EMPHASIS CLASS 1 AND CLASS 2 ASSESSMENT OF ROSEMOUNT PRESSURE AND TEMPERATURE TRANSMITTERS

Emily Saopraseuth, Nicholas Wienhold
Emerson
6200 Innovation Boulevard, Shakopee, MN 55317
{Emily.Saopraseuth, Nicholas.Wienhold}@Emerson.com

Eoin Butler, Sofia Guerra, Heidy Khlaaf
Adelard
24 Waterside, 44-48 Wharf Road, London N1 7UX, UK
{eb,aslg,hak}@adelard.com

ABSTRACT

This paper describes the Class 1 assessment of the Rosemount 3051 Pressure Transmitter and the Class 2 assessment of the Rosemount 644 Temperature Transmitter using Emphasis at SIL 3 and 2 respectively. Emerson has pursued many approvals and certifications on these transmitter platforms. The audit for each of these assessments is unique and probes information at varying levels of detail. As compared to other approvals and certifications audits, the Emphasis assessment is a much more productive and in-depth review of design and project materials. The assessment is focused on reviewing quality procedures, design and project artefacts that prove practical engineering practices, and processes that would lead to good product design.

This paper describes Emerson's approach to the assessment. For this assessment, Emerson answered the over 300 assessment questions and provided over 150 archived documents as evidence for each individual product. Throughout the assessment, Emerson's knowledge of IEC 61508, quality standards, product development processes and software engineering practices showed that, as a smart device manufacturer, Emerson is approaching design processes and procedures with the necessary rigor to produce devices capable of meeting the most stringent requirements.

Key Words: smart devices, safety demonstration, embedded digital devices

1 INTRODUCTION

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 linearisation, and provide better on-line calibration and diagnostics features. Although smart devices are often not developed according to nuclear standards, they still need to be justified to be deployed in nuclear applications. 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. 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 UK nuclear industry has developed an approach to assessing and justifying the development and design approaches of smart devices, which is called Emphasis. This paper describes the Emphasis assessment performed by Adelard of two Rosemount instruments: the 3051 Pressure Transmitter and the 644 Temperature Transmitter. It starts by describing the UK approach to assessing smart devices, followed by a describing of the instruments being assessed. We conclude by discussing the approach and differences between the assessment approach and other certification activities that the instruments had been subject to.

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 pressure and temperature transmitters, 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

2.1.3 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.

The preferred approach in the UK to demonstrate PE is by means of an Emphasis assessment. The Emphasis approach 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.

Emphasis is composed of a questionnaire containing more than 300 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.

Gap	Compensatory measure
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.

3 ROSEMOUNT COMPANY AND PRODUCT OVERVIEW

Emerson's Rosemount business was originally founded as Rosemount Engineering Co. in 1956 by its three founding partners: Frank Werner, Vern Heath and Robert Keppel. The company's first product was the Rosemount Model 101, the world's first temperature sensor that was capable of measuring extremely high temperatures on airplanes moving at mach 2 speeds. In 1961, the first pressure instrument was invented, a pitot-static tube that is installed on virtually every military or commercial jet in the world today. Rosemount instruments were also on every significant American venture into space including: Alan Shepard Jr.'s first American space mission in 1961, John Glenn's first orbit around the earth in 1962, and Niel Armstrong's first steps on the moon in 1969.

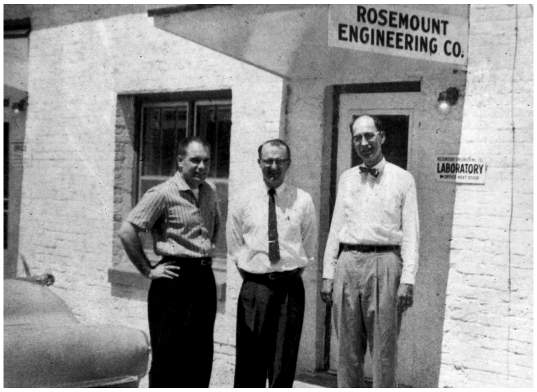


Figure 1: Rosemount Engineering Company founders Frank Werner, Vern Heath and Robert Koppel

By the mid-1960's, Rosemount had solidified its reputation in the aerospace industry. Realizing that this expertise could be valuable in other applications, the company began investing in process control instrumentation. As the industry shift from pneumatic to electronic instrumentation gathered steam, the Rosemount 441 Temperature transmitter was introduced in 1967 and the now iconic Rosemount™ 1151 was introduced in 1969—the analog pressure transmitter that would set the performance standard for decades to come and pave the way for Rosemount Engineering Co. and eventual parent company Emerson to become the leader in the global process automation marketplace.

