Using an Assurance Case Framework to Develop Security Strategy and Policies

Robin Bloomfield[1,2], Peter Bishop[1,2], Eoin Butler[2], Kate Netkachova[1,2]

[1]Centre for Software Reliability, City University of London

[2]Adelard LLP

{reb,pgb,eb,kn}@adelard.com

Abstract. Assurance cases have been developed to reason and communicate about the trustworthiness of systems. Recently we have also been using them to support the development of policy and to assess the impact of security issues on safety regulation. In the example we present in this paper, we worked with a safety regulator (anonymised as A Regulatory Organisation (ARO) in this paper) to investigate the impact of cyber-security on safety regulation.

Keywords: Security-Informed Safety, Assurance Cases, Regulation, Risk Assessment

1 Introduction

Assurance case frameworks have been developed to reason and communicate about the trustworthiness of systems. Over the past five years or so we have been researching the impact security has on safety assurance and have been developing enhancements to the Claims, Arguments and Evidence (CAE) approach [1-3] to deal with some of the challenges posed by the need for increased rigour and complexity of systems. This supports the evaluation we have been doing of critical infrastructure security and safety e.g., [4].

Recently we have also been using the CAE framework to support the development of policy. From a broader perspective we are interested in the innovation potential of engineering methods to support decision making in large organisations and government [5, 6]. In the example we present in this paper, we worked with a safety regulator (anonymised as ARO in this paper) to "Investigate the Impact of Cyber-Security on Safety Regulation". The project developed a proposed regulatory strategy to enable this organisation to provide an adequate response to issues of cyber-security. They regulate complex systems of systems and the assessment of whether systems are safe, and the communication of that assessment to the interested stakeholders, is not complete unless security and cyber issues are taken into account.

The interest to the assurance community is perhaps twofold: one that the frameworks we are developing have a wider applicability to decision analysis and support and second that deploying approaches beyond their initial design intent can provide feedback on our approach to assurance cases.

2 Impact of Cyber Security on Safety Regulation

The project developed a proposed regulatory strategy to enable the ARO to provide an adequate response to issues of cyber-security. They regulate complex systems of systems and the assessment of whether systems are safe, and the communication of that assessment to the interested stakeholders, is not complete unless security and cyber issues are taken into account. The security aspects are increasingly important as there are:

- greater levels of threats and a changing threat in terms of nature, targets and capabilities of the attackers
- significant planned changes to systems, greater connectivity and use of supply chains and products with vulnerabilities
- changes in regulation
- requirements to communicate that effective and sufficient measures have been taken to a variety of stakeholders
- increased expectations of the public for a resilient service and associated systems

To assess the impact and to develop a programme of work we worked collaboratively with a wide range of stakeholders to establish the complex and organisational and regulatory context captured what we dubbed as an "entanglement diagram" that showed the dependencies between the stakeholders. Having established an understanding of the context we used CAE to develop the visions and objectives. We continued detailing the objectives in terms of claims until these were sufficiently detailed to establish a programme of work. There were a complex interlocking array of issues and the use of the CAE provided a vehicle for reasoning and communicating with stakeholders (government regulatory policy experts, government security agencies, domain experts, regulators and assessors).

This paper describes how we developed the vision and objectives using an assurance case approach.

2.1 Vision and Objectives

Having established the system and regulatory context, we then developed a set of structured cyber-related objectives for the ARO starting from the ARO's own strategic vision, taking into account the UK Cyber Strategy, a number of cyber frameworks and maturity models [7-9], and a focused analysis of activities in other sectors. We presented the results of this analysis in terms of a set of structured objectives or claims so that the rationale and interaction of different parts of strategy can be appraised. These are presented within a Claims Argument Evidence (CAE) framework and notation. The regulator was familiar with the notion of outcome-based regulation and the concepts of claims, arguments and evidence.

The approach to deriving the cyber programme objectives is illustrated in **Fig. 1** (the nodes are discussed in detail later and are not meant to be legible in this figure).

