JUSTIFYING DIGITAL COTS COMPONENTS WHEN COMPLIANCE CANNOT BE DEMONSTRATED – THE COGS APPROACH

Sofia Guerra, Nick Chozos, Dan Sheridan
Adelard LLP
Exmouth House, 3-11 Pine Street,
London EC1R 0JH. United Kingdom.
aslg@adelard.com; nc@adelard.com; djs@adelard.com

ABSTRACT

The control and protection of nuclear power plants has become increasingly dependent on the use of commercial-off-the-shelf (COTS) products that were not necessarily developed according to nuclear standards. The UK nuclear regulatory regime requires that a safety case be developed to justify and communicate their safety. Typically, the assessment of COTS components has been done with a focus on standards compliance – compliance to accepted practice was deemed to imply adequate safety. However, there may be a number of difficulties with justifying COTS products related to limited knowledge of the internal structure of the components or their development processes, or where the development process evidence does not meet current accepted best practice.

This paper describes a claim-based approach to the justification of COTS components (called *Cogs*) that was developed in a project sponsored by the UK nuclear industry. The Cogs approach is based on a set of top-level claims that remain the same for the different components but which allows for different types of evidence to be used to support specific COTS products. This allows greater flexibility in making a justification while ensuring that all safety relevant attributes of the COTS are justified. The focus of the project has been two types of COTS components: smart devices and PLCs. For smart devices, the approach has been applied to case studies and guidance is being developed so that it can be considered for deployment by the UK nuclear industry. For PLCs, we are developing an approach for PLC-based systems (i.e., the platform together with the application) that focuses on the behavior of the system rather than on the process followed to develop the platform and the application.

Key Words: Safety justification, commercial-off-the-shelf components, smart instruments

1 INTRODUCTION

Commercial-Off-The-Shelf (COTS) components are increasingly used in nuclear Instrumentation and Control (I&C) applications. While there are several commercial benefits in the use of COTS components, there are also several challenges and concerns with regards to their safety demonstration and justification.

Traditionally, COTS components have been justified by attempting to show compliance with relevant development standards. This standards-based approach works well in stable environments where best practice is deemed to imply adequate safety and the components were developed according to the relevant standards. However, they are often criticized for being highly prescriptive and impeding the adoption of new and novel methods and techniques. A clear example of the difficulties with new technologies in the nuclear sector is the use of FPGAs: while FPGA acceptance within the nuclear industry is rapidly increasing, there are still difficulties in understanding what the licensing expectations will be. This is particularly visible when the FPGA-based system is performing a safety-related function

(rather than a safety function), or the FPGA is a small component of a larger product (e.g., in a smart device).

Standards-based approaches to justification are also inadequate where otherwise high-quality systems were developed in accordance with older or different standards, or just meet industrial good practice. This is often the case when industrial components (such as sensors) were not developed specifically to the nuclear industry. This may be a result of the age of the component, since expectations of 'best practice' have changed over the years; even if a component was developed in accordance with best practice ten years ago it may not meet current expectations.

In addition, a purely standards-based approach does not necessarily provide direct evidence that the I&C system and its software achieve the behavior or the properties required to the desired level of reliability.

The safety justification of COTS components is therefore a priority in the UK nuclear industry's research agenda. Research into I&C in the UK is coordinated by the Control and Instrumentation Nuclear Industry Forum (CINIF). The regulator (Office for Nuclear Regulation) and the licensees are all members of the working group. One of the projects funded by CINIF on this topic is entitled "COTS Goal-based Safety assessment" (Cogs), aimed at developing an approach to the safety justification of COTS products. A diverse range of products falls within the scope of Cogs, including:

- Devices dedicated to a single function (e.g., measurement and alarm annunciation instruments).
- User-programmable and control equipment (e.g., PLCs).
- Certain software-only products, such as special-purpose operating systems.

One of Cogs objectives is to overcome the difficulties with the standards-based approach by focusing instead on directly justifying that the desired behavior, property or reliability has been achieved, using product-specific and targeted evidence.

