JUSTIFICATION OF AN FPGA-BASED SYSTEM PERFORMING A CATEGORY C FUNCTION: DEVELOPMENT OF THE APPROACH AND APPLICATION TO A CASE STUDY

Sofia Guerra and Daniel Sheridan
Adelard LLP
Exmouth House
3-11 Pine Street
London EC1R 0JH
UK
aslg@adelard.com; djs@adelard.com

ABSTRACT

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.

This paper presents work currently being performed on 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 involves developing an approach for the justification which 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.

However, evidence that the design and verification of the system followed a well-structured development process does not provide direct evidence that the system achieves the required behavior. Therefore, the approach also considers behavioral attributes that are important for the system, using a goal-based approach. This is complemented by a risk-informed approach, in which postulated hazards are evaluated to ensure they have been addressed and any remaining vulnerabilities of the system mitigated.

Key Words: FPGA, UK, Category C, goal-based, vulnerabilities

1 INTRODUCTION

Computer or microprocessor-based systems are challenging to license for high-integrity nuclear applications due to the difficulty of validating their functional correctness over astronomically large state spaces. Techniques such as formal methods and statistical testing are expensive for systems of significant complexity.

Field programmable gate arrays (FPGAs) are integrated circuits which can be programmed using a hardware description language (HDL) to implement a given logical function. The advantage over ASICs comes from the ability to easily and cheaply reprogram them, making short production runs and highly custom systems viable.

Being purely digital hardware, FPGAs sidestep some of the difficulties of verifying and licensing microprocessor-based systems, and as such are receiving attention from the nuclear industry. A number of systems implementing Category A functions (the highest safety category) have been licensed for nuclear applications, and there are standards emerging which are focused on this application area (such as IEC 62566 [9]).

This paper presents work currently being performed on the justification of an FPGA that performs a Category C function – 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 involves developing an approach for the justification which 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.

In Sections 2 and 3 we present the background to this work: an overview of the case study that motivates this work, and an overview of the UK nuclear regulatory regime. In Section4, we discuss the development of our justification approach, giving the source standards and discussing their synthesis into a suitable justification approach. Section 5 presents our conclusions and the next steps to be taken in this work.

2 DESCRIPTION OF THE GAG EVM SYSTEM

The *Gag External Vibration Monitoring* (EVM) System is used for detecting flow induced vibration of the gag unit within a fuel assembly of an Advanced Gas-Cooled Reactor (AGR) power station. Each reactor has 332 fuel channels. A fuel plug unit assembly, located at the top of each fuel channel, contains a gag plug device to throttle the flow of coolant gas through the channel. Each gag is required to be monitored for impacting upon the gag orifice also located within the fuel plug unit. This can happen whilst the gag is regulating channel coolant gas which passes over it. Should impacting occur, it may threaten the structural integrity of the gag. If left alone in this situation then eventual damage from the impacts could result in a distorted gag plug or even a broken gag shaft with consequential loss of coolant flow in that channel. This would constitute a breach of normal operation.

The Gag EVM system monitors all fuel channel plug units on both reactors. It is designed to detect the onset of gag impacting and allow prompt action to be taken to control the situation. The system acquires and analyses data from accelerometers which are mounted on the motor mounting plate of each fuel plug unit. The system runs automatically and logs results, alarms, and faults in data files. In addition, hardwired alarms are raised in the central control room in the event of significant vibration activity and equipment failure.

The existing Gag EVM system is becoming obsolete and needs to be replaced so that the minimum reliability of gag instability detection is maintained. The new system consists of FPGA-based detection logic units that acquire and analyze the data from the accelerometers. The FPGAs interface with a PC that logs results, alarms, faults and sound files. A simplified version of the high-level architecture of the system can be seen in Figure 1.

