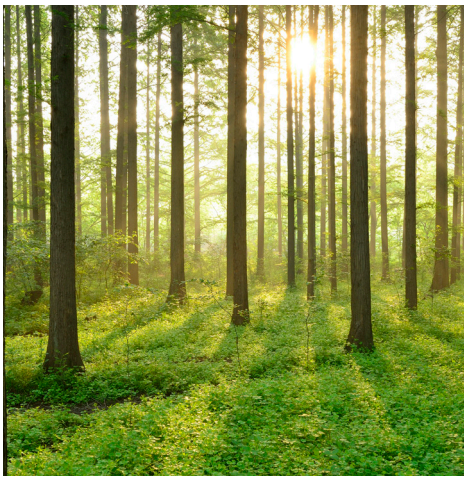
HARMONIZED COMPONENT LEVEL SAFETY DEMONSTRATION

REPORT 2018:475



NUCLEAR

ENERGIFORSK NUCLEAR SAFETY RELATED I&C – ENSRIC

Energiforsk

Harmonized Component Level Safety Demonstration

Feasibility study

SOFIA GUERRA, GARETH FLETCHER, NICK CHOZOS

ISBN 978-91-7673-475-9 | © Energiforsk February 2018 | Cover photo: EDF
Energiforsk AB | Phone: 08-677 25 30 | E-mail: kontakt@energiforsk.se | www.energiforsk.se

Foreword

In normal nuclear power plant development/asset management a number of components are exchanged each year. For each of these exchange projects a licensing/safety demonstration is required. In the Nordic power plants, many of the current components and systems are the same, and when they are exchanged, similar components and systems are chosen.

If a common template could be used for the safety demonstration of components, the safety demonstration for a specific component could be reused in another exchange project, both within the plant and at other Nordic plants. In the UK, a system with common templates is used, this study investigates if a system similar to that in the UK could be used in the Nordic licensing environment and list the challenges of such a harmonized template.

This project was carried out by Nick Chozos, Sofia Guerra and Gareth Fletcher, senior consultants at Adelard LLP. The activity is included in the Energiforsk Nuclear Safety Related Instrumentation and Control program – ENSRIC. The project is financed by Vattenfall, Sydkraft Nuclear/Uniper, Teollisuuden Voima Oy (TVO), Fortum, Skellefteå Kraft, Karlstads Energi and the Swedish Radiation Safety Authority.

Monika Adsten, Energiforsk

Sammanfattning

I denna rapport studeras möjligheten att använda harmoniserad säkerhetsdemonstration på komponentnivå, och i synnerhet om det är möjligt att använda ett system liknande det harmoniserade system som finns i Storbritannien i en nordisk kontext.

Följande aktiviteter har genomförts:

- *Samråd med brittiska experter*. Ett antal intervjuer med den brittiska kärnkraftsbranschen har genomförts. Syftet med samrådet var att förstå de licensieringsmetoder som används i Storbritannien, användningen av mallar för att säkerhetsdemonstrera komponenter, hur mallarna har delats mellan olika investeringsprojekt och hur de skulle fungera i en annan licensieringskontext.
- *Granskning och jämförelse av brittiska och finska regelverk för I&C system.* Vi identifierade likheter och skillnader i den övergripande metoden för bedömning, godkännande och licensiering av styr- och kontrollsystem som används i de två länderna. Denna översyn fokuserade på vägledning från de två tillsynsmyndigheterna (Brittiska Office of Nuclear Regulation, ONR och Finlands STUK) för att fastställa om det fanns några grundläggande skillnader som skulle göra det problematiskt att använda harmoniserad licensiering i det finländska regelverket.
- *Jämförelse av processerna för kvalificerade enheter.* Baserat på resultaten från de föregående två uppgifterna, granskade vi hur de två länderna bedömer och licensierar smarta enheter. Syftet med denna uppgift var att identifiera tillvägagångssätt i Storbritannien som kan skilja sig från det finska tillvägagångssättet och huruvida ett liknande förhållningssätt till det som används i Storbritannien för säkerhetsdemonstration skulle kunna användas i Finland.
- *Fallstudie av kvalificering av en s.k. smart device.* En generell fallstudie har genomförts utifrån olika steg i kvalifikationsprocessen och tillhörande information som skulle redovisas i en säkerhetsbedömning. Fallstudien diskuterar hur skillnaderna som identifierats i den föregående uppgiften skulle påverka de övergripande processerna.

Baserat på dessa aktiviteter drog vi slutsatsen att användningen av harmoniserad säkerhetsdemonstration är möjlig. Att utgå från det brittiska systemet har flera fördelar, men det finns också ett antal tekniska och kommersiella utmaningar som måste övervinnas för att detta ska vara genomförbart.

Summary

This report considers the feasibility of using harmonized component level safety demonstration and, in particular, on using aspects of the UK approach to licensing and qualification of I&C components (and particularly smart instruments) in Finland.

More specifically, we have performed the following activities:

- *Consultations with UK experts.* A number of interviews with industry practitioners in the UK was 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.
- *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. This review focused on the guidance provided by the two regulators (the UK ONR and the Finnish STUK) in order to establish whether there were any fundamental differences that would make the use of harmonised component justification infeasible in the Finnish regulatory context.
- *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 has been developed considering each step of the qualification process and the associated information that would be reviewed as evidence during an assessment. The case study discusses how the differences identified in the previous task would have an impact on the overall processes.

Based on these activities, 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 done 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.

List of content

1 Introduction

This document reports on the feasibility of using harmonised templates for the safety justification of smart devices. It explores whether aspects of the UK approach to licensing and qualifying smart devices may be applicable Finland.

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 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 report considers whether the use of an approach similar to that used in the UK could be deployed in Finland based on a systematic comparison between the two countries' regulations and licensing practices, and 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.

This document is organised as follows: Section 2 provides an overview of the overall approaches to licensing in the two countries. Section 3 provides a summary of the consultations performed with experts in the UK. Section 4 presents the UK approach to assessment of smart devices. Section 5 presents a detailed comparison of the UK and Finnish approaches to qualification of smart devices. Section 6 discusses a case study illustrating the use of shared information from a UK pre-assessment in a Finnish smart device qualification, and finally Section 7 consists of a summary and discussion of the findings of our study.

