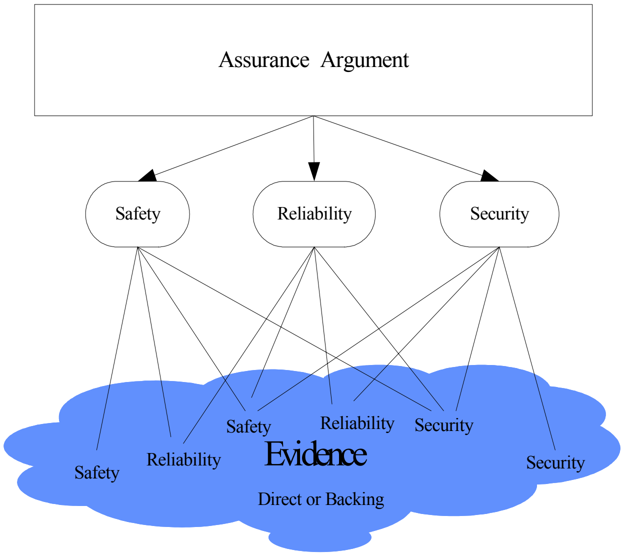


Figure 3: Arguing Assurance from the System's Evidence.

By using a single evolving document contained in the eDC the consistency of assurance information is maintained with a view to reaching the ultimate goal of an acceptable assurance case to all interested parties.

The overall approach is based on the use of an electronic presentation of the assurance case using standard browsers and plug-ins. This provides a readily available and common platform for presentation – removing the need for bespoke tools.

11.2.1 Web browser technology

Web browser technology is the means by which the assurance case is navigated. Providing a non-linear means of information accessibility, it removes the need for the reader to flick through reams of paper.

11.2.2 Ease of evidence retrieval

Claims of assurance to any standard are supported by evidence that is readably available. During the construction of the assurance case any areas that do not have supporting evidence are noted as such, reducing the likelihood that any required evidence is overlooked. The evidence contained within the assurance case need only be generated once yet can be used, if appropriate, in multiple claims. A central repository contains all the evidence allowing it to be accessed throughout the assurance case wherever necessary. This minimises the problems of document management and consistency.

11.2.3 Address Assurance

Addressing the assurance of a system in it's entirety is a large challenge, providing plenty of opportunities for mistakes. The eDC tool addresses all the aspects of assurance by allowing multiple views: breaking the assurance into safety, security and reliability; or breaking the assurance by standards, sub-systems or variants.

11.2.4 Applicable for all stakeholders

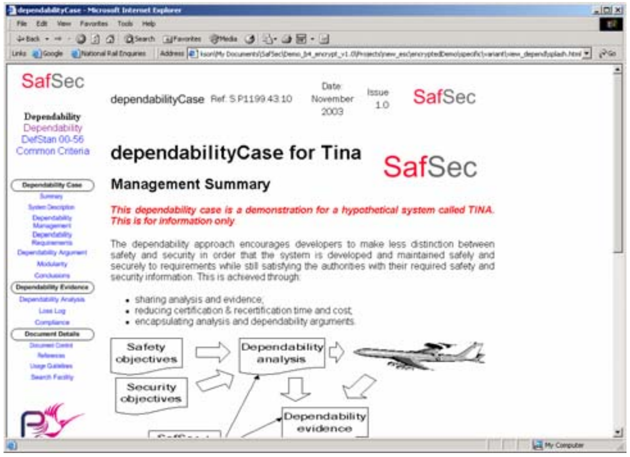
The eDC can be made suitable for all certification bodies. Making the intentions of the assurance case known early in the system development programme, the certification bodies will not be surprised at the end, de-risking the need for substantial re-work at the end of the process.

12. An example eDC

Of course, we cannot hope to give a true representation of the structure and browsing of an eDC in a printed paper, but we can outline its features.

12.1 Management Summary

The management summary is the 'home' page for any assurance case. It provides the background of the system, the standards against which the assurance case is being developed along with links to the system description and the argument. The conclusions and any limitations and caveats that apply to the assurance case are also linked from here.



dependabilityCase Ref: S.P1199.43.10 Date: November 2003 Issue 1.0

dependabilityCase for Tina

Management Summary

This dependability case is a demonstration for a hypothetical system called TINA. This is for information only

The dependability approach encourages developers to make less distinction between safety and security in order that the system is developed and maintained safely and securely to requirements while still satisfying the authorities with their required safety and security information. This is achieved through:

- sharing analysis and evidence;
- reducing certification & recertification time and cost;
- encapsulating analysis and dependability arguments.

Figure 4: The Management Summary of a Dependability Case

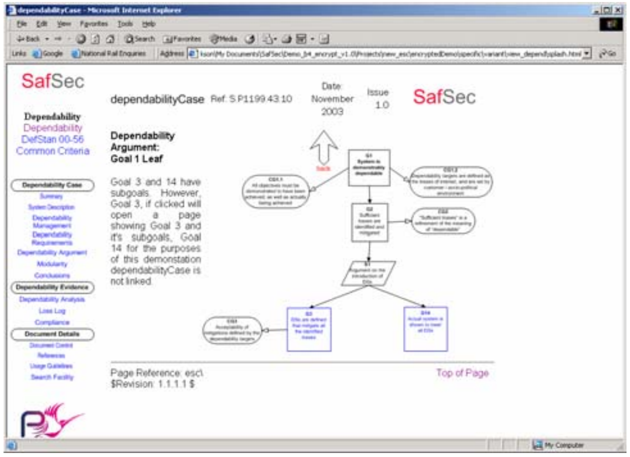
12.2 System Description

The system description provides the context to the assurance case., and the structure in which the evidence sits.

