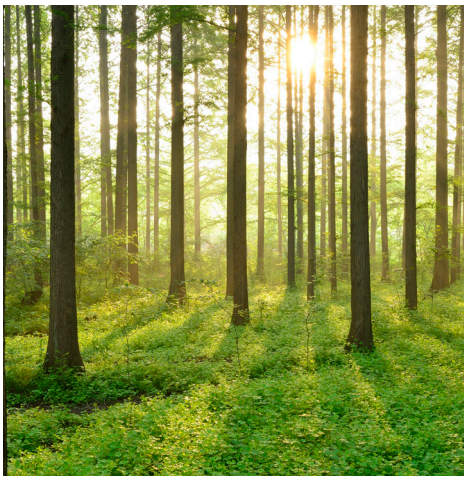
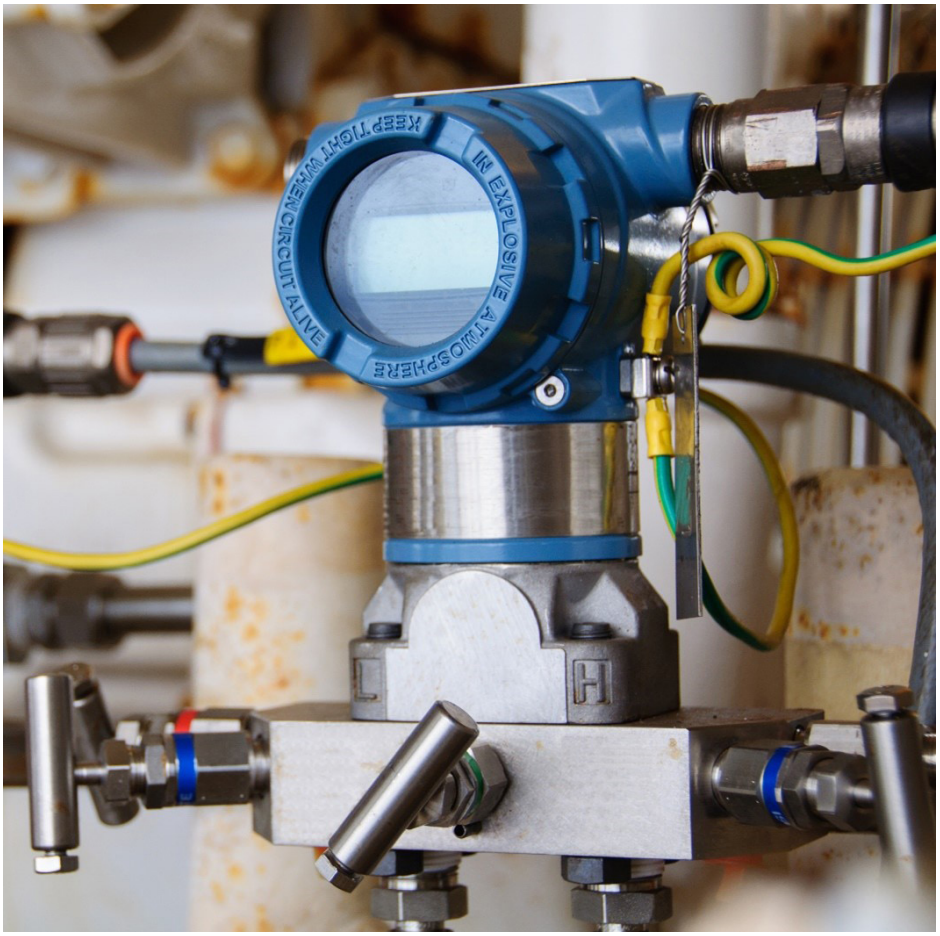
SOFTWARE CERTIFICATION IN NUCLEAR I&C COMPONENTS

REPORT 2022:878



NUCLEAR

ENERGIFORSK NUCLEAR SAFETY RELATED I&C – ENSRIC



Energiforsk

Software Certification in Nuclear I&C Components

SOFIA GUERRA, LUKE HINDE, AND BEN PHILLIPS

ISBN 978-91-7673-878-8 | © Energiforsk July 2022

Energiforsk AB | Phone: 08-677 25 30 | E-mail: kontakt@energiforsk.se | www.energiforsk.se

Foreword

The research and development program Nuclear Safety Related I&C ENSRIC aim to find cost- and time effective methods for long term operation of automation systems in the Nordic nuclear power plants. Traditionally, the nuclear industry relies on nuclear grade products and components used in safety classed applications. These products and services are however manufactured in significantly smaller series and sometimes with other processes and materials compared to industry standard components. Therefore one theme within the area has been to investigate how industry standard or commercial-off-the-shelf (COTS) equipment can be used.

This project within COTS-theme has looked specifically at software certification of I&C products. Digital components often incorporates more or less software, which has to be certified to guarantee safe operation. For COTS equipment this certification relies on international standards such as the IEC 61508. However, the possibillity to use this certification for safety applications are different between countries and different industries. The use of such certification often comes with additional requriements, which can furhter increase the variation. This report gives valuable insights on how the situation looks for the nordic and other nuclear power plants and compares with other safety critical industries.

The study was carried out by a team from Adelard consisting Sofia Guerra, Luke Hinde, and Ben Phillips. The ENSRIC programme is a part of the Energiforsk nuclear portfolio, financed by Vattenfall, Uniper, Fortum, TVO, Skellefteå Kraft and Karlstads Energi.

These are the results and conclusions of a project, which is part of a research programme run by Energiforsk. The author/authors are responsible for the content.

Summary

Commercial-Off-The-Shelf (COTS) field instrumentation containing software is increasingly used in nuclear Instrumentation and Control (I&C) applications. Digital equipment often has functional advantages compared with its analogue counterparts, such as better accuracy and more diagnostics. The increasing prevalence of software also means products without software may not be available, and the cost of developing bespoke components may be prohibitive.

However, there are several challenges and concerns regarding the safety demonstration and justification of COTS equipment containing software. Some traditional methods of quantifying reliability, such as FMEAs, cannot be applied to software, and so there is often a greater focus on justifying the development processes, and on software testing and analysis. Moreover, software is considered valuable intellectual property by the manufacturers, and there may be little incentive for the manufacturers to provide the necessary information and support for additional assessments to justify its use in nuclear power plants. These challenges have led to different approaches being developed in different sectors to address the software aspects of the justification of COTS equipment.

In this project, we reviewed the approaches for safety justification of digital COTS components in both the nuclear industry and other non-nuclear, safety-critical industries, with a focus on the use of certification to international standards as part of the justification. The focus of the work has been on what is often called “smart devices” or “digital devices with limited functionality”, with a particular emphasis on their software, and it does not discuss in detail aspects of the justification common to analogue devices, e.g., environmental qualification and type testing.

From our review, we have extracted and analysed several common themes, including the role of certification in the overall justification and whether certification on its own might be enough, and market factors that might influence the approach and deployment of commercial digital components.

The project was presented at a seminar that took place in Stockholm on 19 May 2022.

