SAFETY DEMONSTRATION OF A CLASS 1 SMART DEVICE

Sofia Guerra, Eoin Butler, Sam George
Adelard LLP
24 Waterside, 44-48 Wharf Road,
London N1 7UX, United Kingdom
aslg@adelard.com; eb@adelard.com; srjg@adelard.com

ABSTRACT

Horizon Nuclear Power intends to build Advanced Boiling Water Reactors (ABWR) at Wylfa and Oldbury in the UK, based on the Hitachi design. In accordance with UK policy for new nuclear build, Hitachi, as the reactor designer, is the requesting party to the Generic Design Assessment (GDA) during which the reactor design will be reviewed by the Office for Nuclear Regulation (ONR) and the Environment Agency.

An important step in the GDA process is to demonstrate the viability of the approach developed by Hitachi-GE for the assessment and justification of smart devices. This was done by means of pilot studies of Safety Class (SC) 1 and SC2 devices. This paper will describe the scope, criteria, process and approach for the SC1 pilot study.

Key Words: smart devices, safety demonstration, source code analysis, embedded devices

1 INTRODUCTION

The nuclear industry is increasingly replacing analog 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.

However, the safety demonstration of a smart device is often challenging. Smart devices are a specific form of COTS (commercial off-the-shelf) products, which are normally sold as a "black box" where there is no knowledge of the internal structure or their development process. Nevertheless, their safety demonstration, particularly for the more critical applications, might require knowledge of the internal structure and development process. The justification of sensors is made more difficult because the software constitutes a valuable intellectual investment, and the civil nuclear companies purchase sensors in small quantities. In addition, for safety applications, the safety justification may require (static or formal) analysis of the software, which may be difficult to perform in industry-standard source code.

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 systems. Therefore, the Office for Nuclear Regulation (ONR) has required that reactor designers for new nuclear power plants demonstrate that they have a viable approach to justifying smart devices.

Horizon Nuclear Power intends to build Advanced Boiling Water Reactors (ABWR) at Wylfa and Oldbury in the UK, based on the Hitachi design. In accordance with UK policy for new nuclear build, Hitachi, as the reactor designer, is the requesting party to the Generic Design Assessment (GDA) during which the reactor design will be reviewed by the ONR and the Environment Agency. Hitachi-GE was supported throughout the GDA process by Horizon Nuclear, who are fully owned by Hitachi, and will be the eventual holder of the nuclear site license for the reactors.

As part of the GDA, Hitachi-GE has developed an approach to justifying smart devices and have demonstrated the feasibility of their approach by performing pilot studies at both Safety Class (SC) 1 and

SC 2. This paper describes Hitachi-GE's approach to justifying smart devices and its application to a temperature transmitter as part of the GDA SC1 pilot study.

2 APPROACH

2.1 UK context

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 harmonization (such as Cemsis [1] and Harmonics [2]), there are still significant differences between the UK and other countries.

The 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 mandate two independent "legs" of the justification for systems dependent on the performance of computer software:

- "Production excellence" (PE), a demonstration of excellence in all aspects of production from the initial specification through to the finally commissioned system, including
  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 a modern standards quality management system
  c) application of a comprehensive testing program formulated to check every system function
- "Independent confidence-building measures" (ICBMs), an independent and thorough assessment of a safety system's fitness for purpose. This is formed of
  a) complete and preferably diverse checking of the finally validated production software by a team that is independent of the systems suppliers
  b) independent assessment of the comprehensive testing program covering the full scope of the test activities

If weaknesses are identified in the PE, "compensatory measures" are applied to address them.

The justification approach used for smart instrument needs to be consistent with these clauses to be acceptable for safety-related systems in the UK nuclear industry.

2.1.1 Smart devices

A smart device is a device that contains a microprocessor, and therefore contains both hardware and software. It is distinguished from a computer by the fact that it is programed to perform a specialized activity, such as measuring a physical quantity or controlling another device, and cannot be reprogramed by the end user in a way that changes this functionality. However, the end user may be able to perform some limited configuration of the device, such as defining sensor types, input or output ranges or alarm thresholds. Examples include uninterruptible power supplies, radiation monitors and gas analyzers.

2.1.2 Classes and SILs

Systems are classified according to the category of the functions they perform in accordance with IEC 61226 [4]. The ONR Technical Assessment Guide (TAG) 46 [5] discusses the reliability claim that might be associated with the Safety Integrity Levels (SIL) of IEC 61508 [6]. This is of particular interest here, as compliance with IEC 61508 is the preferred approach for the PE leg.