Cogs is a claim-based approach, which uses the Claims-Arguments-Evidence (CAE) framework. The key advantage of a claim-based approach is that there is considerable flexibility in how the claims are demonstrated, since different types of arguments and evidence can be used as appropriate. For example, there may not be much product development evidence available for a device, but there may instead be extensive field experience and records of field-reported faults that demonstrate reliable operation. This might be used as an alternative means of demonstrating adequate product quality and compliance with specified behavior [1].

This paper describes the Cogs approach, and how it can be applied to justify smart devices and PLCs.

2 BACKGROUND: CLAIM-BASED JUSTIFICATION APPROACHES

The Claims-Arguments-Evidence (CAE) approach to structuring safety justifications was developed in the EU-sponsored research project SHIP [2]. The Adelard ASCAD manual [3] describes the idea of separating claims, arguments and evidence, and provides a graphical notation to summarize and communicate the justification. The approach has subsequently been refined by application to systems in the defense, nuclear and medical sectors. It is now accepted by the nuclear industry in a number of countries including the UK. The common position document produced by seven European nuclear regulators on licensing safety critical software [4] also recommends the use of CAE if structured justifications are being undertaken.

There is considerable standardization work on structured cases and CAE and activities internationally in a number of sectors. In particular, ISO/IEC 15026-2 [5] provides a definition of the

CAE concept, drawing on Adelard's work. The standards draw on Adelard's work and this is referenced in the supporting technical guidance that forms Part 1 of the standard.

The key elements of the CAE approach are the following:

- **Claims** are statements of something to be true, with associated conditions and limitations. They are typically statements about a property of the system or some subsystem, or about the development approach used. Claims that are asserted as true without justification become assumptions and claims supporting an argument are called sub-claims.
- **Evidence** is used as the basis of the justification of the claims. Evidence consists of established facts used as the basis of the justification of the claims. Sources of evidence may include the design, the development process, prior field experience, testing or source code analysis.
- **Arguments** link the evidence to the claim, or link claims to other, more specific, claims. They are the "statements indicating the general ways of arguing being applied in a particular case and implicitly relied on and whose trustworthiness is well established" [6], together with the validation for the scientific and engineering laws used.

The idea is that claims can be broken down into smaller, more readily justified, sub-claims. This process is called *decomposition*. There are a number of types of decomposition used in the Cogs approach, such as:

- **Architectural decomposition**, where a claim about the system is decomposed into sub-claims about its components and their interconnections.
- **Functional decomposition**, where a system-level function is partitioned into sub-functions.
- **Enumeration**, where the relevant items are identified and then addressed by supplying evidence.
- **Attribute decomposition**, where a claim about the behavior of the system is decomposed into sub-claims about different aspects of the behavior.

To help visualize the whole claim tree and the interaction between its parts, a graphical notation can be used showing shapes representing claims, arguments and evidence connected with arrows to indicate where evidence is used to support arguments, and where arguments are used to support claims. Claim nodes are shown as ellipses, argument nodes are rounded boxes, and evidence nodes are shown as sharp-cornered boxes (see Figure 1 below).

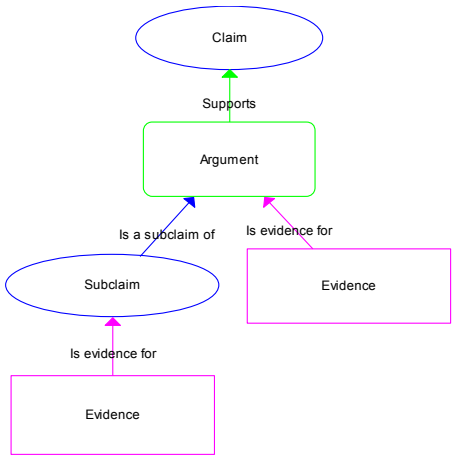

Figure 1: Example of a typical CAE structure in a safety case

3 THE COGS APPROACH

The Cogs approach was developed for the specific context of nuclear applications where, typically, a COTS product is a component within a wider I&C system. The approach was developed with the aim of being generic, i.e., independent of how the product was going to be used, so that it could be reused in a number of applications. Cogs is structured around gathering evidence of the intended behavior of the product and comparing it with available evidence supporting its actual behavior.