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 review starts from the overarching legal requirements for nuclear operations and proceeds to consider how safety assessment, justification and qualification are performed in the two countries. 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 Licensing of nuclear operations

All operators of nuclear facilities in Great Britain are required to comply with the Health and Safety at Work etc. Act 1974 [1] and other relevant statutory provisions. One of these provisions is the Nuclear Installations Act 1965 [2], which requires the licensing of sites that are to be used for the installation or operation of nuclear reactors.

The Office for Nuclear Regulation (ONR) is, according to the applicable regulation, the "appropriate national authority" in England, Wales and Scotland. Therefore, the licensing function is administered in Great Britain by ONR. This is summarised in [5] as follows.

> *No site may be used in GB for the purpose of installing or operating a nuclear reactor or prescribed nuclear installation unless a licence has been granted by ONR and is in force.*

2.1.2 ONR Safety Assessment Principles and the safety case

The ONR has a team of assessors, who are inspectors and technical experts in specific fields. These assessors establish whether a licensee has demonstrated that it understands the hazards associated with its activities and controls them adequately. The assessment of I&C systems is driven by ONR's Safety Assessment Principles (SAPs) [3], which are supported by the Technical Assessment Guides (TAGs). The SAPs are a set of principles to assist in making assessments of safety consistent amongst assessors. The SAPs are not deemed technical standards where full compliance is mandatory - they provide guidance for the assessor and often the designer. However, some parts of the SAPs make explicit reference to legal requirements and as such compliance with these sections is expected.

The contents of the SAPs are summarised in Table 1 below [3].

Principle	Description
Fundamental principles	These principles are founded in UK health and safety law and international good practice, and they underpin all the activities that contribute to sustained high standards of nuclear safety.
Leadership and management for safety	Principles that form the foundation for the leadership and management for safety in the nuclear environment.
The regulatory assessment of safety cases	Principles applicable to the assessment of the production and nature of safety cases.
The regulatory assessment of siting	Principles applied in the assessment of a site, since the nature of a site can have a bearing on accident consequences.
Engineering principles	The major part of the SAPs, which covers many aspects of the design and operation of nuclear facilities.
Radiation protection	Focus on the relevant principles of the Ionising Radiations Regulations 1999.
Fault analysis	Engineering principles concerning the detection and diagnosis of malfunctions in systems.
Numerical targets and legal limits	Probabilistic targets to assist in making judgements regarding the tolerability of risk and the ALARP (As Low As Reasonably Practicable) principle.
Accident management and emergency preparedness	Principles on the procedures around dealing with incidents and accidents.
Other	Other principles regarding radioactive waste management, decommissioning, and control and remediation of radioactively contaminated land.

Table 1: Contents of the UK SAPs

ONR's assessment against the SAPs is based on the licensee's safety case. The safety case is, according to the SAPs [3]:

> *The totality of the documentation developed by a designer, licensee or duty-holder to demonstrate high standards of nuclear safety and radioactive waste management, and any subset of this documentation that is submitted to the Office for Nuclear Regulation (ONR).*

The ONR has produced a TAG entitled "the purpose, scope and content of safety cases" [7] providing detailed guidance on the assessment of safety cases. In this document, the definition of the safety case given above is further elaborated:

> *A safety case is 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. It takes account of experience from the past, is written in the present, and sets expectations and guidance for the processes that should operate in the future if the hazards are to be controlled successfully. The safety case clearly sets out the trail from safety claims through arguments to evidence.*

The safety case is expected to demonstrate that risks are reduced as far as is reasonable practicable (SFAIRP). The concept of SFAIRP is typically expressed in terms of reducing risks to "As Low As Reasonably Practicable" (ALARP), the terms SFAIRP and ALARP being synonymous in guidance documents (Demonstration of ALARP is addressed in detail in ONR's NS-TAST-GD-005 Revision 8 [4]).

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.

A separate set of principles considers security assessment [15].

2.1.3 System and component qualification

Qualification is defined in the SAPs [3] as "the process of demonstrating that a structure, system or component is fit for its intended purpose". The ONR SAPs principle EQU.1 states that:

> *Qualification procedures should be applied to confirm that structures, systems and components will perform their allocated safety function(s) in all normal operational, fault and accident conditions identified in the safety case and for the duration of their operational lives.*

The SAPs further define the scope of these procedures, which 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.

The qualification and justification of a component or a system, along with the design, manufacturing, installation and testing activities are all done in accordance with quality and technical standards. The activities and the rigour to which they are performed is commensurate with the importance of the safety functions the

components and systems support. The following section discusses the UK framework for function categorisation and system classification.

2.1.4 Function categorisation and system classification

The UK approach is based on assigning a certain system Class to a system or sub-system depending on the Category of the function it implements. The approach taken in the UK is largely based on IEC 61226 Nuclear power plants - Instrumentation and control important to safety - Classification of instrumentation and control functions [11].

I&C functions important to safety are organised in three categories: A, B and C, with A being of the highest safety significance:

- Category A denotes the functions that play a principal role in the achievement or maintenance of Nuclear Power Plant (NPP) safety to prevent Design Basis Events (DBE) from leading to unacceptable consequences.
- Category B denotes functions that play a complementary role to the Category A functions in the achievement or maintenance of NPP safety.
- Category C denotes functions that play an auxiliary or indirect role in the achievement or maintenance of NPP safety.

The process of designing the system architecture includes functional assignment: dividing and allocating the functions to be implemented by the I&C system among a range of subsystems. These may be implemented by means of human operators, hardware, and software.

There is not necessarily a one-to-one relation between functions and subsystems. That is,

- a subsystem may implement more than one function
- several subsystems may be needed to implement a single function

The class required of the I&C system is determined by the category of the functions that it will perform or their required integrity targets. Classification may be undertaken at the level of the overall I&C architecture, or separately for each I&C system or subsystem.

