WHAT DOES THE ASSURANCE CASE APPROACH DELIVER FOR CRITICAL INFORMATION INFRASTRUCTURE PROTECTION IN CYBERSECURITY?

A.C. Goodger, N.H.M. Caldwell* , J. T. Knowles†*

** Department of Engineering, University of Cambridge, UK, acgoodger100@gmail.com, nhmc1@hermes.cam.ac.uk*
† In-Lode Ltd, UK, jtknowles55@hotmail.com

Keywords: Assurance Case, Cyber-security, Information-centric, Information Security.

Abstract

This paper describes how the Assurance Case Approach (ACA) was applied for Cyber Security and Critical National Infrastructure resilience, using for a single asset an individual Assurance Case (AC)**,** and for system-of-systems clustering a 'Mesh' case concept**.** Despite its common use in the Safety domain, the ACA concept had not been applied to a dynamic situation. It allowed for Cases to be clustered using a 'Mesh' Case to summarise a particular ecosystem/environment.

This ACA is defined using basic elements of an assurance case ie Claim, argument and evidence – often associated with a legal analogy. Using the case study research method [27], the main methodology as stated in the paper combined the organisational learning cycle [1] with the 6-step based process based on a GSN [16] and CAE [2] notational hybrid for the construction of an argument structure. This was implemented with a CII asset, and further pilotted to demonstrate the ACA for other CII nodes [13]. The clustering using the 'Mesh' cases closely aligns with Interdependency Analysis for the UK interconnected system-of-systems. Further work is required to expand the 'Mesh' case principle for the 21st century information-centric ecosystem to provide a continual resilience work process framework, which eventually must include real-time inputs.

1 Introduction

Today's economy and society is totally reliant on technology as an enabling force for all economic and societal activities. It is now fundamental to protect those information infrastructure technologies, and there is a strategic core which must be maintained i.e. the Critical National Infrastructure (CNI)/Critical Information Infrastructure (CII). The CNI/CII overall environment has become a dynamic and rapidly changing landscape within non-linear timeframes. Thus, small incremental changes and/or large-scale modifications can drastically shape and reshape both the economy and its society with known and often unknown consequences, due to ever-increasing interconnectivities and growing complexities … especially, the information technologies that have come to pervade virtually all aspects of life [9]. Consequently protecting this environment requires a flexible and adaptive approach in near-real-time and real-time mechanisms based on evidential components, on multi-disciplinary inputs and the capacity in dealing within a dynamic information ecosystem.

2 Background/Rationale

2.1 Why is the environment relevant?

In the 21st century society it is critical that all need to adapt, be flexible and to change at variable and faster rates. In addition, not all the interactions between human, technical, physical and information systems are clearly understood and/or defined. Security is now a much broader concept. While often perceived as the 'defence' aspects, it actually is resilience in its totality. This requires co-ordination across all parts of the United Kingdom.

Thus, the business information environment (BIE) is now the global framework, with increasing permeability of boundaries at all levels and a polycentric nature of the global political, societal and economic systems – 'with states as merely one level in a complex system of overlapping and often competing agencies of governance' [14]. Porter's analysis of competitive advantage for nation states has shown that it does not represent the networked ecosystem and/or environment of the 21st century. In the evolving organisational framework, the flexible business network is represented by a production chain and is beyond conventional subcontracting, strategic alliances and the 'integrated network' structure [23]. The complex system-of-systems is not hierarchical; it's emergent and relatively flat as demonstrated within the Key Online Services to the 'Citizen' – a co-operative, relational structure between independent and quasi-independent organisations based on a high degree of trust.

2.2 Challenge

Due to the fluidity and to the rapidly changing nature of the information society and economy, it is essential to provide a flexible and adaptable way of managing Critical Information Infrastructure (CII) assets. One possible route is to take proven principles, methods and techniques from other knowledge domains, i.e. safety, and determine if these could provide relevant mechanisms to capture and manage these CII assets in a real-time manner. Consequently, as shown in this paper the challenge was to prove that Assurance Case Approach (ACA) could be adapted and effectively implemented for CII cyber-security protection, and deliver an integrated oversight for combined safety, security and reliability in a single framework.