Keywords

Nuclear, Software, Certification, COTS, I&C

Sammanfattning

Commercial-Off-The-Shelf (COTS) fältinstrumentering som innehåller programvara används i allt större utsträckning i nukleära instrumentering och kontroll (I&C) applikationer. Digital utrustning har ofta funktionella fördelar jämfört med sina analoga motsvarigheter, såsom bättre noggrannhet och mer diagnostik. Den ökande förekomsten av programvara innebär också att produkter utan programvara kanske inte är tillgängliga, och att kostnaderna för att utveckla skräddarsydd a komponenter kan bli orimligt höga.

Det finns dock flera utmaningar och farhågor när det gäller säkerhetsaspekterna till att motivera användandet av COTS-utrustning som innehåller programvara. Vissa traditionella metoder för att kvantifiera tillförlitlighet, såsom FMEAs, kan inte tillämpas på programvara, och därför är det ofta ett större fokus på att motivera utvecklingsprocesserna och på mjukvarutestning och analys. Dessutom anses mjukvara vara värdefull immateriell egendom av tillverkarna, och det kan finnas få incitament för tillverkarna att tillhandahålla nödvändig information och stöd för ytterligare bedömningar för att motivera användningen i kärnkraftverk. Dessa utmaningar har lett till att olika tillvägagångsätt har utvecklats inom olika sektorer för att ta itu med mjukvaruaspekterna till att motivera användandet av COTS-utrustning.

I detta projekt har vi granskat tillvägagångsätt för att säkerställa att säkerhetsaspekterna är omhändertagna när COTS-komponenter används i både kärnkraftsindustrinoch andra icke-nukleära, säkerhetskritiska industrier, med fokus på användningen av certifiering enligt internationella standarder som en del av motiveringen. Fokus i arbetet har legat på vad som ofta kallas för ”smarta enheter” eller ”digitala enheter med begränsad funktionalitet”, med särskild tonvikt på deras mjukvara, och det diskuteras inte i detalj aspekter av den berättigande som är vanliga för analoga enheter, t.ex. , miljökvalificering och typprovning.

Från vår granskning har vi extraherat och analyserat flera vanliga delområden inklusive certifieringens roll i det övergripande motivet och om certifiering i sig kan räcka, och marknadsfaktorer som kan påverka tillvägagångssättet och tillgängligheten av kommersiella digital komponenter.

Projektet presenterades vid ett seminarium som ägde rum i Stockholm den 19 maj 2022.

List of content

1 Introduction

Commercial-Off-The-Shelf (COTS) equipment containing software is increasingly used in nuclear Instrumentation and Control (I&C) applications. Digital equipment often has functional advantages compared with its analogue counterparts, such as better accuracy and more diagnostics. The increasing prevalence of software also means products without software may not be available, and the cost of developing bespoke components may be prohibitive.

However, there are several challenges and concerns regarding the safety demonstration and justification of COTS equipment containing software. Some traditional methods of quantifying reliability, such as FMEAs, cannot be applied to software, and so there is often a greater focus on the development processes, and on testing and analysis. Moreover, software is considered valuable intellectual property by the manufacturers, and there may be little incentive for the manufacturers to provide the necessary information and support for additional assessments to justify its use in Nuclear Power Plants (NPPs).

Software certification against safety standards such as IEC 61508 could provide a practicable basis for the safety demonstration and justification of COTS equipment containing software. This report contains the results of our review of the use of software certification in the justification of COTS digital equipment for use in safety and safety-related applications in both the nuclear industry and other non-nuclear, safety-critical industries. The approaches adopted in the nuclear industries of different countries are described in Section 3, and a survey of some other safety-critical industries is presented in Section 4. Section 5 contains analysis of these different approaches, including some common themes we have identified.

2 Scope and methodology

The scope of this study was the justification of COTS digital equipment. While all types of COTS digital equipment have been considered, the study has focused on the justification of field equipment, e.g., pressure transmitters, which are typically procured from industrial suppliers, rather than more complex devices such as programmable logic controllers (PLCs) which are often programmed for a specific application and so follow a different justification process.

Information was gathered through a combination of consultations and other discussions with representatives from the relevant industries, research of the publicly available relevant literature, and by capturing Adelard's experiences of the use of COTS products in NPPs and other regulated industry sectors. The selection of sectors was based on discussions during the project kick-off meeting and the expected variety of approaches; Adelard's experiences and the availability of information were also considered. Formal consultations were structured using a set of questions posed to the interviewees to ensure that all relevant topics were covered. This set of questions has been reproduced in Appendix A. We are grateful to our consultees for their assistance.

3 Nuclear power industry

3.1 IAEA

The IAEA recently published two reports that discuss the use of COTS digital equipment in Nuclear Power Plants [1][2]. The reports discuss safety aspects and criteria associated with the safe use of industrial digital COTS components, and the activities required to demonstrate their use. Their scope is smart devices, including field instrumentation, as in this report.

The reports acknowledge the advantages of selecting devices that have been certified to a safety standard such as IEC 61508, and suggest that certification could be one of the selection criteria. Typically, a certified product implies that the manufacturer will already have available relevant evidence to support the justification. This is the case when IEC 61508 certification was done on the basis of the development process rather than on the basis of "prior use" or "proven in use". In fact, [2] expresses a preference for certification based on the development process for nuclear applications, and says that the proven in use approach is only used where there are weaknesses in the documentation of the development process.

However, these reports consider that the certification does not represent an alternative to the qualification process itself, and describe approaches and areas that need to be addressed to justify their use.

3.2 FINLAND

According to the Finnish Nuclear Energy Act, the Finnish Radiation and Nuclear Safety Authority (Säteilyturvakeskus – STUK) specifies detailed safety requirements for nuclear licensees. These requirements are presented in regulatory guidance documentation, which is called the YVL Guides.

YVL E.7 [3] contains requirements for electrical and I&C equipment. Requirements for the qualification of safety-classified software are described in Section 6 of YVL E.7. For class 2 and class 3 software, as defined in YVL B.2 [4], this includes the demonstration that the design and implementation complies with nuclear standards, i.e. IEC 60880 [5] and IEC 62138 [6], however for class 3, other standards intended for the design of safety-critical software can be used. In practice, IEC 61508 [7] is likely to be the only non-nuclear specific standard used for this purpose, although the number of devices justified using IEC 61508 is currently limited.

Many COTS devices used in Finland are field equipment such as temperature transmitters or safety relays. It is always preferred to purchase equipment certified to nuclear standards, but the availability of such equipment is limited. In some cases, SIL-certified COTS equipment used in safety-related applications was initially bought for non-safety classified applications, and then after several years of use it is identified as a potential component to be used for safety-related applications.

The qualification of I&C equipment includes a suitability analysis, which includes operating experience feedback, type approval and software qualification [3]. The YVL E.7 guide discusses requirements for software-based equipment, and it states that the requirements in Common Position report should be met [8]. The requirements for software qualification [3] include compliance with standards and design principles, but does not detail the process that needs to be followed to demonstrate that the requirements have been met. Evidence of SIL certification available from suppliers usually consists of the certificate and a safety manual. For commercially available COTS digital equipment used in safety-related applications, this is usually sufficient to support the justification, and any further activities will be determined based on a number of factors, including the complexity of the device and the evidence available from the certification. If the equipment is to be used in a safety-critical application or has been customised for the application in any way, then assessment of the suppliers' and/or manufacturers' quality management systems is also required. In Finland, this is performed by a licensee's quality department who evaluate suppliers and maintain a list of approved vendors.