Categories A, B and C are usually associated with systems of Class 1, 2 and 3 respectively, where Class 1 has the highest and Class 3 the lowest safety integrity. Functions are principally implemented by a system with the corresponding class or better (Category B implemented by Class 2 or better, for example). However, lower class systems may play a supporting role, e.g., a Class 2 system may play a significant part in supporting a Category A function, and a Class 3 system may play a minor part supporting a Category B function. If a probabilistic integrity target has been calculated, it can be used instead of the category to derive the required system class.

Depending on the class of the system, the requirements for implementation, qualification and overall approach to safety justification vary.

2.1.5 Safety systems containing software

The UK SAPs [3] 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 [6].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

As discussed in Section 2.1.4, 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 with a less onerous claim, the choice of confidence building techniques would take into account the practicability with which the techniques could be applied. For systems subject to a more onerous claim, full visibility of source code, circuit details and process information should be provided, and the chosen techniques should be performed with high levels of rigour.

2.2 THE FINNISH APPROACH

Finland's nuclear activities are governed by three main acts [10]:

- the Nuclear Energy Act 1987 (No. 990/1987 as last amended by Act No.769/2004);
- the Radiation Protection Act 1991 (No. 592/1991, as last amended by Act No. 1179/2005)
- the Nuclear Liability Act 1972 (No. 484/1972, as last amended by Act No. 493/2005)

Permission to construct a nuclear facility requires the approval of the Finnish Government. A consultation procedure must be followed in order to inform the decision of the Finnish Government. This procedure includes an assessment of the proposed facility and its systems.

Licences for the uses of nuclear energy are granted by the Ministry of Trade and Industry (Kauppa-ja teollisuusministeriö) – KTM) or by the Finnish Radiation and Nuclear Safety Authority (Säteilyturvakeskus – STUK).

STUK may supervise the construction and implementation of a licenced facility and its systems, and it may impose requirements and constraints on its design and operation.

2.2.1 STUK YVL guidance

According to the Nuclear Energy Act, STUK is expected to specify detailed safety requirements for the licensee. These requirements are presented in regulatory guidance documentation, which is called the YVL Guides [12]. More detailed technical guidance is given in justification memorandums (separately for each guide).

The safety requirements as explained in the YVL guides are binding for the licensee; however, there is some flexibility in the approach - the licensee may propose an alternative procedure or solution to the one provided in the regulations. If the licensee can convincingly demonstrate that the proposed procedure or solution will implement safety standards in accordance with the Nuclear Energy Act, STUK may still approve that procedure or solution to achieve the required safety level.

The ALARA principle (As Low As Reasonably Achievable) is fundamental in the licensing process for Finland. This is also similar to the UK approach where the ALARP principle is used.

2.2.2 Safety demonstration

On safety demonstration, STUK take the approach shared by international regulators [13]. 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" [14].

Safety justification is typically provided in the preliminary and final Safety Analysis Reports (SAR). These documents provide a summary of the plants' 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.

2.2.3 Function categorisation 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, 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.

2.2.4 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.

In terms of cybersecurity, YVL E.7 places requirements for restrictions to access to the rooms and to software of equipment important to safety by unauthorised personnel. This is done by physical, technical and administrative measures.

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.

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.

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 systems' 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 justification and qualification of systems and components is commensurate to the safety significance of the functions they implement in both countries; a system classification scheme is used both in the UK and Finland. The Finnish approach does not use a function categorisation framework – whereas in the UK functions are allocated to three categories (A, B and C), in Finland there are only descriptions of functions that provide criteria for the assignment of classes to systems.

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

This section summarises the consultations performed for this project [18]. 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.

3.1 CONSULTATION METHOD

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

Each of the interviewees was provided with a consultation brief [19] beforehand, which gave a short background of the project and contained a list of questions that the consultation would be structured around. 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. Smart devices were being assessed for different reasons: from qualifying smart devices for new power plants, to replacing obsolescent devices in existing systems.

3.2 APPROACH TO SAFETY DEMONSTRATION

The Safety Assessment Principles (SAPs) [3] is the key framework used for safety demonstration in the UK. The SAPs, together with the Technical Assessment Guide 46 [6], 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 SILs by including more techniques and measures at higher safety integrity levels (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.

As part of the consultations, we aimed to discover the average SIL of the devices being qualified in the UK nuclear industry. Devices with a modest integrity level up to a SIL 1 were most common, with some done to SIL 2. This translates to a 10^{-1} -10^{-3} probability of failure on demand (pfd) reliability claim.

Some licensees tended to use multichannel systems for high SIL systems to reduce the reliability claim on a single component/channel.

3.3 TEMPLATES, DATABASES FOR COMPONENT LICENSING

3.3.1 Templates

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 discussion around using templates for supporting the process versus using templates that may deskill and limit the assessment process. 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 that contains useful document templates that they have developed in-house. Other licensees only used external templates developed with the industry, such as Emphasis.

3.3.2 Databases

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) [16] database for seismic testing data
- Proactive Obsolescence Management System (POMS) [17] – a commercial database operated by Rolls-Royce

Licensees do not openly share access to their internal component databases; although, most licensees were prepared to share a list of the instruments that they have assessed if it was requested. Some did suggest that an industry wide database within the UK would be useful to all. This could even be taken further by agreeing a joint priority list of required device qualifications across the industry.

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.

3.4 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.

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.

Some licensees were open to sponsoring a joint development of a new device in the electrical area to help with device procurement in some applications.

3.4.1 Perception and views of safety demonstration approaches and industry sharing

The industry believes that the UK regulatory expectation for smart devices is clear. TAG 46 [6] and the SAPs are fairly clear, and what is expected during safety demonstration is understood by the industry.

Generally, the industry as a whole is positive about sharing information. Sharing of pre-assessment information is considered the route forward for the UK industry.

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).

The industry believed that the harmonisation of software qualification had been achieved within the UK, with templates such as Emphasis. However, some believed that there is less harmonisation on hardware testing, such as the specification required for type testing, so there is still more harmonisation that can be achieved.