2.2 What are Assurance Cases?

When used in a CII context, the Assurance Cases Approach (ACA) discussed in this paper is based on a basic model, whose constituent parts makes up the totality of the argument [24]. This is founded on deductive reasoning first formulated by Aristotle using logical arguments, and is known as a syllogism. It typically consists of three component sentences - including 2 premises and one conclusion. A *Premise* is merely a stated proposition. The *conclusion* of an argument must be based upon, and supported by one or more acceptable/accurate/logical premises or reasons. AC arguments partially follow this format. Toulmin [24] partially evolved Aristotle's concept that 2 or more 'claims' and a single conclusion constitute the argument.

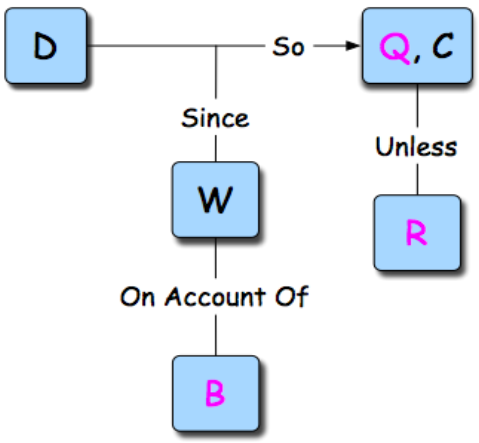

Figure 1: Expanded Toulmin structures.

As in Figure 1, this was expanded to include a justification for the 'claim' with an overall environmental contextual backing and rebuttals if the 'claim' cannot be verified unless the structure is validated [24]. This format provided the central constituent basis for the Assurance Case Approach Main Methodology.

2.3 Transition from the Safety to Security Domains

In one aspect, Assurance Case (AC) methodologies had been applied in the safety domain to the security domain, and this indicated it was also relevant to CII cybersecurity. In safety, the case is based on a body of evidence organised into an argument that holds some complex property i.e. safety, security or reliability, and it demonstrates this transition for its use as a security assurance case [21]. Initially, the security case was applied to software development assurance using the same safety case principles and elements, via the Goal Structuring Notation (GSN) methodology [16]. The application expanded to varying rationales including accounting legal or regulatory (e.g. Sarbane-Oxley or HIPAA), Economic (e.g. insurance) and other non-technical etc., [20]. Consequently, it brought benefits for software development, by potentially decreasing resource requirements and minimising costs to maintain cybersecurity-related issues throughout the information asset lifecycle.

2.4 Research Methodology

The research undertaken and practical pilot implementation used a case study approach [27]. The Assurance Case Approach (ACA) built on previous research and work done by the Adelard consultancy [2, 4]. The research method provided an in-depth examination of a single instance delivering a systematic way of looking at events, collecting data, analysing information, and reporting the results. Furthermore, it utilised practical methodologies i.e. from the safety domain i.e. the Goal-Structuring Notation (GSN) Methodology [16] and Assurance Cases [2,4], and from the educational/organisational domain, the learning cycle [1]. Thus, it enabled the study to relate directly to real world experience and facilitate a repeatable pilot implementation in a complex environment.

3 Assurance Case Approach Main Methodology

Using the case study research combined the learning cycle [1], with GSN methodology [16] to provide the ACA main methodology. Despite its common use for safety critical systems in the Safety domain, the Assurance Cases Approach (ACA) concept had not been applied to a dynamic and turbulent BIE. Within complex systems such as CII, the AC approach collates profiles of assets or groups of assets (aka nodes or cluster of nodes). As Figure 2 shows, this provides system commonality across the safety, security and reliability threads [18].

