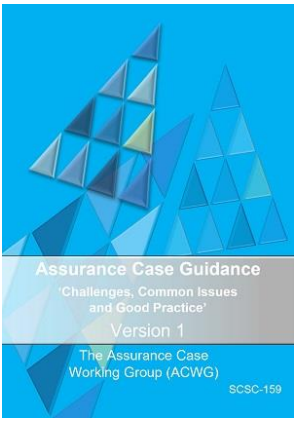
Assurance Case WG – Guidance document and GSN Standard update





The SCSC Assurance Case Working Group (ACWG) has published its first version of the Assurance Case Guidance addressing 'Challenges, common issues and good practice' and an update to the Goal Structuring Notation (GSN) standard. Phil Williams, lead of the ACWG, introduces the updates and explores the relationship between the documents.

The ACWG was established in 2017 with an international cross sector membership from industry and academia. It was formed to provide guidance on all aspects of assurance cases including their construction, review and maintenance. It was envisaged that this be broader than safety and address interaction and conflict between related topics.

One of the working group's initial activities was to take on board the maintenance of the Goal Structuring Notation (GSN) Community standard.

The products of the working group are made freely available under the creative commons licence.

Publishing the Assurance Case Guidance

The assurance case guidance publication has been created by the ACWG to address shortfalls in available guidance. It was decided early on that it should not attempt to repeat or replace established guidance, rather it should focus on topics that are perceived by the ACWG as containing weaknesses or poor practice and where no, or limited, guidance currently exists.

It is intended to be notation-agnostic and, whilst the experience in creating the guidance is predominantly drawn from the safety discipline, it is intended that the underpinning principles of assurance can be applied to any property – focusing on risk-related properties, for example: safety; security; availability.

The guidance is published as a freely downloadable publication on the SCSC website [1] and is also available for order in hard-copy from Amazon. It comprises:

- A framework that introduces the scope and context of assurance cases
- Topic papers, which each address a specific guidance topic
- Supporting information including terminology, references and acknowledgements

"notation-agnostic …focus on topics that are perceived by the ACWG as containing weaknesses or poor practice and where no, or limited, guidance currently exists"

Guidance topics addressed within the initial version are:

Avoiding Bias in Assurance Cases

Assurance cases are occasionally criticised for being biased in the way that they present their argument and evidence. This topic paper identifies several common biases to be aware of (and thus avoid) when constructing, reviewing and using an assurance case.

The paper addresses the perception that safety cases are biased, only considering the argument 'for' a system being safe. It argues that perhaps the case should instead be challenged to demonstrate that a system is not unsafe/unassured?

The paper sets out several types of bias and considers the potential impact on assurance cases. These include 'Cognitive', 'Confirmation', 'Disconfirmation' and 'Conservatism' biases, as well as the 'Observer-Expectancy' and 'Ostrich' effects.

It recommends cultural change to encourage a Hazard/Threat seeking culture, to seek disagreement and to seek, include and discuss counter-evidence.

Risk versus Benefit

This topic paper provides a discussion on the balancing of risk and benefit. It outlines the need to balance risk against benefit and how to tell when such an argument may be required. It provides examples where risk and benefit have been successfully balanced, and of the structure for a risk-benefit argument.

The paper highlights challenges in considering risk and benefit such as cases where risks may not be experienced by the same people as those who experience the benefit and where measures are subjective and use dissimilar units.

Modular Assurance

This topic paper deals with the structure and presentation of large and complex assurance arguments to support reader comprehension and addresses the benefits in managing the impact of change.

Two types of modularisation are considered: 'Basic' – when the author promises to the reader to come back to a side argument that is distracting to cover at this point; and 'Structuring for compositional arguments', which facilitates arguments created by disparate teams or suppliers.

Guidance is provided on: Structuring the argument; The need for clear assurance case module interfaces; The challenges of composing arguments; Presenting the argument case report; and Properties that are complex to argue in a modular way.

The Risk-Confidence-Conformance Approach

This topic paper introduces the concept of an approach that facilitates clear presentation of arguments structured around the three central themes of risk, confidence and conformance. It addresses the benefits of the approach and offers examples of how these can be presented.



Risk: Argument and evidence regarding risk

Confidence: Why the reader should have confidence in the arguments presented under risk or conformance

Conformance: Demonstration that requirements of standards, regulations and legislation have been met

Dialectic Arguments in Assurance Cases

This paper introduces the concept of dialectic arguments and shows how it can be used to add confidence to an assurance argument while it is being authored or during review/evaluation.

Dialectic arguments provide for the 'investigation of truth' through dialogue. It is a relatively new practice and addresses some of the concerns around bias by bringing counter-argument and counter-evidence into assurance cases.

Dialectic challenges can be characterised as:

- Rebuttal – argument and/or evidence that results in a conclusion counter to that intended by the assurance case
- Undercutting – challenges to the reasoning within the assurance case
- Undermining – raising doubts over the trustworthiness of supporting evidence

Future work

The ACWG is preparing to embark on a new series of activities including the preparation of guidance for the topics of 'Proportionality in Assurance Cases' and 'Assurance Cases across the Supply Chain'.