3.5 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 between the countries 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 UK approach to qualification of smart devices

The justification of smart devices will include several steps:

- definition of requirements applicable to the smart device
- demonstration of PE and ICBMs
- additional hardware qualification
- security assessment
- 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 behavioural requirements as well as environmental constraints.

One of the most important steps of the assessment is the demonstration of PE and performance of ICBMs. Emphasis is the preferred approach for justifying PE of smart devices (see Section 3.1).

The aim of Emphasis has been to define a consistent approach that can be followed by all licensees when assessing smart devices and so that the suppliers could reduce the effort in supporting assessments by different licensees as a result of a common understanding of what information is required. It also allows for assessments to be shared between different licensees, and therefore has the potential of reducing assessment cost.

So that an Emphasis assessment can be used in a range of applications (possibly by several licensees), an Emphasis assessment is typically performed in a generic way, i.e., when no specific application of the device is considered during the assessment. In order to use a generic qualification in a specific application of the product, it is necessary to show that the device meets the application requirements and that the application is capable of satisfying any operating conditions or restrictions on use that were identified during the generic assessment.

The assessment belongs to the licensee that funds it and takes technical control of the assessment, but it may be made available to other licensees under an information sharing agreement. Typically, this means that the company receiving the assessment conducts a technical review of the work undertaken during the assessment process.

Emphasis can be considered as the main “harmonised approach” to component assessment that is common and shared across the UK industry. As discussed in Section 3.2, other templates used for the safety justification of components include:

- templates for documenting the assessment of the smart device
- templates for documenting the used of the smart device in a specific application
- templates for performing a technical review of an Emphasis assessment performed by another licensee

The other steps of the assessment (e.g., security assessment, suitability analysis) are done following a licensee specific approach and does not follow a harmonised approach.

5 Comparison between UK and Finnish approaches for smart devices

This section discusses a comparison between the UK and Finnish approaches to smart device qualification in I&C applications. We compare YVL E.7 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 and qualifying this type of devices.

Throughout this section we follow the structure from YVL E.7 and a make comparison to the UK qualification process.

5.1 GENERAL APPROACH

The first major difference to note is that the assessment of smart devices in Finland seems to always be done for a specific application that the device is intended for. In contrast, in the UK, there is a notion of *pre-assessment* that is application independent; the pre-assessment is done using a common approach (or *template*) – Emphasis – which is used across the UK industry to enable sharing and reuse of the assessment.

As mentioned in section 2.1.5, the UK assessment is split into two main parts: a production excellence assessment and implementation of confidence building measures; production excellence may include additional compensatory measures if weaknesses have been during the production excellence assessment. The Finnish assessment approach is not split in this way, and some of the requirements in YVL E.7 would be correspond to production excellence requirements, others to ICBMs. Furthermore, both software and hardware are considered during the production excellence assessment in the UK approach.

5.2 COMPONENT (HARDWARE QUALIFICATION)

5.2.1 Qualification plan

Finnish regulations require a component qualification plan to be submitted to STUK. In the UK, licensees typically have their own internal procedures that require a component qualification plan, which would most likely be a template document designed in-house. The topics required in the Finnish qualification plan are also covered within the UK qualification:

- applicable standards – assessed in the Emphasis assessment for the design and development of the component; other applicable standards are considered during the other steps of the assessment
- design and manufacturing process – covered in the Emphasis assessment
- tests (including software tests, type tests etc.) – testing by the manufacturer, licensee or independent third-party part of PE or ICBMs

- organisations to be used in the qualification – general information within the UK assessment
- operating experience feedback –information in the Emphasis assessment and a review of field data in ICBMs

5.2.2 Testing within qualification

Both Finnish and UK approaches require a testing plan for the qualification. The manufacturer's testing plan and strategy would be contained within Emphasis information as part of the production excellence assessment. Also any testing performed during the ICBMs phase would be planned and the results would be contained within the safety justification. Not all tests carried out during the UK assessment may have been performed by an independent assessor; this is different to the Finnish regulations, where it states all testing should be performed by someone who is independent of the design and manufacture of the electrical or I&C system (para. 515). The UK assessment covers the testing areas required within YVL E.7:

- functional testing - information may be provided during the Emphasis assessment or as an analysis performed during ICBMs
- device conformity testing against the specification – information and certifications in Emphasis
- after factory tests performed by the licensee before installation – testing performed by the licensee after pre-assessment
- operating environment testing – an analysis of operating experience (field data) may be performed as an ICBM

5.2.3 Assessment of the design and manufacturing processes

The Finnish assessment of the design and manufacturing processes during qualification is very similar in the UK. Both require documentation of processes for the various phases of the design, verification and the testing process (para. 525).

5.2.4 Compatibility with the electrical network

Compatibility with the electrical network is performed by the licensee after the pre-assessment during the device qualification in the UK. This analysis would be part of the safety case submitted to ONR. The assessment carried out would be similar to the one performed during the Finnish qualification (Section 5,5 in YVL E.7).

5.2.5 Environmental conditions

Environmental conditions testing within the Finnish regulations is performed in an environment as similar as possible to the intended application (Section 5.6 YVL E.7). In the UK, the environmental conditions considered during the development of the device are reviewed during Emphasis. Whether these meet the application requirements is reviewed when the device is being deployed for a specific application, and additional testing might be required to cover any additional needs that were not tested during R&D.

5.2.6 Electromagnetic compatibility

The EMC coverage in Emphasis is similar to that required by YVL E.7 (para, 558). However, when the assessment would be carried out is different. The EMC requirements depends on the application and are reviewed when the device is being deployed for a specific application.

5.2.7 Operating experience

The UK regulations do not specify in detail the required analysis of operating experience, although different licensees have their own guidance on what to collect, assess and use. Operating experience data from the manufacturer is collected in the UK during the Emphasis assessment. This data would be non-application specific in nature, mainly consisting of returns data and failure reports of devices in the field. A more thorough review of field experience data may be performed as a compensatory measure or an ICBM.