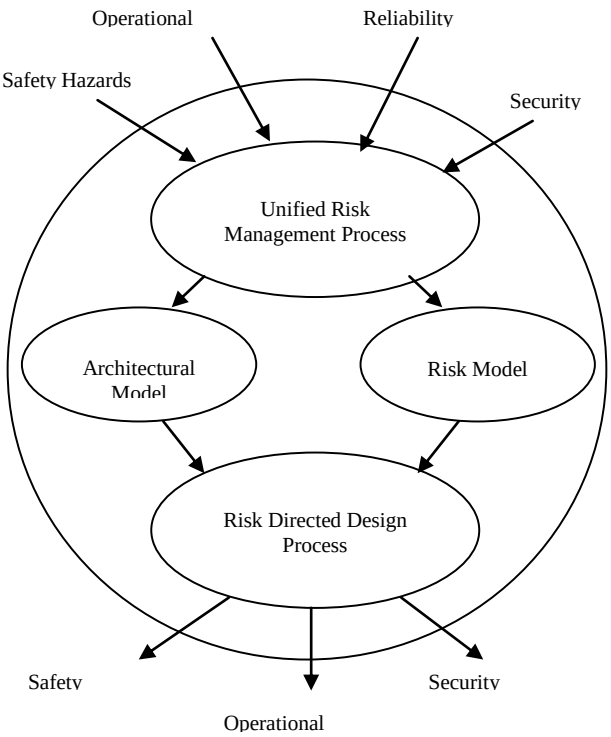

Figure 2: Co-ordinated Safety, Security and Reliability.

This integration is required to:

- Reduce the effort required**.**
- Reduce the reluctance in producing integrated assurance cases**.**
- Show that tools assist in the integration**.**

As in Figure 2, the co-ordinated approach makes for easier identification and resolution of gaps and conflicts. This clarity is a fundamental attribute, and it significantly assists and increases confidence when communicating with key stakeholders. Ultimately, the argument structure supports a number of knowledge domains, and delivers an integrated adoption addressing CII system assurance in several contexts, including ongoing cybersecurity and stakeholders' buy-in with associated confidence for CII assurance.

3.1 Single Asset (aka single node) - The Main Methodology

The single assurance case (aka single node), as in Figure 3, uses the Asset Vulnerability Asset Evaluation and Review Cycle workflow [13] adapted from the learning cycle [1].

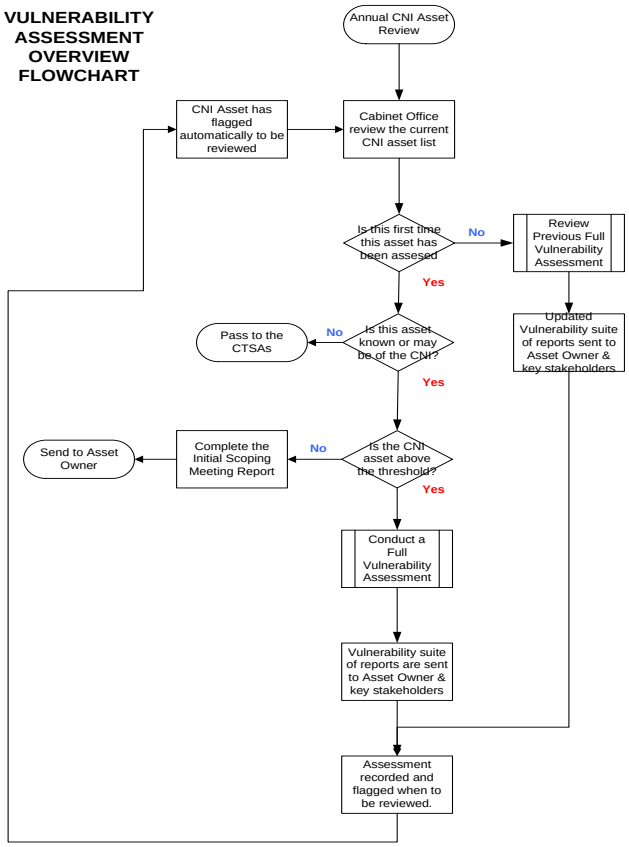

Figure 3: Overview of the CII Asset Vulnerability Asset Evaluation and Review Cycle.

The ACA main methodology principles and terminology combines CLAIMS-ARGUMENTS-EVIDENCE (CAE) [3] and associated aspects of GSN methodology [16] for constructing the Case. This hybrid approach of the GSN methodology and CAE notation delivers an overall completeness and structuring for an ACA [13]. The GSN method [1] had been adapted for ACA, as no equivalent mechanism existed except for the CAE notation [3]. Furthermore, there are different arguments as follows:

- Deterministic or analytical application to derive a false or true claim (given some initial assumptions)**.**
- Probabilistic quantitative statistical reasoning that will derive a numerical value**.**
- Qualitative compliance with rules that have an indirect link to the desired attributes**.**

The deterministic argument is used as part of this Main Methodology, as it provides greater assurance than the other types of argument [3].

