Understanding, assessing and justifying I&C systems using Claims, Arguments and Evidence

GUERRA Sofia[1]

1. Adelard LLP, 3-11 Pine Street, London EC1R 0JH, UK (aslg@adelard.com)

Abstract: I&C systems important to safety need to be demonstrably safe. Usually this is performed by demonstrating compliance with some relevant standards. This paper argues that compliance is not necessarily enough, and suggested using a claim-based approach to understand, assess and justify the safety of I&C systems.

Keyword: safety demonstration; I&C; claim-based approach

1 Introduction

Traditionally, the safety of I&C systems have been demonstrated by attempting to show compliance with relevant development standards. This paper argues that other approaches to safety demonstration are necessary. It suggested using Claims, Arguments and Evidence (CAE) to understand, assess and justify I&C systems, and it describes examples where CAE have been used to complement the traditional standards compliance approach.

2 Background

2.1 Safety principles

The IAEA [1] defines the fundamental safety objective as:

The fundamental safety objective is to protect people and the environment from harmful effects of ionizing radiation.

They then define ten safety principles to be the basis for the development of safety requirements and safety measures that are needed in their entirety to achieve this fundamental safety objective. These include the two below.

Principle 1: Responsibility for safety. The person or the organisation responsible for any facility or activity that gives rise to radiation risks (…) has the prime responsibility for safety.

Principle 2: Safety assessments cover the safety measures necessary to control the hazard, and the design and engineered safety features are assessed to demonstrate that they fulfil the safety functions required of them.

These two principles demonstrate the importance of the organisation responsible for the facilities understanding the hazards and the safety measures necessary to control them. Compliance with standards may not be enough to achieve this – understanding and demonstrating this understanding might not be achievable through pure compliance with standards.

The UK SPAs Fundamental Principle FP.4 is more explicit [2]:

FP.4 The duty holder must demonstrate effective understanding of the hazards and their control (...) through a comprehensive and systematic process of safety assessment.

The key issue here is *understanding* and how to demonstrate such an understanding. Although important, showing compliance with standards does not achieve this.

2.2 Further limitations of compliance approaches

Standards-based approaches to safety demonstration work well in stable environments where best practice is deemed to imply adequate safety and the components were developed according to the relevant standards, as might be the case for conventional or electrical systems. One of the most notable differences between these and software-based systems is related to the discrete nature of software. For example, when a software-based system is tested on a particular input, there is no way to guarantee

Received date: March 11, 2015

what its behaviour will be on other inputs, even if the inputs are "near" to the ones tested.

In addition, given the inherent complexity of software-based systems and the magnitude of its state space, it is difficult to completely understand the behaviour of software-based system. This, together with the fact that no procedures exist for designing completely error-free software, means that software is more prone to design faults.

Standards-based approaches 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 Field Programmable Gate Arrays (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 behaviour or the properties required to the desired level of reliability.

3 Justification approach and CAE

The Claims-Arguments-Evidence (CAE) approach to safety justifications was developed in the EU-sponsored research project SHIP [3]. The Adelard ASCAD manual [4] 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 defence, 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 [5] 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 [6] provides a definition of the CAE concept, drawing on Adelard's work. 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" [7], 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, 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 behaviour of the system is decomposed into sub-claims about different aspects of the behaviour.

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 Fig. 1).

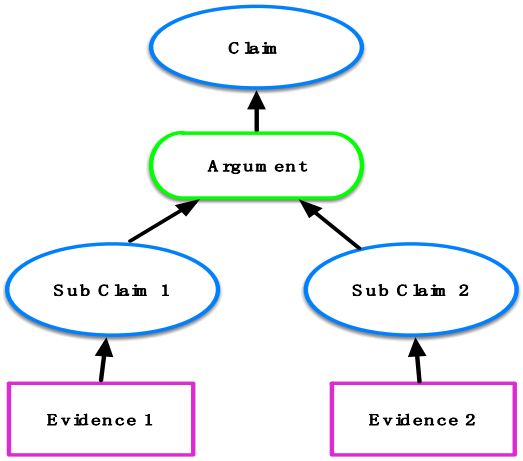

Fig. 1 Example of a typical CAE structure in a safety case.

