TEMPLATES, DATABASES AND OTHER HARMONISED APPROACHES TO THE SAFETY JUSTIFICATION OF EMBEDDED DIGITAL DEVICES

Gareth Fletcher, Sofia Guerra and Nick Chozos
Adelard LLP
24 Waterside, 44-48 Wharf Road, London N1 7UX, UK
{gtf,aslg,nc}@adelard.com

ABSTRACT

This paper describes work funded by Energiforsk to consider the feasibility of using harmonised component level safety demonstration and, in particular, on using aspects of the UK approach to licensing and qualification of smart devices in Finland.

We concluded that the use of harmonised component justification is feasible. In shorter timescales, this seems more likely to succeed if such an approach is developed within Finland. Using the assessments performed in the UK in Finland would have several advantages, but there are a number of technical and commercial issues that would need to be overcome for this to be feasible.

Key Words: Embedded digital devices, commercial-off-the-shelf components, smart devices

1 INTRODUCTION

Embedded digital devices in general, and smart devices in particular, are becoming increasingly common within the nuclear industry. They present several benefits compared to their analogue counterparts, including increased diagnostics and accuracy, while providing cost effective replacements of the analogue components. Given the effort necessary to justify these components and the wide range of applications where a single component can be deployed, there are advantages in using an approach to justification that enables its use in a variety of applications.

Current practice in the Nordic countries requires that a justification is performed for each application where a component is going to be used. However, templates, databases and approaches that are common amongst members of the nuclear industry have the potential to increase the efficiency of safety demonstration and licensing, and to reduce the time and costs for licensees while maintaining a high level of safety. Sharing of information amongst licensees may also allow the community to identify shared challenges and work together to develop approaches to overcome them.

In the UK, there is some degree of harmonisation in the approaches towards component assessment and licensing. Examples of common templates and approaches include the Emphasis questionnaire and process to evaluating production excellence of smart devices, and the so-called two-legged approach to smart device assessment.

This paper explores the feasibility of reusing some of the justification through the use of harmonised templates for the safety justification of smart devices. It explores if aspects of the UK approach to licensing and qualifying smart devices may be applicable in Finland.

We provide a comparison between the two countries' regulations and licensing practices, and summarise our consultations with UK experts. We also discuss the potential benefits of these templates and highlight some issues (e.g., requirements for smart device assessment information sharing between licensees) that need to be taken into account in order to utilise such templates.

2 LICENSING OF I&C COMPONENTS IN THE UK AND FINLAND

This section provides an overview of the regulatory frameworks for the licensing of nuclear installations and operations, focusing on I&C systems and associated justification activities in both countries, and a discussion around their similarities and differences in relation to assessment and qualification of I&C components. This section concludes with a discussion around the main similarities in order to establish how compatible the two approaches are, and to identify any major differences that may need to be addressed so that they do not pose challenges in the adoption of UK practices within the framework used by Finland.

2.1 The UK approach

2.1.1 Safety cases

The Office for Nuclear Regulation (ONR) attaches a number of conditions that it considers necessary or desirable in the interest of safety to each nuclear site licence. The licence conditions require licensees to produce safety cases, which consist of documentation to justify safety during the design, construction, manufacture, commissioning, operation and decommissioning phases. The technical principles that ONR uses to judge a licensee's safety case are described in the Safety Assessment Principles (SAPs) [1].

The safety case is, according to the SAPs [1], "a logical and hierarchical set of documents that describes risk in terms of the hazards presented by the facility, site and the modes of operation, including potential faults and accidents, and those reasonably practicable measures that need to be implemented to prevent or minimise harm."

The plant safety case includes claims for its various systems, including I&C systems that support plant safety functions, such as those that detect dangerous failures or conditions and take preventative action or mitigate the consequences.