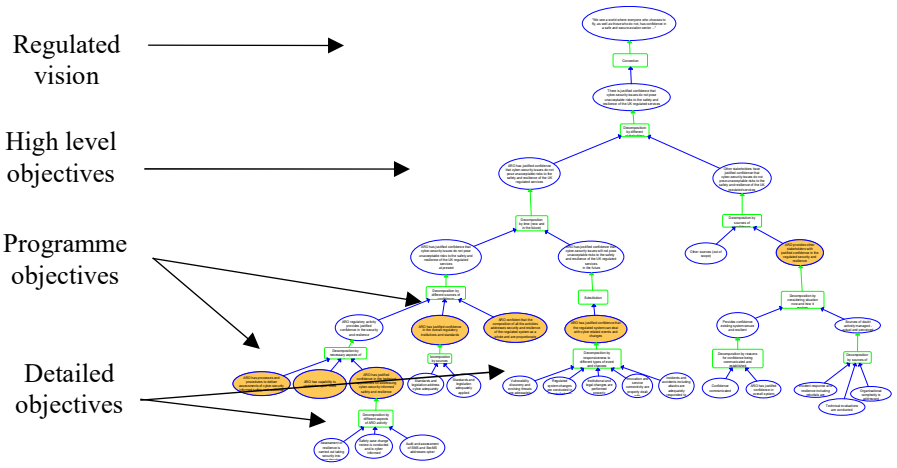

Fig. 1. Schematic of approach

We started with the organisation's strategic vision and then derived high-level cyber-related objectives. We further decomposed these into more detailed objectives, identifying in orange those that form the proposed cyber programme objectives, which are numbered sequentially.

In developing the objectives in this way we can show traceability and rationale for them and also show the coverage with respect to the set of issues identified in the tree structure of **Fig. 1** (some of the claims are outside the scope of the regulator but show its dependence on others).

We have also reviewed the UK Cyber Strategy objectives and from these developed specific strategic objectives that we then mapped to the proposed programme objectives to show how our proposals relate to them and provided another check for coverage of issues.

2.2 Deriving the Programme Objectives

First we derive some high level objectives from the ARO strategic vision as shown in **Fig. 2** below.

High level objectives. The ARO's principal functions and duties are set out in primary legislation. The ARO has a strategic vision that

> *"We see a world where everyone who chooses to use these services, as well as those who do not, have confidence in a safe and secure sector that takes its responsibilities seriously, backed by a regulatory system that actively manages risk and supports consistently high performance."*

Part of this strategic vision "*We see a world where everyone […] has confidence in a safe and secure sector […]"* provides a starting point for the Cyber Strategy. We propose that the cyber component of this vision is interpreted as

> *We see a world where there is justified confidence that cyber-security issues do not pose unacceptable risks to the safety and resilience of the regulated services*

Directly from this interpretation, we derive the top-level objective for the ARO Cyber Strategy in terms of the confidence in the regulated services that both the ARO and other stakeholders have. This is:

> *There is justified confidence that the risks from cyber incidents do not pose unacceptable risks to the safety and resilience of the regulated services*

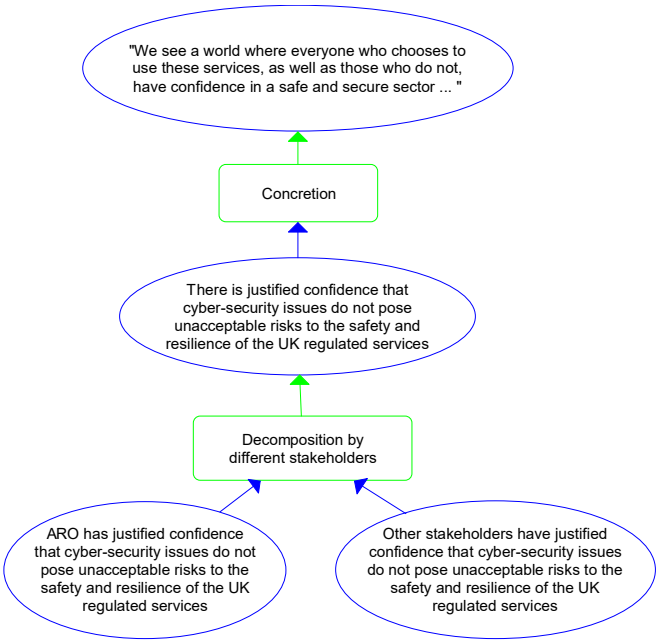

Fig. 2. Deriving the ARO objectives from the vision

ARO confidence. Starting from the claim "There is justified confidence that the risks from cyber incidents do not pose unacceptable risks to the safety and resilience of the regulated services", we divide the top-level objective into the confidence of the ARO and that of other stakeholders. We propose that the objective for ARO is:

> *ARO has justified confidence that cyber-security issues do not pose unacceptable risks to the safety and resilience of the regulated services*

As shown in **Fig. 3** below, this is then split into two sub-objectives, one describing the present situation and another the future.

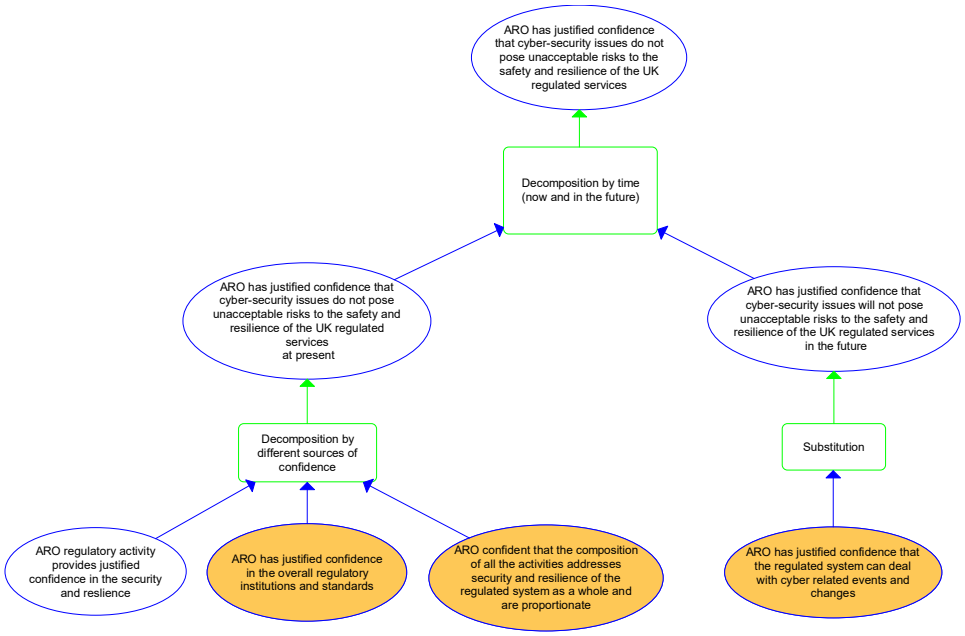

Fig. 3. Confidence now and in the future

Confidence in the present situation is then further expanded in terms of the sources of that confidence, which are:

- the ARO's own regulatory assessment activities
- the overall regulatory approach, the institutions involved and the standards deployed
- a synthesis that all these activities when considered together show that risks from cyber are tolerable

The high-level objective for the future is:

> *ARO to have confidence that in the future the cyber risks will not undermine the safety and resilience of the regulated system*

To support this, we proposed an objective that the regulated system can deal with future cyber-related events and changes. These top-level objectives are summarised in **Fig. 3** in which the key programme objectives are coloured orange.

We now detail these objectives, moving left to right in **Fig. 3**. We first consider ARO's direct regulatory activities as shown in **Fig. 4** below.