In many cases, the COTS devices used are relatively simple and so no additional assessment of the software or the development process is performed. In these cases qualification is done by various black box methods, evaluating the overall functionality of the equipment as a whole. If there are environmental requirements not covered by the certification, e.g., radiation or seismic requirements, these will also be demonstrated by additional testing. It is usually preferred for any additional activities to be performed on the complete device, as access to software or design details is often difficult to arrange with manufacturers and suppliers.

3.3 SWEDEN

The nuclear power industry in Sweden is regulated by the Swedish Radiation Safety Authority (SSM: Strålsäkerhetsmyndigheten). Regulatory requirements are elaborated in SSM regulatory codes; SSMFS 2008:1 defines regulations concerning safety in nuclear facilities [9], with SSMFS 2008:17 describing concerns specific to the design and construction of nuclear power reactors [10]. Both regulations are amended with further SSMFS publications.

There is limited use of programmable electronic devices in Swedish plants. Examples of COTS devices that are used include relays and UPS systems, as well as some systems measuring neutron flux and other radiation measurements, which were specifically designed for the nuclear industry.

The use of programmable electronics in systems important to safety is not recommended, but is not prohibited; their use must be justified. A common example of a justification would be to make use of a device containing software in a diverse system, where only one leg makes use of the digital device and the other is based on an analogue device.

Each device to be used has to be qualified, even if it is part of a diverse system, but each NPP in Sweden defines and uses their own qualification processes. However, the operators of Swedish NPPs have jointly produced technical requirements for

electrical equipment to be used in Swedish NPPs, including specific requirements for programmable equipment, e.g., [11]. The remainder of this section describes an example qualification process used in Sweden based on discussions with experts from a Swedish NPP.

There is a standard qualification report form used to record the information relevant for the device's justification, but the justification itself varies depending on the device.

The most important part of the justification is the operating experience of the device; devices with operating experience in nuclear or similar applications, whether in Sweden or in other countries, are strongly preferred. Devices without sufficient operating experience may be deployed in non-safety-related applications first to build up experience.

Information must be gathered from the manufacturers via workshops and a questionnaire. The focus of this information is the original development process, which also includes the design change process.

Certification is not used in the qualification process in Sweden. It can, however, be useful; devices that have been SIL certified will typically have more information readily available from the manufacturer, such as the safety manual, which provides a lot of the information that is required in the qualification process. The certification alone would never be sufficient. A unique justification must always be made; the certification simply aids the qualification process.

IEC 61508 certification performed based on operating experience of the device, rather than its development process, would in general be more useful for the Swedish qualification process; the information examined and made available as part of the certification would be more relevant.

3.4 UNITED KINGDOM

The ONR Safety Assessment Principles (SAPs) [12] and the associated Technical Assessment Guides (TAGs) are the primary principles that define the overall approach to be followed for nuclear installations in the UK. The SAPs mandate two independent "legs" of the justification for systems dependent on the performance of computer software:

- "Production excellence" (PE), a demonstration of excellence in all aspects of production from the initial specification through to the finally commissioned system, including
  - thorough application of technical design practice consistent with current accepted standards for the development of software for computer-based safety systems
  - implementation of a modern standards quality management system
  - application of a comprehensive testing program formulated to check every system function
- "Independent confidence-building measures" (ICBMs), an independent and thorough assessment of a safety system's fitness for purpose. This is formed of

- complete and preferably diverse checking of the finally validated production software by a team that is independent of the systems suppliers
- independent assessment of the comprehensive testing program covering the full scope of the test activities

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

The justification approach used for COTS digital components needs to be consistent with these clauses to be acceptable for safety-related systems in the UK nuclear industry. The level of justification required depends on the safety function categories (Category A, B or C) and system classes of IEC 61226 [13] (Safety Class 1, 2 or 3). TAG 46 [14] contains guidance on the link between categorisation, classification and pdf/SIL as in IEC 61508 [7]. The reliability claim and safety integrity level (SIL) for an intended COTS component directly influence the amount of verification and validation expected in development and the level of rigour of independent verification of the device's properties.

While the application of specific standards is not mandatory, "…the case for production excellence is greatly assisted by evidence of the systematic application of national and international … standards, coupled with a case by case justification of non-compliances" [14].

Production excellence for COTS smart devices, i.e., "instruments, sensors, actuators or other previously electromechanical components (e.g., relays, positioners and controllers), whose functionality is limited and which feature built-in intelligence, in the form of a microprocessor or HDL-programmed device, to help perform its function" [14] is typically assessed using the Emphasis approach [15], which is a questionnaire derived from IEC 61508 [7], and has been adopted as an industry consensus. Emphasis can be used with different target SILs: a greater reliability claim is supported by compliance with the questions required by the higher SILs. Emphasis assessments require access to a manufacturer's quality documentation, development processes, design documents and other supporting evidence. Third-party product certifications (e.g., commercial certificates of compliance to IEC 61508) can be considered in the assessment of production excellence, but are neither necessary nor sufficient for successful assessment. Compensatory activities must be carried out if weaknesses in the production processes are identified.

In terms of ICBMs, ONR does not specify which activities should be performed, and different licensees have different approaches to define what measures are suitable and necessary. In some cases, certification can be included as one of those measures, but their role as an ICBM is usually limited and it is only one of several other activities, analyses or testing.

3.5 UNITED STATES

It is generally expected that any product being used to fulfil a safety function in a nuclear power plant in the United States would be developed purposely in line with the quality assurance elements of the NRC's requirements described in the US

Code of Federal Regulations [16] and in line with the technical requirements of applicable standards, e.g., IEEE 7-4.3.2-2016. However, for COTS equipment, which by its nature will not have been developed specifically to meet the NRC's requirements, the expectation is that the equipment will be demonstrated to have been produced with equivalent quality. The main approach to demonstrating this for safety-related equipment is a methodology called Commercial Grade Dedication (CGD) [17]. The commercial grade dedication process is carried out by an organisation that operates using a NRC compliant quality assurance program. This organisation may be the manufacturer, the licensee or a third party. Commercial grade dedication consists of two key elements: "Technical Evaluation" and an "Acceptance Process".

The key outcome of the Technical Evaluation element is the identification of "critical characteristics", and acceptance criteria for the critical characteristics. Critical characteristics are properties of the equipment which, once verified, will provide reasonable assurance that the item will perform its intended safety function. These were originally categorised as either 'physical' or 'performance' critical characteristics. With the increasing prevalence of digital COTS equipment, a third category of critical characteristic called 'dependability' was introduced to address the different factors affecting the reliability of software. For equipment containing software, dependability critical characteristics consider aspects such as the development process of the device, the design of the device, the testing performed, and its operating experience. Prior to the completion of the commercial grade dedication process, these aspects are typically evaluated using a critical digital review.