Cogs is generally applicable to several types of product. It aims to support the top-level claim that the device behaves as intended on the condition that certain conditions are met (e.g., the ambient temperature and power supply conditions of the component are met). These are assumptions used in the justification of the component. The main aim is to show that

- the described behavior and functionality of the product is sufficiently to understand its intended behavior and required properties
- the product behaves according to this description throughout its intended lifetime

The Cogs approach consists of

- a set of top-level claims to be justified
- guidance on how to expand and justify the top-level claims

The four top-level claims are the following:

- Claim 1: the behavior and functionality of the component are documented adequately
- Claim 2: the component behaves according to its documentation when deployed
- Claim 3: the component will carry on behaving according to its documentation
- Claim 4: sound development process and design principles were followed

Cogs suggests decompositions of each of these claims, as illustrated in Figure 2.

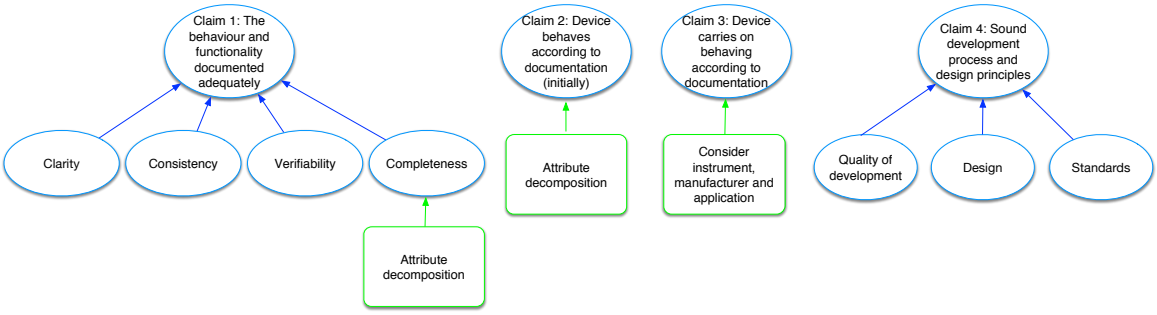

Figure 2: Cogs claims and top-level decomposition

4 USING COGS TO JUSTIFY SMART DEVICES

The nuclear industry is increasingly replacing analogue instruments with their digital "smart" counterparts. Smart instruments can achieve greater accuracy, better noise filtering together with in-built linearization, and provide better on-line calibration and diagnostics features. Given the difficulty in obtaining replacement analogue sensors and the potential benefits of smart instruments, it is important to establish a realistic and flexible approach for justifying their use in safety and safety-related systems.

Although Cogs was developed as an approach to justify COTS components in general, a significant body of work has been developed on using the approach to justify smart devices. By using Cogs, the device is first justified as behaving the way the manufacturer claims, using the available evidence about the device or additional evidence generated to complete the justification. This justification is then used to support a particular application by arguing that all of the conditions necessary for the instrument to behave as claimed are met, and that the device meets the prerequisites of the application. This is discussed in Section 5.

To justify that the device performs as the manufacturer claims, we need to establish the four top-level Cogs claims listed in Section 3. The Cogs guidance includes information on how to justify the four claims and gives argument structures that can be used to justify a smart device. The sections below expand on how to justify each of the top-level claims for smart devices.

4.1 Claim 1: The behavior of the device is described adequately

Clearly, it is not possible to say whether a COTS component is safe or not in isolation – safety depends on the context in which the component operates. So, we cannot claim that a component is "safe" in any direct sense, but we should be able to justify that the component behaves in the way that the manufacturer claims. This is a common concept for hardware based systems which undergo type-approval and once approved are deemed to provide some guaranteed level of service.