Safety claims for I&C systems must be supported in all cases by appropriate safety justifications, for plant enhancements and modification as well as for new plants. According to the SAPs, qualification of equipment should:

- provide a level of confidence commensurate with the safety classification of the structure, system or component
- address all relevant operational, environmental, fault and accident conditions (including severe accidents)
- include a physical demonstration that individual items can perform their safety function(s) under the conditions, and within the time, substantiated in the facility's safety case
- ensure that adequate arrangements exist for the recording and retrieval of lifetime data covering the item's construction, manufacture, testing, inspection and maintenance to demonstrate that any assumptions made in the safety case remain valid throughout the operational life

The qualification of a component may form part of the safety justification of a system (which may be incorporated in the plant safety case). Whereas the qualification process will aim to confirm that the component is fit for purpose, the overall safety justification will seek to demonstrate that the system is acceptably safe.

2.1.2 Function categorisation and system classification

The UK approach is based on IEC 61226 [2], where a certain system Class is assigned to a system or sub-system depending on the Category of the function it implements.

2.1.3 Safety systems containing software

The UK SAPs [1] place particular requirements on the way that software-based safety systems are justified for use in a nuclear installation. A Technical Assessment Guide focusing specifically on software-based systems is also available [3]. The principle ESS.27 on computer-based safety systems introduces the so called “two-legged” approach as a way of “providing proportionate confidence in the final design”:

- demonstration of production excellence (PE)
- independent confidence building measures (ICBMs)

The production excellence leg seeks to justify that the system has been developed following technical design practice and a quality management system consistent with accepted standards, and that a comprehensive testing programme has been implemented.

Independent confidence building measures are performed by an independent agent (i.e., not connected with the system’s supplier) contracted by the licensee. They should provide a thorough and challenging assessment of fitness for purpose, but should be reasonably practicable. This leg consists of

- complete and preferably diverse checking of the software (after validation has been completed) by a team independent of the suppliers
- independent assessment of the full test programme, covering the full scope of the testing activities

The techniques chosen, and the rigour with which they are applied, would depend upon the classification of the system and its integrity target. For systems subject to a more onerous claim, full visibility of source code, circuit details and process information should be provided.

2.2 The Finnish Approach

2.2.1 Safety demonstration

STUK takes the approach shared by international regulators [6],[4]. The aim of safety demonstration is to confirm that the relevant attributes of the system (reliability, availability, performance etc.) meet their specification, and that the specification is acceptable from a safety/security perspective – or that typically, the system meets its safety requirements.

In this process, transparency is called for, and it is also desirable that the licensee’s justification is “logically unarguable, unbiased, comprehensive, transparent and accessible to all relevant parties” [7].

Safety justification is typically provided in the preliminary and final Safety Analysis Reports (SARs). These documents provide a summary of the plant’s most important radiation protection features, explain how requirements for these have been met, and give reference to the wider document set that is produced during design and safety assessment of the system described.

2.2.2 Function categorization and classification

Classification of the nuclear facility’s systems, structures and components is described in YVL B.2. The STUK approach is primarily based on deterministic methods, which may be supplemented, according to YVL B.2 [5], by a Probabilistic Risk Assessment (PRA) and expert judgement.

The nuclear facility’s systems, structures and components are grouped into the Safety Classes 1, 2, and 3, and Class EYT (non-nuclear safety) with Class 1 being the highest. The guide contains descriptions and criteria for assigning classes to systems, based on the significance of the function they perform.

2.2.3 I&C system qualification

In Finland, system qualification aims at determining that the system and its components and cables are suitable for their intended purpose and location of use. The qualification of safety I&C systems and their equipment is based on a preliminary and final “suitability analysis”.

For Classes 2 and 3, it is expected that a qualification plan is produced considering

- applicable standards
- design and manufacturing process tests
- organisations to be used in the qualification analyses
- operating experience feedback

In terms of the software assessment, the qualification plan identifies and discusses all software tools used in development and testing and analysis methods. Section 6 of YVL E.7 discusses software development in more detail. Different requirements apply to different classes of system.

Once factory tests are completed, and before the system is installed in the plant, the licensee must provide evidence that the system meets its requirements.