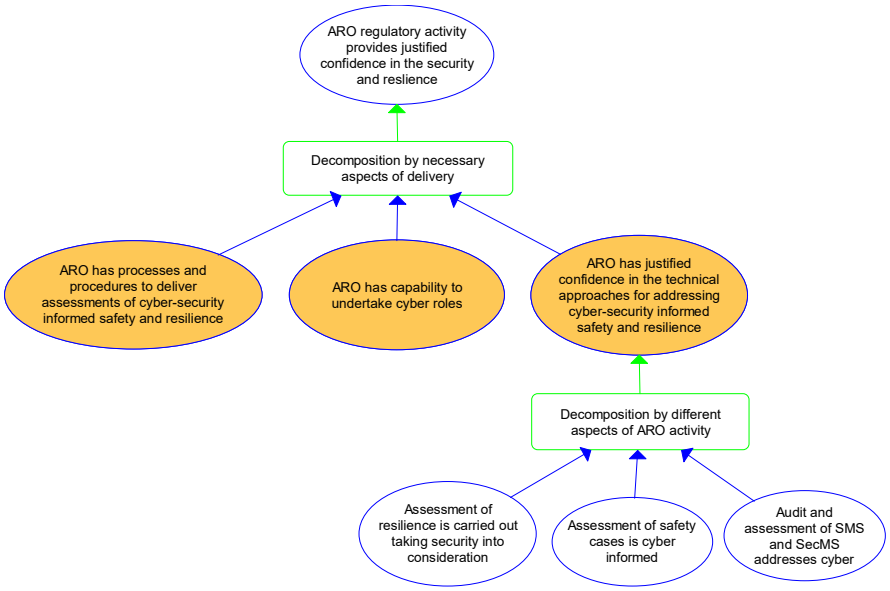

Fig. 4. ARO regulatory activity

For the ARO regulatory activity to provide confidence, we identify three aspects to be addressed. The first two concern governance: the need for appropriate internal processes and procedures, and confidence that ARO has the capability to undertake its role as a regulator of cyber-security activities. These correspond to the programme objectives below:

1. ARO has processes and procedures to deliver assessments of cyber-security-informed safety and resilience
2. ARO has capability to undertake cyber roles

Here we note that, as well as the ARO's capability to undertake its regulatory role, the ARO needs to have the capability to ensure the cyber-security of its own processes, people and technology. Cyber-security related events within ARO, even if restricted to office systems and nothing to do with safety as such, will undermine confidence in the institution as a whole. The adversaries realise this, and as their overall goals may be to undermine confidence in the state and institutions, attacks on confidence and competency are a possibility, both directly and as part of multi-faceted attacks. There will be a need to define and adapt existing processes to deal with cyber issues, e.g. to define roles and responsibilities, multidisciplinary oversight and specialist involvement of cyber-related activities. These should address competency and the need for education, training and awareness.

The third aspect to consider is the need for technical approaches for security-informed safety and resilience. This corresponds to the next programme objective:

3. ARO has defined technical approaches for addressing cyber-security-informed safety and resilience

As shown in **Fig. 4**, these need to support the audit and assessment of Safety Management Systems (SMS) and Security Management Systems (SeMS), the assessment of resilience, and the cyber informed review of safety case changes.

These technical approaches need to take into account that cyber-security issues impact safety assurance and associated risk analyses throughout the system and service lifecycle, with associated changes needed from requirements through development and operation to disposal. The impact varies with the nature of the systems and the extent to which they are already engineered to be trustworthy. Many safety critical components will already have had a high degree of assurance applied to them and this needs to be reviewed and augmented from a cyber perspective. Less critical systems may have minor safety significance, but due to potential connectivity, they may need substantial reengineering and analysis to address security concerns. We provided details of technical approaches to cyber-security informed assessment, vulnerabilities, standards, systemic risks and interdependencies and the need to respond to the faster tempo that security issues may demand.

Returning to the decomposition in **Fig. 3**, the second objective that "ARO has confidence in the overall regulatory approach, the institutions involved and the standards deployed" is detailed by considering the sources of confidence in overall regulation. This is formalised as the fourth programme objective:

4. ARO has confidence in the overall regulatory institutions and standards

This is further elaborated in **Fig. 5** below.