The description of the behavior is adequate when it is

- **complete** – does not leave out any aspects of the behavior that might be relevant to an application
- **clear** – easily understood and not ambiguous
- **verifiable** – makes assertions that are possible to test
- **consistent** – not contradictory

Completeness is difficult to characterize, as it is a concept that needs to take into account the application to be usefully defined. In general, to provide sufficient detail to construct the justification, we need descriptions of the following:

- **the full behavior of the device** – including the functions provided, performance attributes (e.g., time response) and dependability attributes (e.g., reliability and failure recovery)
- **the needs of the device when it is deployed** – for example, physical environment constraints, such as temperature, vibration and humidity limits, or interfacing requirements such as connection types and protocols

The first item on behavior can be developed by an attribute decomposition (see Section 2), breaking behavior into a number of relevant behavioral properties. These include sub-claims for

- **functionality** – the functional behavior of the device, including all the functions and operating modes
- **performance** – characteristics defining the ability to achieve the intended functions, such as accuracy, time response and throughput
- **dependability** – including reliability, maintainability, failure integrity, security, etc.

The Claim 1 decomposition is illustrated in Figure 3.

The needs of the device when it is deployed – the conditions under which the described behavior is guaranteed – may include

- **required resources** (e.g., support libraries, processor power, memory space, disk storage space, communications bandwidth)
- **environmental constraints** (e.g., temperature, EMI, humidity)
- **operational and maintenance assumptions** (e.g., periodic calibration, correct probe connection)

The description of the behavior of a smart device can typically be found in the data sheets, user manuals and possibly product proposals, product specifications or requirements specifications. However, these documents do not always provide a sufficiently precise description of the device to satisfy the claims described. For a full understanding of the behavior, it may be necessary to consult development-time documents such as design documents or even the source code.

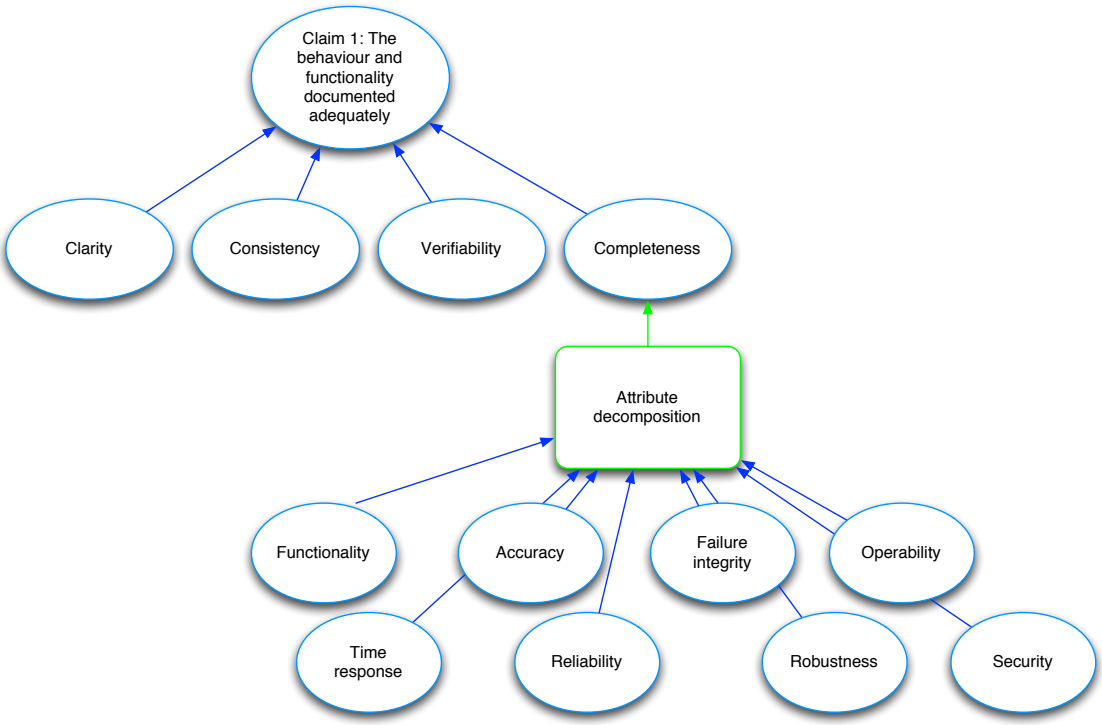

Figure 3: Claim 1 – The description of the behavior is adequate

4.2 Claim 2: Product behaves according to its documentation (initially)

Once an adequate description of the behavior is achieved, the component will be assessed to see whether the behavior actually implements this description. To achieve this claim it is necessary to show that