The Finnish regulations always require an analysis of operating experience by the licensee and it is a more application centric approach (only collecting data from devices in the field).

We also note that both approaches take into account the software versions of firmware in the device (paragraphs 563-4 in YVL E.7).

5.2.8 Type approval

The type approval requirements for smart devices in the UK and Finland qualification process are similar. Both have to be performed by a certified independent third-party and cover the hardware of the smart device.

The Finnish regulations require a type inspection certificate, which confirms that the device conforms to the rated performance values in its specification. The manufacturer often provides evidence of an independent certification similar to what is required in the type inspection during the UK production excellence assessment, as part of their verification and validation phases of development. However, the standard used for the type inspection may be different to that required in the Finnish type inspection.

5.2.9 Qualification of software

The qualification of software in the UK approach is part of the Emphasis assessment and, depending on the safety class of the device, software analysis as part of ICBMs. Emphasis includes a whole section of questions on software that is based on IEC 61508-3 [8] (including the techniques and measures in the appendices of IEC 61508). The focus is on good design practises, simplistic design, and verification and validation techniques. This aligns with software qualification in YVL E.7, where it states that software should

- be designed for clarity and simplicity
- minimise the propagation of the effects from a single software error
- have a structure that enables verification of the requirements set for the system

5.2.10 Software design procedures and processes

Both the UK and Finnish qualification processes focus on the software design procedures and processes used during the software lifecycle. The UK approach seems more detailed in this area, as the Emphasis questionnaire contains many in-depth questions on the whole of the software design and development process. They both focus on the same areas:

- software lifecycle model (para. 621)
- methods used in design, testing and quality assurance (para. 622)
- conditions or limitations of software (para. 623)
- independent evaluation of the final software version (para. 624)

5.2.11 Software tools

Both approaches assess the impact of any potential tool-induced error (para. 629). However, there is a different focus on the UK and Finnish approaches. 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 (para. 625).

As in YVL E.7 (para. 626), Emphasis states that all software development, including any software tools, should be under configuration management.

5.2.12 Existing software

Both qualification approaches take the same view to existing (legacy) software, which is subject to the same requirements as new software. All the software in a smart device is subject to qualification in the UK, unless it has already been previously assessed and it remains unchanged. The requirements in YVL E.7 on existing software are also covered in the UK qualification:

- identification and mitigation by analysis of any deficiencies in software documentation, design or implementation (YVL E.7 para. 640)
- functional analysis (YVL E.7 para. 641)
- under configuration management (YVL E.7 para. 642)

5.2.13 Software testing

Both qualification approaches have detailed requirements on software testing that align with each other:

- all software should have a testing plan (YVL E.7 para. 643), which should be aligned with that of the overall component testing, and the test selection should be adequately justified
- it should take into account the reliability target
- cover all safety functions with their timings
- include self-diagnostic functions
- static and dynamic testing (YVL E.7 para. 648)

5.3 SUMMARY OF COMPARISONS

The approaches to smart device qualification in Finland and the UK focus on the same areas. The main difference that would affect the whole qualification process 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 during the qualification.

The Emphasis requirements on the assessment of production excellence are based on in-depth detailed questions on the development and design processes.

6 Case study

6.1 INTRODUCTION

This section describes the theoretical case study of applying the Finnish nuclear regulations laid out in YVL E.7 [9] to an I&C system that would deploy a smart device that has been previously assessed in the UK. We are assuming that the smart device had been subjected to an Emphasis assessment of the production excellence and any ICBMs that are 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.

Over this section, we compare the information that would be available from the UK pre-assessment against the requirements in YVL E.7. This comparison identifies what would be covered by the UK pre-assessment and what additional information and assessments would need to be done to meet the requirements of YVL E.7.

6.2 GENERAL REQUIREMENTS

The first set of requirements in YVL E.7 (Section 3.1) are general requirements on the licensee. None of the shared information from the UK pre-assessment is relevant here, since the information in the assessment relates to the device and manufacturer.

6.3 REQUIREMENTS SPECIFICATION

YVL E.7 (section 3.2) states that an independent requirements assessment must be carried out to show that the device meets the requirements (scope and accuracy) expected from it. The requirements of this assessment include the device's intended application (see Section 6.4). The UK pre-assessment would provide information on the device functionality and operating constraints and design procedures that could be used in the requirements specification, preliminary and final suitability assessments, and the quality plan.

Additionally, information from Emphasis includes how the requirements specification is maintained throughout its lifetime and traceable verification (YVL paragraphs 321 and 322) to show compliance with the device's specification.

6.4 INFORMATION REQUIRED FOR THE LOCATION AND APPLICATION REQUIREMENTS

Many parts of the YVL E.7 assessment process require information about the intended application, such as the requirements specification (302, 315), suitability analyses (337, 341) and qualification assessment (501). This information is wholly dependent on the intended location and application requirements. A full location and application suitability assessment, as defined in YVL E.7 would have to be carried out to address these requirements.

In Table 2, we provide examples of some of the location and application information that would be needed for the assessment process in YVL E.7, and if any of the information from the UK pre-assessment could be of use. It is not designed to provide a comprehensive list of the information required for the location and application requirements; it only contains some example high-level areas that are most important.

Example of required information	Possible useful information within the UK pre-assessment
Requirements specification - External services that the device needs to function (power supply, communications, water, etc.).	Information in the supporting evidence documentation for questions in the Emphasis assessment relating to design process and initial requirements and operating constraints.
Suitability analysis - Physical installation requirements (space, mounting, connections).	Possible design schematics could have been provided as supporting evidence of the design process during the Emphasis assessment.
Suitability analysis - The operating environment of the device (temperature, EMI, humidity, etc.).	EMI information, environmental type testing and certifications of the device are covered in Emphasis, however, they are not from the application's perspective.
Suitability analysis - Facility level concept requirements (requirement of the intended system upon the device).	No information. The smart device would need to be reviewed against the facility concept requirements.