Updates to the GSN standard

The GSN standard was first published in 2011 by the GSN user community, its maintenance has subsequently been taken up by the Safety Critical Systems Club's ACWG. Version 2 provided an update to consolidate work in progress addressing clarifications from use of Version 1. The standard is complemented by a micro-site of the SCSC's website (https://scsc.uk/gsn), which provides supporting materials including relevant papers, argument patterns and a summary of the changes between version 2 and 3 of the standard.

"Version 3 of the GSN standard provides a major update to address several important extensions to the notation"

Version 3 of the GSN standard [2] provides a major update to address several important extensions to the notation:

Modular Notation Enhancements

Several updates and additions to the definition and guidance associated with modular notation have been included. New terms for module content views have been introduced to clarify the difference between the structure of an argument in GSN and the modules that contain GSN arguments. To reinforce the conceptual differences, some of the modular symbols have been changed to provide greater differentiation. This separation of concepts of structure has also enabled more clarity on how to represent 'containment' of an argument in nested modules – which in turn allows information hiding such that the details of a low-level argument do not need to be made visible in a high level abstracted view of the overall argument.

The update also addressed aspects of the practical use of modular argument that are part of the foundational concepts but were missing from earlier versions of the standard. These include the explicit definition of a module's interface, the formation of inter-module contracts, and the significance of context when forming away-goal relationships between modules.

Confidence Argument Support

New notation extension has been included to support the use of an 'Assurance Claim Point' (ACP) that allows arguments of confidence to be separated from arguments of risk or conformance. These help with providing focus to the thread of the argument in hand without ignoring important side discussions and build on the conceptual work published by Richard Hawkins. See the related discussion of Risk-Confidence-Conformance arguments in the Assurance Case Guidance.

Dialectic Argument Support

A new notation extension has been introduced to support the Dialectic argumentation approach. This allows challenges to the arguments created to be explicitly captured and reasoned about. The challenges may present counter-evidence or counter-argument and record how these impact the original argument. This is a key enabler for the important new approach addressed in the Assurance Case Guidance.

Patterns & Templates

Patterns have been part of the standard from the beginning and defined the graphical symbology and semantics but did not address the wider meta-data associated with a pattern definition from Tim Kelly's original work. This broader definition of a pattern has now been introduced. Templates have also been introduced as a special case of a pattern. A template allows a common repeated pattern in a fully developed argument to be represented by a graphical structure combined with an instantiation table.

General Updates

Several clarifications have been made to the content of the standard, with structural changes to emphasise the core and extension notational elements without the extensions appearing too specialised. These updates are intended to aid readability and provide clarity on the intent of the notation and its use.

Future work

The ACWG is preparing to embark on a further update to consolidate the normative elements of the standard, reinforcing the underlying meta-model and its relationship to the Structured Assurance Case Metamodel (SACM) [3]. It will also address the informative aspects, showing the interrelationship between the core and various extension notations.

The users of the GSN standard and Assurance Case guidance are invited to contribute to the updates to these documents by advising of topics that need to be addressed, or by directly getting involved with the working group. Comments can be registered at the forum (https://scsc.uk/f144). The ACWG can be contacted via its page at https://scsc.uk/gc.

References

[1] SCSC-159, "Assurance Case Guidance - Challenges, Common Issues and Good Practice", Published by SCSC/ACWG, August 2021, Version 1, ISBN: 9798451238592. see https://scsc.uk/SCSC-159

[2] SCSC-141C, "Goal Structuring Notation - Community Standard", Published by SCSC/ACWG, May 2021, Version 3, ISBN: 9798451294949 http://scsc.uk/SCSC-141C

[3] Object Management Group (OMG), Structured Assurance Case Metamodel (SACM), URL: http://www.omg.org/spec/SACM

Note: The version of these documents published on Amazon carries a x.1 version number to signify that there are formatting differences to fit to the standard SCSC hardcopy publication format. The content is essentially the same as the freely available pdf version on the SCSC website.

Phil Williams, Engineer for Safety Limited.

Phil is an independent system safety consultant. He is a Chartered Engineer and Fellow of the Institution of Engineering and Technology. He has over 30 years' experience designing and certifying safety critical systems. He has supported several cross-industry system safety initiatives. Phil is a member of the Safety Critical Systems Club (SCSC) Steering Group and chair of the SCSC's Assurance Case Working Group. Phil is an active member of the BSi GEL65/1 and IST/15 committees; the IEC TC65A MT61508 (developing edition 3 of IEC 61508) and IEC TC65A WG18 (developing IEC 63187 where he is deputy-convenor and principal UK expert). Phil is the lead author of The IET's Code of Practice for Cyber Security and Safety, published in 2020 and available for free download due to the support of the National Cyber Security Centre.