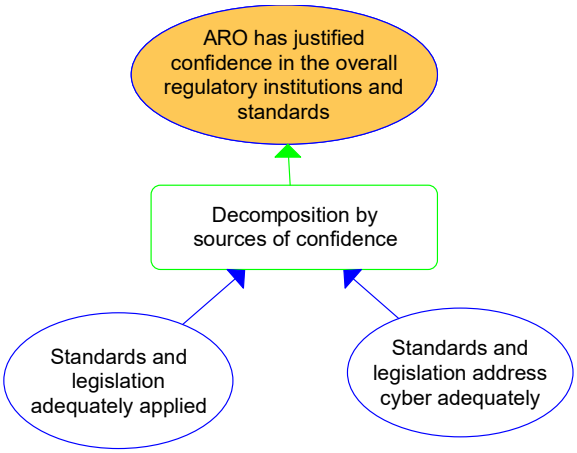

Fig. 5. Sources of confidence in regulation and standards

The confidence that the overall cyber-related risks are tolerable.is based on the regulatory oversight and engagement with the regulated institutions and service providers, and the evaluations that the ARO undertakes itself, i.e.

5. ARO confident that the composition of all the activities addresses security and resilience of the regulated system as a whole and are proportionate

Confidence in the future safety and resilience. Next, we elaborate the "future" branch of **Fig. 3** where we define the following programme objective.

6. ARO has justified confidence that the regulated system can deal with cyber-related events and changes

As shown in **Fig. 6** below this goal is elaborated in terms of the different types of events and changes to which the system has to respond to.

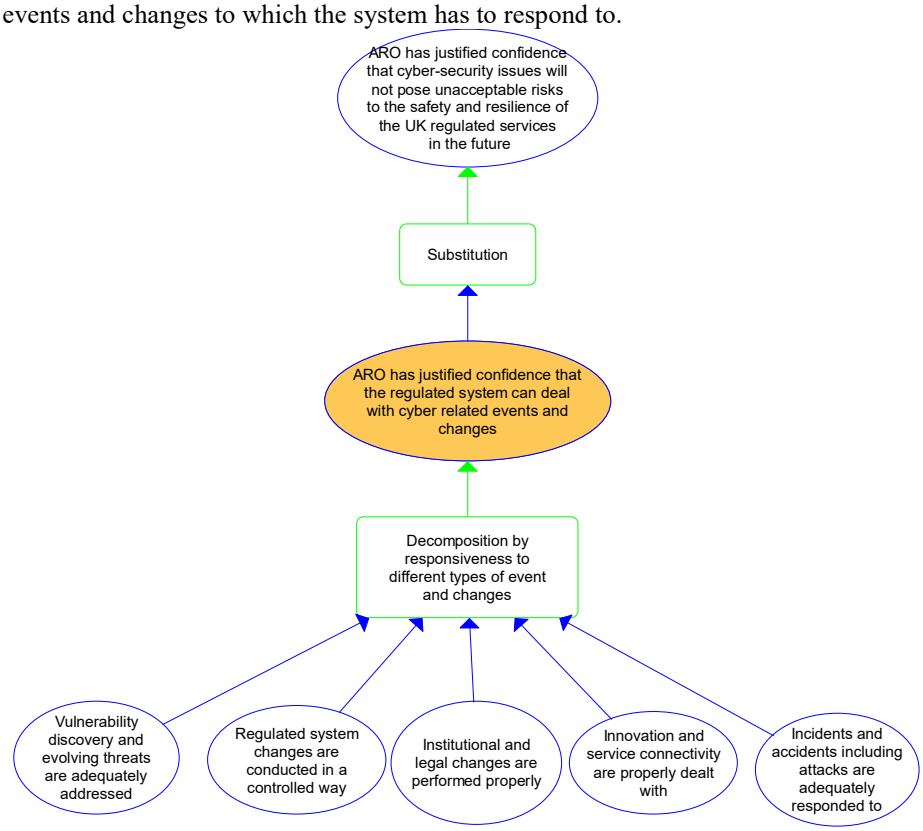

Fig. 6. Ability to deal with future cyber-related events

Some of these, such as vulnerability discovery and new threats, can be considered as changes to the environment, while others are changes to the regulated systems themselves and other innovations and changes to connectivity that redefine what "the system" actually is. There can also be institutional and legal changes that introduce different stakeholders or change the roles, and lastly there will be attacks, incidents and accidents that may have a cyber component.