- the behavior is as described if the needs of the device are satisfied
- the behavior is understood in the presence of postulated internal and external non-nominal conditions

In Claim 1, the claim of description completeness is structured according to the behavioral properties that describe the behavior of the device. Accordingly, an argument for the device behaving in agreement with this description can be decomposed in the same way. For each property, a claim is made that the

behavior achieved by the device is the same as that claimed in the description. Supporting evidence, typically from testing or operational experience together with knowledge of the instrument, is used to justify that each claim holds. The Cogs approach includes guidance on suggested arguments and sources of evidence for supporting claims about each attribute. These suggested arguments are based on the application of techniques that can help produce evidence in support of each of the behavioral attributes.

If there is insufficient evidence available from the manufacturer or other sources to support one of the claims, two possibilities are available:

- **Obtain additional evidence**, by performing additional testing or analysis of the instrument. This could be carried out by the manufacturer, assessor or a third party, and is targeted at directly addressing the gap in the existing evidence.
- **Restrict the ways in which the instrument can be used**, thus avoiding the gap in evidence. For example, security features which are shown to be ineffective can be addressed by requiring the application to provide additional security.

4.3 Claim 3: Product behaves according to its documentation (over the lifetime)

We establish in Claim 2 that the product behaves correctly under ideal conditions at the time of commissioning. However, after installation any product is subject to changes both internally and in its operating context (its environment, the operators and their management, the requirements placed on it, etc.). It is not enough to show that the behavior is as specified; it is also needed to show that the behavior of the component will continue to be as described over its entire lifetime, in spite of the evolving environment, capabilities and any changes, be them deliberate, planned, accidental or out of user's control. This is the subject of Claim 3.

The consistent behavior over the component's lifetime depends on

- the correct environment of the component and the continuing fulfillment of the device needs
- the modifiability of the component and how likely faults are to be introduced when the component is modified, either deliberate changes such as calibration, or unintended changes such as damage or vandalism
- changes due to age being rendered benign by corrective or preventative maintenance

There are several ways to structure this claim. We found it convenient to understand modifications from different points of view, such as

- the device, e.g., considering documentation including maintenance instructions, design features that tolerate aging, ability to test the device, security provisions
- the manufacturer, e.g., considering provision of support, documentation and spare parts
- the application, e.g., considering maintenance procedures, availability of skilled staff, provision of physical security

4.4 Claim 4: the development process meets key principles

Whereas the previous claims focus on the device and its behavior, Claim 4 considers other principles that are not directly related to the device behavior but nevertheless have an important role to play in the safety justification. The principles considered in this claim are related to

- the development process and supporting processes, such as quality assurance processes and configuration management
- design principles

- compliance with identified relevant standards

This claim provides important support for the justification of the device behavior presented in the previous claims, as processes such as configuration management and quality assurance are crucial in the production of traceable and consistent evidence. Evidence that a sound development process was followed and that appropriate quality assurance principles were used increases the confidence in all the evidence generated, the relevance of the evidence in supporting the justification and, consequently, in the overall justification.

A high-integrity development process makes use of design principles, developed through experience and the accumulation of good practice. In general, these are expected to contribute to the reliability of the resulting device, as well as to the success of the overall development process.

Consideration of standards recognizes the experience of others. In some areas the authority and validity of standards is well established; in others, such as software, they can provide a useful framework but may be considered secondary to the need to justify behavior. Nevertheless, it is important to understand whether compliance is claimed and consider it as part of the overall case.

4.5 UK approach and scenarios of use

There are a number of ways in which Cogs can be used. Typically, assessment and justification of smart devices is based on checking compliance with relevant standards. For example, in the UK, the preferred approach to justify smart devices is to assess the development process against IEC 61508 using the *Emphasis* approach [7]. Emphasis consists of approximately 300 questions that need to be adequately answered by the manufacturer, together with a web-based tool for managing answers and storing evidence documents. The assessor reviews the answers and supporting evidence to determine whether compliance with each question has been achieved, or whether additional "compensatory" activities will need to be performed to achieve adequately compliance.