The acceptance process aims to provide reasonable assurance that the equipment meets its requirements, and so is capable of performing its safety function. This involves verification of the critical characteristics using one or more of the following methods:

- special tests and inspections (i.e., tests/analysis on the produced equipment)
- commercial-grade survey (i.e., assessment of the supplier's QA program)
- source verification (i.e., inspections, or witness hold points)
- item/supplier performance records (i.e., consideration of operating experience)

Each of these is associated with a prescriptive flow chart and there are restrictions on the combinations of methods that can be used in various situations. Current practice does not include the use of third party certification as part of these methods for verifying critical characteristics.

Recent research by EPRI [18] considered a SIL-certified device, and aimed to determine whether the SIL certification is sufficient to demonstrate that all dependability-related critical characteristics are satisfied. Based on the outcomes of this work, the Nuclear Energy Institute (NEI) produced guidance NEI 17-06 [19] stating that for the purposes of the CGD process and for the critical digital review, if the device has a SIL certification and accompanying safety manual from a suitable certifying body, then the dependability characteristics can be considered satisfied. This would then allow digital equipment with a SIL certification to follow a similar CGD process as equipment which does not contain software.

Organisations performing IEC 61508 certifications are themselves accredited, typically by national regulatory organisations such as ANSI or DAkkS. In order to make use of a SIL certificate to demonstrate the satisfaction of dependability characteristics, NEI 17-06 requires that US nuclear industry representatives regularly observe the accreditation process followed by the accreditors to ensure that third party IEC 61508 certification continues to be implemented consistently. SIL certificates can only be accepted if they were issued by a certifier that has been accredited by an approved accreditor; no further assessment of the certifiers by the end-user is needed. As part of the work in [18], this accreditor observation process has been followed with ANSI.

The research by EPRI [18] and the guidance produced by NEI [19] is currently under discussion by the NRC.

3.6 FRANCE

The nuclear industry in France is regulated by the Autorité de Sûreté Nucléaire (ASN). COTS digital equipment may be used in a variety of applications at all safety classes. The RFS (fundamental safety rules) and ASN guides describe the safety objectives to be met in approximately 40 technical areas and give examples of techniques and methods for achieving these objectives. The licensee is solely responsible for nuclear safety and cannot pass on this responsibility, and so certifications cannot be used by themselves, but must be supported by reviews and other activities. Électricité de France (EDF) is the sole operator of commercial nuclear power plants in France.

On an operational level, AFCEN industrial codes, such as RCC-E [21], represent a consensus between the main industrial partners in France and are used for defining requirements on a contractual basis. RCC-E constitutes a technical design code for electrical and I&C systems for pressurised water reactors, and is used as the basis for approaches to justifying digital equipment by EDF. For the I&C aspects, RCC-E relies heavily on demonstrating compliance with IEC nuclear standards, such as IEC 61513 and IEC 60880, but provides some clarifications on the interpretations of these standards at a national level. In particular, the focus for COTS equipment is on the quality assurance, verification and validation activities, and how the equipment is used in the system, rather than design choices made during development of the COTS equipment.

The most recent versions of RCC-E have included alternative methodologies which can credit certification according to IEC 61508 or other safety standards for the qualification of industrial digital devices of limited functionality (DDLF), as defined by IEC 62671 [22].

For devices meeting the definition of DDLF which also have a SIL certification, it is possible to qualify these devices using an alternative methodology which credits the SIL certification. There are no restrictions on the safety class of the device, but the SIL certification must certify the exact version of the device to a SIL appropriate to the safety class – SIL 1 for a class 3 DDLF up to SIL 3 for a class 1 DDLF – and the SIL certification must not be based on the "proven in use" method. In addition to a review of the SIL certification, an audit of the designer is undertaken to verify

the certification. The areas considered and level of detail of the audit are graduated according to the safety class of the device, but in all cases include the overall development lifecycle and the software architecture. Subsequent modifications require an updated SIL certification, but an impact analysis to show that the modification does not fundamentally change the device can replace the audit.

Further guidance from AFCEN [23] describes a similar methodology making use of IEC 61508 certification for the qualification of a wider range of class 3 I&C systems, i.e., not just those meeting the definition of DDLF. This guidance follows the same approach of reviewing the IEC 61508 certification, which must be to a minimum of SIL 2, and auditing the manufacturer. For systems more complex than a DDLF, the audit covers a wider range of areas than the equivalent audit for a class 3 DDLF, including auditing of the verification and validation activities.

RCC-E also includes a methodology for qualification of DDLFs using IEC 62671 directly, which acknowledges that this standard covers a broader range of activities than some other standards, and so defines a more limited scope for the assessment, in which the licensee is required to demonstrate compliance with particular clauses of IEC 62671. The focus is on demonstrating that the functionality and performance of the device is suitable for the application, and demonstrating the dependability of the device through an assessment of the development and manufacturing process. If a third party certification to a widely recognised safety standard is available and has been reviewed, including the supporting evidence, this is considered sufficient evidence of dependability and no further assessment of the design and manufacturing is required. RCC-E does not give a comprehensive list of standards for which prior certification can be considered for this purpose, but includes as examples IEC 61508 and the aviation standard DO-178 [26].

3.7 CANADA

The Canadian Nuclear Safety Commission (CNSC) regulates the use of nuclear material and nuclear substances in Canada, including the nuclear power sector. A series of regulatory documents published by CNSC, REGDOCs, define requirements and present guidance for meeting the requirements. REGDOC-2.5.2 [24] describes requirements and guidance related to the physical design of water-cooled nuclear power plants. On COTS equipment, REGDOC-2.5.2 lays out the following requirement [24]:

"If pre-developed software is used in systems or equipment important to safety, then the software (and any subsequent release of the software) shall be developed, inspected, and tested in accordance with standards of a category commensurate with the safety function provided by the given system or equipment."

The CSA standard N290.14 [25] is the principal standard against which computer-based systems will be assessed to meet this requirement. There are four routes defined in the standard by which a device can be assessed: the "recognized program method", the "mature product method", "proof through testing" and the "preponderance of evidence".

The “recognized program method” makes use of third-party certification to standards, including IEC 61508 [7], so certification can be used to assist the qualification process. However, simply presenting certification is not sufficient; the certification and the information it provides is rather used to aid the overall assessment against the standard. In other words, the assessment against the standard must be elaborated, rather than be assumed to be completed because of the certification.

The requirements detailed in the CSA N290.14 are application-specific; therefore, even a device with certification following the “recognized program” method will require further assessment. An example of one such requirement is a failure analysis for the device in its specific application.

4 Non-nuclear safety-critical industries

4.1 AVIATION INDUSTRY IN THE UNITED STATES

In the United States, the Federal Aviation Authority (FAA) issues approvals for airframes as a whole, rather than certifying individual components. The regulatory regime is similar to that operated by the European Aviation Safety Agency (EASA), to the extent that airframe certification performed by the FAA is recognised by EASA, and vice versa.