Incident reporting and subsequent learning from experience is an important part of achieving safety. The tempo and changing nature of the cyber threat makes this particularly critical, and the recognition that failures may occur means that resilience and recovery in particular need to be addressed. An important component of a Cyber Strategy is therefore incident reporting and response: it is an important part of the UK Cyber Strategy and the development of the UK National Cyber Centre.

Supporting other stakeholders. We now return to the second part of **Fig. 2** which considers confidence that other stakeholders have in the regulated system and services. We propose that ARO have responsibilities and objectives here as well as being an authoritative source of confidence for some stakeholders, e.g. the public. We propose a programme objective that

7. ARO provides other stakeholders with confidence in the regulated systems' security and resilience

We propose that the objective be achieved by communicating the ARO's confidence in the system and actively managing sources of actual and perceived risks. This is summarised in **Fig. 7**.

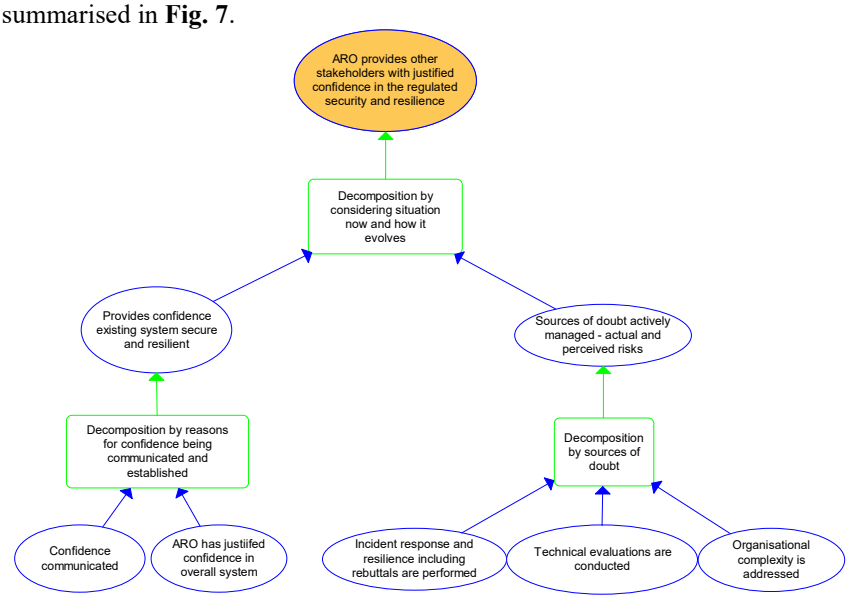

Fig. 7. Supporting other stakeholder confidence

Maintaining confidence in the ARO and for the ARO to discharge its role in supporting the confidence in the sector will need communication as an explicit part of the strategy. This communication should explain the effectiveness and the reasons why there should be confidence in the regulated systems. It should address internal communication within the industry to provide a cyber aware and knowledgeable culture and importantly it should provide expertise, either directly or in support of other spokespeople, to allow accurate reporting of cyber issues. We have already seen the need for effective communications where claims are made about cyber vulnerabilities.

3 Analysis Results and Follow-up

The CAE-based analysis led to a structured set of objectives for the Cyber Strategy that are summarised in **Table 1** below.

Table 1. Proposed objectives of ARO cyber programme

Programme Objectives
1. ARO has processes and procedures to deliver assessments of cyber-security-informed safety and resilience
2. ARO has capability to undertake cyber roles
3. ARO has defined technical approaches for addressing cyber-security-informed safety and resilience
4. ARO has confidence in the overall regulatory institutions and standards
5. ARO confident that the composition of all the activities address security and resilience of the regulated system as a whole and are proportionate
6. ARO has justified confidence that the regulated system can deal with cyber-related events and changes
7. ARO provides other stakeholders with confidence in the regulated systems' security and resilience

To support the ARO we provided an analysis of some of the challenges that this programme needs to address:

- cyber-informed safety assurance
- resilience
- vulnerabilities
- systemic risks and interdependencies
- awareness, training and education
- incident response and organisational learning

From this we developed a set of issues and recommendations to address these issues, and related them to the programme objectives. We developed a preliminary regulatory maturity model to explain and structure the programme of work and to put into context the challenge: achieving these seven objectives. We combined the programme objectives with levels of our maturity model to define an indicative high-level plan. To do this we expanded on the recommendations from our analyses of the challenges to define the steps needed to go from the current "start-up" or "formative" maturity level of the regulated system with respect to cyber, to an "established" level.