Several approaches have been developed to increase rigour and confidence in cases. For example, the idea of blocks for CAE-based assurance cases was presented in [8]. Blocks are derived from an empirical analysis of real cases and standardise the presentation of cases by simplifying their architecture. The Blocks increase the precision and efficiency of the claims in arguments because each claim instantiated from a block inherits a formal representation as part of the block. Blocks can be combined into fragments of cases, where it is possible to define typical structures and templates that could be used in a particular class of problems.

The Blocks presented in [8] include:

- Decomposition – the claim is justified by partitioning it over some aspect of the claim.
- Substitution – the claim is transformed into claim about an equivalent object.
- Evidence incorporation – the claim is directly satisfied by its supporting evidence.
- Concretion – some aspect of the claim is given a more precise definition.
- Calculation or proof – some value of the claim can be computed or proved.

4 Strategies for justification

There are two principal ways of constructing a safety justification [9]. A *process-based* approach focuses on the development process and defined standards and practices, and a *product or system-based* approach focuses on the behaviour required of the system.

These two approaches can be described by referring to the *strategy triangle for safety justification* [9] (see Fig. 2). Each of these different aspects of the strategy are discussed in the following sections.

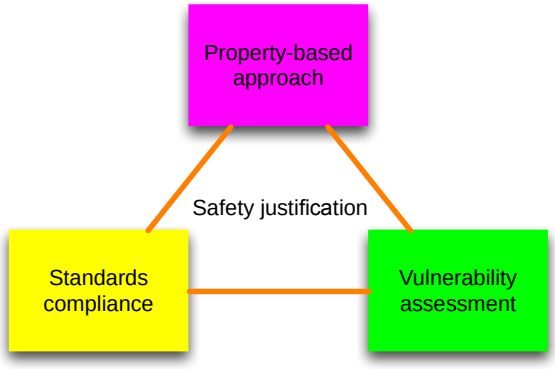

Fig. 2 The strategy triangle of justification.

4.1 Process-based/standards compliance approach

A widely used approach to justifying a I&C system is to provide evidence that they have been designed and verified following a well-structured development process and in accordance with the requirements and recommendations of rigorous standards. For example, when the justification is based on compliance with a standard such as IEC 61508 [11], assessors argue that

the system is acceptably safe by showing that the development process followed is consistent with that described in the standard and by applying a set of techniques and methods that the standards associate with a specific safety integrity level.

There are a number of different standards or regulations that can be used as a basis for the justification of a software-based system. This varies with the type of system, reliability requirement and organization. For example:

- COTS products that have not been developed for the nuclear industry may be assessed against IEC 61508 [10].
- Nuclear specific standards may be used, such as IEC 61513 [12].
- Organisations may have their internal standards, which will typically be based on an international standard adapted to the system and reliability requirements to which they will be used.

4.2 Product or system-based approach

Instead of (exclusively) focusing on compliance with development standards, we can focus on directly justifying the desired behaviour using product or system-specific and targeted evidence. This type of approach can be called the *product or system-based* approach. The focus is directly on the safety requirements for the system, making it applicable even when a compliance with standards cannot be demonstrated. This is often the case for off-the-shelf components (such as smart instruments), where development follows industrial good practice and does not necessarily conform to a recognised safety lifecycle.

Alternative evidence can be presented to demonstrate the safety properties depending on the characteristics of the system under consideration and the process followed to develop it. For example, in applications with limited safety significance, extensive field experience for a component may provide alternative evidence of compliance to the required performance, or alternative arguments can be used to justify expected behaviour when process non-compliances might have been identified. Evidence can also be related to a range of different safety standards by identifying how the requirements in the standards support the various claims. This allows greater flexibility in making a safety demonstration while ensuring that all safety relevant attributes of the system are justified.

This approach is usually linked with specific claims about the product or system being justified, and therefore we described them as *claim-based*. This can follow a structured approach such as *Claims-Arguments-Evidence* (CAE) [3][4].

The system-based approach considers both the properties that the system should exhibit as well as absence of weaknesses. These are described below.