COTS devices intended for use in aircraft tend to be more programmable than field equipment and other digital devices typically deployed in the nuclear industry, which often are designed to only perform a single function, with limited configurability. This is partly influenced by the premium placed on space and weight in aircraft, and also by the reduced cost of certifying fewer devices as part of the aircraft. For ground-based systems, where these factors are less prominent, there is wider use of COTS devices, e.g., in I/O devices or sensors.

Systems containing software on airframes are required to comply with standard DO-178C [26]. DO-178C defines five "software level" based on the consequences of failure of the software. The more serious the potential failure, the more stringent the requirements on the failure rate and the development processes. Although the advice from the FAA describing the use of DO-178C acknowledges that it is possible to demonstrate regulatory compliance by other means, and provides guidance on what would be required by such alternative means, in practice compliance with DO-178C is the only method used.

The market for digital equipment in the aviation industry is large enough that COTS equipment is typically designed with the aviation industry in mind. Suppliers therefore ensure that their development process meets the requirements of DO-178C, and it is generally expected that the supplier will provide full visibility of the design and development process to the customer. This is secured through contractual arrangements between the supplier and the airframe manufacturer and is often provided in the form of a "certification package" which provides all the information required to demonstrate that the supplier has followed the requirements of the standard.

Since only the complete aircraft is subject to approval, the entire aircraft and all components are assessed as a single unit, however the requirements of DO-178C propagate to and apply to the various subsystems. Typically, there tends to be a large supply chain where components are integrated into more complex systems, which are themselves integrated into larger systems, until the subsystems are incorporated into the complete aircraft. The certification packages associated with each component of a system are similarly bundled up and passed through the supply chain to provide the documentation needed for the certification of the aircraft. Compliance of an aircraft with DO-178C is assessed by the FAA, and is demonstrated through documentary evidence, auditing, code review and testing.

In general, if a component from a certified aircraft is reused on a new aircraft, the certification process must be restarted from the beginning, and compliance with all

aspects of DO-178C must be re-evaluated. However, if a manufacturer intends for the component to be reused in a number of different aircraft, the FAA have produced guidance for a software component to be accepted as a Reusable Software Component (RSC) [27]. In addition to the usual certification process, suppliers wishing to gain acceptance for an RSC must produce a documentation package identifying which objectives of DO-178C are satisfied by the documentation package, any restrictions on how the software must be used, and any activities to be performed by the user. If accepted by the FAA, this can then be used to support certification in any subsequent projects by confirming that the user has complied with all identified activities and restrictions.

Ground-based communication, navigation and surveillance equipment is usually assessed to DO-278 [28], a similar standard to DO-178C. However, ground-based systems do not require regulatory approval, and so the assessment against DO-278 is performed by the operator. Access to the necessary information from the supplier must be arranged as part of the procurement contracts. When considering deploying a ground-based system, the operator will identify any gaps between the information provided by the supplier, and the requirements of the standard, an identify appropriate mitigations, or justifications of why the equipment is suitable for use despite the gaps. As with airborne equipment, no certification is given to the software or to individual components of the system, and so further assessments must be performed for its use in other applications.

4.2 RAIL INDUSTRY IN THE UNITED KINGDOM

Most COTS devices used in applications in the UK rail industry are so-called "safety controllers". These devices tend to be more complex and more programmable than most field devices deployed in the nuclear industry.

The rail industry is highly regulated under EU directives, and the market for railway safety equipment is large enough that there are many manufacturers selling products specifically for use by the railway. Railway suppliers develop generic products and applications for railway signalling, which are then configured and installed for customers as a specific railway signalling application.

In the UK, any equipment to be used on the railway requires a safety certificate for the particular equipment and application. This safety certificate certifies that the equipment has been assessed by a Notified Body – one of a list of approved third parties – for conformity to the requirements all relevant Technical Specifications for Interoperability (TSI).

The TSI for control-command and signalling subsystems includes a list of mandatory standards that are to be applied during the certification process, specifically EN 50126 [29], EN 50128 [30], EN 50129 [31] and EN 50159 [32]. These standards are functional safety standards for rail applications. EN 50126 and EN 50129 address the system lifecycle and align with IEC 61508-1. EN 50129 requires the production of a safety case containing

- evidence of effective quality management

- evidence that the design lifecycle has complied with the safety management systems
- technical evidence for the safety of the design in the form of a technical safety report

Safety cases may be specific to the application or type of application, or may be in the form of a generic product safety case, independent of the application, which allows the product to be re-used in multiple different applications. The level of detail and extent of evidence provided is graduated by the Safety Integrity Level (SIL), a concept re-used from IEC 61508.

EN 50128 contains additional requirements for software in systems that include programmable electronics, including requirements for the development process. The standard defines five software safety integrity levels, and proposes techniques and measures appropriate to achieve these. Similarly, EN 50159 contains additional requirements for safety-related data communication.

A typical railway signalling system is integrated from a collection of smaller subsystems, often in a number of stages. At each stage, the integrator has access to the safety certificates of the sub-systems, but not necessarily the safety assessment reports or the safety cases, which are usually considered proprietary. However, the independent assessor for the larger system is sometimes given access to the components' safety cases through a non-disclosure agreement.

4.3 OIL & GAS INDUSTRY IN THE UNITED KINGDOM

Control and instrumentation systems in oil and gas plants in the UK are regulated by the Health and Safety Executive (HSE). The use of COTS equipment is widespread within the UK oil & gas industry, for both safety and non-safety applications.

IEC 61511 [20], the functional safety specialisation of IEC 61508 for process industries, forms the basis of the qualification process for "safety instrumented systems". Devices are expected to hold certification against IEC 61511, and have a safety manual available as a result of the certification. A functional safety assessment must also be performed as part of the qualification process. Certificates alone are insufficient.

Legacy equipment may not have a safety manual available, and may not hold any certification. In these cases, proven-in-use arguments must be relied upon. Such cases will require assessment of the quality system used for the design of the device, as well as an assessment of its suitability for the application. New equipment, however, is expected to hold IEC 61511 certification with a safety manual.

The majority of COTS components are justified to SIL 1, with some justified to SIL 2, and very rarely to SIL 3.

5 Analysis

5.1 RELIANCE ON THIRD PARTY CERTIFICATION

The extent to which third party certification is used in the justification of digital COTS components varies considerably across different sectors and countries. However, in all the sectors we have considered, third party certification is not used without some additional review of the certification reports or of the certifying bodies and, in most cases, with additional activities to complement the certification.

In some sectors, third party certification is not used directly to support the justification. In many such sectors, the justification of COTS components is still performed by demonstrating compliance with standards, e.g., DO-178C in the US aviation industry, or with sector-specific requirements based on standards, e.g., the Emphasis approach in the UK nuclear industry, and the results of third party certification can be used to support this. However, it is the end-user who is responsible for performing the assessment to demonstrate compliance, and they cannot rely solely on certificates issued by a third party.