12.3 Assurance Argument GSN

The assurance argument consists of two components within each page of the argument: a fragment of the goal structuring notation (GSN) diagram; and the supporting commentary. Navigation through the argument is provided by active links in the GSN diagram and via the text. In practice a page of the safety argument will consist of a goal and it's strategy, both supported by context statements and the supporting sub-goals.

At an early stage of the development the assurance argument will only be an outline of the assurance argument. However, developing the assurance argument as fully as possible at an early stage in the system development is a valuable way of managing the assurance programme. Potential solutions (or markers) for the goals, even though these solutions are at a high level, are useful in providing a framework for on-going development.



dependabilityCase Ref: S.P1199.43.10 Date: November 2003 Issue 1.0

Dependability Argument: Goal 1 Leaf

Goal 3 and 14 have subgoals. However, Goal 3, if clicked will open a page showing Goal 3 and it's subgoals. Goal 14 for the purposes of this demonstation dependabilityCase is not linked.

Page Reference: esc\
$Revision: 1.1.1.1 $

Figure 5: Goal Structuring Notation Represents the Dependability Argument

12.4 Further Consideration

Using an eDC will not solve all your assurance issues. The following need to be considered when using the SafSec and eDC approach:

- The assurance will only be as good as the application of the underlying SafSec approach. The eDC does not generate the contents of the assurance case for you: safety, security and reliability experts are still required to do this.
- The eDC supports the necessary configuration management and helps bring to bear the expertise of the personnel, but the expertise has to be available for the eDC to be used to its full.
- The tools and automation of the build are necessary for management of certain items i.e. the loss log remaining separate.

13. Conclusions

The benefits of adopting a SafSec with Reliability approach, within an eDC, to provide assurance of your system are the identification and acknowledgment of commonality within Safety, Security and Reliability; the management of the commonality via web-based tools.

The standards, stakeholders and safety/security/reliability aspects of assurance cases all highlight commonality. The eDC is based on html and is a tool that enables this commonality to be taken advantage of and thereby eases the means of providing assurance while staying within the constraints of the budget holder.

Use of the eDC tool, built around a sound SafSec method augmented with Reliability and implemented by experienced practitioners is an effective and efficient route to providing systems assurance.

Acknowledgements

The authors would like to thank Mark Suitters, FBG, MoD for financial support of the SafSec Project.

References

[1] D. Cooper, D Jackson, and S Lautieri, "SafSec: Integration of Safety and Security Phase II Final Report", 2003. (Freely available by sending a request by email to: praxis-cs-safsec@praxis-cs.co.uk)

[2] T. Cockram, and B. Lockwood, Electronic Safety Cases: Challenges and Opportunities, in proceedings of Safety Critical Systems Symposium 2003, Bristol: Springer

[3] DefStan 00-42, Reliability And Maintainability Assurance Guides, Part 1 and 2, MoD 1997

[4] ISO15408 Common Criteria for Information Technology Security Evaluation, August 1999 (Version 2.1)

[5] DefStan 00-56, Safety Management Requirements for Defence Systems, Part 1 and 2, MoD, 1997

[6] RTCA DO-178B/ED-12B, Software Considerations in Airborne Systems and Equipment Certification, RTCA Inc., December 1992

[7] SW01, Requirements for Software Safety Assurance in Safety Related ATS Equipment, CAP670 Amendment 5, UK Civil Aviation Safety Regulation Group

[8] www.esafetycase.com

Biographies

Samantha Lautieri, Praxis Critical Systems, 20 Manvers St, Bath, BA1 1PX, England. Tel: +44 1225 823775
Email: samantha.lautieri@praxis-cs.co.uk

Samantha Lautieri, BSc, AMIEE is a Software Engineer and Project Manager with Praxis Critical Systems Ltd. She is the Project Manager of the SafSec Project, which has been under contract for 2 years, and has worked on numerous projects with requirements for proving various aspects of assurance.

David Cooper, Praxis Critical Systems, 20 Manvers St, Bath, BA1 1PX, England. Tel: +44 1225 823889
Email: david.cooper@praxis-cs.co.uk

David Cooper is an experienced consultant, working in particular with high integrity systems; often security or safety related. He has extensive experience in both technical consultancy roles and in project management, as well as experience in designing and delivering training courses in high integrity systems development. He has successfully worked with a range of clients to define security and safety requirements, and to develop provably correct architectural designs.

David Jackson, Praxis Critical Systems, 20 Manvers St, Bath, BA1 1PX, England. Tel: +44 1225 823846
Email: david.jackson@praxis-cs.co.uk

Dr David Jackson MA MSc CEng MIEE is a principal consultant with Praxis Critical Systems Ltd, where he co-ordinates the System Engineering service line. He has almost twenty years experience in working on high-integrity systems in the aerospace, rail, telecommunications and automotive markets.

Trevor Cockram, Praxis Critical Systems, 20 Manvers St, Bath, BA1 1PX, England. Tel: +44 1225 823779
Email: trevor.cockram@praxis-cs.co.uk

Dr Trevor Cockram PhD, C Eng, BSc, MIEE, MSaRS is a principal consultant with Praxis Critical Systems Ltd. He is the technical authority for the development of electronic safety cases within Praxis Critical Systems, which are being employed on a number of projects. He has over 25 years experience in defence systems engineering.