There are a number of challenges in using such an approach. These are typical of compliance approaches to justifying COTS components, where a single set of clauses is aimed at covering a variety of different products with varied implementation and behavior characteristics. Some of these challenges are listed below.

- What are the criteria for the assessor to determine whether the evidence provided by the manufacturer is sufficient to support a certain clause? For example, if no criteria are given how does the assessor determine if the testing evidence provided is enough?
- If there is a clear gap in the assessment, such as the manufacturer not being able to provide evidence that a certain clause has been met, how is the assessor to determine the best way of compensating for such a gap? For example, if deficiencies in the design documentation have been identified, should this gap be compensated using a strict compliance approach? Would the manufacturer, or someone else on their behalf, need to develop the design documentation that was identified as being missing, or could a more indirect approach be taken, for instance, using arguments based on source code analysis and operating time?
- If deficiencies in the documentation of the development process have been identified, but there is direct evidence of the product behavior, how can the non-compliances be compensated for and what nature and amount of evidence relating to this product behavior is enough to complete the compensation program? How can we establish what is the minimum process evidence necessary to complete a product based justification?

The examples above also highlight the potential for inconsistent approaches taken by different assessors while performing the assessments. Significant differences in the assessment can result from different interpretations of each of the points mentioned above.

We have been working on integrating the two contrasting approaches in Cogs and Emphasis so that a claim and behavior based approach could be used to complement Emphasis. This was done by developing sub-claims and arguments that link the Cogs top-level claims to the Emphasis questions, as illustrated in Figure 4. In this way, Emphasis can be used for evidence gathering, while Cogs provides the justification context to assess the answers given. The advantages of using both approaches are the following:

- Cogs offers additional technical assessment criteria and guidance for the answers and in particular the supporting evidence, focusing on the behavior of the device.
- The Cogs structure can help to understand the impact of gaps in the Emphasis assessment.
- As a result of the above, it is possible to have a more integrated/principled compensation strategy.
- Cogs also offers options for alternative arguments rather than just a checklist-based assessment, which can be especially useful for justifying "good" devices developed not according to current best practice.
- Finally, it is expected that by using a claim-based approach with these additional technical criteria, there can be more consistency across assessments.

There are several ways in which Cogs could be used. For example, Cogs can be used as a reference to provide additional guidance during an Emphasis assessment; a complete Cogs-Emphasis case can be developed; or Cogs can be used on its own.