Where third party certification is credited as part of the justification, approaches rely on this certification to different extents. In the approach put forward by NEI in the United States, no particular SIL is specified for the IEC 61508 certification, although the chosen SIL must demonstrate that the required characteristics are met, and the certification contributes only to the justification of the software; the justification of the hardware is not affected. In France, the required SIL can be determined by the application, ranging from SIL 1 for class 3 application up to SIL 3 for class 1 applications. The certification can also be used to support the justification of the I&C equipment as a whole, although there may still be further justification required for other aspects such as environmental requirements.

Where certification is credited to demonstrate compliance with certain requirements, the certificate alone is not considered sufficient, and further evidence is needed to support the certification. However, the focus of this additional evidence varies. For example, in the approach proposed by NEI in the United States, the emphasis is on assessing the accreditors to demonstrate the adequacy of the certifying organisation, whereas in France, the audit process for IEC 61508 certification provides additional assessment of the development and manufacturing processes.

An important part of the use of certification is the consideration of any conditions of the applicability of the certification itself to the specific application. For IEC 61508 certifications, this is often included in the safety manual, and any deviations need to be justified.

5.2 DIFFERENCES BASED ON CLASSIFICATION

COTS components are used to perform safety or safety-related functions at a variety of safety categories (A to C), and as such are classified to a range of safety

classes (1 to 3). The precise definitions of these safety classes vary by country, but are typically similar to those defined in IEC 61226 [13]. In similar fashion, many standards offer a graded approach to their compliance; IEC 61508 [7] imposes increasingly rigorous requirements for each Safety Integrity Level, from SIL 1 to SIL 4. Demonstration of compliance to higher SILs in IEC 61508 (or industry-specific iterations of this standard) roughly corresponds to a system's use in higher safety classes, though the exact safety class and SIL target for any given system varies with country, industry, and the exact application. The UK ONR TAG 46 assessment guide provides one example of how categorisation, classification and SIL are linked for the UK nuclear industry [14].

Along with the differences between countries and industries in how certification is used in the qualification process for COTS devices, there are differences in the grading of the certification that is used or required.

As described in Section 3.6, the French nuclear industry allows for justifications of DDLF devices to use SIL certification as part of the qualification process, and can do this for qualification to any safety class – though the SIL certification must be to a level commensurate with the class, namely SIL 1 for a class 3 DDLF up to SIL 3 for a class 1 DDLF. Justifications of devices more complex than a DDLF can make use of IEC 61508 certification in a similar way, but the certification must be to at least SIL 2, and may only be used as part of the qualification process for Class 3 I&C systems.

The guidance produced by NEI in the United States elaborating how IEC 61508 certification can be used as part of the CGD process [19] advises simply that the SIL of the IEC 61508 certification being used must meet or exceed the SIL determined to be appropriate for the application. This guidance is under discussion by the NRC.

For the nuclear industries in countries such as the United Kingdom, where certification is predominantly used only to aid access to required information for the assessment processes, certification will be most useful when the SIL of the certification meets the SIL target for the assessment. There are, however, no requirements for this, as certification is not explicitly required or incorporated into the assessment process.

Overall, the use of certification is more common for equipment of a lower safety class, particularly class 3, and the use of certification for higher classes typically requires certification to a higher SIL, or is not used. However, there is no clear consensus between countries or industries on any specific level of certification – particularly IEC 61508 certification – that should or should not be used, nor to what safety class of system certification can or cannot be used to justify a device.

5.3 CERTIFICATION BASED ON OPERATING EXPERIENCE

As an alternative to assessments of the means for avoiding and controlling systematic faults in software and hardware, IEC 61508 provides for an alternative "proven in use" route to certification. This route relies on evidence of sufficient previous operating experience, which demonstrates that the dangerous failure rate

is acceptable for the required SIL. The use of such proven in use arguments, and the acceptance of IEC 61508 certificates based on this route, varies significantly.

In some sectors where the IEC 61508 certificate is not relied on directly but is used to provide evidence for the justification, certification through the proven in use route is accepted or even preferred. For example, operating experience is often a significant part of the justification approach in Swedish NPPs, and a certification through this route provides additional evidence to support this part of the justification.

In some cases, no distinction is made between the different routes to IEC 61508 certification, such as in the guidance of NEI 17-06. However, the use of certification following the proven in use route is often discouraged. For example, the methodology for using IEC 61508 certified components described in the French RCC-E explicitly prohibits the reliance on certificates following the proven in use route. The common position of several nuclear regulators [8] is that operating experience should only be used as a substitute for factory or system tests, and should not be used as evidence for the quality of the development process.

The reliable use of operating experience data to support the justification depends on several factors such as the quality of the problem reporting, including versions of devices. Operating experience to support certification is typically collected by the manufacturer, but licensees often have data from their own use, possible in non-safety applications, that can be used to complement the justification. It is expected that the factors that have an impact on the quality of the data are considered by the certifier and the licensee.

5.4 INFORMATION PROVIDED BY CERTIFICATION

Experts consulted as part of this project typically reported that certified components, particularly those certified to IEC 61508, were preferred, and were often more straightforward to justify. This was the case even in sectors where third party certification is not used directly to support the justification of COTS components. Equipment developed in line with, and certified to comply with, IEC 61508 will have followed a well-defined lifecycle, with documentation available to support this.

Another major reported benefit of IEC 61508 certification is the information provided by the certification reports, and in particular the safety manual. Obtaining the necessary information on COTS products, and particularly on the development process, from the manufacturers or suppliers can be difficult, especially in the nuclear sectors where the number of components needed can be very small compared to the production volume. However, where equipment has a SIL certification, the manufacturer will usually be willing to provide the certificates, safety manual and sometimes other certification reports to support the justification process. The information available in the safety manual and other certification documentation can vary depending on the component, certifying body and the route used for certification (i.e., assessment of development process or proven in use), but should contain details of the functionality of the equipment, the SIL it has been assessed to and any assumptions or restrictions on use.

5.5 EQUIPMENT DEVELOPED FOR SPECIFIC INDUSTRIES

There is a preference in many industries for components to be developed to industry-specific standards, e.g. IEC 61513 for the nuclear industry, or IEC 61511 in process industries. However, in contrast to the nuclear industry where such components can be difficult to obtain, COTS equipment developed to industry standards is widely available in industries such as aviation, and its use is commonplace. In some cases, this can extend to the integration of several components into complete systems. The primary driver of this is that the economies of scale in these larger industries make the development of such components commercially viable. Manufacturers and suppliers of COTS equipment targeted at a particular industry are typically familiar with the requirements for justification of this equipment, and will provide documentation packages to support this.

One factor which has increased the market size in some sectors, and hence the availability of components developed specifically for the sector, is the alignment of approaches across several countries. This can be seen in European rail industry with the development of technical specifications for interoperability, and in the aviation industry, with the alignment of requirements and mutual acceptance of airframe certification between the FAA and EASA. The development of a more integrated approach across the nuclear industries in Europe or worldwide would present a stronger business case for manufacturers to support justifications of their COTS equipment, or even to develop components intended for use in the nuclear sector. The anticipated development of small modular reactors is likely to lead to an increase in the demand for digital COTS equipment in the nuclear sector; an integrated approach to justification would further strengthen the case for manufacturers to develop components for the nuclear industry, and for the feasibility of large scale adoption of small and advanced modular reactors worldwide.