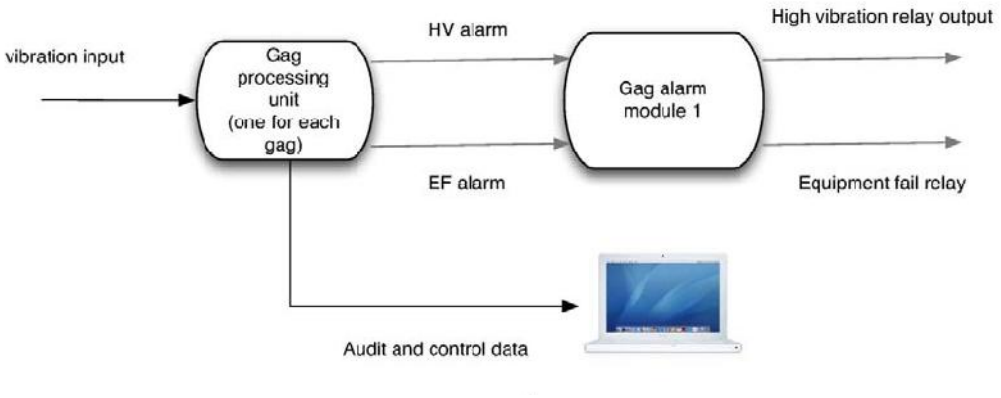

Figure 1. Gag EVM simplified architecture.

The functions performed by the FPGA include:

- Signal level and integrity monitoring
- Amplification, analog-to-digital conversion, and kurtosis calculations on received signals
- Set-point monitoring and alarm decision outputting via relays
- Audio conversion of suspect signals
- Communications with separate computers to supply statistics

3 UK NUCLEAR REGULATORY REGIME

The UK has a specific approach to how it assesses and licenses command, control and protection systems. Despite the internationalization of the supply chain and effective collaboration with international agencies (IAEA, OECD), standards committees (IEC), working groups (NRWG) and projects to encourage harmonisation (such as Cemsis [1] and Harmonics [2]) there are still significant differences between the UK and other countries.

The UK Office for Nuclear Regulation (ONR) Safety Assessment Principles (SAPs) [3] are the primary principles that define the overall approach to be followed for nuclear installations in the UK. The SAPs have been revised in the past few years and have been brought into line with IAEA guidance.

The SAPs have the following clauses on computer-based safety systems.

> Where the system reliability is significantly dependent upon the performance of computer software, the establishment of and compliance with appropriate standards and practices throughout the software development life-cycle should be made, commensurate with the level of reliability required, by a demonstration of 'production excellence' and 'confidence-building' measures.
>
> 'Production excellence' requires a demonstration of excellence in all aspects of production, covering initial specification through to the finally commissioned system, comprising the following elements:

a) Thorough application of technical design practice consistent with current accepted standards for the development of software for computer-based safety systems.

b) Implementation of an adequate quality assurance programme and plan in accordance with appropriate quality assurance standards.

c) Application of a comprehensive testing programme formulated to check every system function.

Independent 'confidence-building' should provide an independent and thorough assessment of a safety system's fitness for purpose. This comprises the following elements:

a) Complete and preferably diverse checking of the finally validated production software by a team that is independent of the systems suppliers, including:

• independent product checking providing a searching analysis of the product;

• independent checking of the design and production process, including activities needed to confirm the realisation of the design intention;

b) Independent assessment of the test programme, covering the full scope of test activities.

Should weaknesses be identified in the production process, compensating measures should be applied to address these. The type of compensating measures will depend on, and should be targeted at, the specific weaknesses found.

In the UK, we refer to this approach of *production excellence* and *confidence building* as the *two-legged approach*.

Although an FPGA can result in a final product that is hardware only, with no run-time software, the process used to develop the application is software-intensive, using advanced software tools to design, implement and verify the application. There is a growing international consensus that the regulatory review of FPGA-based systems should treat the application development process in a manner similar to software development, invoking many of the same standards and guidelines that are used for software-based systems, with some adaptation. Therefore, there is the expectation that the justification approach used for FPGA-based systems needs to be consistent with these clauses to be acceptable for safety-related systems in the UK nuclear industry.

For a system performing a Category C function, excellence of production is typically supported by

- Good commercial practice
- Development process evidence
- Compliance with international quality assurance standards

while independent confidence building measures might include

- Commissioning tests to demonstrate that the instrument adequately performs its required functions
- Data on prior use
- Evidence of the manufacturer's pedigree

4 JUSTIFICATION APPROACH

There are several strategies that can be deployed in the safety justification of I&C systems. The three main approaches can be characterized [4] as a triangle of

- the use of accepted standards and guidelines
- justification via a set of claims/goals about the system's safety behavior
- an investigation of known potential vulnerabilities of the system

This is illustrated in Figure 3.