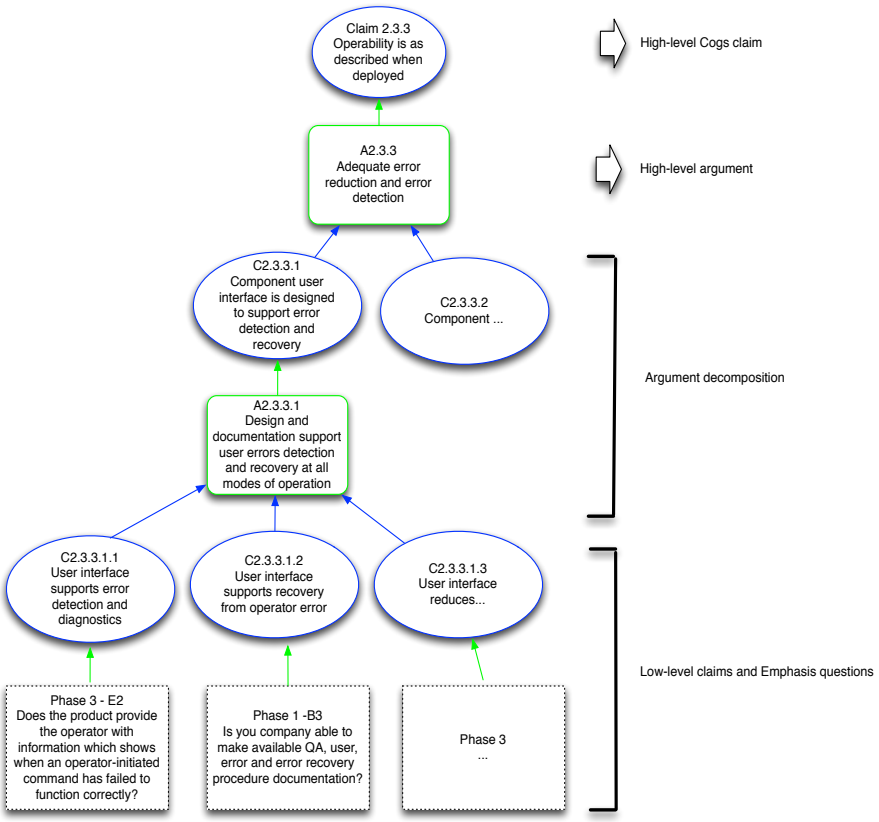

Figure 4: Relationship of system and component claims

4.6 Level of maturity

The Cogs approach and the Cogs-Emphasis integrated approach have been applied to case studies, which demonstrated their applicability and benefits. We have also applied the Cogs principles to design a justification for a smart device for which a compliance case would have not been possible. There is interest from licensees in deploying it, so we expect that other Cogs-based justification will be performed in the near future.

5 INTEGRATING A COGS CASE WITHIN AN APPLICATION

Until a COTS component is used in an application, it is not possible to say whether it is "safe" – safety depends on the context in which it operates. This means that an application-independent Cogs justification must be adapted for each application it will be used in. For a particular system using a COTS component, the justification is in two parts:

- the COTS component behaves according to its description/documentation
- the COTS component is suitable for the application context

This is illustrated in Figure 5 below.

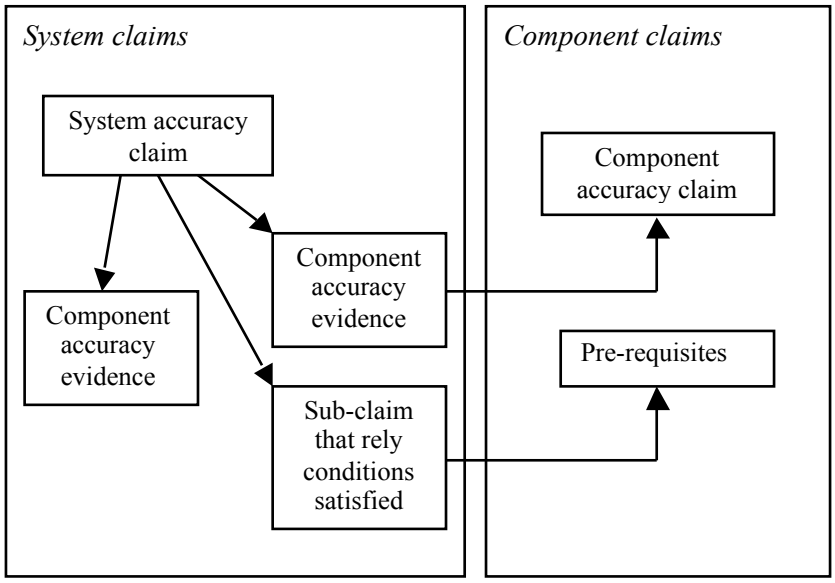

Figure 5: Relationship of system and component claims

Note that the specified behavior of the COTS component is conditional – the behavior of the component is only guaranteed if a specified set of conditions is met. For example, a smart sensor would have rely on the satisfaction of pre-requisites such as ambient temperature range, power supply, EMI levels, periodic recalibration and a working probe before it can guarantee that it will output a measurement of a specified accuracy.

To demonstrate the component is suitable for the application, the safety justification for the specific application has to show the following properties:

- **The component's behavior is adequate.** In the figure above, we show that the accuracy of the component (and others) is sufficient to achieve the overall accuracy needed for the application.

- **Additional functionality will not affect the behavior of the overall system.** For example, if the device can be configured for different types of measurement probe, the unused options must not have an adverse impact on the system.
- **The required conditions of the component are met** (e.g., the ambient temperature and power supply conditions of the component are met). These are assumptions used in the justification of the COTS component.