6 Conclusions

In this report, we reviewed the approaches for safety justification of digital COTS components across a number of countries and sectors, with a focus on the use of certification to international standards as part of the justification.

Demonstrating compliance with standards or comparable sets of requirements as part of the justification is commonplace among all industries and sectors we considered. However, the acceptance of certification as evidence of this compliance varies considerably. Nevertheless there is a general preference among all safety-critical industries surveyed for the use of equipment which has been certified.

Certification to IEC 61508 or other safety standards can be used in some sectors and some countries as part of the justification. In these cases, the certificate alone is not sufficient, and certification is typically used as part of a clearly defined and well documented process that includes activities to review or verify the certification reports and the certifying body. In addition, it is crucial that any assumptions, conditions of use or any other restrictions are taken into consideration when deploying the devices in any application, and any deviations are clearly justified.

The acceptability and practicality of a justification approach using certification against a generic safety standard such as IEC 61508 is intrinsically linked to business and market factors. This includes

- The availability of devices developed to specific industry standards, as for the aviation and railway sectors, where the large number of devices to be deployed incentivises the development of a sector specific supply chain.
- The availability of certified devices to the necessary SIL – for example, the majority of COTS components used in the UK oil & gas industry are justified to SIL 1, which implies that the industry finds certification most useful for justifying devices in lower safety category applications, and as such use more devices certified to lower SILs. Given the limited market for SIL 3 certified products, there is limited motivation for manufacturers to follow the corresponding expensive development process.
- Access and cooperation from the manufacturer – if a licensee is only buying a limited number of devices, it might be difficult to get the cooperation from the manufacturer necessary to access information and evidence to support the case.
- Cooperation from certifiers and accreditors – the approach currently being developed in the US shifts the support required from manufacturers to certifiers and accreditors. This is likely to be feasible in the US, given the limited number of certifiers/accreditors active and the number of devices that would become available as a result of such activity. For smaller countries or licensees, it is less clear whether such approach would be feasible.

Most of these market constraints can be overcome if greater harmonisation of approaches between countries and licensees is achieved. Although this has been on the agenda for a number of years, it may become essential for the next generation

of reactors to be successful. The internationalisation of SMR providers and the economic characteristics of such reactors means that their wide adoption will be influenced by their licensing costs.

7 Glossary

Term	Definition
ANSI	American National Standards Institute
ASN	Autorité de Sûreté Nucléaire
CGD	Commercial Grade Dedication
CNSC	Canadian Nuclear Safety Commission
COTS	Commercial-Off-The-Shelf
CSA	Canadian Standards Association
DAkkS	Deutsche Akkreditierungsstelle
DDLF	Digital Device of Limited Functionality
EASA	European Aviation Safety Agency
EDF	Électricité de France
EN	Europäische Norm
EPRI	Electric Power Research Institute
FAA	Federal Aviation Authority
FMEA	Failure Modes and Effects Analysis
HDL	Hardware Description Language
HSE	Health and Safety Executive
IAEA	International Atomic Energy Agency
ICBM	Independent Confidence-Building Measure
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
I/O	Input/Output
I&C	Instrumentation & Control
NEI	Nuclear Energy Institute
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
ONR	Office for Nuclear Regulation
PE	Production Excellence

Term	Definition
PLC	Programmable Logic Controller
RSC	Reusable Software Component
SAP	Safety Assessment Principle
SIL	Safety Integrity Level
SMR	Small Modular Reactor
SSM	Strålsäkerhetsmyndigheten
STUK	Säteilyturvakeskus
TAG	Technical Assessment Guide
TSI	Technical Specifications for Interoperability
UPS	Uninterruptible Power Supply

8 Bibliography

[1] Challenges and Approaches for Selecting, Assessing and Qualifying Commercial Industrial Digital Instrumentation and Control Equipment for Use in Nuclear Power Plant Applications. IAEA Nuclear Energy Series No. NR-T-3.31, 2020.

[2] Safety Aspects of Using Smart Devices in Systems Important to Safety of Nuclear Power Plants. Safety Reports Series No. 111. To be published.

[3] YVL E.7. Electrical and I&C equipment of a nuclear facility, 15 Mar 2019.

[4] YVL B.2. Classification of systems, structures and components of a nuclear facility, 15 June 2019.

[5] International Electrotechnical Commission, IEC 60880 Nuclear Power Plants: Instrumentation and Control Systems Important to Safety – Software Aspects for Computer Based Systems Performing Category A Functions, 2006.

[6] International Electrotechnical Commission, IEC 62138 Nuclear Power Plants: Instrumentation and Control Systems Important to Safety – Software Aspects for Computer Based Systems Performing Category B or C Functions, 2018.

[7] International Electrotechnical Commission, IEC 61508 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, 2010.

[8] Licensing of safety critical software for nuclear reactors, Common position of international nuclear regulators and authorised technical support organisations, Revision 2018.

[9] Strålsäkerhetsmyndigheten, SSMFS 2008:1 The Swedish Radiation Safety Authority's Regulations concerning Safety in Nuclear Facilities, 2008.

[10] Strålsäkerhetsmyndigheten, SSMFS 2008:17 The Swedish Radiation Safety Authority's Regulations concerning the Design and Construction of Nuclear Power Reactors, 2008.

[11] TBE Group, Technical Requirements for Electrical Equipment, Programmable electronics with fixed application, TBE 106:2-1, Issue 3, April 2020.

[12] ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition, Liverpool, 2014.

[13] International Electrotechnical Commission, IEC 61226 Nuclear power plants - Instrumentation and control important to safety - Classification of instrumentation and control functions, 2009.

[14] ONR, "Technical Assessment Guide - Computer Based Safety Systems", NS-TAST-GD-046, Rev. 5, Liverpool, 2019.

[15] S Guerra, N Chozos, D Sheridan, Justifying Digital COTS Components when Compliance Cannot be Demonstrated - The Cogs Approach. In 9th International conference on nuclear plant instrumentation, control & human-machine interface technologies (NPIC&HMIT 2015). Charlotte. North Carolina.

[16] U.S. Code of Federal Regulations, Title 10, Chapter 1, Appendix B to Part 50, Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Facilities. Office of the Federal Register, National Archives and Records Administration, U.S. Government Printing Office, Washington, DC.

[17] Electric Power Research Institute, Plant Engineering: Guideline for the Acceptance of Commercial-Grade Items in Nuclear Safety-Related Applications: Revision 1 to EPRI NP-5652 and TR-102260, EPRI 3002002982, 2014.

[18] Electric Power Research Institute, Safety Integrity Level (SIL) Certification Efficacy for Nuclear Power, EPRI 3002011817, 2019.

[19] Nuclear Energy Institute, Guidance on Using IEC 61508 SIL Certification to Support the Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Related Applications, NEI 17-06 Rev B, 2019.

[20] International Electrotechnical Commission, IEC 61511 Functional Safety – Safety instrumented systems for the process industry sector, 2017.

[21] AFCEN, RCC-E Design and construction rules for electrical and I&C systems and equipment, 2019.