2.3 Discussion

There are several similarities in the regulatory approaches in the UK and Finland. Clearly, both countries operate on a licensing scheme, where an independent regulator has the role of assessing a proposed implementation. Both regulators (the ONR and STUK) provide detailed technical guidance (SAPs and TAGs in the UK, and the YVL guides and supporting memoranda in Finland) and their assessment is performed against these. The SAPs set high-level principles, while the YVLs are more detailed and prescriptive on what the licensee should do. As expected, both regulators have the authority to influence the design and implementation of the proposed systems, and in the end the regulators will have to provide approval prior to the system’s commissioning.

In the UK, the safety case is the basis for the assessment process. The concept of safety cases is not used in Finland where the documents capturing the safety justification are the Safety Analysis Reports (SARs). Safety cases take a claim-based approach and a hierarchical linkage from claims to the documentation is expected to illustrate the rationale for the approach selected towards reducing risk to an acceptable level. SARs consider the facility’s key design features and explain how these have been met. In both countries, the licensee is given some flexibility in demonstrating that a proposed system is acceptably safe. In both countries, this is done by demonstration of reduction of risk to an acceptable level – in the UK, this is based on the ALARP principle, and in Finland, this is based on the ALARA principle. The term ALARA is used interchangeably with ALARP outside the UK.

The Finnish qualification approach has no concept of an application independent qualification; all qualification assessments must take the requirements of the intended application into account.

The activities involved in the qualification of components are similar in both countries, with an assessment that the device is fit for the intended purpose and that it was manufactured and developed to a high level of quality. Also, both approaches require the detailed assessment of system software (firmware) if the component contains any. For computer-based safety systems, the UK approach is split into the two independent legs (production excellence and independent confidence building measures).

Overall, our conclusion based on the review of the two regulatory approaches is that they are grossly similar, and that the processes for assessment of safety in the two countries are aligned and compatible.

3 UK CONSULTATIONS

The objective of the consultations was to understand the approach to safety demonstration of smart devices in the UK, the use of templates for such demonstrations and the feasibility and practices of sharing the safety demonstrations.

The consultations took place with stakeholders from the UK nuclear industry, which included AWE, EDF Energy, Horizon Nuclear Power, ONR and Sellafield Ltd. In total, we spoke to ten people either face-to-face or over telephone. With the exception of the regulators, our interviewees worked for licensees and are involved with qualifying I&C components in different areas of the nuclear industry.

The questions were structured around four different themes:

- their approach to safety demonstration
- their use of templates, databases and approaches for component licensing
- their experience of sharing information through templates, databases and approaches
- their views on and their perception of the approaches used for safety demonstration of components and their sharing

The diversity of our interviewees allowed us to obtain a wide perspective on these topics over the whole UK nuclear industry.

3.1 Approach to safety demonstration

The Safety Assessment Principles (SAPs) [1] is the key framework used for safety demonstration in the UK. The SAPs, together with the Technical Assessment Guide 46 [3], mandate two independent "legs" (PE and ICBMs) for the justification of systems dependent on the performance of computer software as described in Section 2.1.

The justification approach used for a smart instrument is required to be consistent with this approach to be acceptable for safety-related systems in the UK nuclear industry. The Emphasis approach is the preferred approach to demonstrate PE for smart devices 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.

Emphasis is composed of a questionnaire containing around 400 questions derived from IEC 61508 [8], which cover the overall approach to quality management and the design and development processes followed for both hardware and software. The Emphasis questionnaire is configured for different safety integrity levels (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.

3.2 Templates, databases for component licensing

Templates can be understood as providing different patterns for different aspects of the safety demonstration; and can be distinguished between templates for documenting the process, and templates for the assessment itself:

- templates for documents to record each step of the lifecycle, from specification to design to commissioning
- templates to record the conclusions of the assessment
- templates to review assessments done by different licensees

- templates that describe the assessment approach to be used, such as Emphasis

There was a general agreement that templates that shape the assessment itself need to be used with caution; so that the assessor is not limited by what is in the template and is able to develop an adequate safety demonstration. The industry did not want to use templates like checklists for this reason.