4.2.1 Property-based approach

A property-based approach focuses directly on the behaviour of the system and explores claims about the satisfaction of the requirements and the mitigation of potential hazards. This approach is usually linked with specific claims about properties of the system being justified (*e.g.*, time response, accuracy).

Different properties can be considered for different types of systems or components, and the approach is generally applicable to any I&C system. Table 1 gives an example of behavioural attributes that have been used to justify an FPGA-based system [14].

Table 1 Example of behavioral attributes

Category	Attributes	Discussion
Functionality	Functionality	The function performed by the system
Performance	Timing	Includes time response, permissible clock frequencies, propagation delays, *etc.*
	Accuracy	Affected by analogue/digital conversion, processing functions, IP cores, *etc.*
Availability	Availability	Readiness for correct service, a system-level attribute supported by component attributes such as reliability

Category	Attributes	Discussion
Reliability	Absence of faults	This may be connected with a vulnerability analysis
	Fault detection and tolerance	Internal detection of faults
Robustness	Robustness	Tolerance to out-of-normal inputs and stressful conditions
Failure recovery	Failure recovery	The ability to recover from failures through error detection and reporting, such as sounding an alarm

4.2.2 Vulnerability-aware approach

Vulnerabilities are weaknesses in a system. They could lead to a hazardous situation (*e.g.*, if a divide by zero is not caught by error handling) but are not strictly a hazard. Experience has shown that bad things can occur from them and so should be considered within a vulnerability analysis viewpoint. Therefore, possible vulnerabilities that would affect the ability of the system to exhibit the properties in Section 4.2.1 are considered here.

There are several methods and techniques that can be employed to perform a vulnerability analysis for a component and its system. Lessons learned from internal and external sources should be incorporated into the vulnerability assessment. At component level, these approaches will aim to identify both generic failure modes and their causes, or to provide evidence of their absence, as well those specific to the system being analysed. Table 2 gives an example of behavioural attributes that have been used to justify an FPGA-based system [14].

Table 2 FPGA-based system example vulnerabilities

Class	Name	Description
Timing errors	Routing-related errors	Timing hazards due to a gate combining signals which take different routes on the chip. Exacerbated by logic synthesis replicating parts of the design to increase fan-out.
	Asynchronous designs	Timing hazards due to a gate combining signals which take different routes on the chip. Also applies to designs such as pulse generators which take advantage of this effect in conventional logic but are unreliable in FPGAs.
	Processed clocks	Clocks generated using asynchronous logic such as ripple counters, gated clocks, or multiplexed clocks leading to timing hazards on clock lines.
	Clock skew	Clock signals take time to traverse the chip, so different parts of the design are clocked at different times leading to timing hazards.
	Meta stability	If an external signal changes during the hold time of the flip-flop it feeds, the flip-flop may be left in an intermediate state for a short period of time.
Tool-chain errors	Logic synthesis errors	Errors introduced by bugs in the logic synthesis tools.
	Place and route errors	Errors introduced by bugs in the place-and-route tools.
	Logic embedding errors	Errors in transmitting the design to the FPGA.
IP cores issues	Vendor-specific explicit inclusion	Use of IP cores limits the portability of the design between platforms, limiting design reuse.
	Implicit inclusion	Automatic inclusion of IP cores in the design as part of logic synthesis, to improve efficiency or size. These IP cores may have subtly different functionality or limitations that the original circuit did not.

5 Understanding, reasoning and communicating

The use of CAE is the basis for demonstrating and communicating our understanding and facilitates evaluations and challenge of the justification being developed. CAE can be used as:

- A tool for brainstorming and developing the overall structure, the architecture, of a case.
- A means for analysing and evaluating a justification in a more rigorous and in a more standardised manner.

- A way of summarising a justification and communicating it to other stakeholders.

6 Using CAE to combine process and system approaches

There are a number of benefits in combining process and system approaches. In [13] we described a number of advantages in using both a process and product-based assessment approach in conjunction for systems with a modest integrity requirement, as they provide flexibility, understanding and documentation of the system behaviour that is commensurate with the reliability requirement.