[22] International Electrotechnical Commission, IEC 62671 Nuclear power plants – Instrumentation and control important to safety – Selection and use of industrial digital devices of limited functionality, 2013.

[23] AFCEN, Class 3 Design Qualification of Systems using Equipment Families Certified According to IEC 61508, 2019.

[24] Canadian Nuclear Safety Commission, Physical Design – Design of Reactor Facilities: Nuclear Power Plants, REGDOC-2.5.2, 2014.

[25] CSA Group, Qualification Of Digital Hardware And Software For Use In Instrumentation And Control Applications For Nuclear Power Plants, N290.14, 2015.

[26] RTCA, Inc., DO-178C, Software Considerations in Airborne Systems and Equipment Certification, 2012.

[27] Federal Aviation Authority, AC 20-148, Reusable Software Components, 2004.

[28] RTCA, Inc., DO-278, Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems, 2011.

[29] CENELEC, EN 50126 – Railway applications – The specification and demonstration of reliability, availability, maintainability and safety (RAMS), 1999.

[30] CENELEC, EN 50128 – Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems, 2011.

[31] CENELEC, EN 50129 – Railway applications – Communications, signalling and processing systems – Safety related electronic systems for signalling, 2003.

[32] CENELEC, EN 50159 – Railway applications – Communication, signalling and processing systems, 2010.

Appendix A: Consultation brief

- What types of digital COTS devices are typically used in safety applications in the sector?
    - Focus on field equipment, e.g., temperature sensors, pressure transmitters, but may also include other COTS devices.
    - Are the COTS devices being used only in new applications/plants, or are they being used to replace old equipment as well? Does this affect the qualification process? Does the qualification process limit the potential applications for which a device can be qualified?
    - Are these products typically designed with this specific industry/application in mind, or are they often more generic?
- In what applications, or for what functions, are they used?
    - Focus on safety-critical and/or safety-related applications. If standards use grading, which grades are typically used?
- Do you use certification as part of the software qualification process?
    - Is software certification a part of the qualification of COTS devices? Is the certification pre-existing, or is it obtained as part of the qualification process? Is the selection of COTS devices influenced by the existence of certification?
- Which standards are used for the certification?
    - These will generally be international standards; they could be both generic industrial standards, e.g., IEC 61508, and industry-specific standards, e.g., IEC 62138.
- What evidence of certification is required?
    - This will typically include a certificate from a third party that the relevant standards have been met but will often also require additional supporting evidence such as test reports and audit reports from the third party certification.
- Are there any restrictions on the type of certification or how it might be used?
    - Do you have specific requirements on certification conditions, certification body, certification approach (e.g., based on operating history vs review of development artefacts)?
- Are any assurance activities carried out in addition to the software certification?
    - The focus of this should be activities in addition to those already carried out by the manufacturer, and those that were performed as part of certification in accordance with standards. For example, this could include additional reviews of standards compliance to confirm the conclusions of the certification such as a review of manufacturers' documents or an audit of the manufacturer, or additional assurance activities such as commissioning tests, black box testing and software analysis.

- What support and information are required from the manufacturer?
    - What support is required from the manufacturer for the software qualification process, if any? Is data required from the manufacturer, e.g., data sheets, development documentation, test results? Is access to the source code required?
- What other inputs are required for the qualification process?
    - This should also include any required information on the intended application for the device, such as safety requirements, or data on the system in which it will be used.
- Software qualification process
    - Is there a standardised process to follow, or is this done on an ad hoc basis?
    - As much detail as possible should be provided on the software qualification process, including how the certification is used as part of the qualification process, the different steps of the process, any guidelines or flowcharts used to determine qualification options and activities, and the expected output documentation.
- What challenges have there been, and what lessons have been learned?
    - This could include difficulty finding COTS devices with appropriate certification, or difficulty in other parts of the process, e.g., obtaining access to the necessary development documents or certification reports.
    - Have there been any examples of COTS devices that were particularly difficult to qualify, and how were these difficulties resolved?
- How useful is the output documentation?
    - Does the output documentation vary depending on the certification used, or depending on other qualification activities performed? This includes changes to which documents are produced, and changes to the format and content of documents such as the safety manual. Which documents, if any, are the most useful?

Appendix B: Seminar on software certification in nuclear I&C components

A seminar on software certification in nuclear I&C components took place online on 19 May 2022. The program is reproduced below:

9:30	**Welcome** *Urban Andersson, Energiforsk*
9:40	**Software certification in nuclear I&C components – project summary** *Luke Hinde, Adelard, UK*
10:10	**Status of I&C equipment qualification in Finland – experience and results of Finnish national KELPO project and further steps** *Hannu Malmberg, Fortum, Finland*
10:50	**Forsmark NPP perspective regarding qualification of programmable electronics in safety applications** *Mattias Hansson, Vattenfall, Sweden*
11:30	**Lunch**
12:20	**Certification from manufacturer perspective – how the lessons learned from the process industry can be applied in balance of plant applications** *John van Gorsel, Emerson Automation Solutions*
13:00	**Certification against functional safety standards – current uses in the qualification of COTS digital devices with nuclear safety significance** *Silke Kuball, EDF Energy, UK*
13:40	**Regulatory expectations for justification of COTS devices in the UK** *Tim Parkes, ONR, UK*
14:10	**Coffee**
14:30	**NEI Guidance to utilize SIL certification** *Andrew M Nack, Rivermist and Alan Campbell, Nuclear Energy Institute, US*
15:00	**Risk-informed design: a modern approach to I&C** *Matt Gibson, EPRI, US*
15:30	**Panel on challenges of licensing COTS digital components** *Yong Chang Liu, CNSC, Canada; Tim Parkes, ONR, UK; Silke Kuball, EDF Energy, UK; Mattias Hansson, Vattenfall, Sweden; Hannu Malmberg, Fortum, Finland*
16:15	**End of seminar**

During the seminar, the results of the project were presented. This was followed by presentations of current practices, experience and research into the use of software certification in the justification of nuclear I&C components in the United States, UK, Sweden and Finland.

The seminar concluded with a panel discussion, during which a number of topics were discussed, including

- the role of certification in the justification of I&C components, and the need for scrutiny of the certification process

- what additional evidence and activities are needed to use a certified I&C component in a nuclear power plant
- the role of operating experience in the justification of nuclear I&C components
- the need for clearly defined processes for qualifying software
- the importance of market and business cases as a factor in determining whether certification is considered, and how it is considered
- the potential for harmonisation across different countries, particularly with the development of SMRs

SOFTWARE CERTIFICATION IN NUCLEAR I&C COMPONENTS

In this project, we reviewed the approaches for safety justification of digital COTS components in both the nuclear industry and other non-nuclear, safety-critical industries, with a focus on the use of certification to international standards as part of the justification. The focus of the work has been on what is often called "smart devices" or "digital devices with limited functionality", with a particular emphasis on their software, and it does not discuss in detail aspects of the justification common to analogue devices, e.g., environmental qualification and type testing.

From our review, we have extracted and analysed several common themes, including the role of certification in the overall justification and whether certification on its own might be enough, and market factors that might influence the approach and deployment of commercial digital components.