Table 2: Example location and application requirements for the case study

6.5 CONFIGURATION MANAGEMENT

Configuration management is covered in detail in YVL B.1. The Emphasis questionnaire requires that an appropriate Configuration Management System (CMS) is in place, which should uniquely identify all hardware and software components (including support tools) that make up the device. The CMS also extends to any third-party components that are not produced in-house, including third-party software libraries and tools. This section of the Emphasis questionnaire would provide a useful source of information about the configuration management processes of the device and the manufacturer. However, it would not provide any information about the configuration management of the intended system or plant; these requirements would need to be addressed by the licensee who knows the procedures in place at their nuclear facilities.

6.6 QUALITY MANAGEMENT

The requirements on quality management at nuclear facilities is outlined in YVL guides (YVL A.3, A.5 and B.1). There is a section within the Emphasis questionnaire relating to the Quality Management System (QMS) of the supplier; the pre-assessment would not consider any quality arrangements of the licensee (Section 3 in YVL A.3). The information provided by Emphasis would address requirement 410 of YVL E.7, since it requires a certified QMS that covers the processes involved all stages of the design and manufacture of the device (design,

production, testing), such as being ISO 9001 compliant. Emphasis also asks for information on the QMS of the manufacturer's suppliers (relevant to section 3.4 in YVL A.5 concerning quality management in the supply chain, and paragraph 629 and in YVL A.3).

The UK pre-assessment would not contain much information for the quality plan required for the procurement of devices (411 in YVL E.7 and 630 in YVL A.3).

6.7 SUITABILITY ANALYSES

6.7.1 Preliminary suitability analysis

The preliminary suitability analysis focuses on establishing that the selected device is suitable for the intended application. The preliminary suitability report provides documentation and traceability of the device selection. Table 3 shows what information from the UK pre-assessment could be used within the preliminary suitability assessment regarding verifying the smart device against the requirements specification (341). Again, this table only provides a high-level overview.

Component characteristics	Possible useful information within the UK pre-assessment
Functional features	Emphasis requires that the functional features are well defined (documented) and no unintended functions are present in the device. A formal validation of safety functions of the device may have been performed as an ICBM.
Performance	The performance requirements of the device would need to be evaluated against the needs of the intended application. Emphasis does contain information regarding stress testing and product design verification tests (DVT), worst case timing analysis. Other performance testing may have been performed depending on the class of the smart device.
Reliability	Reliability testing, FMEDA and monitoring the performance of devices in the field, including failure-rates, are part of Emphasis. It also covers any available independent SIL certification performed by third-parties.
Endurance of environmental conditions	Information regarding EMI, environmental type testing and certifications of the device are in Emphasis. However, they are application independent and would need to be reviewed against the requirements of the intended application.
Electrotechnical dimensioning and protection	The electrical requirements of the device as part of the Emphasis assessment, but it is not covered in the context of the application in the UK pre-assessment.
Operation of the component in case of disturbances or transients in the electrical network	Information on electrical stress limits and EMC immunity is in Emphasis. This information would need to be evaluated against the electrical network of the system at the nuclear facility.
The applicability of the standards used in the design and manufacture of the component	Information about any standards used in the design and development of the device is contained within Emphasis.

Component characteristics	Possible useful information within the UK pre-assessment
Testability and maintainability	The level of maintainability and testability of the device in the field are discussed within Emphasis. It also asks about device manuals.
Service life	Emphasis covers obsolescence management and the process for future device modifications. This would need to be compared against the intended service life of the system. Note, that Emphasis is performed on a specific device configuration (hardware and software) defined in the scope of the assessment; any updates to the device configuration, such as a change in sensor or firmware, require an impact analysis before the new version can be used.

Table 3: Information for the preliminary suitability assessment

The type testing (type inspection) and device certification information in the UK pre-assessment mentioned in Table 3 would also be useful for requirements 346 and 347 relating to type testing and approval.

The competence of the manufacturer and their procedures are also assessed during the preliminary suitability analysis (343). One of the aims of the Emphasis questionnaire is show that the manufacturer is highly competent at producing their products, by evaluating their procedures and processes. The evaluation also covers their organisation and staff competence, training and management. Furthermore, much of this information can be used within the qualification plan for the device (344 and 345), outlining the strategy to be used in qualifying the device.

6.7.2 Final suitability analysis

The final suitability analysis is performed after the device qualification process (Section 6.8). It pulls everything together from the assessment process and provides the component's use in the intended application.

The majority of UK pre-assessment information would have already been used during the device qualification or preliminary suitability assessment.

Requirements specific to the Finnish qualification process, such as the independent assessment of the qualification procedure (para. 352) and deviations from information in the preliminary assessment (para. 357) may be covered by the shared UK pre-assessment information. ICBMs may contribute to the independent assessment of the qualification procedure, and compensatory measures may cover some of the deviations/gaps in information in the preliminary assessment.

Table 4 shows areas where UK pre-assessment information could be used during the final suitability analysis. This table only provides a high-level overview of areas in the final suitability analysis related to the smart device identified in YVL E.7.

Areas in final suitability analysis	Possible information from UK pre-assessment
Post-factory tests (para. 349)	Any post-factory tests performed by the licensee (non-application specific), for example, functional testing of the received device. This would also include any tests performed by a third-party as part of the assessment.
Qualification test results (para. 350)	The shared UK information would only cover tests performed as part of the UK pre-assessment, such as part of ICBMs or included within the Emphasis questionnaire.
Compatibility with the facility's electrical network (para. 350)	Any useful information would have been used in the preliminary assessment. No new information would be available from the UK pre-assessment documentation.
Qualification to environmental conditions (para. 350)	Any useful information would have been used in the preliminary assessment or device qualification. No new information would be available from the UK pre-assessment documentation.
EMC properties (para. 350)	Some EMC and EMI information about the device is provided Emphasis. It is likely that the UK pre-assessment information would not fully cover this requirement and further testing during the qualification process may be required.
Operating experience feedback (350) and service life (para. 354)	Emphasis covers field experience and feedback of devices, including failure-rates and returns. The data would be non-application specific, and therefore, would need to be reviewed against the demands of the intended application. It would most likely not fully cover this requirement.
Type tests and type approval (para. 350)	Any type testing and type approval certification performed during the UK pre-assessment is available. However, they may have been performed to a different specification than what is required.
Software qualification (para. 350)	See software qualification (Section 6.9).