The correspondence in IEC 61508 between SILs and probability of failure on demand (pfd) (for demand usage) or maximum permissible probability of failure per annum (pfa) (for continuous usage) is presented in Table I. Although there is debate on the reliability claims that can be made for each SIL, the relationship between class of system and SIL is usually accepted as that in Table I.

Table I: Safety integrity levels – reliability claims

IEC 61508 SIL	IEC 61508 probability of failure per demand (pfd) range	Maximum acceptable pfd/pfa	Class of system
1	$\geq 10^{-2}$ to $<10^{-1}$	10^{-1}	Class 3
2	$\geq 10^{-3}$ to $<10^{-2}$	10^{-2}	Class 2
3	$\geq 10^{-4}$ to $<10^{-3}$	10^{-3}	Class 1
4	$\geq 10^{-5}$ to $<10^{-4}$	10^{-4}	Class 1

2.2 Hitachi-GE's approach

2.2.1 Production Excellence

Demonstrating Production Excellence (PE) requires the manufacturer of the smart device to show that all aspects of design, development and production are consistent with best practice and are performed in the context of an adequate quality management system. Additionally, the manufacturer must demonstrate that they have performed a testing program that verifies all functions of the device.

In Hitachi-GE's approach, shown in Figure 1, PE is demonstrated either by means of an Emphasis assessment or using alternative nuclear design standards, which can be applied if the smart device was developed according to such a standard. The Emphasis approach is the preferred approach in the UK, and was developed by a consortium of UK nuclear license holders. It has now been accepted by all UK nuclear licensees and by ONR, and thus is an industry consensus.

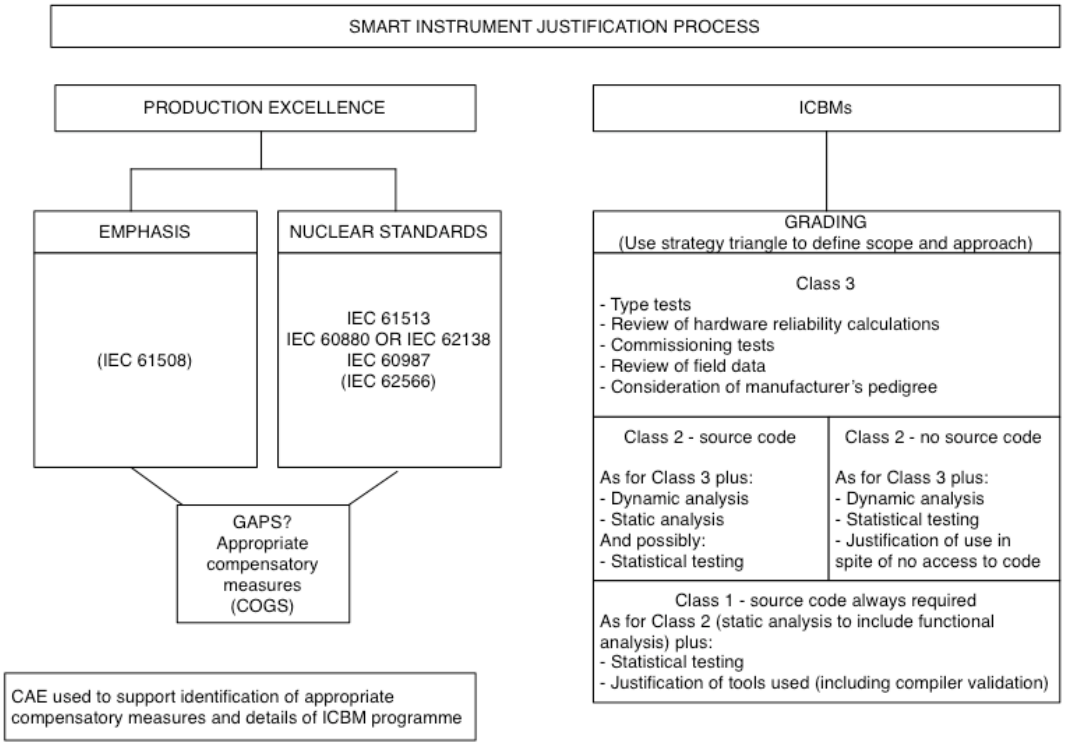

Figure 1: Hitachi-GE approach

Emphasis is composed of a questionnaire containing around 400 questions derived from IEC 61508 [6], which cover the overall approach to quality management and the design and development processes followed for both hardware and software. The Emphasis questionnaire can be configured for different SILs by including more techniques and measures at higher SILs, as defined in IEC 61508. The manufacturer is expected to respond to each question with a brief explanation and to provide evidence to support their answer.