3.1 Rosemount 3051 Pressure and 644 Temperature Transmitters

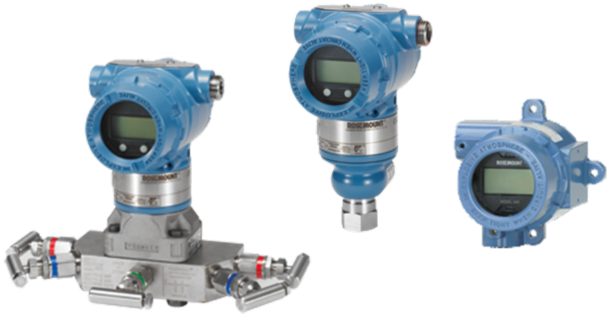


Figure 2: Rosemount 3051C, 3051T, 644 Transmitters (From left to right)

The Rosemont 1151 and 441 have long since been succeeded by their modern descendants, the Rosemount 3051 and 644 transmitters. These transmitter models have an installed base of millions of units. These products have several certifications from over 20 different agencies and self-certifications to standards for hazardous locations, electro-magnetic compatibility, Safety Instrumented Systems, metrology and custody transfer. Countless hours of internal testing have also been completed to ensure the suitable for a variety of applications with 3-sigma conformance to all specification printed in their respective data sheets.

3.1.1 The Rosemount 3051 Pressure Transmitter

The Rosemount 3051 is the second-generation Rosemount pressure transmitter that originally launched in 1988. Over the life of this product, the 3051 has been updated four (4) times with a total of 8 million units installed around the world. Adelard performed the Emphasis assessment for Class 1 and Class 2 (using Emphasis at SIL 3/SIL 2) on the latest revision of the 4-20 mA HART version that was released in 2012. For several years, the 3051 has consisted of two different models, both of which were assessed. The inline variation (3051T) has a single isolating diaphragm making it suitable for measuring gauge and absolute pressure, while the coplanar variation (3051C) has two isolators making it suitable for measuring differential pressure as well as gauge and absolute pressure. The devices otherwise share the same hardware and software designs.

3.1.2 The Rosemount 644 Pressure Transmitters

After a few different generations of temperature transmitters, Rosemount released the 644 in 2003. Over the life of this product, it has been updated once in 2012 and has an installed base of over 1.5 million units. Adelard assessed the latest revision of the 4-20 mA HART 644 head mount transmitter that was released in 2012 for Emphasis Class 2.

4 EMERSON’S NEW PRODUCT DEVELOPMENT PROCESS

The Emerson’s New Product Development (NPD) process utilizes a phase-gate process that integrates proven Emerson practices (user-driven marketing and pricing, global engineering, preferred parts and suppliers) with industry best practices in new product development. Every gate has defined criteria like a checklist along with each phase having defined deliverables for each function to complete. At the end of the phase, a gate review takes place. This is where specific deliverables as well as an overview of the projects adherence to the process are reviewed. There are four NPD decision options including rework and re-review, continue to the next phase, terminate project, or put the project on hold. This higher-level review is an additional check of process and content in addition to the detailed peer review process defined in the lower level product development process.