The document templates were typically developed in-house by licensees, while approach templates such as Emphasis were developed by the industry as a whole. However, there is an agreement between some licenses on what the assessment reports should contain; this is to ease sharing of those assessments between each other. The use of templates varied among the licensees. Some licensees used internal company standards and guidance notes; one had an engineering wiki page that contains useful document templates that they have developed in-house. Other licensees only used external templates developed with the industry, such as Emphasis.

There were various different internal databases of components used by licensees:

- device reliability database - containing failure rates based on history of use
- approved list of instruments
- database of instruments that have been through assessment
- Seismic Qualification Utility Group (SQUG) [9] database for seismic testing data
- Proactive Obsolescence Management System (POMS) [10] – a database operated by Rolls-Royce

3.3 Experience of sharing information

The industry is willing and open to sharing information/assessments. Sharing of device qualification assessments between licensees was normally agreed on a quid pro quo basis (one-for-one), where both of the licensees benefit from the exchange. In some cases, licensees sold the assessments to other licensees, if there was not one that could be exchanged. The supplier of the assessed smart device has to be involved when an assessment is sold/shared as non-disclosure agreements (NDAs) need to be arranged.

Databases would need to be shared with care, as there may be devices that are assessed for a specific application, and therefore, any application specific assumptions or limitations would need to be considered, as well as the specific versions of the firmware/software and hardware that have been assessed.

Sharing on an international scale was perceived to be more difficult, as countries have different regulators with different expectations, particularly for software qualification; however, it might still be possible to share some parts of the assessment.

A common theme brought up during the consultations was that there would be more manufacturer buy-in (willing to invest more time and effort), and earlier on in the qualification process, if there was a wider market for the manufacturer to sell to once the assessment had been completed (for example, if the qualification assessment was shared across the UK nuclear industry or internationally).

3.4 Recommendations

Some of the UK licensees would be open to sharing information and assessments with the Nordic countries. Given the different regulatory regimes between Finland and the UK, it might not be feasible to share complete assessments until further harmonisation has been achieved. However, there might be some parts of the assessment that could be usefully shared, for example, some of the Production Excellence information or the Emphasis assessments. Nevertheless, there would be some commercial barriers with sharing this information that would need to be overcome, including agreements on sharing confidential intellectual property from suppliers and reaching mutually beneficial arrangements for sharing.

4 COMPARISON BETWEEN UK AND FINNISH APPROACHES

Table I compares YVL E.7 [11] subsections 5 and 6 to the UK component qualification process. The information on the UK qualification process is based on the ONR SAPs and TAGs, the information given to us during the consultations (see Section 3), and on our own experience with assessing this type of device.

Table I. Comparison of UK and Finnish approaches

	UK	**Finland**
General approach	Pre-assessment concept: assessment done using a common approach (Emphasis), application independent, to enable sharing and reuse.	Assessment done for a specific application.
	Assessment divided in two part: production excellence and ICBMs.	No such distinction.
Hardware qualification		
Qualification plan	Qualification plan typically required by licensees' internal procedures. Scope is similar in both countries.	Qualification plan required to be submitted to STUK.
Testing	Testing required as part of production excellence (Emphasis) and ICBMs. PE testing is performed by designer or manufacturer.	Testing required to be done independently of the design and manufacture of the component.
Assessment of design and manufacturing processes	Similar in both countries.	
Environmental conditions	Environmental testing done during development of device reviewed during Emphasis. When the device is being deployed, the conditions are compared with those of the application and additional testing is performed if required.	Testing done in an environment as similar as possible to the intended application.
EMC	As above.	As above.
Software qualification		
Qualification of software	The qualification of software based on the two-legged approach: Emphasis assessment and ICBMs.	The focus is on good design practices, simplistic design, and verification and validation techniques.
Software design procedures and processes	Similar in both countries. However, the UK approach seems more detailed in this area, as the Emphasis questionnaire contains many in-depth questions relating to the whole software design and development process.	
Software tools	The UK qualification approach encourages manufacturers to use well-known certified software tools or have evidence that the tools do not introduce errors into final product.	The Finnish approach uses prior operating experience feedback of tools used in the design, implementation and testing of software of systems.
Existing software	Both qualification approaches take the same view to existing (legacy) software, which is subject to the same requirements as new software.	