The following subsections describe examples where the traditional standards/process-based approach was not sufficient that illustrate the benefits of considering product/system based approaches. The two approaches are combined by considering the claims they may support, and developing arguments to build an safety demonstration.

6.1 Like-for like replacement

Control and protection functions are long lived in comparison with the lifetimes of the equipment technologies that implement them. This implies that changes will need to be made to the I&C systems, infrastructure and the associated safety justifications over the lifetime of the plant.

Indeed, there is often no choice but to change; the renovation is unavoidably dictated by a variety of circumstances including declining reliability of old installed equipment, reduced spare part availability, inability to maintain existing equipment, or requirements from the licensing.

Often, the renovation aims at being a "like-for-like replacement", where the aim of the project is to replace old equipment with new technology following equivalent requirements. However, this type of replacement is seldom truly 'like-for-like', as new technologies, and the opportunity for operational improvements, are sources of new requirements that may interact with the existing plant in unforeseen ways.

In a replacement project, it is often the case that the documentation on the surrounding system is limited, and therefore tests or other types of analysis may be required to fully understand the impact that the system under development has on the overall plant. By developing an explicit system approach, it is necessary to establish a complete set of behavioural attributes (as described in Section 0), which will support the understating of the required behaviour of the new system. In addition, following a process-based approach to justification, we are able to make the case for documenting the interfaces between the plant and the system, as well as any additional requirements and design decisions, all of which are crucial for the operation and maintenance of the system. These aspects may otherwise be overlooked, especially given the modest integrity target.

6.2 FPGA based system

Field Programmable Gate Arrays (FPGAs) have been gaining interest in the nuclear industry for a number of years. Their simplicity compared to microprocessor-based platforms is expected to simplify the licensing approach, and therefore reduce licensing project risks compared to software-based solutions. However, few safety-related applications have been licensed in the nuclear industry; those that have are typically safety applications at Category A, and work on standardizing the licensing approach has been focused on this category.

In [14] we presented the justification of an FPGA that performs a Category C function, *i.e.*, a function of the lowest safety category. The FPGA is part of the system monitoring vibration of the gags of the fuel assembly in one of the UK nuclear plants. Part of this work involved developing an approach for the justification that is consistent with the UK nuclear regulatory framework and commensurate with the safety category of the function performed. We draw on a number of standards, including those for software performing a function of similar criticality.

The justification strategy needed to take into a number of different aspects:

- The UK regulatory regime.
- International standards and approaches.

- Reliability requirements on the function being performed.
- Feasibility of obtaining supporting evidence.

In the UK, the justification of software-based systems and what has been called *complex hardware* (which includes FPGAs) is based on two aspects: excellence of production and confidence building. Part of the argument used for the first leg is based on compliance with best practice, which is often considered as the consensus-based decisions recorded in the sector specific sectors.

However, there were no relevant standards for this type of systems performing a function with a relatively low integrity target. IEC has recently published a standard [15] for FPGA-based systems performing Category A functions, but no corresponding standard exists for systems performing Category C functions.

The justification approach we took adapts the requirements of a number of relevant standards by taking into account a more behavioural view of why the requirements are important. Requirements clauses are weighted according to how onerous their implementation is, to similar clauses of software-based systems for systems of similar reliability requirements, but also according to their direct contribution to showing that the behavioural attributes have been met and that specific vulnerabilities have been addressed.

The lack of relevant standards together with the fact that this was the first FPGA-based safety-related system to be deployed in the civil nuclear industry in the UK means that the justification has attracted great interest from the industry. The level of scrutiny is higher than what would be expected for a system performing a function of this category. Therefore, all the decisions taken on the justification approach need to be traceable and justifiable. By combining a pure standards-based with more behavioural/system based approaches, we achieved a justification approach that has a sound technical basis. It focus on the functions and the system that implements them rather than on compliance with checklists.

6.3 Smart instruments

The nuclear industry is increasingly replacing analogue sensors with their digital "smart" counterparts. Smart sensors can achieve greater accuracy, better noise filtering together with in-built linearization, and provide better on-line calibration and diagnostics features.