Table II: Example of gaps and compensatory measures

Gap	Compensatory measure
No formal configuration management.	Manufacturer must rectify this.
No justification of test coverage of requirements.	Manufacturer must reconstruct traceability from requirements to tests and justify any requirements not directly tested.
Development documentation (requirements, specification, design) not available.	If source code is obtainable, the licensee performs reverse-engineering (static analysis) to demonstrate that code performs its expected functions.

When weaknesses are identified during the PE assessment, compensatory measures (CMs) are required to address those gaps. The CMs should be specific to the gaps identified. A possible way of defining the CMs is a Claims-Argument-Evidence (CAE) approach that would support analysis of the impact of the gaps in the overall safety justification, such as the Cogs approach described in [7].

2.2.2 Independent confidence building measures

The independent confidence building is an "independent and thorough assessment of a safety system's fitness for purpose" [3]. The measures should be "commensurate with the level of reliability required and preferably diverse" from those techniques used during the lifecycle [4].

The program of measures to be carried out are defined using a Claims-Argument-Evidence approach based on the *strategy triangle for safety justification* (shown in Figure 2) [8]. This strategy is property-based, vulnerability-aware and standards-informed.

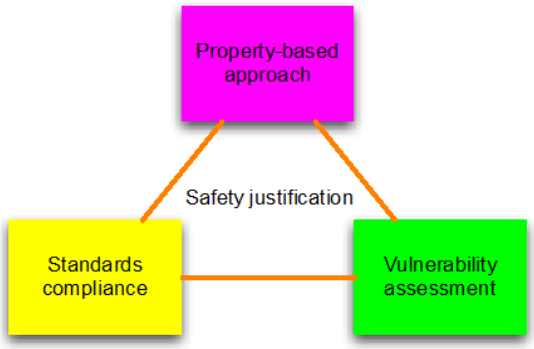

Figure 2: The strategy triangle of justification

- Property-based approach – A property-based approach focuses directly on the behavior of the device and explores claims about the satisfaction of the requirements and the mitigation of potential hazards. A selection of techniques can be made, each of which supports one or more of the properties.
- Vulnerability assessment – 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. Some

techniques, such as static integrity analysis, are particularly suited to identifying vulnerabilities. The techniques used to support the property-based approach and the vulnerability assessment may overlap.
- Standards compliance – This is satisfied by the PE demonstration.

Hitachi-GE's approach includes an indication of the ICBMs that may be appropriate for each class. The grading of the ICBM program is reflected not only in the techniques applied (e.g., whether static analysis is applied), but also in what specific activities are performed (e.g., which static analysis techniques are applied) and how they are applied (e.g., application to the complete code or only the main line code, or the rigor with which they are applied).

3 SCOPE, OBJECTIVES AND CRITERIA

The justification of smart devices will follow a lifecycle, which includes the following steps:

- definition of requirements applicable to the smart device
- demonstration of PE and ICBMs
- additional hardware qualification
- demonstration that the smart device is suitable for the application
- production of justification report

The first step consists of defining the requirements imposed on the smart device by its intended application. This includes behavioral requirements as well as environmental constraints. The objective of the GDA pilot study is to demonstrate to ONR the viability of the PE and ICBM process by applying these methods to an SC1 device. Therefore, the pilot study focused on the second step of the lifecycle listed above, and would be considered successful if the methods were feasible, i.e.:

- suppliers are prepared to support the assessments and provide the necessary information
- the approaches identified can be successfully applied to smart devices

4 CASE STUDY

The device selected for the case study was Moore Industries' (MII) STZ temperature transmitter. The main functionality of the STZ is to measure the temperature indicated by a sensor (e.g., thermocouple or resistance thermometer) and produce a corresponding analog signal. The signal is transmitted via an industry-standard 4-20 mA loop that also powers the instrument. The STZ has several advanced features, such as dual/redundant sensors, sensor diagnostics and HART communication. It can be configured using the HART protocol via the 4–20 mA output or by a PC using a dedicated port as shown in **Figure 3**.