Software testing	Similar in both countries; the approaches have detailed requirements on software testing that align with each other.

The approaches to smart device qualification in Finland and the UK focus on the same areas. The main difference is that the UK tends to separate the qualification in two steps: an application independent assessment of the smart device using a common approach/template using Emphasis, and a step of using this assessment within an application, which would involve suitability analysis and performance of application specific testing and analysis. The Finnish approach takes into account information and requirements of the intended application of the smart device throughout the qualification.

The Emphasis requirements are based on in-depth detailed questions on the development and design processes and is more detailed than the corresponding activities in Finland.

5 CASE STUDY

We performed a theoretical case study of applying the Finnish nuclear regulations laid out in YVL E.7 [11] to an I&C system that would deploy a smart device that had previously been assessed in the UK. We assumed that the smart device had been subjected to an Emphasis assessment for the production excellence and any ICBMs were independent of a specific application. For example, for a Class 2 smart device, there might have been static and dynamic code analysis performed. The assessments performed would be shared with the Finnish licensee responsible for the I&C system.

We compared the information that would be available from the UK pre-assessment against the requirements in YVL E.7. This comparison identified what would be covered by the UK pre-assessment and what additional information and assessments would need to be completed to meet the YVL requirements.

A UK pre-assessment of a smart device would provide useful information for the qualification against STUK nuclear regulations. Since the UK pre-assessment does not cover the specific application requirements, areas of YVL E.7 that specify requirements for the specific application would need to be addressed. Emphasis would mostly provide useful information to support the qualification process, suitability analyses and software qualification laid out in the YVL regulation guides. Any requirements on the licensee would be out of the scope of the shared information. In addition, not all information from the production excellence assessment template (Emphasis) would be useful to Finland, as it includes a greater level of detail specifically designed for the UK qualification process.

The shared UK pre-assessment information would be generic. Therefore, any information or supporting evidence contained within a shared assessment would need to be reviewed against the requirements of the intended application; this is also the case when a pre-assessment is used in the UK.

6 CONCLUSIONS

The objective of this project was to determine if a system using harmonised templates for the component level safety demonstration for I&C and electrical components could be used in the Finnish licensing environment in the nuclear energy sector, and to identify the challenges facing such an implementation. The project focus was on reviewing the UK approach to licensing smart devices and their use of templates to potentially increase the efficiency of safety demonstration and licensing and to reduce the time and costs for licensees while maintaining a high level of safety.

We performed the following activities:

- *Review and comparison of the UK and Finnish regulatory frameworks for I&C systems.* We identified commonalities and differences in the overall approach to assessment, approval and licensing of I&C systems used in the two countries.
- *Consultations with UK experts.* A number of interviews with industry practitioners in the UK were conducted. The objectives of the consultations were to understand the licensing approaches used in the UK, the use of templates for justifying components and the practicality of sharing these templates between difference licensees.
- *Comparison of the processes for smart devices qualification*. Based on the results from the previous two tasks, we reviewed how the two countries assess and license smart devices. The aim of this task was to identify approaches in the UK that may be different to the Finnish approach and whether a similar approach to that used in the UK for component justification could be used in Finland.
- *Smart device qualification case study.* A generic case study was developed considering each step of the qualification process and the associated information that would be used as evidence.

Overall, templates can be understood as providing different patterns for different aspects of the safety demonstration, and can be distinguished between templates for documenting the process, and templates for the assessment itself:

- templates for documents to record each step of the lifecycle, from specification to design to commissioning
- templates to record the conclusions of the assessment
- templates to review assessments done by different licensees
- templates that describe the assessment approach to be used, such as Emphasis

The UK assesses smart devices in such a way that the device, once assessed (through Emphasis), can be used to justify its use in several applications. The suitability evaluation of the device for a specific application is separate from the assessment of the development process and behaviour of the device. Therefore, Emphasis is the basis of a harmonised approach that is repeatable and reusable.