6 USING COGS TO JUSTIFY A PLC-BASED SYSTEM

In addition to the work on justifying smart devices, we have also been working on using Cogs to justify PLCs. Although it is clear that the approach is also applicable to PLCs, there are a number of decisions on how to apply it, e.g., whether to begin the decomposing of the top-level claims by considering the architectural components of the PLC (*architectural decomposition)* or by considering the different behavioral attributes as for smart devices. We have examined the different ways that Cogs justifications of the different PLC components can be combined, and suggested a strategy for collecting, matching, and fulfilling conditions for the composition of the justification arguments of the different architectural components.

We have also developed a Cogs based approach to justify an operating system of a PLC. We suggested a revised set of behavioral attributes that cover the important claims that need to be justified about an operating system such as determinism and non-interference.

More recently, we have been working on developing an approach to justify a PLC-based system, i.e., a system based on a PLC platform with a specific application loaded. This is in contrast to attempting a generic justification of a PLC platform. The approach is based on high-level view of the PLC's components and the behavioral attributes are defined on the PLC as a whole (i.e., the PLC with the running application). As for the smart device approach, the focus is on behavior rather than development process.

The strategy is to review the behavioral attributes relevant to the application and define which can be shown at application logic level on its own (assuming generic behavior of the platform), which need to be shown by considering the only the platform, and which are applicable to both application and platform. Application logic behavior can be demonstrated by a combination of techniques such as testing, simulation, modeling or analysis. The platform must be shown to satisfy its requirements. For modest reliability requirements, this could potentially be done by a review of the platform documentation. An argument must be made for the correct execution of the application by the platform, and that this is achieved with appropriate reliability.

For any complex system, the role of the tools must also be taken into account. These include the tools used to build and compile the application.

We are currently developing the details of the approach by applying it to case studies.

7 CONCLUSIONS

This paper describes the Cogs approach to justifying the use of COTS components in nuclear safety applications. Cogs is based on a flexible, claim-based framework and aims to contribute a number of benefits:

- Consistent treatment of diverse products.
- Flexibility when compliance with standards cannot be demonstrated.
- Focus on behavior rather than on process.

- Addresses lifetime issues and integrates well with the overall C&I safety case.
- Effort reduction when the same product is used in several applications.
- Effort reduction when a product undergoes revision and upgrade.

The focus of the project has been two types of COTS components: smart devices and PLCs. For the smart devices, the approach has been applied to case studies and guidance is being developed so that it can be considered for deployment by the UK nuclear industry. For PLCs, we are developing an approach for PLC-based systems (i.e., the platform together with the application) that focuses on the behavior of the system rather than on the process followed to develop the platform and the application. Although the work done so far has been focused on smart devices and PLCs, other COTS components could be justified using a similar approach, e.g., FPGA-based systems, operating systems, other pre-developed software.

We are currently developing guidance so that the approach can be considered for deployment to justify smart devices in the UK. The application of Cogs to PLCs is less mature, and needs to be further developed and trialed before guidance can reasonably be developed.

8 ACKNOWLEDGMENTS

This work was funded by the UK Control and Instrumentation Control and Instrumentation Nuclear Industry Forum (CINIF).

9 REFERENCES

1. S. Guerra, P. Bishop, R. Bloomfield and D. Sheridan, "Assessment and Qualification of Smart Sensors," *Seventh International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT)* (2010).
2. P. G. Bishop and R. E. Bloomfield, "The SHIP Safety Case – A Combination of System and Software Methods", *SRSS95, Proceedings of 14th IFAC Conference on Safety and Reliability of Software-based Systems*, Brugge, Belgium, 12–15 September, (1995).
3. "Adelard Safety Case Development Manual", Adelard, ISBN 0 9533771 0 5 (1998).
4. "Licensing of safety critical software for nuclear reactors – Common position of seven European nuclear regulators and authorised technical support organizations", Bel V, BfS, Consejo de Seguridad Nuclear, ISTec, ONR, SSM & STUK, http://www.onr.org.uk/software.pdf (2013).
5. "ISO/IEC 15026-2:2011, Systems and software engineering – Systems and software assurance, Part 2: Assurance case." (2011).
6. S. E. Toulmin, "The uses of argument", Cambridge University Press (1958).
7. R. Stockham, "Emphasis on safety", E&T Magazine, Issue 02 (2009).