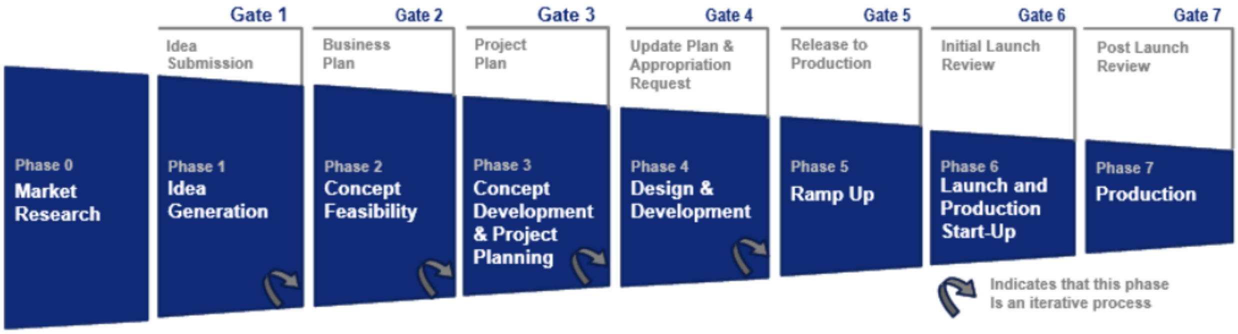


Figure 3: Emerson's new product development stage gate process

4.1 Product design and development process

The product design and development process has been established to ensure that product designs fulfill identified user needs and satisfy all expectations for quality, safety, performance and reliability. It defines the standard approach used by the Engineering & Design functional area for realizing new product designs and major revision to existing designs. The process establishes a framework for iterating from initial design concepts through increasingly lower levels of detail to arrive at a final design solution. The product design is verified and validated throughout the development lifecycle. This process fits within the NPD process and has specific phases identified. Each phase has inputs and outputs that have listed responsibilities and consumers of the artifact.

As stated above, there are inputs and outputs defined for each phase of the product design and development process. These inputs and outputs are defined for each functional area and are explained in detail in the process. These artifacts are created within a specific functional area (or multiple functional areas) and then subjected to the peer review process. The peer review process is a rigorous process that requires subject matter experts as well as a cross functional review panel that includes members not on the development team. Referencing specifically the Rosemount 3051 project there were over 230 peer reviews on the software architecture design phase alone. This is just an example of the amount of reviewing that goes on through the project development process. Products that require compliance to IEC 61508 have additional deliverables and actions become part of the NPD process.

As can be seen from Figure 3, a project starts with market research and idea generation. This is part of both the NPD & product design and development processes. During this time, a customer requirements document (CRD) is drafted. This document undergoes extensive peer review per the process and forms the base/starting point for any project. Starting from the CRD lower level requirements documents start getting formulized. Each document containing lower and lower level of detail. Each document also gets extensively peer reviewed as part of this process. As part of the overall process a configuration management plan (CMP) is also created to control changes to these and other documents. The CMP will define where the document gets stored and the process that is required in order to make updates to it. This plan will define a group of people that are required to approve each change and lists out all of the artifacts that are required to undergo official configuration management.

Through this process each document and design artifact flow from the previous. This allows complete traceability through our requirements down to the detailed design. This traceability is checked for each product/project with special attention given to any safety impact.

As an example of our iterative design process, software engineering processes utilize a scrum-sprint methodology in which feature points are planned and executed in sprints. When those sprints are planned, coded and tested, each step in the process is peer reviewed to ensure completeness and accuracy.

Static analysis tools and independent testing accompany peer reviews to ensure effective software design. Configuration management is also completed as a part of these processes as each issue is brought to a change control team to review. These reviews may change any of the project documents to ensure they are logical and accurate. This software process is design to meet and exceed the requirements of IEC 61508 (e.g., V-model).

It is not enough to just have the defined process, but it needs to be verified that the process is being followed. In addition to the defined gate reviews there are multiple ways that this gets reviewed during the lifecycle of a product/project. One of these is the internal audit process. These internal audits check project documentation to ensure the project is following the defined processes. This could include checking peer reviews, documentation trails, configuration items, etc. to ensure compliance. Another way the process gets checked is through external audits. The process gets externally audited by a certifying agency ever few years. During these audits the entire process from start to finish including any sustaining activities is reviewed and approved.

4.2 Change management

Change management is an integral part of the design and development process as mentioned previously. There is a rigorous process setup during development to ensure items are being revision controlled and changes are being agreed upon and reviewed. A process is in place that defines the engineering change order process including conditions that indicate the need for change, authorization, dissemination, implementation, and archiving. It specifies a format and method for new and existing product documentation. This process is followed throughout the development of a new product as well as throughout a product's entire lifecycle (sustaining efforts).