4 Discussion and Conclusions

The role of the safety regulator is complex and the work highlighted the complexity and interconnectedness of the organisations involved, captured in an entanglement diagram. The issues that need to be addressed are also many and interlocking and the development and use of CAE as a presentation and reason framework helped tackle this complexity and provided a vehicle for reasoning and communicating with stakeholders (government regulatory policy experts, government security agencies, domain experts, regulators and assessors).

As shown above, we used the CAE Blocks [3] as a structuring mechanism. These were presented informally without side conditions. For decomposition blocks the names of the block is followed by the type of argument e.g. "decomposition by the sources of doubt" to indicate we were decomposing by these sources. The validity of the decomposition was assessed by stakeholder review and workshops. We also provided more succinct descriptions of some nodes to improve legibility and communication aspects: a balance has to be made between preciseness of claim and how this is described on a graphical canvas. The usage of the CAE Blocks is shown in Table 2.

Table 2. Usage of CAE Blocks

Blocks	Usage
Concretion	1 use. Stakeholder preferred "interpretation" to "concretion".
Substitution	1 use. "Not posing unacceptable risks" is substituted by "dealing with cyber events and changes".
Decomposition	A variety of uses: by types of stakeholder, sources of confidence (3), sources of doubt (1), aspects of role, aspects of delivery (2), now and future (2).
Evidence incorporation	In later part of project not reported here.
Calculation	Not used.

In terms of directions and future work, we hope to publish the maturity model that supports the definition of the detailed programme of work and we would like to apply the approach to different regulator in different domains. The usage of CAE Blocks

provides some indications of what might be provided by more domain specific or instantiated blocks for this type of application. From a broader perspective our work can be seen as a part of a wider initiative to see how engineering methods can be used "off label" to support decision making in industry and government.

Acknowledgments. This work has been partially supported by the UK EPSRC project "Communicating and Evaluating Cyber Risk and Dependencies" (CEDRICS, EP/M002802/1), which is part of the UK Research Institute in Trustworthy Industrial Control Systems (RiTICS).

References

1. Adelard Safety Case Development Manual, © Adelard, ISBN 0 9533771 0 5, 1998
2. Bishop, P.G., Bloomfield, R.E.: A Methodology for Safety Case Development. In: Redmill, F., Anderson, T. (eds.) Industrial Perspectives of Safety-critical Systems: Proceedings of the Sixth Safety-Critical Systems Symposium, Birmingham 1998, pp. 194-203. Springer London (1998).
3. Bloomfield, R.E., Netkachova, K.: Building Blocks for Assurance Cases. In: IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW) 2014, pp. 186-191, doi:10.1109/ISSREW.2014.72.
4. Bloomfield R, Bendele M, Bishop P, Stroud R, Tonks S. The risk assessment of ERTMS-based railway systems from a cyber security perspective: Methodology and lessons learned. In International Conference on Reliability, Safety and Security of Railway Systems 2016 Jun 28 (pp. 3-19). Springer International Publishing.
5. Bloomfield, R.E., Netkachova, K. and Stroud, R., Security-Informed Safety: If it's not secure, it's not safe, 5th International Workshop on Software Engineering for Resilient Systems (SERENE 2013) 3-4 October, Kiev, Ukraine.
6. Bloomfield, R. E., Wetherilt, A.: Computer trading and systemic risk: a nuclear perspective. Foresight study, The Future of Computer Trading in Financial Markets, Driver Review DR26. Government Office for Science (2012).
7. The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world. November 2011.
8. Cyber Security Capability Maturity Model (CMM) - Pilot, Global Cyber Security Capacity Centre University of Oxford, 2014 retrieved from http://www.oxfordmartin.ox.ac.uk.
9. US Department of Energy (DOE) Cyber-security Capability Maturity Model (BuildSecurityIn) Department of Homeland Security - https://cwe.mitre.org/top25/ 2016.