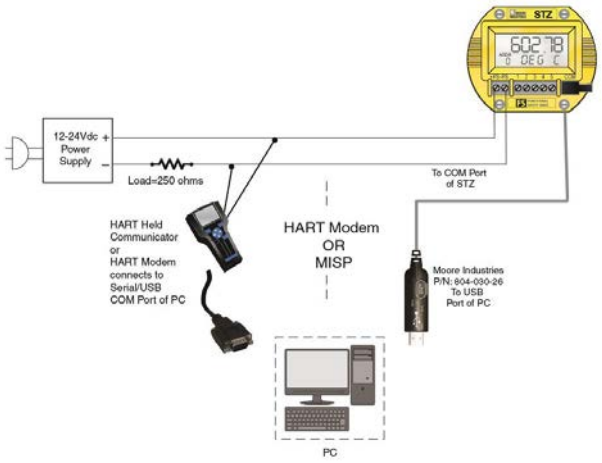

Figure 3: Schematic of the STZ's interfaces

For the purposes of the pilot study, a functional envelope was defined that encompassed the scope of the device's functionality that was to be considered in the assessment. For instance, the functionality envelope excluded consideration of the HART communications function, as the manufacturer does not recommend use of this feature while the device is fulfilling a safety function.

5 PRODUCTION EXCELLENCE

The assessment of PE at Class 1 was performed using Emphasis to SIL 3 (i.e., the tool selected the IEC 61508 techniques and measures Highly Recommended or Mandatory at SIL 3).

The assessment was carried out in stages. After a preliminary stage to agree access to commercially sensitive material, MII worked through the Emphasis questionnaire over a period of a few weeks. We visited the manufacturer's premises for three days to review the answers provided. This is useful as it involves the personnel responsible for the device's development, allowing any misunderstandings to be quickly cleared up and discussions to be held effectively. Following the site visit, we reviewed the answers and evidence, made judgements on the answers to each question, and identified any shortcomings as "gaps".

MII prepared for the site visit meticulously; they had detailed and comprehensive answers to all Emphasis questions and had provided evidence to support the answers given. In addition, we had reviewed all the answers and most of the evidence prior to the site visit. As a result, the assessment and site visit ran effectively (and faster than expected). This reflected the experience of the supplier with the assessment process and the level of preparation prior to the site visit.

A limited number of gaps between the production process and the Emphasis expectations were identified, and are feasible to address. The use of CAE and Cogs provided a strong principled justification for the compensatory measures program.

6 INDEPENDENT CONFIDENCE BUILDING MEASURES

The approach to defining the confidence building program is based on the *strategy triangle for safety justification* (shown in Figure 2). The property-based aspect aims to show that the expected behavior of the smart device is met. This part of the triangle seeks to establish that

- ICBM Claim 1: The STZ performs the full range of behaviors required of it.
- ICBM Claim 2: The STZ is free from unexpected behaviors.

The vulnerability-based assessment addresses vulnerabilities that would affect the ability of the device to exhibit the properties covered in ICBM Claim 1. This part of the triangle seeks to establish that

- ICBM Claim 3: The smart device is free from typical code defects.
- ICBM Claim 4: The device performs appropriately in adverse conditions.

For ICBM Claim 1, the most rigorous analyses (e.g. formal proof and simulation-based testing) were applied to the core run-time functionality. Auxiliary functions (e.g. HART and serial port functions) are not used in normal operation and configuration changes made via these interfaces can be checked prior to deployment. Assurance for auxiliary functions is primarily based on testing. Focusing rigorous techniques on core functionality is only valid if we show that auxiliary functions do not interfere with main line functions in normal operation, so we performed a non-interference analysis to justify the two-part approach.

For ICBM Claims 2, 3 and 4, the selected techniques were applied to the entire code body. This is necessary because software flaws in any part of the code could affect the core run-time functionality. A summary of the techniques performed, their application, tools used and the claims supported can be seen in Table III**: List of claims and supporting analyses**. The tools were selected to be diverse from those used by MII during development.

In addition, we performed a review of the architecture of the device and complexity metrics analysis (which was used to inform code review). As part of the study, we identified other analysis that would be performed to complete the assessment but that were not part of the feasibility activities (e.g., review of the code against the requirements to support Claim 2). For the pilot study, enough of each of the ICBMs were performed to establish their feasibility, but were not carried through to their final conclusion. The following sections summarize the main activities performed as part of the ICBMs.