A part of this process is what we call a Safety Impact Analysis (SIA). This is required for all products regardless of how "simple" the change may be. The analysis will critique the change and record any impacts that it could have to the safety of the device. It includes a description of how the change impacts functionality, safety, user interfaces, etc. and will also evaluate any complier and/or library changes. The analysis will record any re-verification or re-validation activities required. These steps must start with integration and need to be completed and peer reviewed prior to the change taking effect. Any re-verification and re-validation activities will be stored in the Engineering project file. The SIA itself is also stored for traceability and reference.

The change management process is followed throughout the entire lifecycle of the product starting with the initial creation and including the obsolescence. A customer facing portion of that process is the NAMUR NE-53 labelling. Each Rosemount 3051 and 644 are labelled with a HW & SW number corresponding to the version of the device. NAMUR NE-53 has specific requirements on how and when it is required to increment these values in a hierarchy of change (xx.xx.xx format). This along with the HART software revision that can be read from the transmitter is a visual indication to the end user they have the correct version.

During any change process Rosemount keeps the end user in mind. A challenge that is always considered is the legacy install base. A design goal for all projects is backwards compatibility. Our users want to be able to buy the same 3051 and 644 as they did before. For example, the current Rosemount 3051 output electronics can retrofit a Rosemount 3051 sensor dating back almost 20 years. Both the Rosemount 3051 and 644 have HART 5 and 7 selectability to ensure that the products are meeting current standards while also supporting legacy installations. Typically, HART revisions, or drastic hardware enhancements are the only time where there may be a purposeful change in that direction.

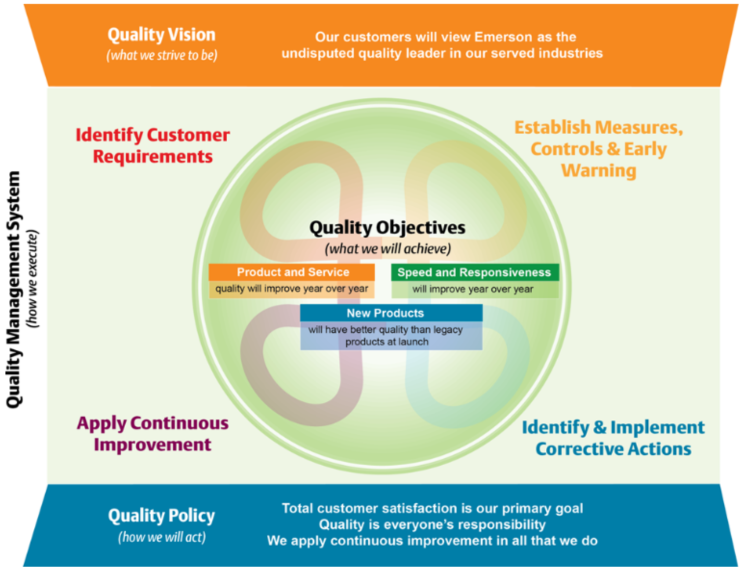
5 ROSEMOUNT QUALITY AND MANUFACTURING PROCESSES

5.1 Quality Policy and Quality Certifications

In accordance with the ISO 9001:2015 quality management standard, Rosemount maintains and executes an extensive quality management system. From the beginning, Rosemount has had a strong culture of quality, starting one of the founders, Frank Werner. Werner held his employees to the same standard he followed: “Do it right, do it better than anyone else, and do it with pride that you are the best, doing something no one else could do as well.” Today, that quality culture lives on through many long-term employees who espouse this culture.

To ensure Rosemount products meet all relevant quality standards, a Global Quality Leadership Team has created quality management system requirements as described in an extensive quality manual. Figure 4 shows Rosemount’s quality management system graphic. It includes the vision, objectives and policy in addition to four key quality behaviors.

1. Identifying Customer Requirements - Understanding the users of our projects and their unique challenges to work towards meeting and exceeding their expectations.
2. Establishing Measures, Controls and Early Warning - Putting systems in place to determine if the parts and processes that go into our products are under control.
3. Identifying and Implementing Corrective Actions - Implementing immediate fixes for easier problems or using root cause analysis, such as the DMAIC process, for systemic problems.
4. Applying Continuous Improvement - Making small product or process changes that over time add up to larger improvements that ensures Rosemount meets and exceeds customer’s needs.