3.2 The Vulnerability-Related Case Lifecycle

Figure 3 indicates the cyclic flow and the "living document" nature of security assurance cases, which evolve as information/physical assets change through their life-cycle [12]. All workflows are documented using a graphical format.

- Initial Scoping Phase - If this asset has not previously been assessed, then the ACA Main Methodology has an initial scoping phase to determine its level of resilience

criticality. If the asset identified lies on the CNI, then a full assessment using the ACA is conducted, and if not the CNI/CII process is completed at this stage.

- Full Vulnerability Assessment Phase - Then if the CNI/CII asset is considered about the CNI resilience critical threshold, then the Full vulnerability assessment phase is conducted. Using the learning cycle as the basis [1], then an initial evaluation of it establishes the baseline. At this stage, the argument structure is developed to establish a trustworthy status for the Claim and Sub-Claims.
- Argument Development Structure - The main part of the evaluation is construction of the argument. There are three main objectives with an Assurance Case [1]:
  - Making the argument clear - in language of the individual statements and flow of the AC.
  - Making the argument defensible – appropriate rationale to support the argument.
  - Making the argument mutually understandable – provide context to minimise ambiguities.

  As in Figure 4, the overall process involves 6-steps used in a GSN approach in the CAE notation.

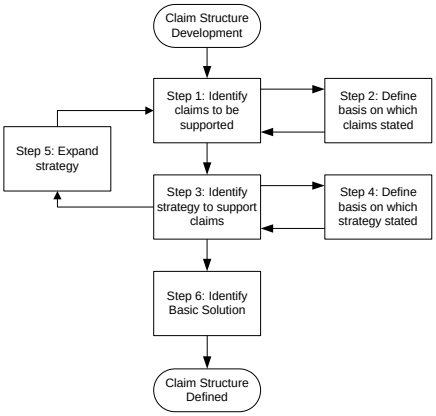

Figure 4: The Overall claims definition process.

As Figure 4 indicates, the ACA is recursive – a claim is identified with the appropriate strategy to support it. The claim must be clearly stated and understandable from the audience's perspective due to associated evidence. In some instances, it is relevant to have Sub-Claims with supporting arguments to group the evidence. Where further Sub-Claims are required, then the process returns to Step 1. AC provides a relevant 'audit trail' that represents the claim made and a defensible argument to support an optimal answer [26].

- Ongoing CII Vulnerability Assessment - The final phase is the continued and ongoing evaluation of a CNI/CII asset. The ACA Main Methodology adopted the single-loop and the double-loop principle, similar to those used for recursive organisational learning [1]. The initial iteration established the baseline for the CII asset and contributed to developing the larger CII landscape. Furthermore, the learning aspect is required for agile resilience processes that need to be maintained on a regular basis.

3.3 Clustering of Assets using The Main Methodology

In expanding the ACA Main Methodology for individual CII assets to input into the larger BIE led to the grouping of single ACs within a particular domain. This is referred to as a 'Mesh' case. This can be visualised as the 3-D atomic structure of a molecule. The 'Mesh' claim provides a lateral approach for interdependencies between individual assurance cases.

The 'Mesh' domain has an overall claim that other claims will link to provide the relevant evidence, and to support a defensible objective. The topology is based on a mesh network topology. It is not hierarchical but is related to interdependencies between ACs. As in the ACA methodology used in the Case Study, then the 'Mesh' claim provides overarching confidence. The 'Mesh' claims, defined as with the single case top-level claims, use the same ideas as put forward in the 6-step method. The 'Mesh' claim uses straightforward language e.g. "Public Sector A is medium vulnerability". The wording is not over-simplified but does still allow for a realistic argument structure assessment. The remaining steps apply as for a Single Case.

4 Piloting and Implementation of the Single Asset and 'Mesh' Cases

The case study proved and established that the ACA could be adapted to CII assets for cybersecurity. It had shown, by combining existing models, that the process was based on a sound foundation from the safety domain [13]. The next question was could this be applied to a system-of-systems approach, a problem that was out of scope of the original Case Study. The business requirement urgently required an integrated approach across several CNI/CII assets, and the 'Mesh' case was piloted with a further 2 assets. It was found that the approach scaled to multiple assets viewed as a system-of-systems, and that an overall 'Mesh' claim could be validated to provide an ongoing assessment for assets within this particular domain.