Table III: List of claims and supporting analyses

Claim supported	Analysis technique	Tools used
Claim 1: The smart device performs the full range of functionality required of it.	Formal code verification	Frama-C
	Non-interference analysis	Frama-C Doxygen
	Verification of linearisation tables	Octave
	Simulations-based testing	LDRA
	Device-based testing	LabVIEW Sensor simulation hardware
Claim 2: The smart device is free from unexpected functionality.	Code review	Doxygen
Claim 3: The smart device is free from typical code defects.	Code review of C code	Doxygen
	Code review of assembly code (concurrency and stack)	Manual review
	Coding standards compliance checking	PolySpace Bug Finder
	Run-time exception analysis	PolySpace Bug Finder
	Concurrency analysis	Frama-C
	Control flow analysis	Frama-C
	Worst case stack analysis	Frama-C
	Review of past compiler bugs	N/A
	Device-based testing	LabVIEW
Claim 4: The device performs adequately in adverse conditions.	Device-based testing	LabVIEW

6.1 Static analysis

We used a range of integrity static analysis techniques to build confidence that certain classes of bugs were absent and to show that auxiliary functions (e.g. configuration) could not interfere with the main-line functionality. We used PolySpace Bug Finder to look for departures from coding standards and places where control flow might encounter undefined semantics (i.e., what are usually called “run-time errors”).

Along with the general bug-finding tool, which covers a broad spectrum of problems and potential deviations from design intent, we also used a number of more specific techniques to address areas where code problems are likely. We performed a concurrency analysis on interrupts in which we used an Adelard Frama-C plug-in [9] to identify shared variables, which we then analyzed manually to check for deadlock and data corruption problems. We also carried out an analysis to establish whether there were any computationally feasible branches of the call graph that would cause a stack overflow.

6.2 Formal proof

The formal code verification focused on functional analysis, involving constructing a mathematical specification for a function, and demonstrating rigorously that the code meets that specification. We used

Frama-C [9], with the WP or Jessie plug-ins, which are based on weakest precondition calculi. We framed predicate claims about functions using Frama-C's ACSL specification language.

In order to demonstrate the feasibility of the technique, we selected a function from the mainline code that was relatively complex. Since the ICBM program includes integrity static analysis, which also addresses safe use of the C language, we focused our attention on proving all the user-specified behaviors. We did not identify any issues with the code requiring sentencing or code modification.

6.3 Simulation-based testing

Simulation-based testing was done using LDRA Testbed [10], a tool that enables simulation-based unit testing, integration testing, code coverage analysis, etc. This testing focused on the accuracy of the scaling and trimming calculations. In each case, we attempted to demonstrate that

- the logic of the code is correct
- there are no calculation errors in the code as tested
- validation and defensive programming have been implemented as needed
- the code satisfies the higher-level system and software requirements

We used both unit testing and integration testing techniques in simulation testing. Unit testing examines individual functions in isolation, while integration testing examines several functions together to show how the code flow from one function to another provides the required higher-level functionality.

The simulation-based testing program performed was only a subset of that which would be required for a full assessment. The application to this pilot study demonstrates the feasibility of extending the scope to a full assessment using the application of similar testing processes.

6.4 Device-based testing

We performed device-based testing using a custom-designed setup based on National Instruments CompactDAQ [11] hardware, and controlled via LabVIEW virtual instruments [10]. Additional hardware, including a HART modem and digitally-controlled relays were also used. For the feasibility study, we restricted the input sensors to three-wire RTDs. A schematic of the apparatus is shown in Figure 4 below.

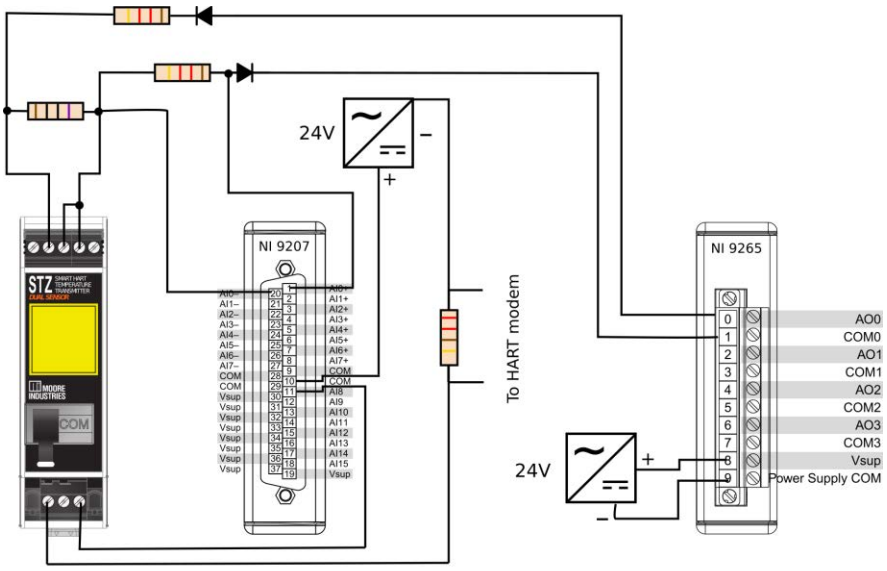

Figure 4: Schematic of the device-based testing apparatus

The device-based testing program was complementary to the tests already performed by MII, e.g., extending the scope of activity exercised in the long-term tests. The areas of focus are shown in Table IV.