Our customers will view Emerson as the undisputed quality leader in our served industries

Total customer satisfaction is our primary goal
Quality is everyone’s responsibility
We apply continuous improvement in all that we do

Quality Vision
(what we strive to be)
Quality Management System
(how we execute)
Identify Customer Requirements
Establish Measures, Controls & Early Warning
Quality Objectives
(what we will achieve)
Product and Service
quality will improve year over year
Speed and Responsiveness
will improve year over year
New Products
will have better quality than legacy products at launch
Apply Continuous Improvement
Identify & Implement Corrective Actions
Quality Policy
(how we will act)

Figure 4: Emerson's quality management approach

5.2 Manufacturing Processes

While manufacturing processes and procedures are not subjected to Emphasis assessment, they are critical to producing a consistent, quality product. Rosemount has many processes to ensure that transmitters are built properly every time. Through a series of automated processes and extensive procedures, pressure and temperature transmitters are ensured to be built correctly and consistently every time.

Several audit procedures are completed to ensure every transmitter meets its specification. Red light process that will stop the production line if any employee identifies any potential issues. Calibration of every transmitter on the final assembly line. "Out of Box Quality" checks to ensure the transmitter was built with the correct parts and labels. Lastly, Rosemount executes an audit schedule where extensive design verification tests are performed on batches of pressure sensors to ensure the manufacturing procedures and automated processes are in control.

6 ASSESSMENT

The Rosemount 3051 was assessed at SIL 3 (i.e. using the Emphasis tool configured to require the IEC 61508 techniques and measures Highly Recommended or Mandatory at SIL 3) to support use at Class1, while the 644 is currently being assessed at SIL 2 to support use at Class 2. The decision on what level the assessment should be conducted was based on practicalities related with availability of resources to support the assessment rather than on the quality of the devices.

The assessment was carried out in stages. After a preliminary stage to agree access to commercially sensitive material, Rosemount entered answers to the Emphasis questionnaire into an online tool over a period of a few weeks. Adelard visited Rosemount's premises for seven days to discuss and understand the development procedures, the approach to design and verification and to review the answers provided. This is an invaluable part of the assessment as it involves the personnel responsible for the device's development, and allows any potential misunderstandings to be quickly cleared up and discussions to be held effectively. Following the site visit, Adelard reviewed the answers and evidence, and made judgements on the answers to each question.

Rosemount had prepared for the site visit very well; they provided useful answers to all Emphasis questions and had identified and provided evidence to support the answers given. This helped the site visit to run smoothly and ahead of schedule. Where feasible, areas of commonality between the devices were identified so that it was not necessary to review the same material twice, enhancing the efficiency of the assessment.

Following the site visit, Adelard continued assessing the answers and documentation provided to be able to assess whether the development processes and overall design met the Emphasis requirements at the required SILs. This was supported by regular discussions with Rosemount, where further clarifications and documentation was provided to be able to complete the assessments.

7 CONCLUSIONS

From Rosemont's perspective, the process for the Emphasis approval was one of the most rigorous and focused audits of our designs and processes than we have ever experienced. This was not a simple process of checking boxes based on a quality manual or process we have in place on our intranet site. The auditor's requested to see proof that the processes were followed and that they were effective in achieving the goals they were designed to achieve. There was also extensive inquiry into how the device firmware was written, and many aspects of the performance of the firmware to minimize the possibility of bugs in the implementation. A product that endures this level of scrutiny must have not only a good design but have clear proof and accurate documentation that shows that quality and good design principles were designed in from the beginning.

The assessment of the 3051 pressure transmitter has been completed to SIL 3 (or to SIL 2 in a configuration in which the hardware fault tolerance (HFT) is 0). This is the first smart device to have been completely assessed to Emphasis at SIL 3 in the UK. The assessment is currently being technically verified by the UK licensees. At the time of writing, the assessment of the 644 temperature transmitter is still ongoing, approaching completion. The level of engagement and the quality of processes followed made the assessment process progress smoothly and efficiently.

8 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.