A further outcome from the Case Study using the Single Case was to deliver a basis for establishing a pattern method and associated high-level steps. In applying the 'Mesh' case built on work from the Arlington Workshop on Assurance Cases in 2005, the pattern method was discussed and reviewed as delivering [4]:

- Top-level contents/structure – clearly identifies the risks/vulnerabilities and risks, how the risks have been mitigated/addressed, estimated level of residual risk and assurance of risk tolerance.

- Attributes – maintainable (modular to avoid cascade changes), reusable, understandable/re-viewable, recursive, efficient (cost effective), convincing, accurate, useful to decision maker (e.g. appropriate level of information), mature tool support.

These patterns need to be properly documented to understand the rationale, and the provenance for devising the evidence capture. The idea of developing a library of patterns (or templates) provide for reuse, repeatability and ease of documentation. This is more cost effective and if introduced correctly minimised the effort in the AC design. Furthermore, the pattern method provides the basis for 'Mesh' Cases [13].

As in the safety domain, it uses the same argument structure template (without the changing context and supporting evidence) to assess different systems or services. The international standard describes a 'meta-claim' that provides confidence of the overall argument meta-structure of individual cases (the meta-structure of the claim is included within the proposed ISO15026 re-write) [2].

Consequently, the 'Mesh' case is operating at multiple level/dimensions in a near real or real time situation, and has inputs from the defined evidence structure and links with ISO15026 [15] for the AC meta-model [11]. The Case is monitored at boundary points – such as SLAs between layers organisationally and technically, that in addition feedback in an expected manner. It uses cases to manage the rapidly changing environment**,** allows communications with stakeholders and assists an organisation's reaction to emergent behaviours from the ever-changing BIE.

5 What does ACA deliver for Cybersecurity?

The ACA has demonstrated a proven approach from the Safety domain. Building on this knowledge, the ACA provides a flexible approach and the insights from this research have been used as input into several recommendations – assurance case establishment (single and mesh cases) and supporting the risk management approach for UK Information Assurance Government Standards - IS1/IS2 and CIIP (Critical Information Infrastructure Protection) Four-pillar Framework. Consequently in the dynamic BIE, which can be referred to as a Hypercompetition Model environment [7], the ACA provides an overarching structure which operates at many levels that can be tracked for whatever rationale, and can be used in the 21st century CII environment.

6 Conclusion and Future Work

The use of the ACA for vulnerability assessment for the public sector CII protection (CIIP) was and is required – due to the unbounded world of Globalisation [23], Cyberspace, Cloud Computing [22], and dramatic changes in the nature, format and delivery of public sector information services online [5,6]. The end-to-end ACA evidence-based mechanism provides an overall asset lifecycle method to capture, maintain and manage a specific asset within the dynamic environment. Ultimately, it meets the CIIP challenges to minimise resilience risk to the CNI, and potentially will work as part of a CIIP risk-based toolset.

The ACA supports the 'survivability' concept [19], the 21st century landscape requirement for a new resilience paradigm [10] linked with cybersecurity. The rate of change has increased dramatically in the last 20 years, with greater 'turbulence'. Further work is required to automate the ACA 'mesh' case approach for the 21st century information centric universe, and this to be dovetailed with dependability cases.

Dependability Cases are not a new concept [25]. They evolved from Safety cases – this is an expansion on the AC. They provide clear, defensible and usable arguments to operate in a given context [17, 8]. In turn, this provides confidence for delivering different viewpoints of the system's operation – specifically linked with system-of-systems (SoS - whose attributes are complexity, autonomy and geographic dispersion). The dependability requires a framework to be devised to overcome a number of challenges [13].

Acknowledgements

The authors would like to thank CESG for financial support towards one of the author's MSc qualification.