Table 4: Final suitability assessment information

6.8 QUALIFICATION

The qualification process would be the area that would benefit the most from a UK shared pre-assessment, in particular Section 5.4 (YVL E.7) on the assessment of the design and manufacturing process of electrical and I&C equipment; this is covered in great detail by Emphasis.

The licensee must prepare a qualification plan for Safety Class 2 and 3 devices. The UK pre-assessment information would be very useful for the qualification plan. For example, testing information obtained as part of the UK pre-assessment would only need to be reviewed/verified, allowing the testing strategy to focus on areas with less coverage, and reduce duplication of results. The design and manufacturing process review may only require a more lightweight evaluation given the in-depth detail provided in the Emphasis assessment.

Table 5 describes areas where UK pre-assessment information could be used during the qualification process.

Qualification area (YVL section)	Possible information from UK pre-assessment
Applicable standards (para. 507)	Emphasis contains information on any standards the device was developed to, calibration and testing standards used, and the standards used during the manufacturing process.
Design and manufacturing process (Section 5.4)	Emphasis contains in-depth information on the whole design and manufacturing process.
Tests (Section 5.3)	Emphasis would contain detailed information regarding the testing performed by the manufacturer during the development of the device. This would include any verification and validation testing, including the testing process and any supporting tools used. ICBMs may include application independent tests performed during the UK pre-assessment, such as functional testing.
Organisations to be used in the qualification (para. 507)	The UK pre-assessment would include all organisations that were involved in the assessment.
Operating experience feedback (Section 5.9)	Emphasis includes information on field experience and feedback of deployed devices, including failure-rates and returns.
Compatibility with electrical network (Section 5.5)	Some electrical compatibility information of the device is covered in Emphasis, but it is unlikely to fully cover this requirement. For example, the information required about the plants electrical network.
Qualification to environmental conditions (Section 5.6)	Emphasis covers the testing of the device to the environmental limits in the device's specification.
Type approval (Section 5.10)	Type testing (inspection) and type approval certification performed during the UK pre-assessment would be available. The standard that this was performed to would need to be reviewed.
Software tools (511)	See Software qualification (Section 6.9).
Software testing (512)	See Software qualification (Section 6.9).

Table 5: Information for the Qualification process

6.9 SOFTWARE QUALIFICATION

Since we are using a smart device in the case study, the system software contained within the device must also be qualified. The UK pre-assessment information would cover the design and implementation processes of the software during the development of software in great detail, as well as verification and validation. We expect that the information from the UK pre-assessment would provide good coverage of most areas of the software qualification process in YVL E.7.

Table 6 shows the software qualification areas for devices that contain software from YVL E.7, which are compared to the possible information from the UK smart device pre-assessment.

Software qualification area (YVL section)	**Possible information from the UK pre-assessment**
Design and architecture (Section 6.1)	Emphasis contains information about the design and architecture (para. 602 and 603). It focuses on the use of good design practises derived from IEC 61508-3 [8]. The software structure is also considered which would be relevant to clauses 604, 605 and 606.
Platform (firmware) and application software (Section 6.2)	Since the case study is limited to smart devices, which are not reprogrammable, application software is not applicable in this case. Emphasis contains detailed information regarding the development of the device's firmware.
Software design procedures and processes (Section 6.3)	Emphasis contains detailed information on the software design process and procedures. The information within Emphasis should cover (621-623): lifecycle, design and implementation methods, and limitations/conditions of use. 624 relates to the software of the nuclear facility so this is not covered.
Software tools (Section 6.4)	Details of any software tools (e.g., compilers and libraries) used during development are contained within Emphasis. Information on software tools includes: the reason for their selection, if they are certified (629), and their configuration management (626 and 627) and version updates.
Cybersecurity and isolation of data transfer (Section 6.5)	Emphasis only includes security information on maintaining the integrity of the device in operation, such as a password protected configuration to prevent unauthorised changes (634). Security assessments are performed separately and unlikely to be shared between licensees.
Existing software (Section 6.6)	The UK pre-assessment process is only applied to existing software. Deficiencies in the documentation and implementation of the design process of legacy (old) software would be subject to further analyses and testing as part of compensatory measures, which could potentially be shared.
Software testing (Section 6.7)	Emphasis contains detailed information regarding the testing of software during the development process, including test plans (643 and 644) and procedures (645), coverage (650), testing tools, calibration and validation of test results. Static and dynamic testing of software (648) could be part of the development process or ICBMs, which could be shared. Final testing of the software after installation (646, 647) would need to be performed by the licensee.

Table 6: Information for use in the Software qualification

6.10 INSTALLATION AND COMMISSIONING

The installation and commissioning phase of the UK nuclear safety demonstration process is performed after the device pre-assessment has been completed. This part of the safety demonstration is also specific to the intended application and the facility in question. Therefore, this would need to be performed by the Finnish licensee.

Safety, installation and user manuals are often used as supporting evidence to some Emphasis questions. However, these are usually publicly available from the device manufacturer.

The full installation and commissioning process in YVL E.7 (Section 7) would need to be performed on the UK assessed smart device:

- receiving inspection (software and configuration correspond to the design, suffered any damage during transport)
- scope, actions, responsibilities and records of the installation and coupling inspections and functional tests
- commissioning testing and verify that the component or system installed complies with the approved plans
- verify correction of any defects and faults discovered during previous phases
- parameters of a software-based component or system have been set and recorded according to the configuration management system

6.11 CASE STUDY SUMMARY

An 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 all areas of YVL E.7, it would mostly provide useful information to support the qualification process (Section 6.8), suitability analyses (Section 6.7) and software qualification (Section 6.9) laid out in the YVL regulation guides. Any requirements on the licensee would be out of the scope of the shared information. Also, not all information from the production excellence assessment template (Emphasis) would be useful to Finland, as it is 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 before it can be used in a smart device assessment.