Smart instrument that have been in the market for many years are often seen as trustworthy items. We have found on a number of occasions that adopting a process standards-compliance based approach to assessing older instruments is prone to difficulties. This can be because the development process, which was considered good practice 20 years ago, is no longer consistent with current standards.

In [16] we described the justification of smart instruments where the standards approach was complemented with claim-based product approaches by considering its intended behaviour (*e.g.*, demonstration of accuracy, reliability, *etc.*) and together with assessments of potential vulnerabilities in the smart device implementation. In some cases, the manufacturer may be able to supply some development process evidence, but not enough to provide sufficient confidence in the product. In these situations, it is possible to complement the development process evidence with claims about meeting specified device behaviour such as functionality, time response or robustness to abnormal inputs. Some of this evidence could be drawn from assessment techniques such as static analysis and black-box testing, while evidence of field experience and field-reported faults could also be analysed to demonstrate reliable operation.

7 Conclusion

This paper highlights the importance of understanding I&C systems, their related hazards and possible mitigations. The safety demonstration of I&C systems needs to demonstrate and communicate this understanding. For this, compliance with standards may not be enough, especially for software-based systems and COTS products, where often compliance is impossible to demonstrate. It suggested using Claims, Arguments and Evidence (CAE) as a way to support

understanding, reasoning and communication between different stakeholders.

Acknowledgement

This paper is based on work performed with several colleagues at Adelard, including Peter Bishop, Robin Bloomfield and Dan Sheridan.

References

[1] IAEA Fundamental Safety Principles, SF-1, IAEA safety standards series, ISSN 1020-525X, 2006.

[2] Office for Nuclear Regulation, Safety Assessment Principles for Nuclear Facilities. 2014 Edition, Revision 0.

[3] BISHOP P. G., and BLOOMFIELD R. E.: The SHIP Safety Case – A Combination of System and Software Methods". In: *SRSS95, Proceedings of 14th IFAC Conference on Safety and Reliability of Software-based Systems*, Brugge, Belgium, 12–15 September, (1995).

[4] Adelard Safety Case Development Manual, Adelard, ISBN 0 9533771 0 5 (1998).

[5] 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).

[6] ISO/IEC 15026-2:2011, Systems and software engineering – Systems and software assurance, Part 2: Assurance case. 2011.

[7] TOULMIN S. E.: The uses of argument, Cambridge University Press, 1958.

[8] BLOOMFIELD R., and NETKACHOVA K.: Building Blocks for Assurance Cases. In: 2nd International Workshop on Assurance Cases for Software-intensive Systems (ASSURE), International Symposium on Software Reliability Engineering, Nov 2014, Naples, Italy.

[9] BISHOP P. G., BLOOMFIELD R. E., and GUERRA S.: The future of goal-based assurance cases. In: Proceedings of Workshop on Assurance Cases. Supplemental Volume of the 2004 International Conference on Dependable Systems and Networks, pp. 390-395, Florence, Italy, June 2004.

[10] STOCKHAM R.: Emphasis on safety, E&T Magazine, Issue 02, 2009.

[11] IEC 61508. Functional safety of electrical/electronic/programmable electronic safety-related systems. 2010.

[12] IEC 61513. Nuclear power plants – Instrumentation and control important to safety – General requirements for systems. 2011.

[13] GUERRA S., and SHERIDAN D.: Compliance with Standards or Claim-based Justification? The Interplay and Complementarity of the Approaches for Nuclear Software-based Systems. In: Proceedings of the Twenty-second Safety-critical Systems Symposium, Brighton, UK, 4-6th February 2014.

[14] GUERRA S., and SHERIDAN D.: Justification of an FPGA-based system performing a Category C function: development of the approach and application to a case study. In: 8th American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies NPIC & HMIT 2012.

[15] IEC 62566. Development of HDL-programmed integrated circuits for systems performing category A functions. 2012.

[16] GUERRA S., BISHOP P. G., BLOOMFIELD R., and SHERIDAN D.: Assessment and qualification of smart sensors. 7th American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies NPIC & HMIT 2010.