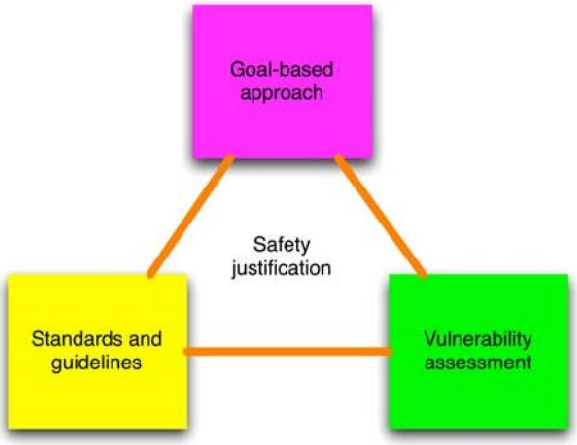

Figure 2. The safety justification triangle.

The first approach (working clockwise from bottom-left) is based on demonstrating *compliance to a known safety standard*. This is a common strategy. For example, a manufacturer of an instrument may claim compliance with IEC 61508 [6].

The second approach is *goal-based* – where specific safety goals for the systems are supported by arguments and evidence at progressively more detailed levels. This typically follows a structured or graphical approach such as *claims-arguments-evidence* (CAE [5]) or *Goal Structuring Notation* (GSN [8]). The CAE approach forms the basis for the Generic Design Assessment currently being performed in the UK for new nuclear build.

The final approach is a *vulnerability-based* argument, where an exploration of potential vulnerabilities is made, based on prior system experience and experience of related systems. It must be demonstrated that potential vulnerabilities within a system do not constitute a problem. This may be considered a 'bottom-up' approach as opposed to the 'top-down' approach of goal-based methods.

These approaches are not mutually exclusive, and a combination can be used to support a safety justification, especially where the system consists of both off-the-shelf components and application-specific elements. We have applied the integration of the three approaches to justifying smart instruments, were the requirement for production excellence in the SAPs was met by demonstrating compliance to an acceptable standard, while the requirement for independent confidence-building measures was addressed

by a combination of goal-based assessments (e.g., demonstration of accuracy, reliability, etc.) combined with assessment of potential vulnerabilities in the smart device implementation.

4.1 Standards Compliance for FPGAs

For conventional systems, the standards compliance argument would involve assessing the development process and design against relevant nuclear standards for a system performing a Category C function. However, the only available international standard which directly addresses FPGAs in nuclear applications is IEC 62566, "Development of HDL-programmed integrated circuits for systems performing category A functions" [9]. This is naturally too stringent to be applied directly to systems performing Category C functions. We therefore considered several sources of information in order to make a disciplined judgment on which aspects to include and which to exclude. Sources of information were:

- International standards concerned with software in nuclear applications at lower criticality levels
- International standards that address electrical and electronic systems in general industrial applications
- Company standards which address software and hardware systems at low criticality levels

These are summarized in Table I.

Table I. Data sources

Name	Criticality covered	Type of system addressed	Type of application	Scope
IEC 62566	Category A	FPGA	Nuclear	International
IEC 61508 part 2 Annex F	All SILs	FPGA	General industrial	International
IEC 60880	Category B and C	Software	Nuclear	International
Research report on FPGAs	All categories	FPGA	Nuclear	International
Company modest integrity guidelines	Category C / Sub-SIL	Software	Nuclear	Company

4.2 Goal-based Assessment of FPGAs

A goal-based assessment [4] is used to argue that specific high-level claims are met by the device. It may be used to focus the review of the verification activities performed by the manufacturer and ensure that all aspects of the behavior have been demonstrated. We have been pioneering an approach to structuring goal-based assessments using *behavioral attributes* which allow us to provide separate arguments focusing on specific aspects of behavior. These are summarized in Table II.

The advantage of a goal-based approach is that there is considerable flexibility in how top-level claims are demonstrated, since different types of arguments and evidence can be used for different systems. For example, the device might not have much product development evidence, and hence an approach based on process may be difficult to justify, but it may have extensive field experience and records of field-reported faults that demonstrate reliable operation. So, this might be used as an alternative means of demonstrating adequate product quality and compliance with specified behavior.

Table II. Example 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 analog/digital conversion, processing functions, IP cores, etc.
Availability	Availability	Readiness for correct service, a system-level attribute supported by component attributes such as reliability.
Reliability	Absence of faults	This may be connected with a vulnerability analysis, as discussed in Section 4.3.
	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.

Alternatively, evidence could be explicitly generated to demonstrate goal-based claims about compliance with specified device behavior such as functionality, time response or robustness to abnormal inputs. This evidence could be generated using a range of assessment techniques including static analysis, black-box testing and field experience.