7 Overall summary and discussion

The objective of this project is to determine if a system using harmonised templates for the component level safety demonstration for I&C and electrical components can 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 have performed the following activities:

- *Consultations with UK experts.* A number of interviews with industry practitioners in the UK was 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.
- *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. This review focused on the guidance provided by the two regulators (the UK ONR and the Finnish STUK) in order to establish whether there were any fundamental differences that would make the use of harmonised component justification infeasible in the Finnish regulatory context.
- *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 has been developed considering each step of the qualification process and the associated information that would be reviewed as evidence during an assessment. The case study discusses how the differences identified in the previous task would have an impact on the overall processes.

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 separated 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 taking into account the intended application from the outset. 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 be the need for a closer alignment between UK and Finnish regulations, which is unlikely to be achieved in the near future.

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

Therefore, we believe 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. We recommend to build on UK experience, but develop the details in way that would work for the specific of the Finnish 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.

We also consider two further possibly transferable approaches: The component databases (SQUG and POMS). Neither require an NDA, and they could provide information on forthcoming obsolesce of devices by manufacturers and type certification information. It is likely that the type certification would not be to the required standard; however, it would identify products that have been through type testing in the past and manufacturers that are familiar with the process.

8 Acknowledgements

Adelard would like to thank Steve Gregory, Paul Caspall-Askew, Austin Dale, Steve Frost, Mark Bowell, Dan Gray, Sam Robinson, Dai Jenkins, Peter Wyman and Barry Hogan for taking part in the consultations.

9 Glossary

ALARA	As Low As Reasonably Achievable
ALARP	As Low As Reasonably Practicable
AWE	Atomic Weapons Establishment
DBE	Design Basis Events
EMC	Electro Magnetic Compatibiliy
EMI	Electro Magnetic Interference
I&C	Instrumentation & Control
ICBM	Independent Confidence Building Measure
IEC	International Electrotechnical Commission
NDA	Non-Disclosure Agreement
NPP	Nuclear Power Plant
ONR	Office for Nuclear Regulation
pfd	probability of failure on demand
PRA	Probabilistic Risk Assessment
PE	Production Excellence
PLC	Programmable Logic Controller
POMS	Proactive Obsolescence Management System
SAP	Safety Assessment Principle
SIL	Safety Integrity Level
SQUG	Seismic Qualification Utility Group
STUK	Radiation and Nuclear Safety Authority
TAG	Technical Assessment Guide
T&M	techniques and measures
YVL	Regulatory Guides on nuclear safety

10 Bibliography

[1] UK Health and Safety at Work Act (HSW), 1974. http://www.legislation.gov.uk/ukpga/1974/37/contents

[2] UK Nuclear Installations Act, 1965, https://www.legislation.gov.uk/ukpga/1965/57

[3] ONR Safety assessment principles for nuclear facilities (SAPs). 2014 Edition. http://www.onr.org.uk/saps/saps2014.pdf

[4] ONR, Guidance on the demonstration of ALARP (As Low As Reasonably Practicable). NS-TAST-GD-005 Revision 8, July 2017, http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-005.pdf

[5] ONR, Licensing nuclear installations, 4th edition, January 2015, http://www.onr.org.uk/licensing-nuclear-installations.pdf

[6] ONR, Nuclear Safety Technical Assessment Guide 46 Computer Based Safety Systems, NS-TAST-GD-046 Revision 4, February 2017, http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-046.pdf

[7] ONR, The Purpose, Scope, and Content of Safety cases, 2016, http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-051.pdf

[8] IEC 61508: 2010, Functional safety of electrical/electronic/programmable electronic safety-related systems

[9] STUK, Electrical and I&C Equipment Of A Nuclear Facility, Guide YVL E.7, 2013, https://www.stuklex.fi/en/ohje/YVLE-7

[10] OECD, Nuclear Legislation in OECD and NEA countries: Finland, 2008, https://www.oecd-nea.org/law/legislation/finland.pdf

[11] IEC 61226: 2009 Nuclear power plants - Instrumentation and control important to safety - Classification of instrumentation and control functions

[12] 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-

[13] Regulator task force on Safety Critical Software, 2015, Licensing of safety critical software for nuclear reactors. Common position of international nuclear regulators and authorised technical support organisations. http://www.belv.be/images/pdf/15-12%20Common%20position%20-%202015-12-17%20(secured).pdf

[14] VTT, Safety demonstration of nuclear I&C – an introduction, 2015. http://www.vtt.fi/inf/julkaisut/muut/2016/VTT-R-00167-16.pdf

[15] GuONR, Security Assessment Principles for the Civil Nuclear Industry, Edition 0, 2017, http://www.onr.org.uk/syaps/

[16] SQUG, Seismic Qualification Utility Group https://squg.mpr.com/

[17] Rolls-Royce, Proactive Obsolescence Management System, https://www.rolls-royce.com/products-and-services/nuclear/nuclear-services/software-solutions/poms.aspx#overview

[18] Fletcher G, Guerra S, Chozos N. Consultation summary. Adelard document reference D/1098/150003/2, issue v0.2. December 2017.

[19] Fletcher G, Guerra S. Harmonized Component Level Safety Demonstration/Licensing Documentation: Consultation Brief. Adelard document reference W/2681/150003/1, issue v1.0, June 2017.

HARMONIZED COMPONENT LEVEL SAFETY DEMONSTRATION

A number of components are exchanged each year, according to standard nuclear power plant development. For each of these exchange projects a licensing/safety demonstration is required, which is a time consuming and costly process both for the regulator and for the nuclear power plant.

Re-using parts of this documentation could be feasible when new projects using the same components are started, given that the documentation is made in a harmonized manner.

This study concludes that such a system could be developed, based on the experience from a similar system that is implemented in the UK.

Energiforsk is the Swedish Energy Research Centre – an industrially owned body dedicated to meeting the common energy challenges faced by industries, authorities and society. Our vision is to be hub of Swedish energy research and our mission is to make the world of energy smarter!

Energiforsk