References

[1] C. Argyris, D. Schon. "Organisational Learning: A theory of action perspective", Addison-Wesley, Reading, Massachusetts, (1978).
[2] P.G. Bishop, R.E. Bloomfield , A.S.L. Guerra. "The future of goal-based assurance cases", Adelard and City University, London, (2006).
[3] P.G. Bishop, R.E. Bloomfield , A.S.L. Guerra. "*Report on the application of safety techniques to security (v2)*", Adelard Report, (2009).
[4] R.E. Bloomfield, A.S.L. Guerra, M. Masera, A. Miller, O. Sami Saydjari. "*Assurance Cases for Security – Workshop on Assurance Cases for Security*" delivered at SEI, Arlington, VA (13-5 June 2005), Adelard, (2005).
[5] Cabinet Office. "*Government ICT Strategy*", Crown Copyright, (2009).
[6] CESG. "*Miscellaneous - Requirements for Secure Delivery of Online Public Services Part 2: Security Components*" (Issue No: 1.0 - July 2010), (2010).
[7] R. D'Aveni. "*Hypercompetition: managing the dynamics of strategic manoeuvring*", Free Press, New York, (1994).
[8] G. Despotou, T. Kelly. "*The Dependability Case as a means of Establishing System Assurance*", in proceedings of the 26th International System Safety Conference, Vancouver (ISSC), Canada – 25-29/08/2008, www.despotou.eu/index.php/publications/52-poster/ (2008)
[9] P. Dickens. "*Global Shift – Reshaping The Global Economic Map in the 21st Century*", Sage Publications, London, (2003).
[10] R.J. Ellison, C. Woody. "*Survivability Analysis Framework*", Software Engineering Institute, Carnegie

Mellon, (2010).
[11] L. Emmet. "*International Standardisation of Assurance Cases – including ISO15026 and OMG (presentation)",* www.adelard.com/web/../standards_update_omg_15026.pdf, (2010).
[12] J. Goodenough, H. Lipson, C. Weinstock. "*Arguing Securing – Creating Security Assurance Cases*", Carnegie Mellon (https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/assurance/641-BSI.html) (2008)
[13] A.C. Goodger. "*Assurance Cases (The New Approach to Vulnerability Assessment of a UK Government Sector Critical National Infrastructure Asset)*", MSc Information Security Dissertation, Royal Holloway University of London (2010).
[14] P. Hirst, G. Thompson. "*Globalisation in Question: The International Economy and the Possibilities of Governance*", Polity Press, Cambridge (1999).
[15] ISO. "*Information technology — System and software integrity levels*" (ISO/IEC 15026:1998), (1998).
[16] T. Kelly. "*A Six-Step Method for Developing Arguments in the Goal Structuring Notation (GSN)*", GSN-solutions.co.uk, (1998).
[17] J.C. Laprie. "*Dependability: Basic Concepts and Terminology*" (ed), Springer-Verlag, Vienna, Austria, (1992).
[18] S. Lautieri, D. Cooper, D. Jackson, T. Cockram. "*Assurance Cases: how assured are you?*" DSN -2004, www.praxis-his.com/downloads/whitepapers/AssuranceCase_DSN04.pdf (2004).
[19] H.F. Lipson, D.A. Fisher. "*Survivability — A New Technical and Business Perspective*", www.cert.org/archive/pdf/busperspec.pdf (1999)
[20] H. Lipson, N. Mead, A. Moore. "*Can We Ever Build Survivable Systems from COTS Components?"* - Proceedings of the 14th International Conference on Advanced Information Systems Engineering (CaiSE), Toronto, Ontario, Canada, (May 2002), Heidelberg, Germany: Springer-Verlag (LNCS 2348), (2002).
[21] H. Lipson. "Assurance Case Overview", Carnegie Mellon University, (https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/assurance/641-BSI.html), (2008).
[22] P. Mell, T. Grance. "*Effectively and Securely using Cloud Computing*", US National Institute of Standards and Technology (NIST), (2009).
[23] M.E. Porter. "*The Competitive Advantage of Nations*", Macmillan, London, (1990).
[24] S. Toulmin. "*The Uses of Argument*" – Updated Edition (on 1958 version), Cambridge University Press, Cambridge, (2003).
[25] C.B. Weinstock, J.B. Goodenough. "*Towards an Assurance Case Practice for Medical Devices*", Software Engineering Institute, Carnegie Mellon, (2009).
[26] B. Wilson. "*Soft Systems Methodology*", John Wiley & Sons Ltd, Chichester, West Sussex, (2001).
[27] R.K. Yin. "Case Study Research: Design and Methods", Sage, Newbury Park, California, (1984).