4.3 Assessment of Potential Vulnerabilities of FPGAs

There are a range of potential vulnerabilities in a FPGA-based system that could affect its behavior. Typical examples might be related to power distribution and management, the potential for differences between simulated and synthesized behavior of the circuit, and the timing and use of delays in the circuit.

Our approach to vulnerabilities has been developed with smart instruments in mind, and much of our work to date has focused on vulnerabilities that arise in embedded systems running software written in C. We have developed techniques such as *integrity static analysis* – where static analysis of the source code of a device is used to eliminate classes of potential fault [10]. We have found that it is necessary to revisit much of this work in order to develop an approach for FPGAs.

Compared to embedded software development, the normal work flow for FPGA development includes a large amount of static analysis. Techniques such as *static timing analysis* (where the delays along paths in the circuit design are compared with timing constraints given by the designer) are widely available and eliminate well-known classes of vulnerabilities. Like software, however, FPGA designs are vulnerable to errors in the tool chain; logic synthesis tools generally have a much smaller user base than C compilers, while also suffering from much greater complexity.

A summary of some of the vulnerabilities we have identified for FPGAs is given in Table III.

Table III. 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.
	Metastability	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.

This type of assessment can increase confidence if no vulnerabilities are found, but it is difficult to argue that all possible types of vulnerability have been considered. In practice, for devices with a low safety integrity target, the software is examined for a specific set of vulnerability types (e.g., where the analysis can be supported by tools). A vulnerability assessment can therefore be viewed as a means of *challenging* a claim that a device is adequately safe – i.e., it can help to refute the validity of a device justification but it cannot be used as the only support for a claim that a system is safe.

5 CONCLUSIONS

The implementation of the FPGA-based Gag EVM system is still under development. The justification strategy needs 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 are no relevant standards for this type of systems performing a function with a relatively low integrity target. IEC has recently published a standard [9] for FPGA-based systems performing Category A functions, but no corresponding standard exists for systems performing Category C functions.

The justification approach we are taking adapts the requirements of a number of relevant standards by taking into account a more behavioral 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 behavioral attributes have been met and that specific vulnerabilities have been addressed.

The lack of relevant standards together with the fact that this is 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 rule-based approach typical of the standard compliance approach with more behavioral based approaches, we achieve a justification approach that has a sound technical basis, and focus on the functions and the system that implements them rather than on compliance with checklists.

The next steps in this justification process will be a review of the process evidence generated by the manufacturer of the Gag EVM system against the combined standards, making use of the goal-based approach to address non-compliances.

6 REFERENCES

1. "CEMSIS – Cost-effective modernisation of systems important to safety." A Nuclear Energy research project under the European Union FP5 program, http://cemsis.org (2004).
2. "Harmonics – Harmonised Assessment of Reliability of Modern Nuclear I&C Software." A Nuclear Energy research project under the European Union FP7 program, http://cordis.europa.eu/projects/rcn/97431_en.html (2011).
3. "Safety Assessment Principles for Nuclear Facilities", Health and Safety Executive, UK, http://www.hse.gov.uk/nuclear/saps/index.htm.
4. P. Bishop, R. Bloomfield and S. Guerra, "The future of goal-based assurance cases," *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.
5. P. Bishop and R.E. Bloomfield, "The SHIP Safety Case – A Combination of System and Software Methods", in *SRSS95, Proc. 14th IFAC Conf. on Safety and Reliability of Software-based Systems*, Bruges, Belgium, 12–15 September 1995.
6. "Functional safety of electrical/electronic/programmable electronic safety-related systems", IEC 61508 parts 1–7, International Electrotechnical Commission, 2010.
7. P. Bishop, R. Bloomfield, S. Guerra and N Thuy, "Safety justification frameworks: integrating rule-based, goal-based and risk informed approaches", in *Proceedings of NPIC 2012,* San Diego, USA, July 2012.

8. T P Kelly, “Arguing Safety – A Systematic Approach to Safety Case Management”. Ph.D. Thesis, Department of Computer Science, University of York, UK. 1999.
9. “Development of HDL-programmed integrated circuits for systems performing category A functions”, IEC 62566, International Electrotechnical Commission, 2012.
10. P.G. Bishop, R.E. Bloomfield, T.P. Clement, A.S.L. Guerra and C.C.M. Jones, “Integrity Static Analysis of COTS/SOUP”, in *Proceedings SAFECOMP 2003*, pp. 63-76, 21-25 Sep, Edinburgh, UK, 2003, (c) Springer Verlag.