Table IV: The device-based testing program

Focus area	Test description
Measurement accuracy	Test that the accuracy for a simulated 3W-RTD is consistent with the device's specification, taking into account the accuracy of the test equipment.
Time response	Test that the time response of the analogue output to a step change is in specification for a simulated 3W-RTD.
Filter/damping	Test that the time response of the analogue output to a step change is in specification for a simulated 3W-RTD when a damping time is set.
Analogue output modes	Check that the configured analogue output mode is set in response to a wire-break failure.
Sensor corrosion detection	Check that a difference in the resistances of two leads attached to the same side of a 3W-RTD triggers a failure response.
HART disable feature	Check that selecting HART "read-only" and "disable" modes function as expected.
Preservation of configuration	Check that a configuration is preserved through a power interruption and that interruption of the configuration process leaves the device in a safe state.
PACTware negative testing	Check that it is not possible to configure inappropriate values through the PACTware interface.
Stress test	Check that the accuracy and time response are in specification when the device is subjected to a high workload.
Tolerance of abnormal inputs	Verify that the device can tolerate and respond correctly to inputs far outside its configured range.

7 CONCLUSIONS

In order to demonstrate feasibility of the Hitachi-GE's approach to the justification of Safety Class 1 smart devices, we performed a pilot study where the approach was partially applied to the MII temperature transmitter STZ. MII provided access to all the required information to be able to perform the assessment and supported any following questions that were necessary to complete the assessment. Without cooperation from the supplier, this assessment would have been impossible.

With regard to the assessment of PE, it is clear that the pilot study benefited from MII's familiarity with the nuclear processes and their rigorous approach developing their products. During the development process MII had taken into account the consideration of compliance with the necessary standards. Therefore, it is likely that with some other suppliers the assessor will encounter more challenges both from a management and from an assessment point of view.

With regard to the ICBMs used to assure the device functionality and absence of vulnerabilities, there were no technical "showstoppers". Our experience with the pilot study suggested that any assessment program should have a preliminary assessment phase that reviews the software design and potential analysis

issues before planning the resources, tools and approaches needed to implement the assessment activities. This would need to consider the tools and techniques used by the manufacturer during development.

The use of CAE to support the assessment of gaps in PE and to design the ICBM program was useful in providing a principled justification of the activities performed. Based on the results obtained, we conclude that the Hitachi-GE approach to the justification of Safety Class 1 smart devices is technically feasible.

8 ACKNOWLEDGMENTS

We thank Horizon, Hitachi-GE and Moore Industries for allowing us to share this study. Several of our colleagues, including Peter Bishop, Catherine Menon and Philippa Ryan, contributed to this work.

9 REFERENCES

1. CEMSIS - Cost-effective modernisation of systems important to safety. http://cemsis.org.
2. Harmonics project. See http://harmonics.vtt.fi.
3. Safety Assessment Principles – 2014 edition (Rev 0, November 2014). http://www.onr.org.uk/saps/.
4. "Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions," IEC 61226 (2010).
5. Office for Nuclear Regulation, *ONR Guide: Computer Based Safety Systems*. Nuclear Safety Technical Assessment Guide NS-TAST-GD-046, Revision 3, April 2013.
6. IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems, 2010.
7. Sofia Guerra, Nick Chozos and Dan Sheridan. Justifying Digital COTS components when compliance cannot be demonstrated – The Cogs approach. In NPIC & HMIT 2015.
8. P Bishop, R Bloomfield and S Guerra. 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, June 2004.
9. Frama-C. http://frama-c.com.
10. LDRA Testbed and Tool Suite, Liverpool Data Research Associations (LDRA), http://www.ldra.com/en/testbed-tbvision, October 2016.
11. National Instruments, CompactDAQ, http://www.ni.com/data-acquisition/compactdaq.
12. National Instruments, LabVIEW, http://www.ni.com/labview/.