The concept of assessing components independently of a specific application is not part of the Finnish regulatory framework. Components are assessed considering the intended application. Assessing components independently of a specific application is a requisite to be able to reuse these assessments. We did not identify any reason why this could not be done within the Finnish regulatory regime.

Within the UK, there are several bilateral agreements between different licensees to share component assessments. These agreements increase the benefits for both the supplier (potential access to a larger market) and the licensee (save assessment effort).

There is no apparent regulatory reason for Finland not to adopt a similar approach. The assessments could potentially be shared within Finland or between Finland and the UK. Independently of the geographical boundary, there are both technical and commercial challenges that would need to be addressed. Clearly, these are more challenging if agreements would need to be established with the UK licensees.

On the technical side, it would be necessary for Emphasis to be acceptable in both countries. This would require collaboration between the UK and Finnish nuclear industries to possibly modify the existing set of questions so that they were acceptable to all concerned. At the moment, there is little reason for the UK to change an approach that is working. There would have to be a need for closer alignment between UK and Finnish regulations, which is unlikely to be achieved in the near future.

From a commercial perspective, there would be issues related to sharing suppliers' IP as well as interests related to the vast investment of the UK nuclear industry to develop Emphasis.

Therefore, we recommend that the best way forward is for the Finnish nuclear industry to build on the UK experience and develop their own approach to harmonised component assessment, in a way that would work for the specifics of the Finnish nuclear industry. Nevertheless, in the long term, having a common approach or more closely aligned regulatory approaches across both countries would be beneficial to both the industries and suppliers.

7 ACKNOWLEDGMENTS

This work was funded by Energiforsk within the research program ENSRIC, Energiforsk Nuclear Safety Related Instrumentation and Control systems [12].

8 REFERENCES

1. ONR, Safety assessment principles for nuclear facilities (SAPs). 2014 Edition. http://www.onr.org.uk/saps/saps2014.pdf, last accessed October 2018
2. IEC 61226: 2009 Nuclear power plants - Instrumentation and control important to safety - Classification of instrumentation and control functions
3. ONR, Nuclear Safety Technical Assessment Guide 46 Computer Based Safety Systems, NS-TAST-GD-046 Revision 4, February 2017
4. OECD, Nuclear Legislation in OECD and NEA countries: Finland, 2008, https://www.oecd-nea.org/law/legislation/finland.pdf, last accessed October 2018
5. STUK, Regulatory Guides on nuclear safety and security (YVL), http://www.stuk.fi/web/en/regulations/stuk-s-regulatory-guides/regulatory-guides-on-nuclear-safety-yvl-, last accessed October 2018
6. “Licensing of safety critical software for nuclear reactors – Common position of international nuclear regulators and authorised technical support organizations”, Bel V, BfS, CNSC, Consejo de Seguridad Nuclear, ISTec, KAERI, KINS, NSC, ONR, SSM & STUK, http://www.onr.org.uk/software.pdf, last accessed October 2018
7. VTT, Safety demonstration of nuclear I&C – an introduction, 2015. http://www.vtt.fi/inf/julkaisut/muut/2016/VTT-R-00167-16.pdf, last accessed October 2018
8. IEC 61508: 2010, Functional safety of electrical/electronic/programmable electronic safety-related systems
9. SQUG, Seismic Qualification Utility Group, https://squg.mpr.com/, last accessed October 2018
10. Rolls-Royce, Proactive Obsolescence Management System, https://www.rolls-royce.com/products-and-services/nuclear/nuclear-lifecycle.aspx#overview, last accessed October 2018
11. STUK, Electrical and I&C Equipment Of A Nuclear Facility, Guide YVL E.7, 2013, https://www.stuklex.fi/en/ohje/YVLE-7, last accessed October 2018
12. Sofia Guerra, Gareth Fletcher, Nick Chozos, Harmonized Component Level Safety Demonstration, 2018, http://www.energiforsk.se/program/karnkraftens-styr-och-kontrollsystem-ensric/rapporter/harmonized-component-level-safety-demonstration-2018-475/, last accessed October 2018